

UNIVERSITY OF BUEA

P.O Box 63,
Buea South West Region
CAMEROON
Tel: (237) 3332 21 34/3332 26 90
Fax: (237) 3332 2272

REPUBLIC OF CAMEROON

PEACE-WORKFATHERLAND



**FACULTY OF ENGINEERING AND TECHNOLOGY
DEPARTMENT OF COMPUTER ENGINEERING**

Course Title: SYSTEM ADMINISTRATION (UNIX, LINUX, WINDOWS), CEF 473

Course Instructor: Dr. DJOUELA Ines

**Windows System Administration - An Application to
Windows Server**

Presented By:

Names	Matricules	Specialty
KAMCHE YANN ARNAUD	FE21A208	Software
DJEUTIO QUOIMON ANDERSON ROY	FE21A169	Software
NKEMZI FOLEFACK GIL	FE21A276	Software
TETUH WIBINAH ENGONWEI	FE21A322	Networking
OJONG-ENYANG OYERE	FE21A297	Software
ABANGMA ARRAH JESUS MCLOUIS	FE21A124	Software
CHE BLAISE NJI	FE21A157	Software
TAKOH CLOVERT NFUA	FE21A311	Networking
MONDOA ROBERT NASOA NDIVE	FE21A241	Software

TABLE OF CONTENTS

1. Introduction	4
1.1 Background.....	4
1.2 Objectives.....	4
2. User and Group Management.....	5
2.1 Overview.....	5
2.1.1 Creating and Managing User Accounts.....	5
2.1.2 Password Policies and Security.....	6
2.1.3 User Permissions and Access Control.....	7
2.2 Group Management.....	8
2.2.1 Creating and Managing Groups.....	8
2.2.2 Group Policies and Best Practices.....	9
3. File System and Disk Management.....	11
3.1 File System Overview.....	11
3.1.1 NTFS vs. FAT32.....	11
3.1.2 File and Folder Permissions.....	13
3.2 Disk Management.....	14
3.2.1 Disk Partitioning.....	14
3.2.2 Volume Mounting and Mapping.....	16
3.2.3 Disk Quotas and Storage Management.....	17
4. Active Directory and Domain Services.....	20
4.1 Introduction to Active Directory.....	20
4.1.1 Components of Active Directory.....	20
4.2 Domain Services.....	20
4.2.1 Domain Controllers and Replication.....	20
4.2.2 DNS and DHCP in Active Directory.....	23
5. Group Policy Management.....	25
5.1 Group Policy Overview.....	25
5.1.1 Creating and Linking Group Policies.....	25
5.1.2 Security Settings and Policy Inheritance.....	27
6. Extra Topics.....	28
7. Conclusion.....	37
8. Recommendations.....	37
9. References.....	38

Abstract

This technical report explores the practical applications of Windows System Administration within Windows Server environments. Focusing on critical components such as user and group management, file system and disk management, Active Directory, Group Policy and additional concepts like Security/Access Control, Hyper-V and Virtualization. This report aims to provide in-depth insights into the methodologies and best practices employed by system administrators.

1. Introduction

1.1 Background

The evolution of enterprise computing has led to the prominence of Windows Server as a versatile operating system, meeting the dynamic requirements of contemporary IT environments. System administrators serve as the linchpin in harnessing the full potential of Windows Server, ensuring optimal functionality, security, and reliability. This report aims to provide practical insights into Windows System Administration, focusing on key areas such as user and group management, file system and disk optimization, Active Directory services, and Group Policy management.

1.2 Objectives

The primary objectives of this report are:

User and Group Management:

- Understanding the principles of least privilege and secure password policies.
- Efficient creation and management of user accounts.
- Streamlined user permission assignment through group management.

File System and Disk Management:

- Differentiating between NTFS and FAT32 file systems.
- Implementing access controls and configuring file and folder permissions.
- Exploring disk partitioning, volume mounting, and disk quota strategies.

Active Directory and Domain Services:

- Introducing the components of Active Directory (Domains, Trees, Forests).
- Exploring the role of Domain Controllers and the synchronization mechanism in directory replication.
- Understanding the integration of DNS and DHCP within Active Directory.
- Examining trust relationships and authentication protocols.

Group Policy Management:

- Outlining the role of Group Policy in maintaining consistent settings.
- Providing insights into creating, linking, and managing group policies.
- Exploring security settings and policy inheritance.

2. User and Group Management

2.1 Overview

User and group management form the bedrock of a secure and organized IT environment. This section provides both theoretical and practical insights into creating and managing user accounts, enforcing password policies, and strategically managing user permissions.

2.1.1 Creating and Managing User Accounts

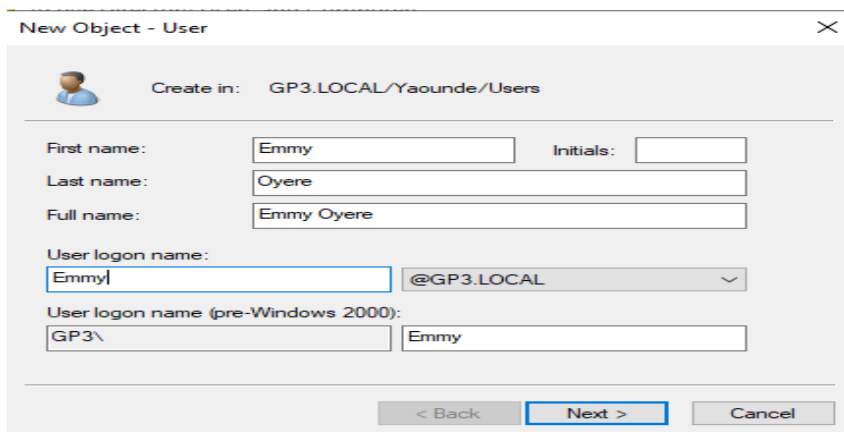
Theoretical Approach:

- User accounts are fundamental entities within Windows Server, representing individuals with access to the system.
- Account creation involves defining user attributes such as username, password, and group membership.

Practical Application:

1. Open Active Directory Users and Computers
2. Navigate to the "Users" container.
3. Right-click and select "New" -> "User."
4. Follow the wizard to input user details.
5. Set password policies, ensuring complexity and regular updates.

Screenshot: User Account Creation



The screenshot shows the 'New Object - User' wizard in the Active Directory Users and Computers console. The title bar reads 'New Object - User'. The path 'Create in: GP3.LOCAL/Yaounde/Users' is displayed. The wizard contains the following fields and values:

- First name: Emmy
- Last name: Oyere
- Full name: Emmy Oyere
- User logon name: Emmy
- User logon name (pre-Windows 2000): GP3\Emmy

At the bottom, there are three buttons: '< Back', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

Figure 1 user account creation.

2.1.2 Password Policies and Security

Theoretical Approach:

- Password policies enhance security by defining parameters such as complexity, expiration, and account lockout.
- Policies are enforced through Group Policy, ensuring consistency across the network.

Practical Application:

1. Configure password policies in Group Policy Management.
2. Define complexity requirements, expiration periods, and lockout policies.

Screenshot: Password Policy Configuration

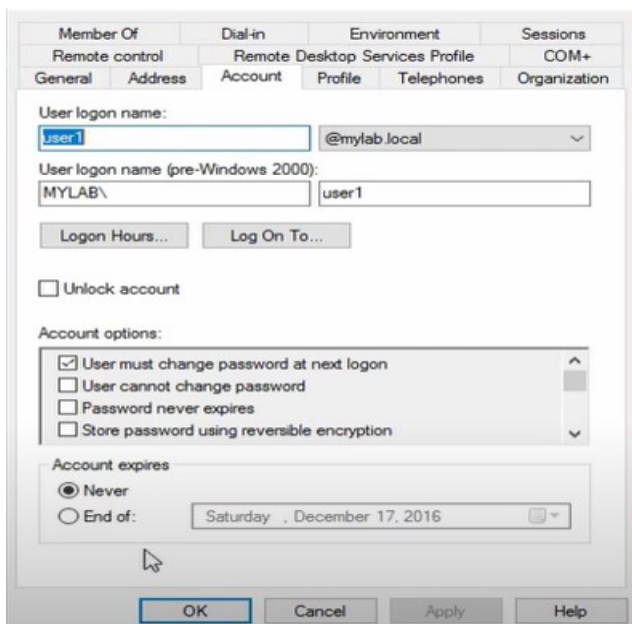


Figure 2 Setting expiration periods and account options.

2.1.3 User Permissions and Access Control

Theoretical Approach:

- Access Control Lists (ACLs) regulate user permissions, ensuring the principle of least privilege.

- Fine-grained control allows for precise assignment of rights to files, folders, and network resources.

Practical Application:

1. Use Access Control Lists (ACLs) to define permissions.
2. Assign specific rights to users or groups based on roles.

Screenshot: ACL Configuration

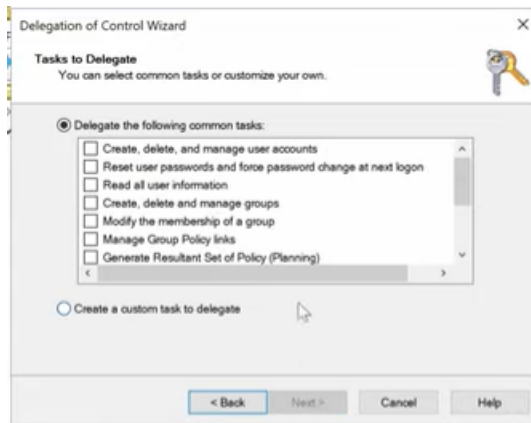


Figure 3 giving permissions to a group of users.

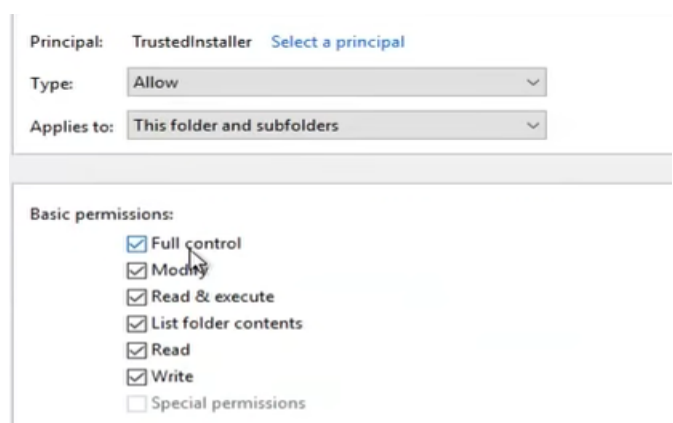


Figure 4 Assigning rights to users.

2.2 Group Management

This section focuses on the theoretical and practical aspects of creating and managing groups, emphasizing their role in efficient user permission assignment.

2.2.1 Creating and Managing Groups

Theoretical Approach:

- Groups in Active Directory categorize users based on roles or responsibilities.
- Group creation involves specifying a group name and scope.

Practical Application:

1. Open Active Directory Users and Computers

2. Navigate to the "Users" container.
3. Right-click and select "New" -> "Group."
4. Specify a group name and scope.

Screenshot: Group Creation

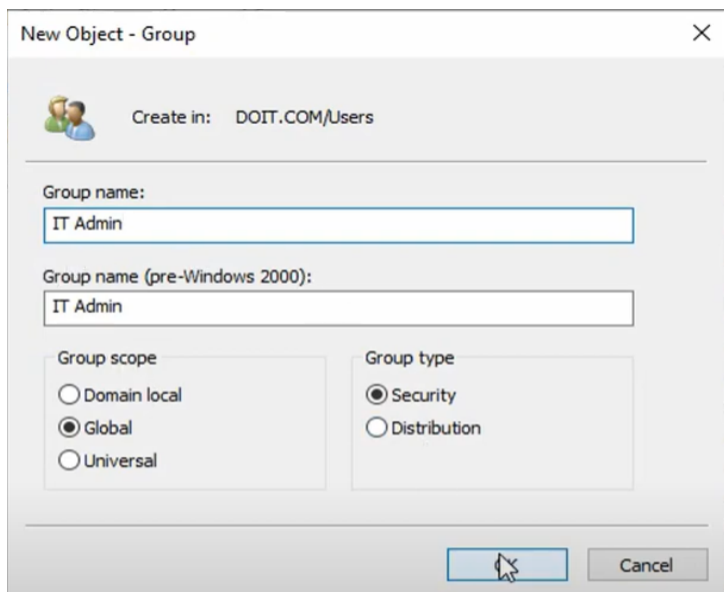


Figure 5 group creation.

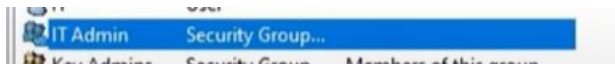


Figure 6 group created successfully.

2.2.2 Group Policies and Best Practices

Theoretical Approach:

- Group policies define configurations for users and computers within an Active Directory environment.
- Security settings, login scripts, and other configurations are set using Group Policy Management.

Practical Application:

1. Define group policies based on organizational requirements.
2. Set security settings and configurations in Group Policy Management

Screenshot: Group Policy Configuration

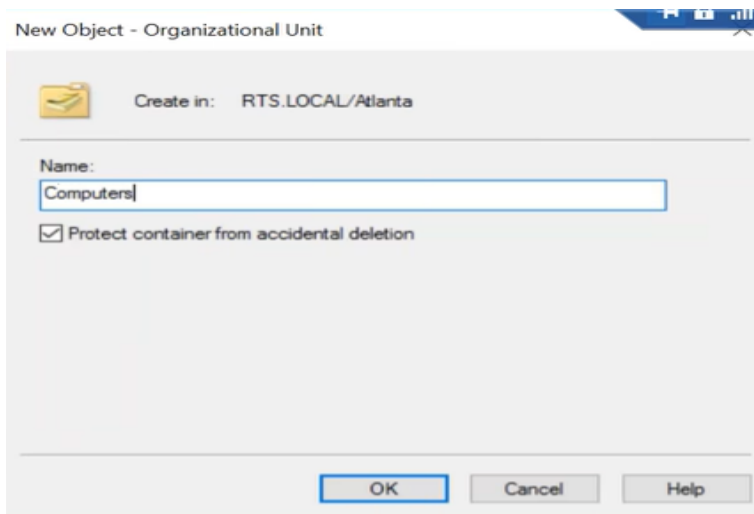


Figure 7 creating an organizational unit.

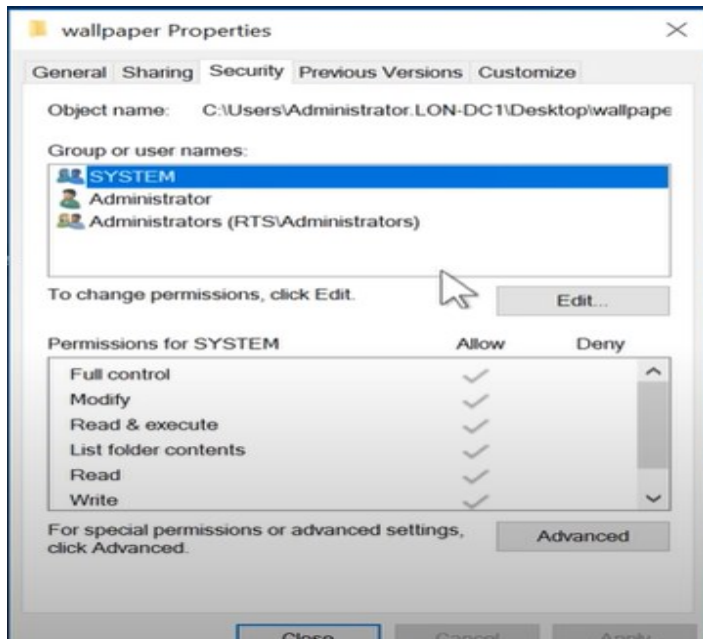


Figure 8 security settings and configuration.

3. File System and Disk Management

3.1 File System Overview

3.1.1 NTFS vs. FAT32

Understanding the distinction between NTFS (New Technology File System) and FAT32 (File Allocation Table 32) is crucial for effective file system management on Windows Server.

NTFS:

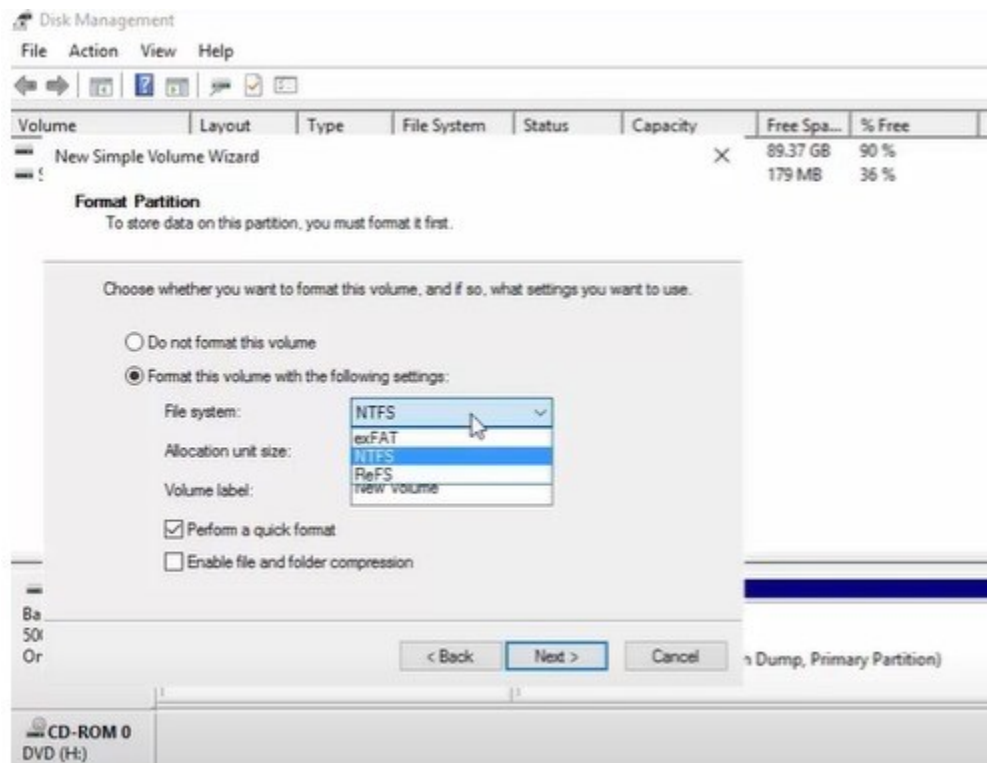
- Theoretical Approach:

- Advanced Features: NTFS supports advanced features such as file and folder-level permissions, encryption, compression, and auditing, enhancing security and data integrity.
- Large Volume Support: NTFS allows for larger partition sizes, accommodating volumes up to 256 terabytes, making it suitable for modern, scalable storage requirements.
- Reliability: NTFS incorporates journaling, which helps recover the file system quickly after a system failure, ensuring data consistency.

- Practical Application:

1. Open Server Manager on Windows Server.
2. Access File and Storage Services -> Volumes -> File Systems.
3. Choose the target volume, right-click, and select Format.
4. Choose NTFS as the file system and set other relevant options.

Screenshot: NTFS Format in Server Manager



FAT32:

- Theoretical Approach:

- Compatibility: FAT32 is more compatible with various operating systems and devices, making it suitable for removable storage like USB drives.
- File Size Limitation: FAT32 has a file size limit of 4 GB, which might be a limitation when dealing with large files.
- Simplicity: FAT32 is simpler and may be more suitable for smaller storage requirements where advanced features of NTFS are not necessary.

- Practical Application:

- Format removable drives with FAT32 using the Disk Management tool.

Screenshot: FAT32 Format in Disk Management



Recommendation: For Windows Server, NTFS is recommended for system drives and volumes where advanced security features are essential.

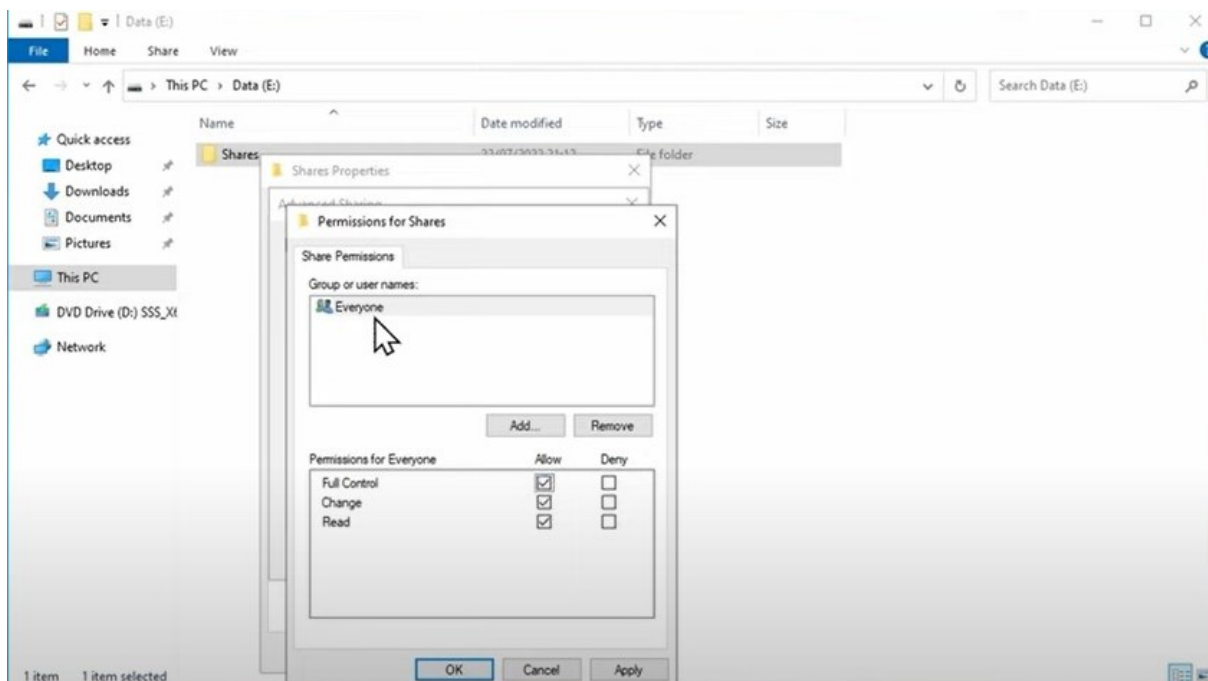
3.1.2 File and Folder Permissions

Implementing robust access controls through file and folder permissions is vital for maintaining data security and integrity on Windows Server.

Practical Steps:

1. Server Manager: Open Server Manager and navigate to File and Storage Services -> Shares.
2. Share Creation: Right-click and create a new share, setting permissions during the share creation process.
3. Advanced Security Settings: For more granular control, navigate to the file or folder, right-click, and choose Properties -> Security.
4. Permission Levels: Assign specific permission levels such as Read, Write, Execute, or Full Control based on user roles.

Screenshot: Setting File Permissions in Server Manager



Best Practices:

- Use Groups: Organize users into groups and assign permissions to groups, simplifying permission management.
- Regular Auditing: Enable auditing of file and folder access for security monitoring.
- Documentation: Maintain documentation of permission assignments for reference and audits.

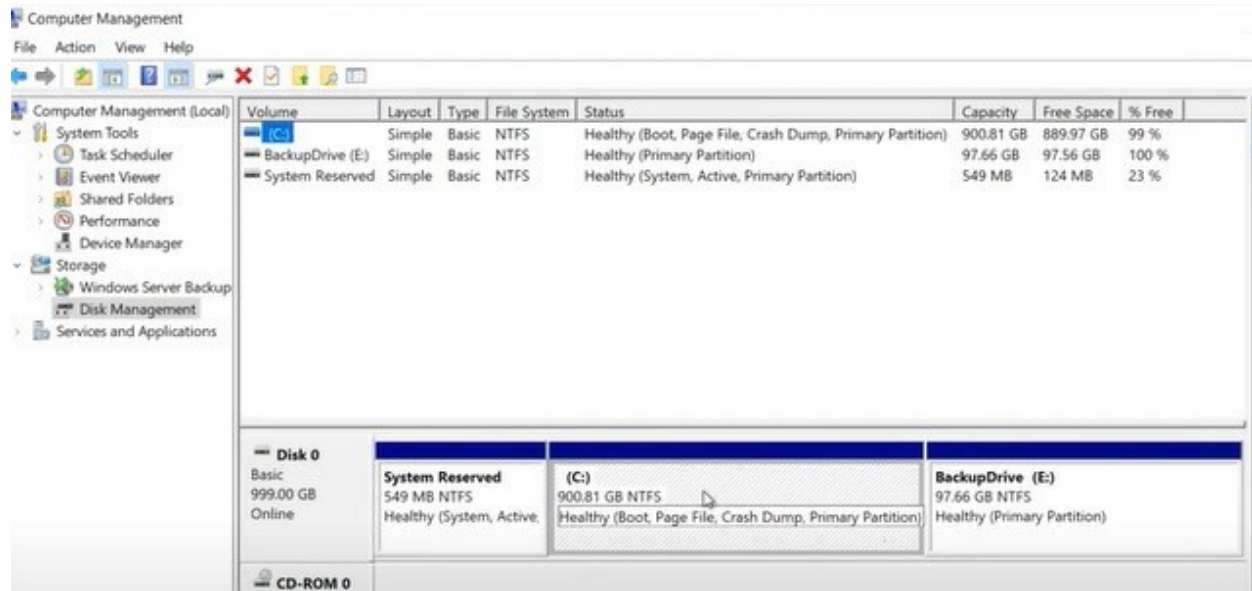
3.2 Disk Management**3.2.1 Disk Partitioning**

Efficient disk partitioning is essential for optimal resource allocation and organization on Windows Server.

Practical Steps:

1. Server Manager: Open Server Manager and navigate to Storage -> Disk Management.
2. Select the Disk: Right-click on the target disk and choose Shrink or Extend based on the requirement.
3. Allocate Space: Specify the size for the new partition or extend an existing one.

Screenshot: Disk Partitioning in Server Manager



Benefits:

- Isolation: Logical partitioning helps isolate system files from user data, improving system stability.
- Data Organization: Logical partitioning aids in organizing data based on usage or importance.
- Backup and Recovery: Separate partitions make it easier to back up and recover specific data without affecting the entire system.

3.2.2 Volume Mounting and Mapping

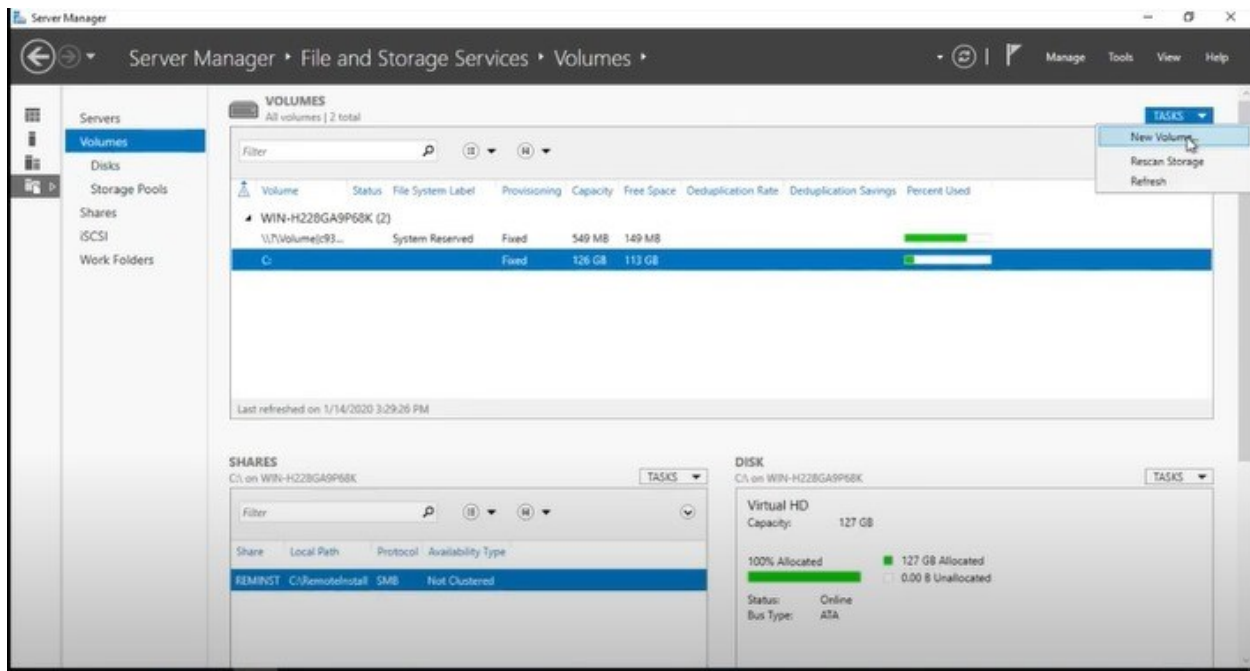
Volume mounting and mapping play a crucial role in seamless data access and simplified resource accessibility across the network on Windows Server.

Volume Mounting:

- Theoretical Approach: Mounting involves making a partition accessible in a specific directory (mount point) within another partition.

- Practical Application: Use the Disk Management tool to mount volumes to directories.

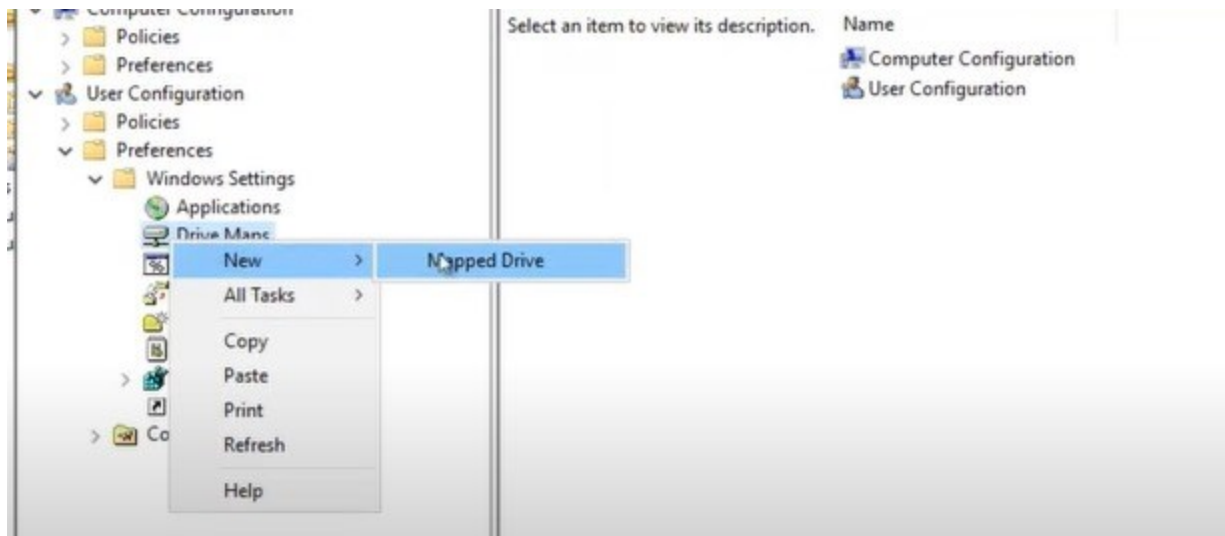
Screenshot: Volume Mounting in Disk Management



Volume Mapping:

- Theoretical Approach: Mapping involves connecting network drives to local drive letters for simplified access.
- Practical Application: Use File and Storage Services -> Shares to create mapped network drives.

Screenshot: Network Drive Mapping in Server Manager



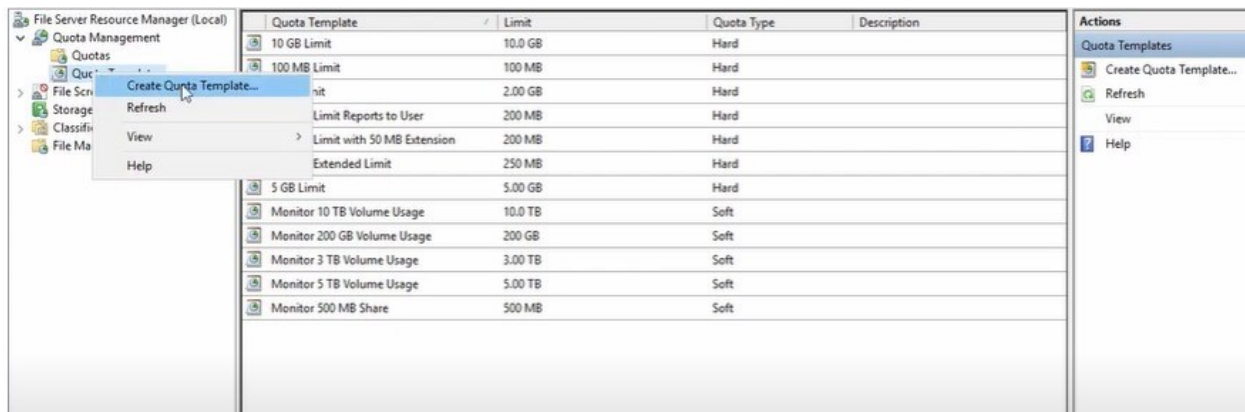
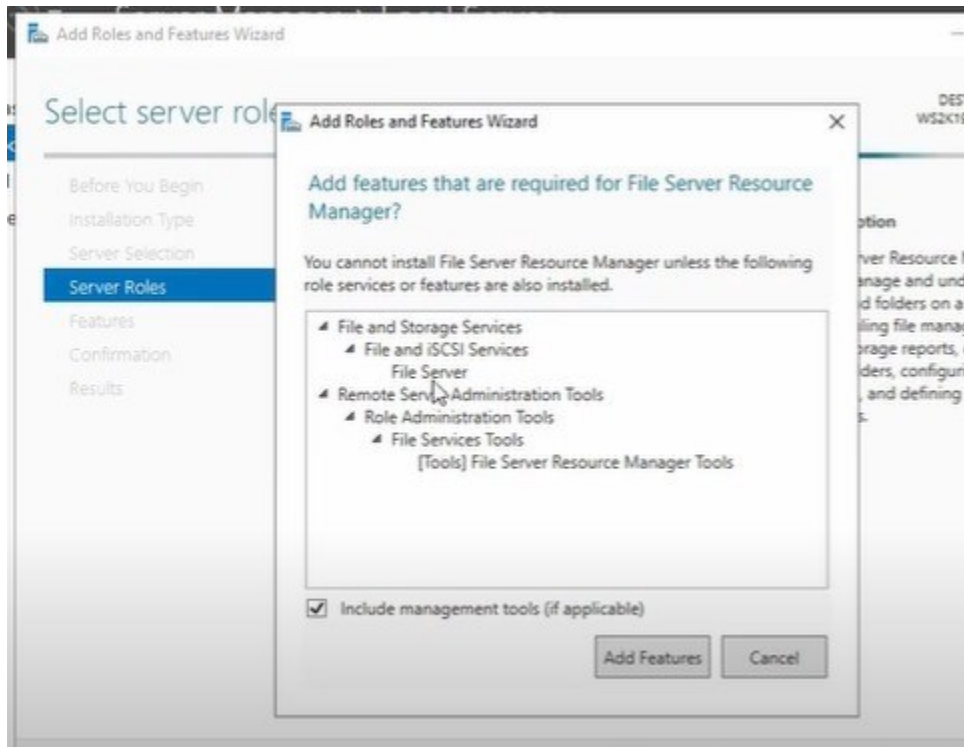
3.2.3 Disk Quotas and Storage Management

Efficient disk quotas and storage management strategies are crucial for optimizing disk space allocation and usage on Windows Server.

Disk Quotas:

- Theoretical Approach: Disk quotas restrict the amount of space a user or group can consume on a particular partition.
- Practical Application: Configure disk quotas through File Server Resource Manager (FSRM) in Server Manager.

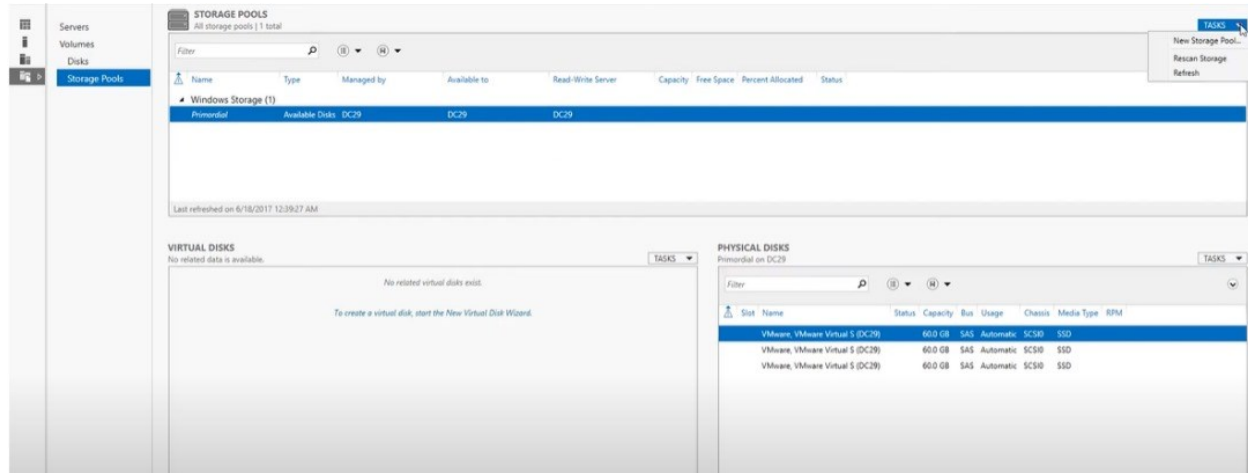
Screenshot: Configuring Disk Quotas in FSRM



Storage Management:

- Regular Monitoring: Utilize tools like Performance Monitor to monitor disk space usage regularly.
- Implement Storage Policies: Define and enforce storage policies through Storage Spaces or third-party tools.
- Automated Tools: Consider using automated tools for disk cleanup and optimization.

Screenshot: Storage Policies in Storage Spaces



Best Practices:

- Regularly review and adjust disk quotas based on evolving storage needs.
- Implement automated alerts for critical disk space thresholds.
- Utilize tiered storage for optimal data placement based on usage patterns.

4. Active Directory and Domain Services

4.1 Introduction to Active Directory

4.1.1 Components of Active Directory

Overview:

Active Directory (AD) is a crucial component in Windows Server environments, providing a centralized system for managing and organizing network resources.

- **Domains:** Organizational units grouping network objects with unique domain names.
- **Trees:** Groups of domains sharing the same namespace.
- **Forest:** Collection of domains sharing a common schema, configuration, and global catalog.

4.2 Domain Services

4.2.1 Domain Controllers and Replication

Theoretical Approach:

- Domain Controllers (DCs): Servers responsible for authenticating users and maintaining directory databases.
- Directory Replication: Synchronization mechanism for maintaining consistency among domain controllers.

Practical Application:

1. Server Manager: Open Server Manager on a Windows Server machine.
2. Add Roles and Features: Navigate to Manage -> Add Roles and Features.
3. Role Selection: Choose Active Directory Domain Services during the role selection process.
4. Configure Domain Controller: Follow the wizard to configure a new domain controller, specifying domain details and replication settings.

Select installation type

DESTINATION SERVER
Group3-PC.GP3.LOCAL

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

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

☒ **Role-based or feature-based installation**

Configure a single server by adding roles, role services, and features.

☐ **Remote Desktop Services installation**

Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

Select destination server

DESTINATION SERVER
Group3-PC.GP3.LOCAL

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

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

☒ Select a server from the server pool

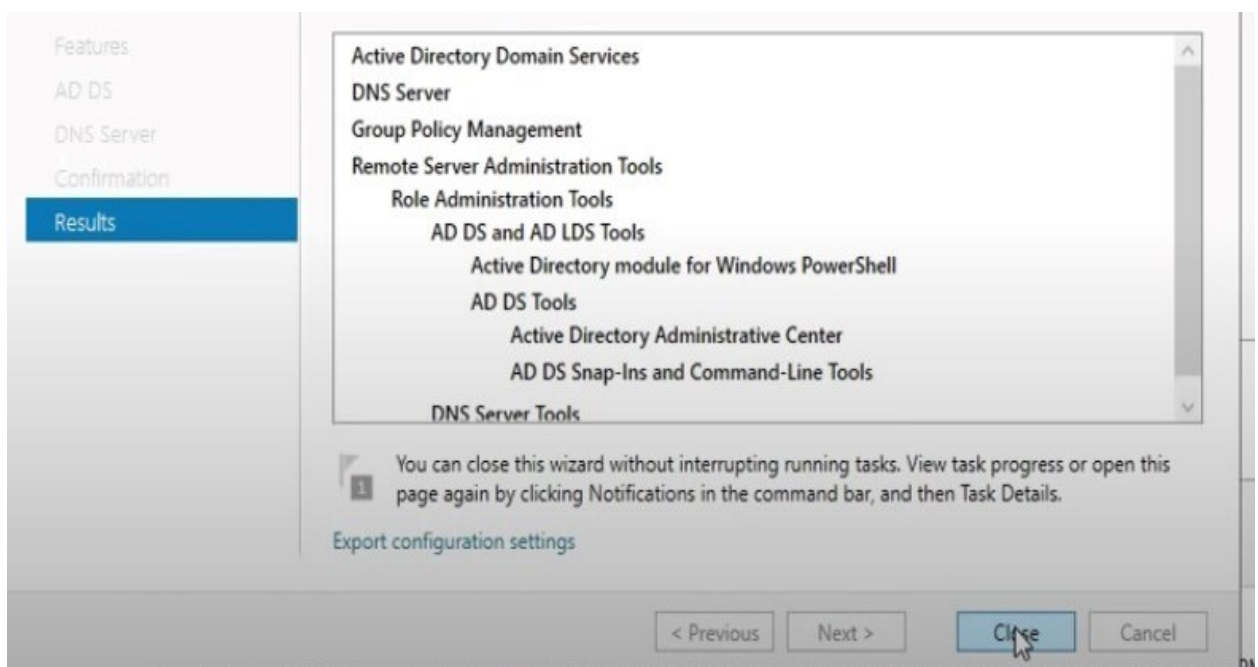
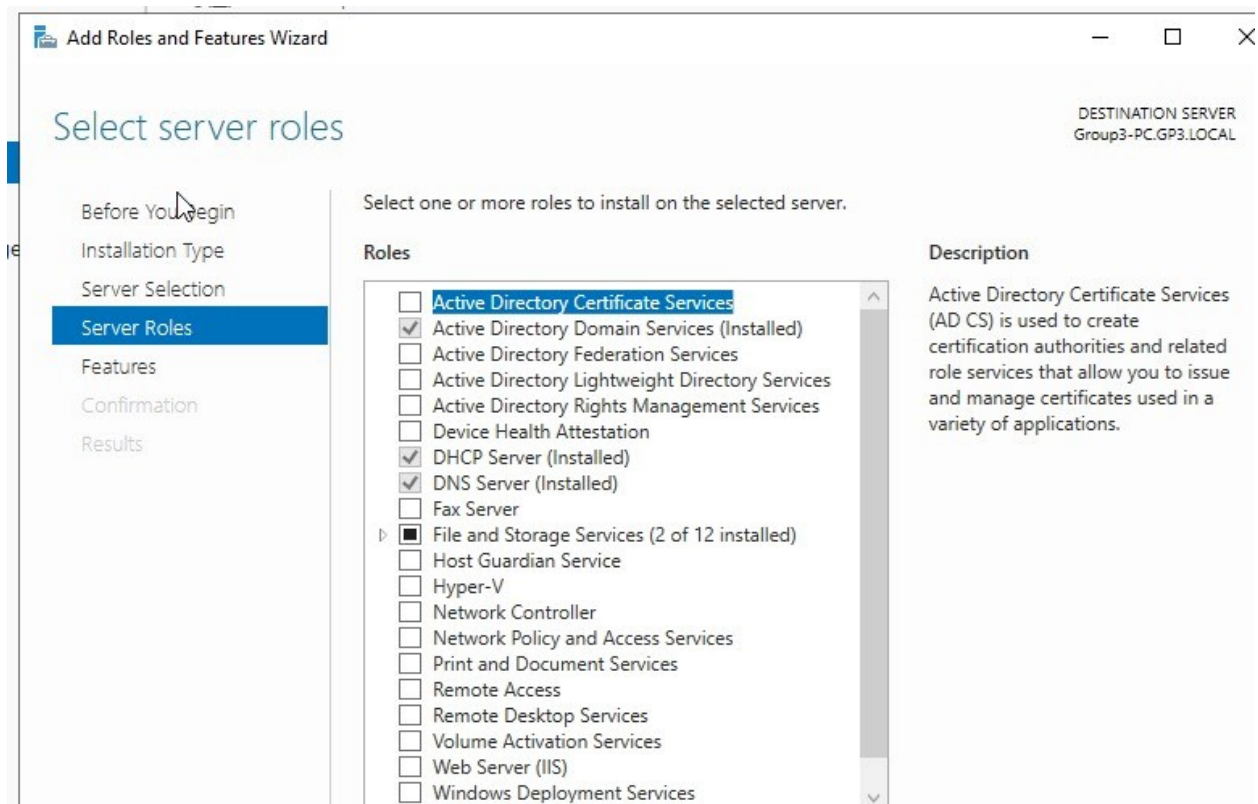
☐ Select a virtual hard disk

Server Pool

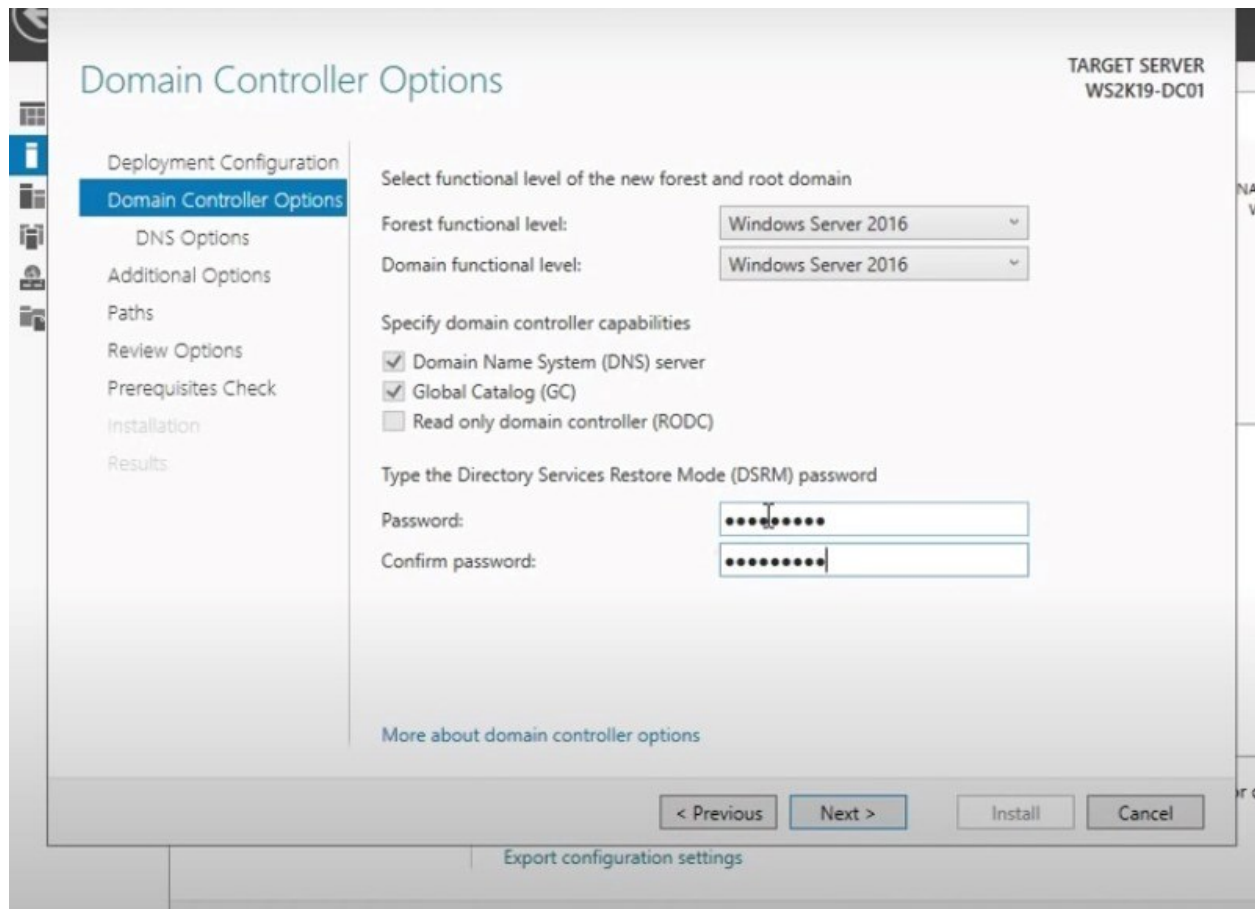
Filter: <input type="text"/>		
Name	IP Address	Operating System
Group3-PC.GP3.LOCAL	192.168.100.1	Microsoft Windows Server 2019 Datacenter Evaluation

1 Computer(s) found

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



Screenshot: Configuring Domain Controller Wizard



4.2.2 DNS and DHCP in Active Directory

Theoretical Approach:

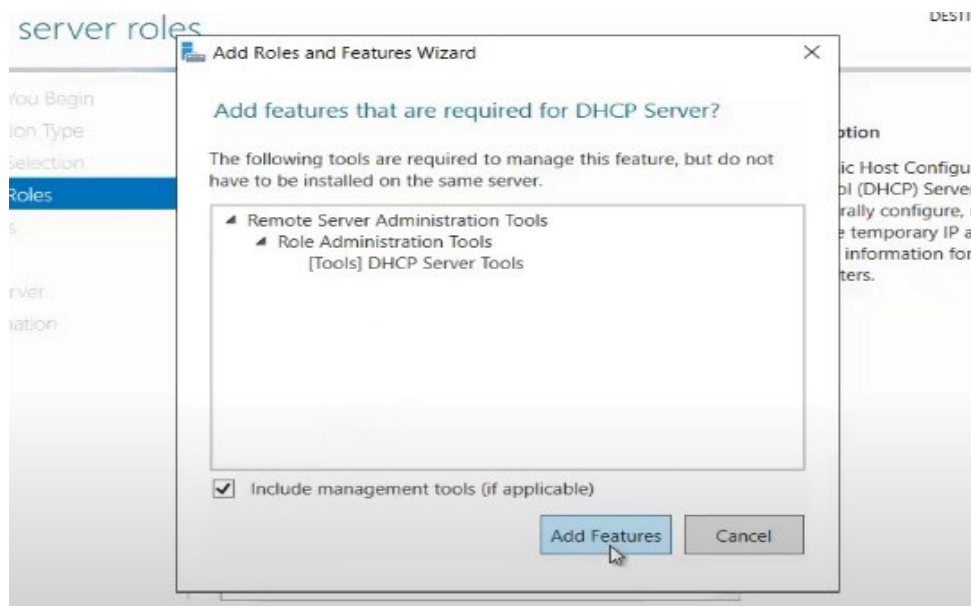
Integration of Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) is crucial for network functionality.

Practical Application:

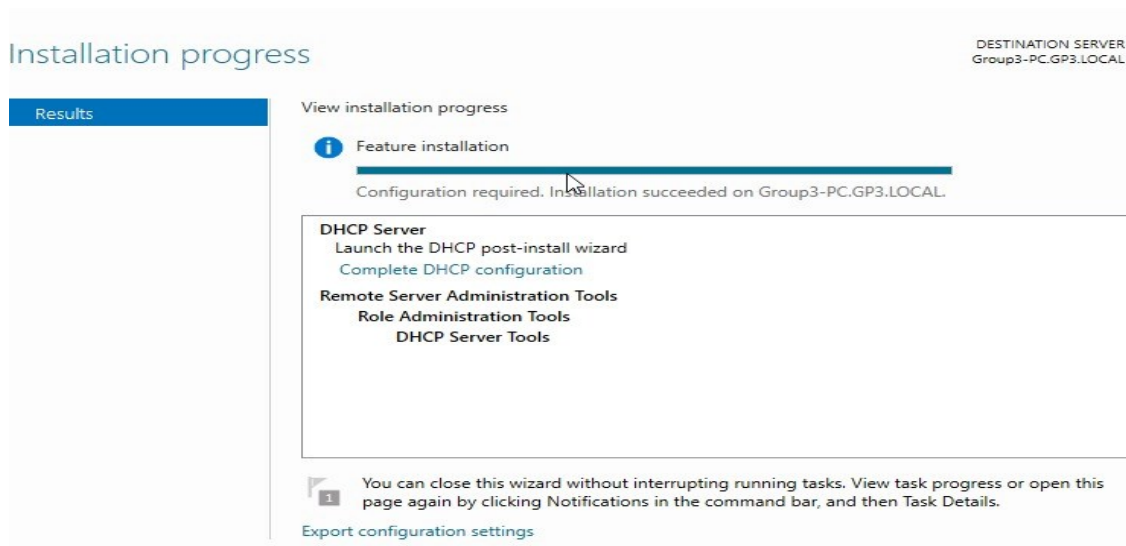
1. Server Manager: Open Server Manager on a Windows Server machine.
2. Add Roles and Features: Navigate to Manage -> Add Roles and Features.
3. Role Selection: Choose DNS Server and DHCP Server during the role selection process.

4. Configuration: Follow the wizard to configure DNS zones and DHCP settings.

Screenshot: Adding DNS and DHCP Roles in Server Manager



Screenshot: Configuring DNS Zone



5. Group Policy Management

5.1 Group Policy Overview

Overview:

Group Policy is a powerful tool in Windows Server 2019 that allows administrators to define and enforce settings for users and computers. It plays a crucial role in ensuring a standardized and secure IT environment.

5.1.1 Creating and Linking Group Policies

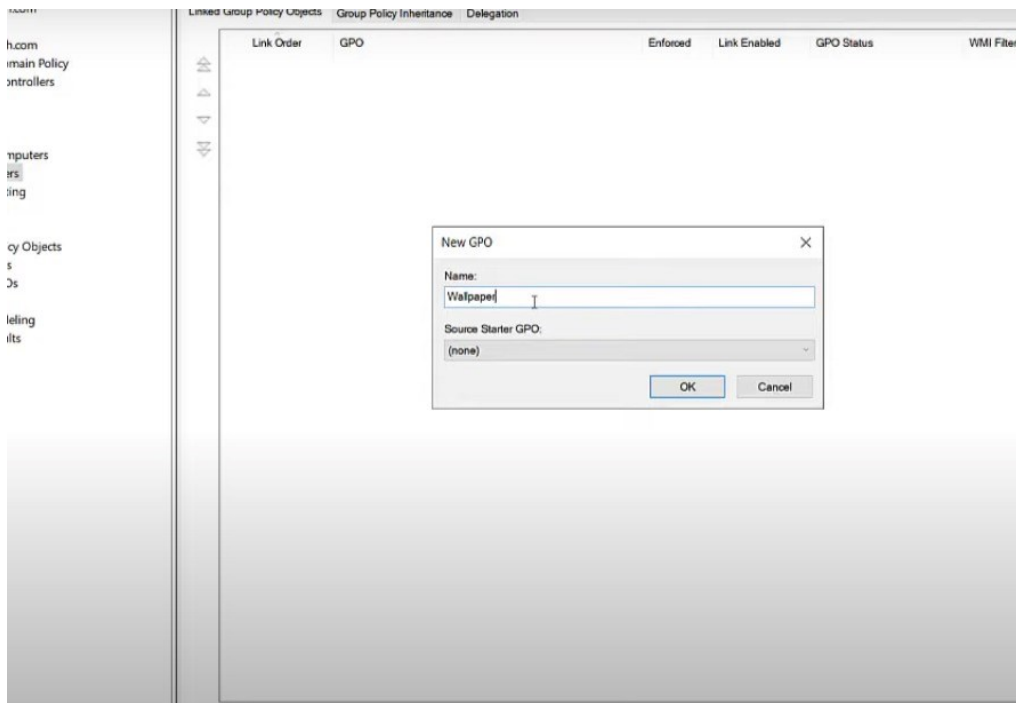
Theoretical Approach:

- Group Policy Objects (GPOs): These are containers for policies that can be linked to sites, domains, or organizational units (OUs).
- Scope of Application: GPOs can be linked to specific Active Directory containers, affecting users and computers within those containers.
- Settings Configuration: GPOs enable the configuration of a wide range of settings, including security settings, desktop configurations, and more.

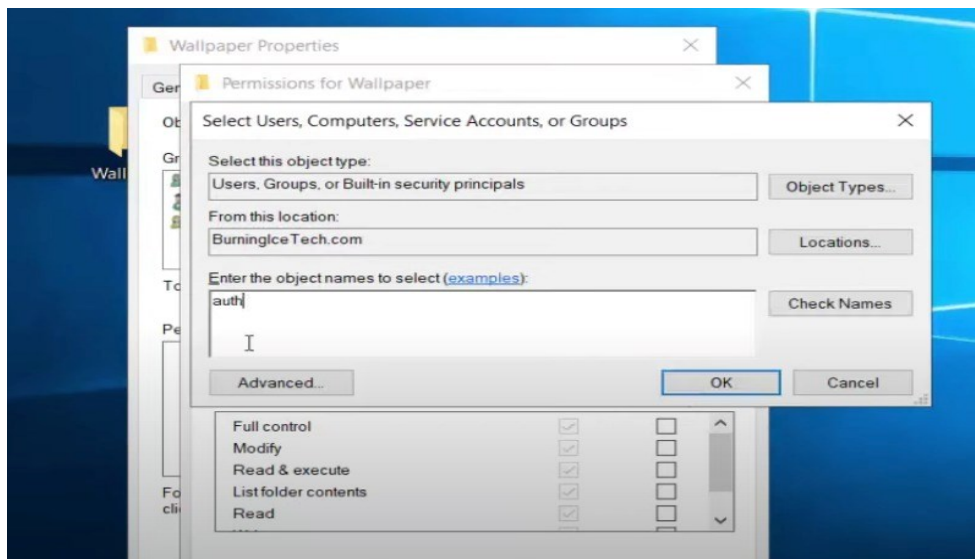
Practical Application:

1. Group Policy Management Console (GPMC): Open the Group Policy Management Console on a Windows Server 2019 machine.
2. Create a New GPO: Right-click on the desired domain or OU, select Create a GPO in this domain, and Link it here.
3. Name and Configure: Provide a name for the new GPO and configure settings such as administrative templates, security options, etc.
4. Link the GPO: Once configured, link the GPO to the appropriate domain, OU, or site.

Screenshot: Creating a New GPO in GPMC



Screenshot: Configuring GPO Settings



5.1.2 Security Settings and Policy Inheritance

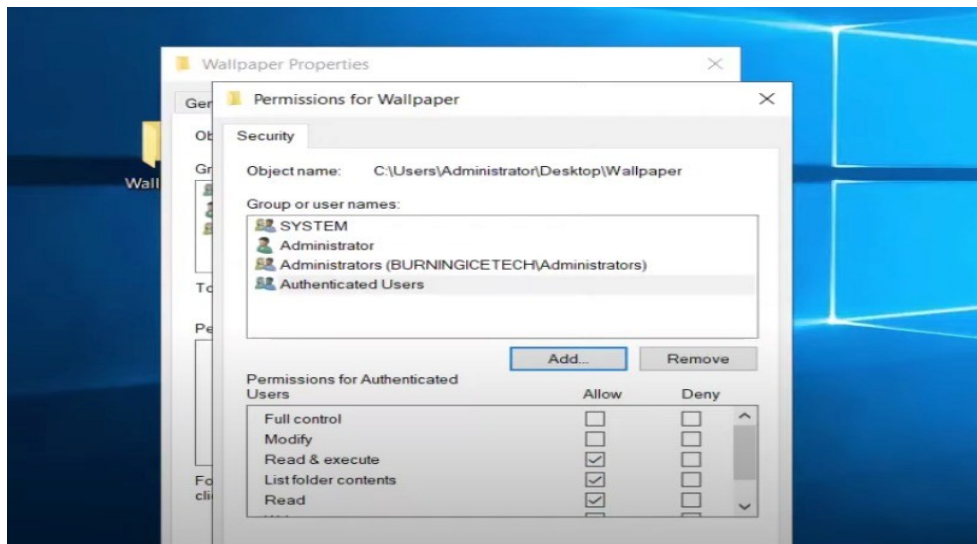
Theoretical Approach:

- Security Settings: GPOs allow the configuration of security settings to enforce security policies across the network.
- Policy Inheritance: GPOs are inherited hierarchically, starting from the domain level down to specific OUs. However, settings at lower levels can override higher-level policies.

Practical Application:

1. Group Policy Management Console (GPMC): Open the Group Policy Management Console on a Windows Server 2019 machine.
2. Edit Existing GPO: Right-click on an existing GPO and select Edit to modify security settings.
3. Security Configuration: Navigate to Computer Configuration -> Policies -> Windows Settings -> Security Settings to configure security policies.
4. Inheritance Control: Understand and manage policy inheritance by linking GPOs strategically to control which policies apply to specific OUs.

Screenshot: Configuring Security Settings in GPO



Best Practices:

- Clearly document and organize GPOs to avoid confusion.
- Regularly review and update GPO settings to align with security and configuration requirements.

EXTRA TOPICS

1. Security and Access control

Introduction to Windows security

The digital transformation and remote work trends create opportunities but also introduce risks. To address this, organizations are adopting a Zero Trust security model, including Windows 11, which prioritizes safety and integrity before granting access. Windows 11 enhances security through advanced hardware and software protection, ensuring hybrid productivity without compromising safety.

Security Principles:

- **Least Privilege:** Grant users only the minimum permissions required for their tasks.
- **Defense in Depth:** Use multiple security layers to protect resources.
- **Regular Auditing:** Monitor access and activities to detect potential issues.

How Windows 11 enables Zero Trust protection

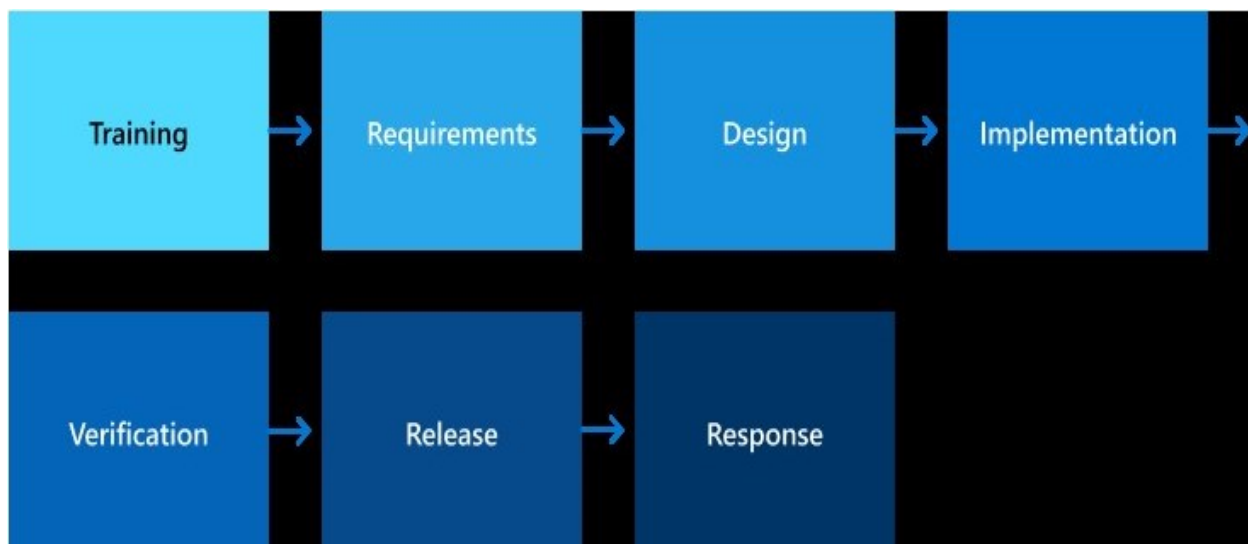
A Zero Trust security model gives the right people the right access at the right time. Zero Trust security is based on three principles:

1. Reduce risk by explicitly verifying data points such as user identity, location, and device health for every access request, without exception
2. When verified, give people and devices access to only necessary resources for the necessary amount of time
3. Use continuous analytics to drive threat detection and improve defenses

Security Foundation

Security and privacy should never be an afterthought when developing secure software, a formal process must be in place to ensure they're considered at all points of the product's lifecycle. Microsoft's Security Development Lifecycle (SDL) embeds comprehensive security requirements, technology specific tooling, and mandatory processes into the development and operation of all software products.

Microsoft SDL consists of seven components including five core phases and two supporting security activities. The five core phases are requirements, design, implementation, verification, and release. Each of these phases contains mandatory checks and approvals to ensure all security and privacy requirements and best practices are properly addressed.



Types of security are stated below.

- a. **Hardware Security**
- b. **Operating System Security**
- c. **Application Security**
- d. **Cloud Security**
- e. **Identity protection**

1. ACCESS CONTROL

Purpose:

Regulates who can access resources (files, folders, devices, etc.) and what actions they can perform.

- **Key Concepts:**

- **User Accounts:** Unique identities for users, each with a username and password.
- **Groups:** Collections of users with similar access needs, simplifying management.
- **Permissions:** Define allowable actions (e.g., read, write, execute) for users or groups on resources.
- **Access Control Lists (ACLs):** Store permissions associated with each resource.

The key points that make up access control are:

- Permissions
- Ownership of objects
- Inheritance of permissions
- User rights
- Object auditing

a. Permissions

Permissions define the type of access that is granted to a user or group for an object or object property. For example, the Finance group can be granted Read and Write permissions for a file named FETstaff.dat.

The permissions attached to an object depend on the type of object. For example, the permissions that can be attached to a file are different from those that can be attached to a registry key. Some permissions, however, are common to most types of objects. These common permissions are: **Read, Modify, Change Owner, Delete.**

b. Ownership of objects

An owner is assigned to an object when that object is created. By default, the owner is the creator of the object. No matter what permissions are set on an object, the owner of the object can always change the permissions.

Note: An administrator who needs to repair or change permissions on a file must begin by taking ownership of the file.

By default, the owner is the entity that created the object. The owner can always change permissions on an object, even when the owner is denied all access to the object.

Ownership can be taken by:

- An administrator.
- Any user or group who has the Take Ownership permission on the object.
- A user who has the “Restore files” and directories user right.

c. Inheritance of Permission

Inheritance allows administrators to easily assign and manage permissions. This feature automatically causes objects within a container to inherit all the inheritable permissions of that container. For example, the files within a folder inherit the permissions of the folder. Only permissions marked to be inherited are inherited.

d. User rights

User rights grant specific privileges and sign-in rights to users and groups in the computing environment. Administrators can assign specific rights to group accounts or to individual user accounts. These rights authorize users to perform specific actions, such as signing in to a system interactively or backing up files and directories.

User rights are different from permissions because user rights apply to user accounts, and permissions are associated with objects. Although user rights can apply to individual user accounts, user rights are best administered on a group account basis.

e. Object Auditing

Windows object auditing is a security feature that allows you to track and monitor access to various objects and resources in the Windows operating system.

Objects that can be audited include files, folders, registry keys, Active Directory objects, and more.

Object auditing helps in detecting and investigating security incidents, identifying unauthorized access attempts, and monitoring user activity. It is configured through the Security Policy settings on Windows systems, including local security policies or Group Policy for domain-joined systems. Monitoring and analyzing audit logs can be done using tools like the Event Viewer, PowerShell cmdlets, or third-party security information and event management (SIEM) solutions.

2. PowerShell Scripting

What's PowerShell Scripting.

PowerShell is a cross-platform task automation solution made up of a command-line shell, a scripting language, and a configuration management framework. PowerShell runs on Windows, Linux, and macOS.

As a scripting language, PowerShell is commonly used for automating the management of systems. It's also used to build, test, and deploy solutions, often in CI/CD environments

Getting started with PowerShell.

Whether you are a software developer, an IT professional, or a technology enthusiast, many of you need to run multiple operating systems. Hyper-V lets you run multiple operating systems as virtual machines on Windows.

Below are some basic PowerShell commands, their aliases and description

COMMAND NAME	ALIAS	DESCRIPTION
Get-Help Get-Command	(None)	Display help information about PowerShell command Get-Command (which lists all PowerShell commands).
Get-ChildItem	dir, ls, gci	Lists all files and folders in the current working directory
Get-Location	pwd, gl	Get the current working directory
Set-Location	cd, chdir, sl	Sets the current working location to a specified location
Get-Content	cat, gc, type	Gets the content of the item at the specified location
Copy-Item	copy, cp, cpi	Copies an item from one location to another
Remove-Item	del, erase, rd, ri, rm, rmdir	Deletes the specified items
Move-Item	mi, move, mv	Moves an item from one location to another
New-Item	ni	Creates a new item

Out-File	>, >>	Send output to a file. When you wish to specify parameters, stick to Out-File.
Invoke-WebRequest	curl, iwr, wget	Get content from a web page on the Internet
Write-Output	echo, write	Sends the specified objects to the next command in the pipeline.
Clear-Host	cls, clear	Clear console

Some PowerShell for Administrators commands

a. User Management

- Get-LocalUser: Lists local user accounts.
- New-LocalUser or net: Creates new local users.
 - i.e **net user /add username userpassword**
- Remove-LocalUser or delete: Deletes local users.
 - i.e **net user /delete username**
- Managing Account Properties:
 - **net user username /active:yes|no:** activates or deactivates an account.
 - **net user username /expires:date:** sets an account expiration date.
 - **net user username /times:times:** restricts logon hours

b. Group Management

- Creating Groups:
 - **net localgroup groupname /add:** creates a new local group.
- Deleting Groups:
 - **net localgroup groupname /delete:** removes an existing local group.
- Adding Users to Groups:
 - **net localgroup groupname username /add:** adds a user to a group.
- Removing Users from Groups:
 - **net localgroup groupname username /delete:** removes a user from a group.

c. Permissions:

- **Get-Acl:** Displays ACLs for files or folders.
- **Set-Acl:** Modifies ACLs.
- **Grant-Acl:** Grants permissions to users or groups.

3. Hyper-V and Virtualization

Introduction to Hyper-V and Virtualization.

Whether one is a software developer, an IT professional, or a technology enthusiast, many people will need to run multiple operating systems. Hyper-V lets you run multiple operating systems as virtual machines on Windows.

Hyper-V specifically provides hardware virtualization. That means each virtual machine runs on virtual hardware. Hyper-V lets you create virtual hard drives, virtual switches, and a number of other virtual devices all of which can be added to virtual machines.

Installing Hyper-V

In order to install Hyper-V on a PC, one needs to do the following

- Create a txt file and name it **hyperV** on your desktop screen a paste the following
pushd "%~dp0"
*dir /b %SystemRoot%\servicing\Packages*Hyper-V*.mum >hyper-v.txt*
for /f %%i in ('findstr /i . hyper-v.txt 2^>nul') do dism /online /norestart /add-package:"%SystemRoot%\servicing\Packages\%%i"
del hyper-v.txt
Dism /online /enable-feature /featurename:Microsoft-Hyper-V -All /LimitAccess /ALL
Pause
- Save it as a **.bat** file e.g. hyperV.bat
- Right click on the bat file on your desktop and run it as administrator. This will take some time to search and download the necessary resources for a hyper-virtual machine.
- A window like the one below will appear.

```

C:\WINDOWS\System32\cmd.exe
Processing 1 of 1 - Adding package Microsoft-Hyper-V-Services-Package~31bf3856ad364e35~amd64~~10.0.22621.608
[=====100.0%=====]
The operation completed successfully.

C:\Users\m_la\Downloads>disM /online /norestart /add-package:"C:\WINDOWS\servicing\Packages\Microsoft-Hyper-V-Services-
Package~31bf3856ad364e35~amd64~~10.0.22621.755.mum"

Deployment Image Servicing and Management tool
Version: 10.0.22621.1

Image Version: 10.0.22621.755

Processing 1 of 1 - Adding package Microsoft-Hyper-V-Services-Package~31bf3856ad364e35~amd64~~10.0.22621.755
[=====100.0%=====]
The operation completed successfully.

C:\Users\m_la\Downloads>del hv-home.txt

C:\Users\m_la\Downloads>DisM /online /enable-feature /featurename:Microsoft-Hyper-V -All /LimitAccess /ALL

Deployment Image Servicing and Management tool
Version: 10.0.22621.1

Image Version: 10.0.22621.755

Enabling feature(s)
[=====100.0%=====]
The operation completed successfully.
Restart Windows to complete this operation.
Do you want to restart the computer now? (Y/N)

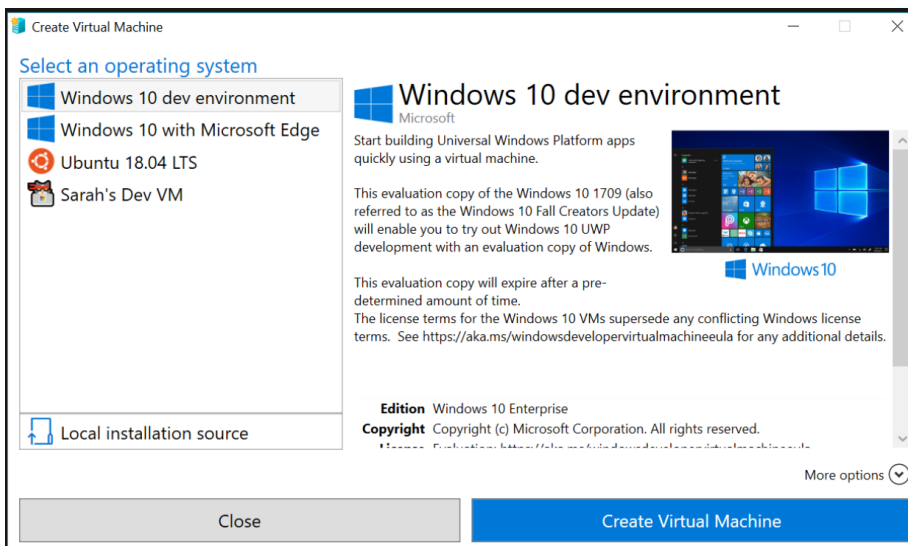
```

- After your PC restarts, all features of Hyper-V would have been installed. Check the installation with the following commands
 - Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V – All
 - DISM /Online /Enable-Feature /All /FeatureName:Microsoft-Hyper-V
- Search for windows feature in the menu bar and enable Hyper-V.

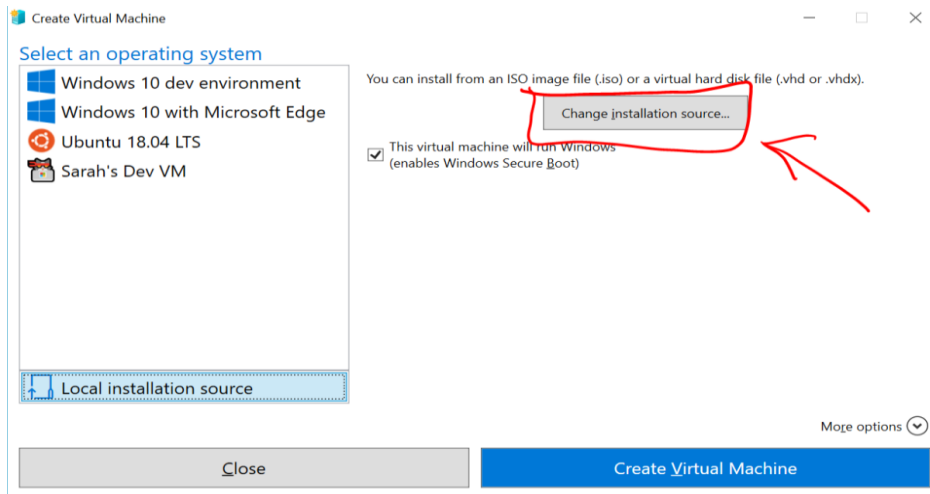
Creating a Virtual Machine

Following the steps below will lead you to creating a virtual machine with Hyper-V

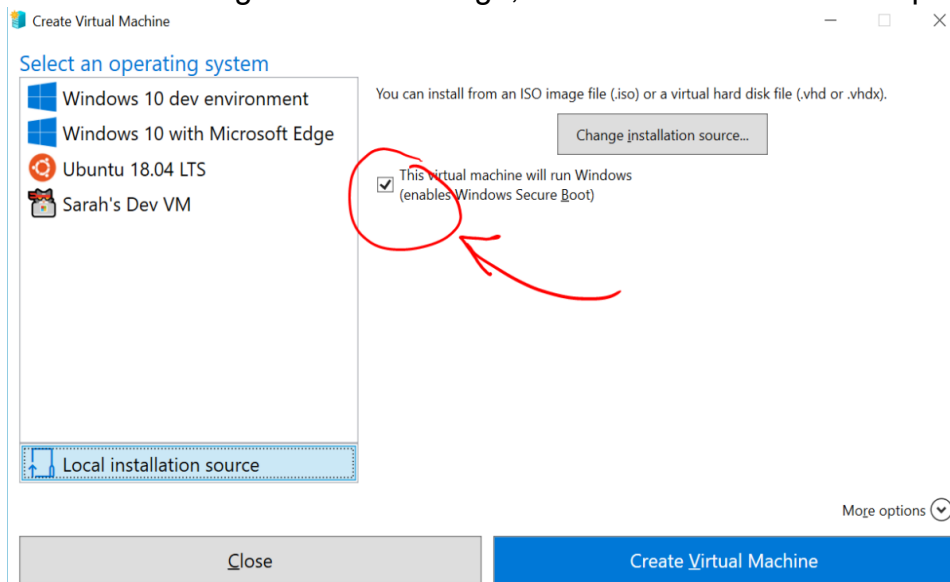
- Search for Hyper-V Quick Create from the start menu
- Select an operating system or choose your own by using a local installation source



- If you want to use your own image to create the virtual machine, select Local Installation Source.
- Select Change Installation Source.



- Pick the .iso or .vhdx that you want to turn into a new virtual machine.
- If the image is a Linux image, deselect the Secure Boot option.



- Select "Create Virtual Machine"

That's it! Quick Create will take care of the rest. With that you would have created your first virtual machine.

6. Conclusion

In conclusion, effective Windows System Administration within Windows Server environments requires a balanced understanding of theoretical concepts and practical applications. By mastering user and group management, file system and disk optimization, Active Directory services, and Group Policy management, sysadmins can navigate the complexities of Windows Server, ensuring the optimal functioning and security of IT infrastructures.

7. Recommendations

Based on the insights provided in this report, the following recommendations are suggested for Windows System Administration within Windows Server environments:

- Conduct regular training sessions for system administrators to stay updated on the latest features and best practices.
- Implement automated backup and recovery mechanisms to enhance data resilience.
- Continuously monitor and audit user accounts and permissions to identify and mitigate security risks proactively.

8. References

1. Microsoft. (2021). Windows Server Documentation. Retrieved from (<https://docs.microsoft.com/en-us/windows-server/>)
2. Minasi, M., Mueller, J., & Warren, W. (2019). Mastering Windows Server 2019: The complete guide for IT professionals to install and manage Windows Server 2019 and deploy new capabilities, 2nd Edition. Wiley.
3. ITProMentor. (2020). Understanding NTFS Permissions. Retrieved from (<https://itpromentor.com/ntfs-permissions/>)
4. Microsoft. (2021). Group Policy Overview. Retrieved from ([https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731745\(v=ws.11\)\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731745(v=ws.11))))
5. Russinovich, M. E., Solomon, D. A., & Ionescu, A. (2012). Windows Internals, Part 1: System architecture, processes, threads, memory management, and more (6th Edition). Microsoft Press.
6. Schwartz, D. L. (2020). Active Directory: Designing, Deploying, and Running Active Directory (6th Edition). O'Reilly Media.
7. Mueller, S., Panek, W., & Zacker, C. (2019). Exam Ref MD-100 Windows 10. Microsoft Press.