Why would you choose a domain based network over workgroup based network

1. Centralized Management: Domain networks allow centralized administration of user

accounts, permissions, and resources, making it easier to manage numerous users and devices.

2. Enhanced Security: Domains offer stronger security features. Administrators can enforce

policies and manage security settings to ensure compliance and reduce unauthorized access

risks.

3. Scalability: Designed to support thousands of users and devices, domains are ideal for

larger organizations needing network expansion without extensive reconfiguration.

4. Efficient Resource Sharing: Resources like files, printers, and applications can be shared

more efficiently in a domain. Permissions can be precisely set to control access.

5. Group Policy: Domains enable the use of Group Policies to automate software, update, and

configuration deployments across devices, reducing administrative effort and ensuring network

consistency.

Step to configure to install active directory on window server 2012.....

What is GPO

Group Policy Object (GPO) is a feature in Windows Server that lets administrators manage and

configure system settings, software, and user environments within an Active Directory domain.

GPOs allow centralized and automated tasks such as:

Security Settings: Enforcing password policies and user permissions.

Software Deployment: Managing software installations, updates, and removals across multiple

computers.

Purpose of GPO

1. Enforcing Security Policies: GPOs ensure consistent security by enforcing settings like

password requirements, account lockout policies, and user permissions, helping maintain

organizational security standards.

2. Centralized Software Management: They facilitate the centralized installation, updating, and

removal of software across multiple domain computers, reducing the need for manual installations

and ensuring users have necessary applications.

3. Standardizing User Environments: GPOs configure user environments by setting desktop

backgrounds, start menu layouts, and other personal settings, providing a uniform user experience

and enhancing productivity.

4. Registry-Based Policy Management: Through administrative templates, GPOs manage

registry-based policies to configure various Windows and application settings, such as disabling

USB ports, adjusting Internet Explorer settings, and controlling Control Panel access.

5. Data Management and Mobility: GPOs redirect folders like Documents and Desktop to

network locations, ensuring data is centrally stored and backed up. Roaming profiles allow user

settings and data to be consistent across different network computers, offering a seamless

experience.

Important of GPO

1. Improved Security: GPOs ensure consistent enforcement of security policies across all

devices and users, protecting the network from unauthorized access and threats.

2. Centralized Management: They allow administrators to manage and configure settings from

one location, minimizing the need for manual configuration on individual machines.

3. Automation: GPOs automate tasks like software deployment, updates, and system settings

application, saving time and reducing errors.

4. Consistency: Standardizing configurations ensures uniform settings across all devices and

user environments, enhancing reliability and user experience.

5. Policy Enforcement: GPOs enforce organizational policies, such as password rules and user

permissions, ensuring compliance with internal and external regulations.

6. Increased Productivity: Pre-configured environments provided by GPOs boost user

efficiency and reduce downtime caused by misconfigurations or missing software.

7. Scalability: GPOs facilitate the management of large networks by applying policies at

various levels, such as domains, organizational units, and groups, enabling scalable and flexible

IT management.

Types of GPO:

1. Local GPOs: These are applied to individual computers and affect only the local machine.

Each Windows computer has a single default local GPO.

2. Domain GPOs: These are linked to Active Directory objects like domains, organizational

units (OUs), or sites. Managed from a domain controller, they can be applied to multiple users and

computers within the domain.

3. Starter GPOs: These act as templates for creating new GPOs. They come with a set of

predefined settings that can be used to ensure consistency when setting up new GPOs.

4. Default Domain Policy: This built-in GPO applies to all users and computers within the

domain, typically used for enforcing domain-wide security and account policies.

5. Default Domain Controllers Policy: This built-in GPO specifically targets domain controllers

and is used to enforce security settings and configurations unique to these servers.

How GPO are executed

1. Local GPOs: Applied first, affecting only the individual local computer.

2. Site GPOs: Applied next, targeting computers based on their physical location within the

network.

3. Domain GPOs: Applied to all users and computers within the domain.

4. Organizational Unit (OU) GPOs: Applied last, based on the hierarchy of OUs where the user

or computer resides.

What is the purpose of starter GPOs

1. Template Provision: Offer predefined sets of policy settings that can be used as templates

for new GPOs, ensuring consistency across the organization.

2. Consistency Maintenance: Ensure uniform configurations by using a standard set of policies,

reducing discrepancies and errors.

3. Time Efficiency: Save time by providing a base set of configurations, so administrators don’t

need to start from scratch each time.

4. Management Simplification: Make the creation and management of GPOs easier by offering

templates that incorporate best practices and common settings.

5. Policy Standardization: Help maintain adherence to organizational standards and policies by

starting with a consistent template for new GPOs.

The difference between hypervisor 1 and hypervisor 2.

1. Installation: Type 1 Hypervisor: Installs directly on the physical hardware, bypassing the

need for a host operating system.

- Type 2 Hypervisor: Runs on top of an existing host operating system.

2. Performance: Type 1 Hypervisor: Generally provides better performance and lower latency

because it interacts directly with hardware.

Type 2: Typically has slightly reduced performance due to the additional layer of the host OS.

3. Resource Utilization: Type 1: More efficient in resource management, as it has direct

access to hardware resources.

Type 2 : Shares resources with the host operating system, which can lead to overhead and less

efficient resource allocation.

4. Use Case:

Type 1: Ideal for data centers and enterprise environments where high performance, scalability,

and security are critical.

Type 2: Suited for development, testing, and desktop virtualization where convenience and ease

of use are prioritized.

What is block inheritance

block inheritance refers to the ability of a subclass or derived class to inherit the properties,

methods, and behavior of a parent class or superclass, and then build upon or modify that

behavior. In block inheritance, the subclass inherits a "block" of code from the parent class, which

includes the class's attributes (data) and methods (functions).

What is a backup ,The reason to backup GPO and the process to do it on Windows server.

A backup is a process of creating copies of data, files, or system configurations to ensure that they

can be restored in case of data loss, corruption, or system failure. Backups are crucial for data

recovery and maintaining business continuity.

### Reasons to Backup Group Policy Objects (GPOs)

1. Data Protection: It protects against accidental deletion or corruption of policy settings. It

Ensures that you can restore policies and configurations if they are lost or damaged.

2. Recovery from Errors: Changes to GPOs can sometimes cause unintended issues or errors.

Having a backup allows you to revert to a previous working state if a recent change causes

problems.

3. System Migration: When upgrading or migrating servers, you need to move GPOs to the

new environment. Backing up and restoring GPOs ensures that all policy settings are preserved

during the migration process.

4. Compliance and Auditing:Many organizations are required to keep records of changes and

configurations for compliance reasons. It helps maintain a history of configurations for auditing and

regulatory compliance.

5. Disaster Recovery: In the event of a major system failure or disaster, restoring GPOs can be

critical for reestablishing normal operations. It enable quick recovery and continuity of IT services.

##How to Backup on Windows Server 2012:

1. Install Windows Server Backup:

- Steps: Access Server Manager, go to `Manage` > `Add Roles and Features`, and install the

`Windows Server Backup` feature.

2. Configure Backup Settings:

- Steps: Open `Windows Server Backup` from Administrative Tools. Use the `Backup

Schedule` wizard to set up regular backups or `Backup Once` for a single backup.

3. Choose Backup Type:

- Steps: Select between `Full Server` backup (includes system state, applications, and data)

or `Custom` backup (specific files, folders, or volumes).

4. Designate Backup Destination:

- Steps: Choose a backup destination, such as a local disk, network share, or external

storage device, ensuring it has enough space.

5. Schedule Regular Backups:

- Steps: Set up a backup schedule to automate the backup process, ensuring consistent data

protection.

6. Monitor Backup Status:

- Steps: Regularly review backup status and logs to confirm backups complete successfully

and without issues.

What is virtual hard disks. Explain why as a system admis you will choose and explain VHD OR

VHDx.

A Virtual Hard Disk (VHD) is a file format that represents a virtual hard drive. It simulates a

physical hard drive within a virtualized environment, allowing operating systems and applications

to interact with it as if it were a real disk.

Reasons to Choose VHDx

#### 1. Larger Capacity: VHDx supports virtual disk sizes up to 64 TB, significantly exceeding the

2 TB limit of VHD. This expanded capacity is beneficial for applications that require large amounts

of storage, such as large databases or extensive virtual environments.

- Benefit: The larger capacity of VHDx is essential for organizations that need to handle

substantial storage requirements within their virtual machines. It allows for the creation of larger

virtual disks without the need for complex configurations or multiple disks.

#### 2. Improved Performance: VHDx includes advanced features that enhance performance,

such as block-level performance improvements and more efficient space allocation. These

features help optimize I/O operations and reduce overhead.

- Benefit: VHDx is ideal for performance-sensitive applications or high-demand virtual

environments. It provides better performance and efficiency, which is crucial for environments

where speed and responsiveness are critical.

#### 3. Enhanced Resilience: VHDx provides built-in protection against data corruption caused by

unexpected power failures. It includes features that help maintain data integrity and reduce the risk

of file corruption.

- Benefit: Enhanced resilience improves reliability and minimizes the risk of data loss in

virtualized environments. This feature is particularly important in scenarios where data integrity

and uptime are critical.

#### 4. Dynamic Disk Support: VHDx supports dynamic resizing and disk expansion without

requiring a shutdown of the virtual machine. This allows administrators to adjust the size of the

virtual disk as needed without interrupting operations.

- Benefit: Dynamic disk support offers greater flexibility and ease of management. It allows for

on-the-fly adjustments to disk size, which is useful for adapting to changing storage needs without

impacting the availability or performance of the virtual machine.

Under what conditions will you use differencing and pass through.

### Differencing Disks: Differencing disks are virtual disks that record changes made to a base

virtual disk, keeping the base disk unchanged while capturing modifications in a separate child

disk.

When to Use Differencing Disks:

1. Testing and Development: Perfect for creating test environments or development scenarios

from a standard base image. Each differencing disk can track changes without altering the original

disk.

- Benefit: Allows for the rapid setup of multiple testing environments and saves time and

resources.

2. System Customization: Useful for generating customized versions of a virtual machine from

a standard template. Custom configurations or updates can be stored in differencing disks while

the base disk remains unchanged.

Benefit: Simplifies managing various configurations or versions from a single base image.

3. Rollback Capabilities: Facilitates reverting to a previous state by removing the changes

recorded in the differencing disk.

Benefit: Makes it easy to undo changes or recover from errors without affecting the original

disk.

4. Resource Efficiency: Manages storage effectively by saving only the changes rather than

duplicating entire virtual disks.

Benefit: Conserves disk space and reduces data management needs.

### Pass-Through Disks: Pass-through disks are physical disks assigned directly to a virtual

machine, bypassing the virtualization layer to provide direct access to the hardware.

When to Use Pass-Through Disks:

1. Performance Needs: Ideal for scenarios requiring high performance, such as applications

with high I/O demands that cannot be handled efficiently by virtual disks.

Benefit: Delivers near-native performance by accessing the physical disk directly.

2. Compatibility Requirements: Necessary when a virtual machine needs access to specific

hardware features or settings that virtual disks cannot provide.

- Benefit: Ensures compatibility with legacy applications or systems dependent on physical

disk properties.

3. Large Storage Demands: Useful when a virtual machine needs more storage than virtual

disks can handle efficiently.

Benefit: Provides access to physical disks with large storage capacities.

4. Direct Hardware Access: Required for tasks needing direct access to hardware, such as

using specialized devices or performing disk-level operations.

Benefit: Allows direct interaction with physical storage devices for certain administrative or

specialized tasks.

Why external, internal and private in virtualization.

### External Network

Purpose: To connect VMs with external resources like the internet and other networks outside

the host.

Reasons to Use:

1. Internet Access: Enables VMs to access the internet and external services, which is crucial

for activities such as updates and web hosting.

2. Connectivity: Facilitates communication between VMs and other machines or networks

outside the host environment.

### Internal Network

Purpose: Allows VMs on the same host to communicate with each other but not with the

external network or the host machine.

Reasons to Use:

1. Isolation: Provides a secure environment where VMs can interact privately without external

network exposure.

2. Testing and Development: Ideal for scenarios where internal communication is needed

without external network access.

### Private Network

Purpose: Creates a network segment for VMs on the same host to communicate exclusively

with each other, with no access to external networks or the host machine.

Reasons to Use:

1. Security: Ensures a high level of security by restricting communication to a closed network,

safeguarding against external threats.

2. Segmentation: Supports network segmentation by isolating specific applications or services

from external interference.

Why and how do we backup and monitoring

#### Monitoring

Purpose: To oversee system performance, detect potential issues, and ensure the server

operates efficiently.

Reasons to Monitor:

1. Performance Management: Identifies performance issues, such as high CPU or memory

usage, to enhance system efficiency.

2. Issue Detection: Alerts administrators to emerging problems before they affect operations,

allowing for early intervention.

3. Security Monitoring: Detects unauthorized access or security threats to protect the server

environment.

4. Compliance and Reporting: Provides data and reports to meet regulatory and organizational

compliance requirements.

How to Monitor on Windows Server 2012:

1. Use Performance Monitor:

- Steps: Open `Performance Monitor` from Administrative Tools. Add and configure

performance counters to track metrics like CPU usage, disk I/O, and memory usage.

2. Set Up Alerts:

- Steps: Configure alerts in `Performance Monitor` to notify administrators of specific

conditions or exceeded thresholds, such as high CPU usage or low disk space.

3. Review Event Logs:

- Steps: Use `Event Viewer` to check system, application, and security logs for warnings or

errors. Regularly monitor these logs to detect and address issues.

4. Utilize Windows Server Essentials Dashboard (if applicable):

- Steps: For Windows Server 2012 Essentials, use the dashboard to monitor server health,

backup status, and performance metrics.

5. Use Task Manager and Resource Monitor:

- Steps: Open `Task Manager` or `Resource Monitor` for real-time insights into system

performance, processes, and resource usage.

### Major Types of Virtual Hard Disks

1. VHD (Virtual Hard Disk)

- Description: The original virtual hard disk format, introduced by Microsoft. It is used to

create virtual disks that mimic physical hard drives in virtual machines.

- Key Features: Supports up to 2 TB of disk space. Commonly used in older virtualization

platforms and has broad compatibility with various systems.

2. VHDx (Virtual Hard Disk Extended)

- Description: An updated version of the VHD format introduced with Windows Server 2012.

It offers enhanced features over the standard VHD.

- Key Features: Supports up to 64 TB of disk space, includes protection against data

corruption from power failures, and offers better performance and dynamic resizing capabilities.

3. VMDK (Virtual Machine Disk)

- Description: Developed by VMware, this format is used primarily with VMware's

virtualization products but is also supported by other platforms.

- Key Features: Can be used for different disk types such as thin provisioned and eager

zeroed thick disks. Provides high performance and flexibility for VMware environments.

4. VHDL (Virtual Hard Disk Library)

- Description: A format used by various virtualization solutions to manage virtual disk libraries

and provide access to virtual disk images.

- Key Features: Typically used for managing large volumes of virtual disk images and often

integrated into advanced virtualization setups.

To install an Active Directory Domain Services (AD DS) database on a Windows Server 2012,

follow these steps:

### Step 1: Install Active Directory Domain Services

1. Log in to the Server:

Log in to the Windows Server 2012 with an account that has administrative privileges.

2. Open Server Manager:

Open the Server Manager from the taskbar or start menu.

3. Add Roles and Features:

- In Server Manager, click on "Manage" and then select "Add Roles and Features."

- Click "Next" on the "Before you begin" page.

4. Select Installation Type:

- Choose "Role-based or feature-based installation" and click "Next."

5. Select Destination Server:

- Select the server you want to install AD DS on and click "Next."

6. Select Server Roles:

- On the "Select server roles" page, check the "Active Directory Domain Services" box.

- A dialog box will appear asking to add required features. Click "Add Features."

- Click "Next."

7. Select Features:

- On the "Select features" page, you can add any additional features if needed, but for a basic

AD DS installation, click "Next."

8. AD DS Information:

- Read the information about AD DS and click "Next."

9. Confirm Installation Selections:

- Review your selections and click "Install."

10. Complete the Installation:

- Wait for the installation to complete, then click "Close."

### Step 2: Promote the Server to a Domain Controller

1. Open the AD DS Configuration Wizard:

- After installation, in Server Manager, click on the yellow notification triangle and then click

"Promote this server to a domain controller."

2. Deployment Configuration:

- Choose whether to add a domain controller to an existing domain, add a new domain to an

existing forest, or add a new forest.

- For a new AD DS installation, select "Add a new forest" and enter a root domain name. Click

"Next."

3. Domain Controller Options:

- Choose the forest and domain functional levels (Windows Server 2012).

- Check the "Domain Name System (DNS) server" and "Global Catalog (GC)" options.

- Set the Directory Services Restore Mode (DSRM) password. Click "Next."

4. DNS Options:

- Ignore the DNS delegation warning if it appears and click "Next."

5. Additional Options:

- Verify the NetBIOS name and click "Next."

6. Paths:

- Specify the location of the AD DS database, log files, and SYSVOL folder, or use the default

locations. Click "Next."

7. Review Options:

- Review your selections and click "Next."

8. Prerequisites Check:

- The wizard will run a prerequisites check. Once completed successfully, click "Install."

9. Installation:

- The server will be configured as a domain controller, and it will automatically reboot once the

process is complete.

### Step 3: Post-Installation Tasks

1. Verify Installation:

- After the server reboots, log in using the domain credentials.

- Open "Active Directory Users and Computers" from the start menu to verify the AD DS

installation.

2. Configure DNS (if necessary):

- Ensure that the DNS settings are properly configured for the domain.

3. Create and Manage User Accounts and Groups:

- Begin creating and managing user accounts, organizational units (OUs), and groups as

needed.

### Basics of Group Policy Inheritance

1. Group Policies: These are rules and settings that control what users and computers can do

in a network. Think of them as instructions or guidelines.

2. Hierarchy Levels: Group policies are applied at different levels:

- Local: Each computer has its own settings.

- Site: A group of computers in a specific geographical area.

- Domain: A large group of computers managed together.

- Organizational Unit (OU): Smaller groups within the domain, like departments.

### Order of Application

1. Local Policies: These are applied first to each individual computer.

2. Site Policies: If a computer is part of a site (like all computers in a specific building), these

policies are applied next.

3. Domain Policies: These policies are applied to all computers in the domain. They override

local and site policies if there are conflicts.

4. OU Policies: These are applied last and are the most specific. They override local, site, and

domain policies if there are conflicts.

### How Inheritance Works

- Inherited Policies: Policies from higher levels (like the domain) are passed down to lower

levels (like the OU).

- Blocking Inheritance: Sometimes, you might not want a lower level to follow higher-level

policies. You can block inheritance to stop higher-level policies from applying.

- Enforced Policies: To make sure a policy always applies, you can enforce it. Even if a lower

level tries to block it, the enforced policy will still apply.

### Practical Example

1. Local Policy: Every computer has a rule that says screensavers should start after 5 minutes.

2. Site Policy: For all computers in the "New York" site, the rule is changed to 10 minutes.

3. Domain Policy: For the entire company, the rule is set to 15 minutes.

4. OU Policy: For the "HR Department" OU, the rule is set to 20 minutes.

In this case, a computer in the HR Department in New York will have a screensaver start time of

20 minutes because the OU policy is the most specific and is applied last.

### Key Points

- Policies are applied from the most general (local) to the most specific (OU).

- More specific policies override more general ones.

- You can block or enforce policies to control which rules apply.

Group policies in a Windows environment are inherited based on the hierarchical structure of

Active Directory. Here’s how they work:

1. Hierarchy: Group policies are applied in a specific order based on the Active Directory

hierarchy: Local -> Site -> Domain -> Organizational Unit (OU). Policies at higher levels in the

hierarchy can be overridden by policies at lower levels.

2. Local Group Policy: This is the first level of policy application. Each computer has its own

local group policy, which is applied first.

3. Site-Level Group Policy: Policies defined at the site level in Active Directory are applied

next. A site represents one or more IP subnets and is used to manage network traffic and

resources.

4. Domain-Level Group Policy: Policies applied at the domain level affect all users and

computers within the domain. These policies override site-level policies if there are conflicts.

5. Organizational Unit (OU) Group Policy: The most specific level, OUs can have their own

policies that apply only to the users and computers within that OU. These policies override

domain, site, and local policies.

6. Inheritance: By default, group policies are inherited from parent containers (like domains or

OUs) to their child containers. However, inheritance can be blocked or enforced:

- Block Inheritance: An OU can be configured to block inheritance, meaning it will not inherit

policies from its parent containers.

- Enforced Policies: Policies can be set to “Enforced” (previously known as "No Override"),

meaning they will apply even if inheritance is blocked at a lower level.

7. Order of Application: If multiple policies apply to a single user or computer, they are

processed in the following order:

- Local Group Policy

- Site Group Policies (applied in alphabetical order)

- Domain Group Policies (applied in alphabetical order)

- OU Group Policies (applied from the parent OU down to the child OU, in order)

8. Conflict Resolution: When settings in multiple GPOs conflict, the last applied policy takes

precedence. For example, if a domain policy and an OU policy have conflicting settings, the OU

policy will apply because it is processed last.

9. Loopback Processing: In certain scenarios, such as with terminal servers, loopback

processing can be enabled. This means that user policies can be reapplied based on the

computer's location in Active Directory, which can be useful for applying different user policies

based on the computer being used.

This hierarchical structure and the ability to block or enforce policies provide a flexible and

powerful way to manage configurations and settings across a network.

1. Production Checkpoint:

- What it is: A checkpoint that uses backup technology within the guest operating system to

create a consistent and application-aware backup.

- Purpose: To create a more reliable and stable backup of the virtual machine that is suitable

for production environments.

- How it works: It uses Volume Shadow Copy Service (VSS) in Windows or File System

Freeze in Linux to ensure that the applications are in a consistent state.

- Example: If you have a virtual machine running a critical database, a production checkpoint

will ensure that the database is properly quiesced and that the backup is consistent and reliable,

minimizing data loss and corruption risk during a restore.

2. Standard Checkpoint (also known as a Classic or Snapshot Checkpoint):

- What it is: A checkpoint that captures the state, data, and hardware configuration of a

running virtual machine.

- Purpose: Useful primarily for development and testing scenarios where a quick restore

point is needed without the need for application consistency.

- How it works: It captures the current state of the virtual machine, including memory and

system state, but does not ensure application consistency.

- Example: If you're developing an application and want to test different configurations, a

standard checkpoint allows you to quickly revert to a previous state if something goes wrong

without worrying about the application state.

Nested virtualization is a technology that allows you to run a virtual machine (VM) inside another

VM. In other words, it enables you to create a virtualized environment within a virtualized

environment. This technique is also known as "nested hypervisors" or "virtualized virtualization".

Here's a breakdown of the concept:

1. \*Host machine\*: The physical server or computer that runs a hypervisor (e.g., VMware, HyperV, or KVM).

2. \*Outer VM\*: A virtual machine created on the host machine using the hypervisor.

3. \*Inner VM\*: A virtual machine created inside the outer VM, using a nested hypervisor.

Nested virtualization allows for:

- \*Deeper virtualization\*: Running multiple layers of virtualization, enabling more complex and

flexible virtualized environments.

- \*Improved testing and development\*: Isolating test environments within VMs, making it easier to

test and develop software.

- \*Enhanced security\*: Creating secure, isolated environments for sensitive applications or data.

- \*Better resource utilization\*: Optimizing resource allocation by running multiple VMs within a

single outer VM.

WORKGROUP

• No centralised Authentication

• No centralized Administration

• Maximum of 20 computers

supported for accessing a shared

file or folder at the same time

DOMAIN

• Centralized Authentication

• Centralized Administration

• Unlimited number of computers

WORKGROUP NETWORK DOMAIN BASED NETWORKING

Why Domain based networking

Domain-based networking, specifically using Active Directory (AD) domains in Windows Server environments, is preferred for large networks due to

several key benefits:

• Centralized Management: AD domains provide a centralized management

framework, allowing administrators to manage network resources, user

accounts, and security settings from a single location. This significantly

simplifies the administration and maintenance of a large network, as

changes can be made globally and propagated across the domain.

• Scalability: AD domains are designed to handle large networks with

thousands of users and computers. The hierarchical structure of domains,

sites, and organizational units (OUs) allows for efficient organization and

management of network objects. Administrators can delegate specific

administrative tasks to lower-level administrators based on the domain's

organizational structure.

6

• Security and Access Control: AD domains offer robust security

features, including user authentication, authorization, and access

control. Domain controllers authenticate user credentials and control

access to network resources based on user/group memberships and

Group Policy settings. This ensures that only authorized users can

access specific resources and helps enforce security policies

consistently across the network.

• Single Sign-On (SSO): With an AD domain, users can use a single set of

credentials to access various network resources, including file shares,

printers, applications, and email. This eliminates the need for users to

remember multiple usernames and passwords, improving user

experience and reducing the risk of weak or compromised passwords.

7

• Group Policy: Group Policy allows administrators to enforce

standardized configurations, security settings, and software

deployments across the domain. This helps maintain consistency and

ensures that all computers and users adhere to the organization's IT

policies. Group Policy also simplifies software installation and update

management, reducing administrative overhead.

• Redundancy and Fault Tolerance: AD domains support multiple

domain controllers that replicate directory information, providing

redundancy and fault tolerance. If one domain controller fails, others

can continue to authenticate users and provide access to network

resources. This enhances network availability and reduces the impact

of single points of failure.

8

Active Directory terms

Logical components

• Domains

• Domain trees

• Forest

• Organisational Units

• Containers

Physical compnonents

• Domain Controllers

• Read-only Domain controllers

9

Active Directory Domains and Forest

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.

10

Active Directory Domains and Forest

11

Installing Active Directory

Prerequites

• Static IP address

• Computer name

• DNS server address defined

• Location of database defined

• NOTE: Steps to install active directory

12

Active Directory Domains and Forest

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

13

Understanding Active Directory Objects

• User Objects

• Authentication of the user at user at logon

• Access control

• Group Objects

• Assigning of permissions

• Computer Objects

• Authentication of the computer at startup

14

Organisational Units (Ous) 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

OUs are containers within an AD domain used to organize and manage

objects such as users, computers, and other AD resources.

• Create OUs to:

• Configure objects by assigning GPOs to them

• Delegate administrative permissions

DOMAIN CONTROLLERS:

• These are servers that host the AD DS database (Ntds.dit) and SYSVOL

• Host the Kerberos authentication service and Key Distribution Centre services platform authentication

• For best practices, a domain environment should have two domain

controllers of which one serves as a backup in case of failure

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 domain controllers to

hold a copy of the global catalog

• When you have multiple sites, you should also make at least on

domain controller at each site global catalog server

What are GPOs?

A feature of Windows Server called Group Policy enables

administrators to control and enforce settings across numerous

computers in an Active Directory (AD) domain. Security

configurations, software deployment, folder redirection, and other

aspects of user and computer configurations can all be managed

centrally through Group Policy.

• 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

Benefits of GPOs

Benefits of GPOs in computer networks:

• Centralized Management: GPOs provide a centralized management approach,

allowing administrators to define and apply configurations from a central

location. This simplifies the administration process and ensures consistent

settings across the network.

• Consistency and Standardization: GPOs enable administrators to enforce

standardized configurations and policies across the network. This consistency

helps ensure that all computers and users adhere to organizational standards,

security policies, and best practices.

• Time and Cost Savings: With GPOs, administrators can automate the

configuration and management of network resources, saving time and reducing

administrative overhead. They can push out configurations and software

deployments to multiple computers simultaneously, eliminating the need for

manual configuration on each machine.

• Enhanced Security: GPOs play a crucial role in strengthening network

security. Administrators can enforce security settings, restrict access

to resources, and configure auditing and logging policies. This helps

protect against unauthorized access, data breaches, and security

vulnerabilities.

• Granular Control: GPOs offer granular control over policy settings.

Administrators can target specific users, groups, or computers,

applying different policies based on criteria such as location,

department, or job role. This flexibility allows for customized policy

enforcement and ensures that policies are tailored to specific needs.

• Simplified Software Deployment: GPOs simplify the deployment and

management of software applications. Administrators can push out

software installations, updates, and patches across the network,

ensuring that all computers have the necessary software and

reducing the risk of outdated or vulnerable applications.

• Compliance and Auditing: GPOs help organizations meet regulatory

compliance requirements by enforcing policies and configurations

that align with industry standards. GPOs also provide auditing

capabilities, allowing administrators to track policy changes, monitor

user activity, and generate reports for compliance purposes.

Overview of GPO scope and inheritance

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

1. Local GPOs: Local Group Policy Objects (GPOs) are a feature of Microsoft

Windows operating systems that allow administrators to define and enforce

policy settings on individual computers. Unlike Group Policy settings applied

through Active Directory domains, which are managed centrally and applied

to multiple computers, local GPOs are specific to a single computer and are

managed locally on that machine.

2. Site-level GPOs: Site-level Group Policy Objects (GPOs) are a type of GPO in Microsoft Active Directory that allows administrators to apply policy settings to computers and users based on their physical network location. Site-level GPOs are linked to AD sites, which represent physical network locations such as offices, branches, or data centers.

3. Domain-level GPOs: Domain-level Group Policy Objects (GPOs) are an integral part of Microsoft Active Directory (AD) and provide a means for administrators to define and enforce policy settings across an entire domain. Domain-level GPOs are linked directly to the AD domain and apply to all users and computers within that domain.

4. Organizational Unit GPOs: Organizational Unit (OU) Group Policy Objects (GPOs) are a type of GPO in Microsoft Active Directory that allows administrators to apply policy settings to specific OUs within a domain.

Altering Group Policy Processing

• Block inheritance: Blocking inheritance is a feature in Group Policy that allows administrators to prevent the inheritance of Group Policy settings from parent containers to child containers within

an Active Directory (AD) domain. When inheritance is blocked, Group Policy settings defined at

higher levels in the AD hierarchy, such as domain-linked GPOs, site-linked GPOs, or parent OU- linked GPOs, are not applied to objects within the child containers.

• Enforced: The "Enforced" setting in Group Policy is a feature that allows administrators to ensure the application of specific Group Policy Objects (GPOs) regardless of inheritance blocking or other policy conflicts within an Active Directory (AD) domain. When the "Enforced" setting is enabled on a GPO, it takes precedence over any inheritance blocking or policy conflicts that might exist.

• Security filtering: Security filtering in Group Policy is a mechanism that allows administrators to selectively apply Group Policy Objects (GPOs) to specific users, groups, or computers within an Active Directory (AD) domain. By using security filtering, administrators can control which objects will receive and apply the settings defined in a GPO, providing a more granular approach to policy application.

• NOTE: You should be able to explain how group policies are inherited.

Starter GPOs

• Introduced in Windows Server 2008, starter GPOs are templates for Group Policy settings. These objects enable an administrator to create and have a pre-configured group of settings that represent a baseline for any future policy to be created.

• A starter GPOS provides a template like function for Group Policy Objects. When a Starter GPO is created, the administrator can configure any settings in the Administrative Templates part of the Group Policy.

Backing up GPOs

• Group Policy objects are critical for managing Windows Server infrastructure. To avoid severe service issues, administrators must configure GPOs carefully and be prepared to revert any changes quickly by backing them up before modifying them.

• GPOs do not automatically re-link themselves to OUs, domains or wherever they were applied so you would have to link them again when restored

Gpudate is a command-line utility from Microsoft that comes with all versions of the windows operating system. It is a utility that controls the application of group policy objects on assigned Active Directory computers. gpudate /force will process all GPOs regardless if they have changed or not. gpudate is run on the client device to update policy changes made in the server.

• Gpresult is used to verify the GPOs that are currently applying to a user and a computer account.

Command:

gpresult /r

Gpresult /h (name of file).html

HYPERVISORS

TYPE 1 VIRTUALIZATION

• The virtualization capability built into Windows Server 2012, called

Hyper-V, uses a different type of architecture. Hyper-V uses Type I virtualization, in which the hypervisor is an abstraction layer that interacts directly with the computer’s physical hardware—that is, without an intervening host OS.

• The parent partition accesses the system hardware through the

hypervisor, just as the child partitions do. The only difference is that

the parent runs the virtualization stack, which creates and manages

the child partitions.

VIRTUALIZATION ARCHITECTURES

TYPE 2 VIRTUALIZATION: hypervisor runs on top of a host OS

• By using the Type II hypervisor, you create a virtual hardware

environment for each VM. You can specify how much memory to

allocate to each VM, create virtual disk drives by using space on the

computer’s physical drives, and provide access to peripheral devices.

• Type II virtualization can provide adequate VM performance,

particularly in classroom and laboratory environments, but it does not

provide performance equivalent to separate physical computers.

Therefore, it is not generally recommended for high-traffic servers in

production environments.

33

Overview of Hyper-V

• Hyper-V is a hardware virtualization server role available for Windows Server. It Provides a software layer known as the Hypervisor, used to control access to physical hardware it Supports many types of guest operating systems including:

o All supported Windows versions

o Linux

• General Hyper-V features can be grouped as follows:

o Management and connectivity

o Portability

o Disaster recovery and backup

o Security

o Optimization

Overview of Hyper-V

• System requirements for installing the Hyper-V server role include:

o A 64-bit processor

o Sufficient memory –Minimum 4GB

o 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:

o Server Manager

o Install-WindowsFeature PowerShell cmdlet

Overview of Hyper-V Manager is a graphical user interface used to manage both local and remote Hyper-V host machines

• Other management tools include:

o Windows PowerShell

o Windows Admin Center

Best practices for configuring Hyper-V hosts

• Consider the following when provisioning Windows Server as a Hyper-V host:

o Provision the host with adequate hardware

o Deploy virtual machines on separate disks. solid state drives performs better

o Do not collocate other server roles

o Manage Hyper-V remotely

o 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:

o Both the Hyper-V host and the guest virtual machine must be Windows

Server 2016 or later

o Sufficient amount of static RAM

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

38

VM generation versions

Generation 1 VMs:

o Support 32 and 64-bit operating systems

o Only support boot volumes a maximum of 2 TB

o Supports legacy BIOS

Generation 2 VMs:

o Support only 64-bit operating systems

o Support secure boot (ensures that non of the boot files are corrupted) and

shielded VMs (encryption of virtual hard drives for virtual machines and restricts access from the hyper-v host to the virtual machine)

o Support boot volumes a maximum of 64 TB

o Supports Unified Extensible Firmware Interface (UEFI)

39

• VM settings VM settings are grouped into two main areas:

o Hardware

o Management

• Available hardware components depend on the generation version of

the VM

• There are no differences in management settings in between

Generation 1 and Generation 2 machines.

• Server 2008 will be run as a Generation 1, server 2012 and newer

versions will be run as Generation 2 virtual machines.

• You can’t change the generation of a virtual machine after creation.

40

Storage options in Hyper-V

Consider the following factors when planning storage for virtual hard

disks:

o High-performance connection to external storage storage

o Redundant storage

o High-performance storage (SSD will have a better performance)

o Adequate growth space

Virtual hard disk formats and types

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

A full backup is often considered the most

secure, reliable method of copying data. A few

additional advantages include: Restore and

recovery times are shorter because complete

data is always readily available. All data is

backed up at once, making version control easy

to manage

ICT 322 48

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

ICT 322 49

Overview of Task Manager

Task Manager is a tool that enables

you to: • Verify and monitor resources

performance and usage (RAM, CPU,

etc) for your server.

• Manage processes, applications and

services.

• Manage users connected to your server (see the applications and

processes they use, disconnect users,

access to the users account manager)

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

issues

ICT 322 50

Overview of Resource Monitor

• Resource Monitor is a great tool to

identify which program/service is

using resources like program,

applications, network connection

and memory usages. It is a

PowerShell-based feature that

enables you to document virtual

machine usage.

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

ICT 322 51

Overview of Performance Monitor

• The Microsoft Windows Performance

Monitor is a tool that administrators

can use to examine how programs

running on their computers affect the

computer's performance. The tool can

be used in real time and also be used

to collect information in a log to

analyze the data at a later time.

• Performance Monitor enables you to

observe current performance statistics

or to study historical data that Data

Collector Sets have gathered

ICT 322 52

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

ICT 322 53

Overview of baselines, trends, and capacity

planning

By calculating performance baselines for your server environment, you can

more accurately interpret realtime monitoring information

By establishing a baseline, you can:

• Interpret performance trends

• Perform capacity planning

• Identify bottlenecks

• Analyze performance trends to predict when existing capacity is likely to

be exhausted

• Plan the capacity for the key hardware components such as processor, disk,

memory, and network

Considerations for monitoring virtual machines

Considerations for monitoring virtual machines:

• Virtual machines must be assigned sufficient resources for their

workload

• If multiple virtual machines run on a host, ensure the host has

enough resources

• Resources are shared, so performance of one virtual machine can

affect the performance of others

• You must remember to monitor the resource utilization on the host

as well as the guests