Identity and Access Management (IAM) Project: Active Directory (On-Premises) Deployment for DamaniTech Solutions.

Implementation of On-Premises Active Directory for Centralized Identity and Access Management

Organisation: **Damanitech**

Date: 01 October, 2025

Prepared by: Dada A. Ojuko (Cybersecurity Analyst)

1. Scope of Work

This project encompasses deploying an **on premise Active Directory Domain Controller** (AD DS) to provide centralized **Identity and Access Management (IAM)** for DamaniTech Solutions. The implementation includes domain setup, client integration, creation of Organizational Units (OUs) aligned to regional offices, security group design, user provisioning, and enforcement of access control policies using Group Policy Objects (GPOs).

2. Organisation IT Structure

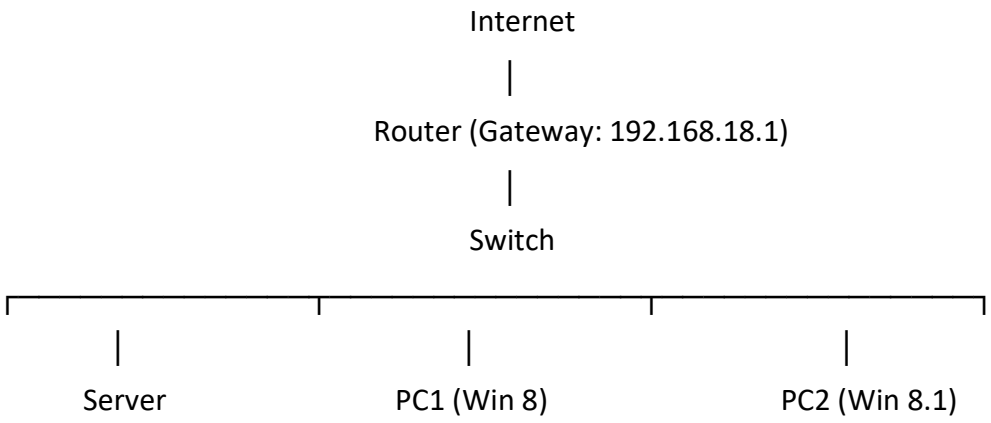
The simulated environment reflected a small IT services firm with distributed offices:

- **1 x Windows Server** – Domain Controller (AD DS + DNS)
- **2 x Client PCs** – Windows 8
- **Two OUs** – HR and IT Departments
- **Departmental Groups** – Created within each OU to represent business functions.

3. Project Objectives

- Deploy **Active Directory Domain Services (AD DS)** for centralized IAM.
- Configure regional **Organizational Units (OUs)** to mirror company structure.
- Provision **security groups** to manage access by department.
- Create **user accounts** and assign them to relevant groups.
- Apply **Group Policies** to enforce access restrictions.
- Demonstrate IAM governance in an on-premises enterprise setup.

4. Network Design



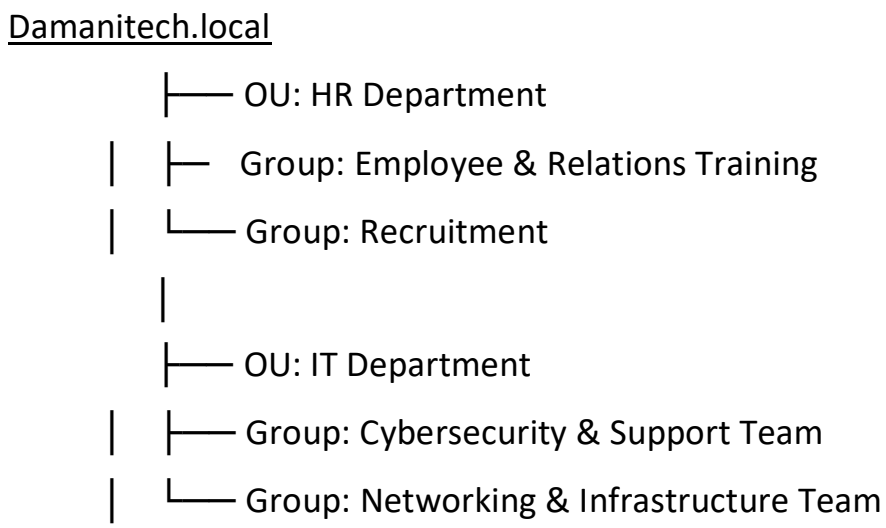
Device	IP Address	Role
Windows Server	10.0.2.3	AD Domain Controller (DC)
Windows 8 PC 1	DHCP	Client (HR Department OU– HR)
Windows 8.1 PC 2	DHCP	Client (IT Department OU – IT)

5. Domain Configuration

- **Domain Name:** damanitech.local
- **Server Name:** DAMANITECH
- **Static IP:** 10.0.2.3
- **Roles Installed:**
    - Active Directory Domain Services (AD DS)
    - DNS Server

6. Organizational Units (OUs) and Groups

The directory structure was created as follows:



7. Users and Group Memberships

Two test users were provisioned to demonstrate IAM principles:

Username	**OU**	**Group Membership**	**Assigned Policy**
Nelson.IT	IT OU	IT Department	**Unable to shutdown**
Keisha.HR	HR OU	HR Department	**Disable removable disk access**

8. Group Policy (GPO) Implementation

Two GPOs were created and linked to specific users through security filtering:

1. **GPO Name:** NoShutdown
    - **Linked to:** IT Department OU (IT User – Nelson)
    - **Policy:**

      User Configuration → Administrative Templates → Start Menu and Taskbar

→ Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands

- **Result:** Nelson cannot shut down the assigned PC.

2. **GPO Name:** DisableRemovableDrives
    - **Linked to:** HR Department OU (HR User – Keisha)
    - **Policy:**

      Computer Configuration → Administrative Templates → System → Removable Storage Access → Deny all access

      Result: Keisha cannot use USB or external drives.
    -

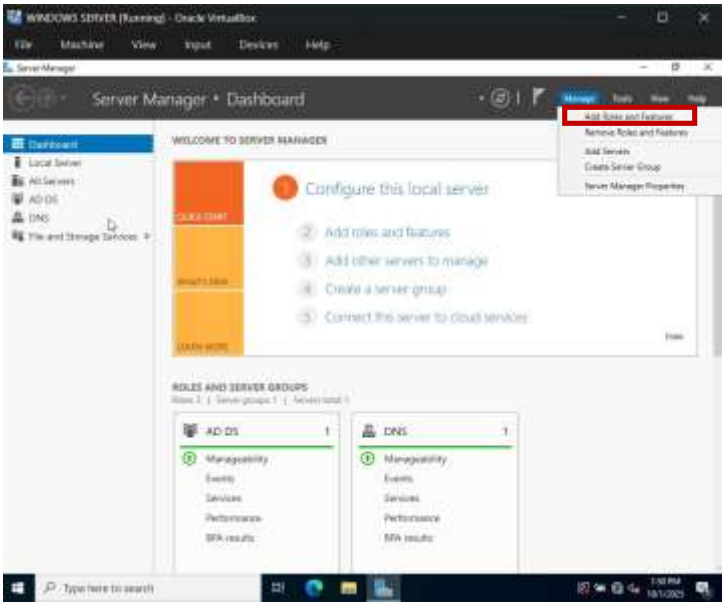
9. Key Takeaways

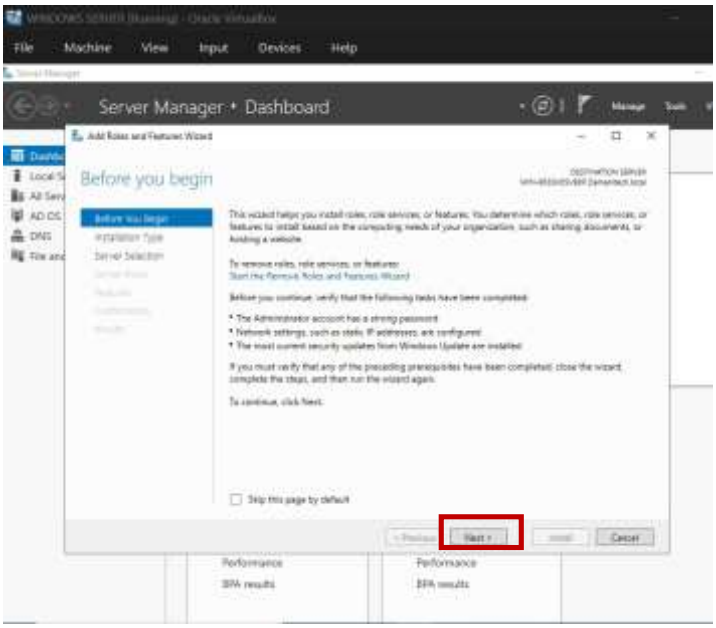
- Successfully implemented an **IAM framework** on Active Directory.
- Mapped **business structure (regions and departments)** into OUs and groups.
- Demonstrated **access control enforcement** using Group Policy Objects (GPOs).
- Learned how to provision and manage **users, groups, and security policies**.
- Applied **identity governance principles** in a real-world simulated enterprise environment.

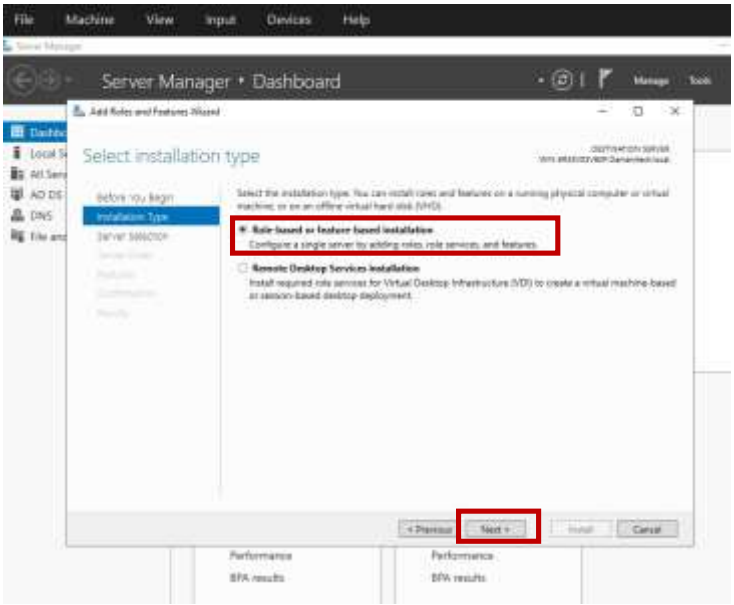
10. Screenshots (Evidence)

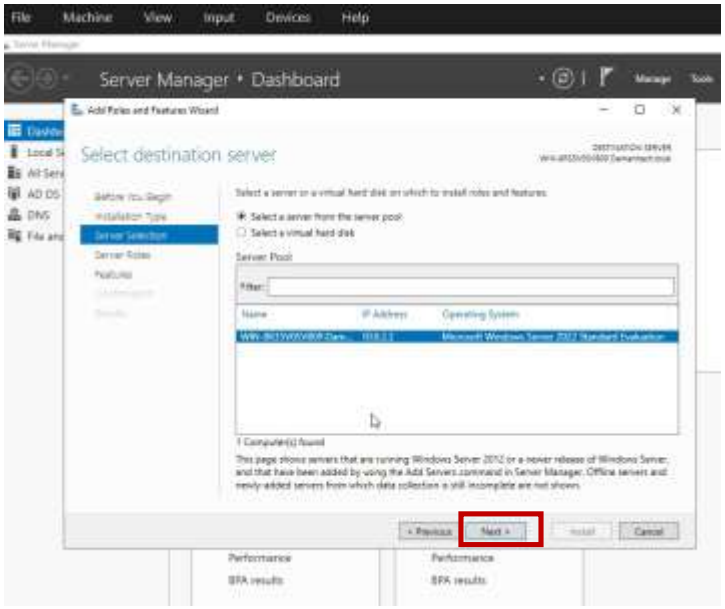
- OU and group structure in ADUC
- GPO editor settings
- User login results showing applied restrictions.

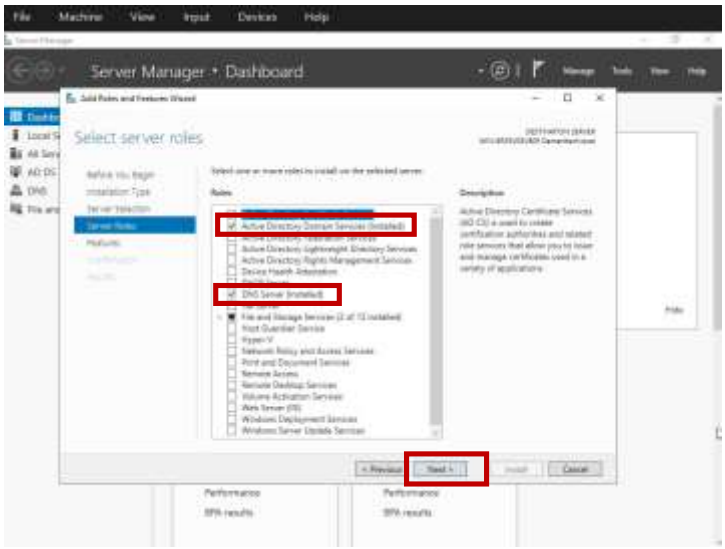
Follow the step by step screenshot below as a guide.

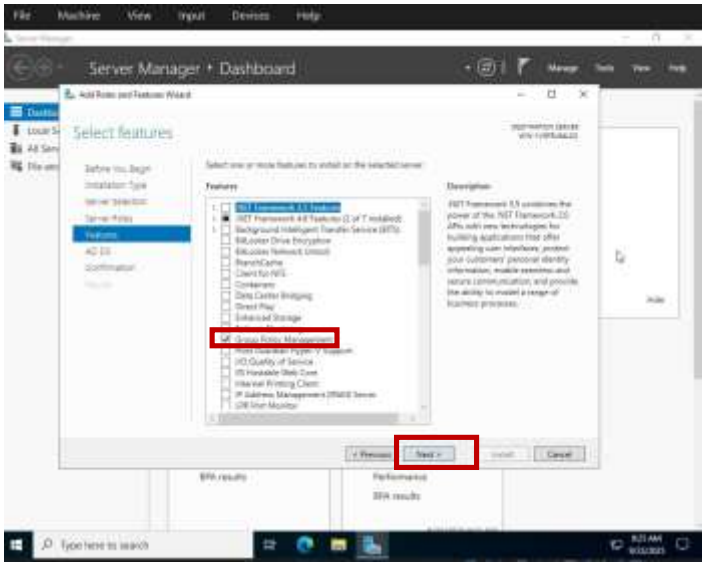

Server Manager • Dashboard
Add Roles and Features
Configure this local server
Add roles and features
Add other servers to manage
Create a server group
Connect this server to cloud services
ROLES AND SERVER GROUPS
AD DS
DNS
Manageability
Events
Services
Performance
BPA results

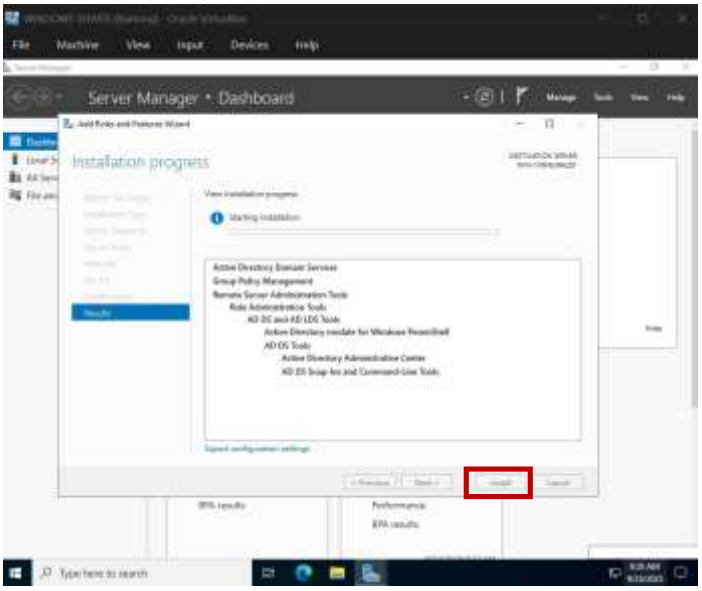

Server Manager • Dashboard
Add Roles and Features Wizard
Before you begin
Before you begin
Installation Type
Server Selection
Skip this page by default
Next >
Cancel
Performance
BPA results

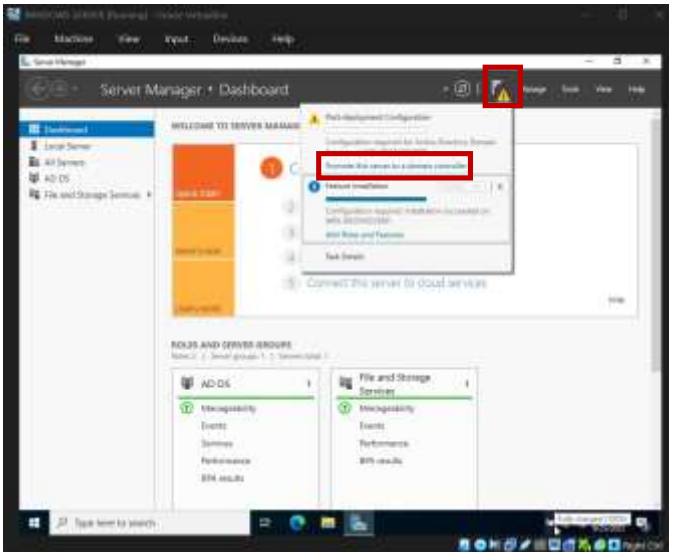

File
Machine
View
Input
Devices
Help
Server Manager • Dashboard
Add Roles and Features Wizard
Select installation type
Before you begin
Installation Type
Server Selection
Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.
Remote Desktop Services installation
< Previous
Next >
Install
Cancel
Performance
BPA results

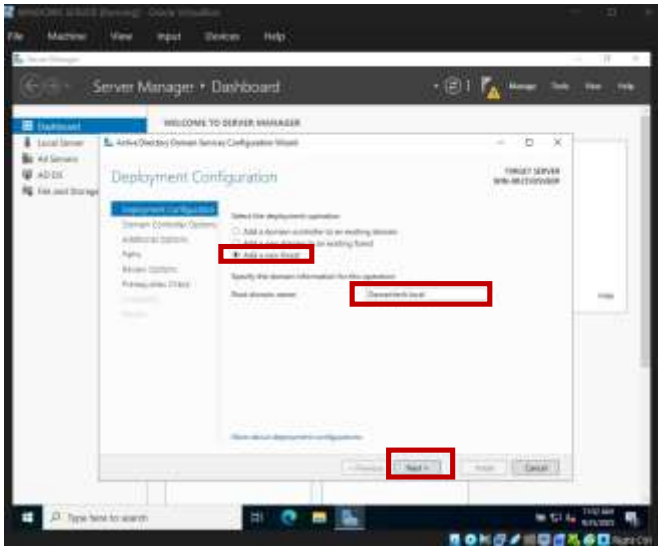

File Machine View Input Devices Help
Server Manager • Dashboard
Add Roles and Features Wizard
Select destination server
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
1 Computer(s) found
Previous
Next >
Install
Cancel
Performance
BPA results

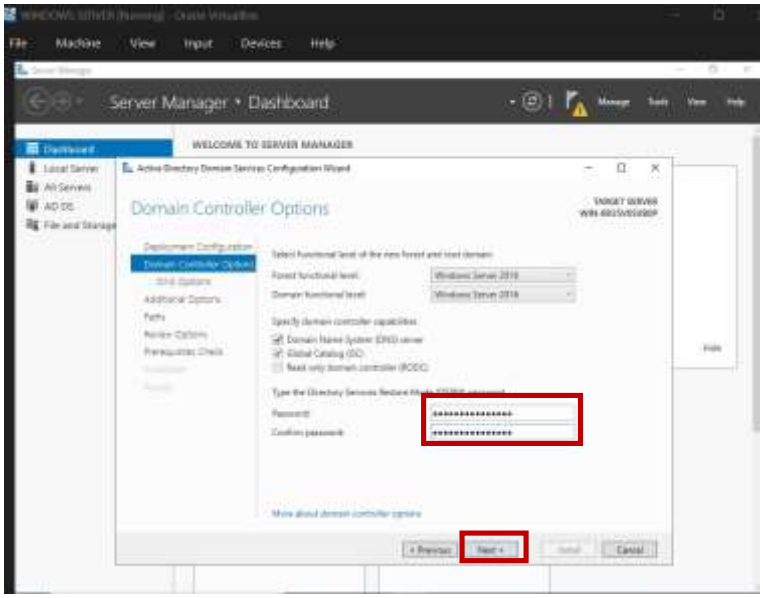

File Machine View Input Devices Help
Server Manager • Dashboard
Add Roles and Features Wizard
Select server roles
Roles
Active Directory Certificate Services (Installed)
DNS Server (Installed)
Previous
Next >
Install
Cancel
Performance
BPA results

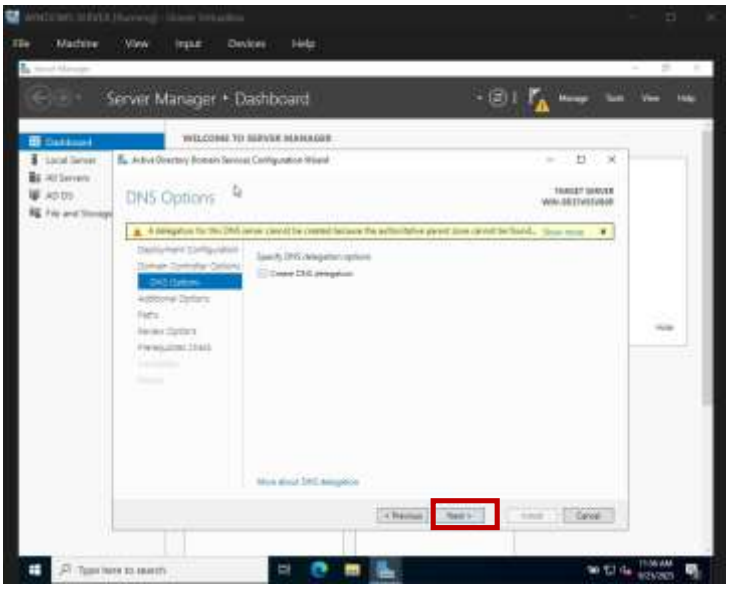

File Machine View Input Devices Help
Server Manager • Dashboard
Add Roles and Features Wizard
Select features
Features
Group Policy Management
Previous
Next >
Install
Cancel
Performance
BPA results
Type here to search

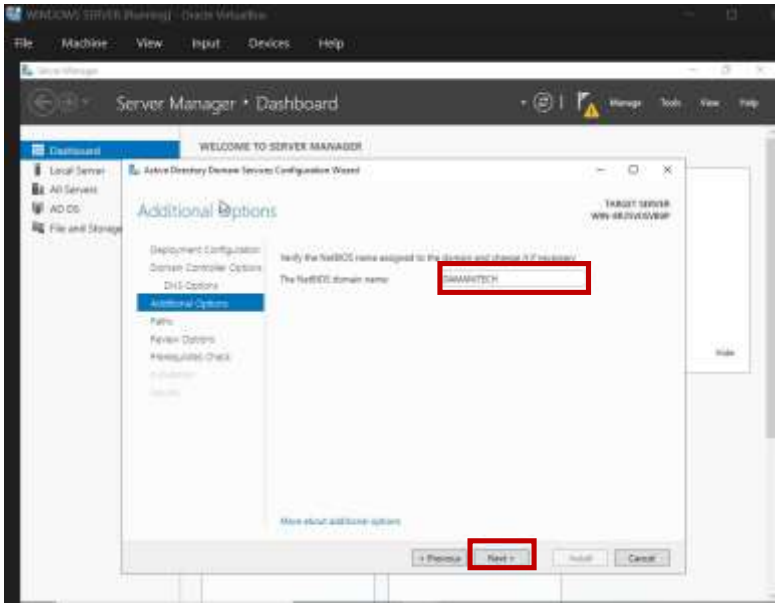

Server Manager • Dashboard
Installation progress

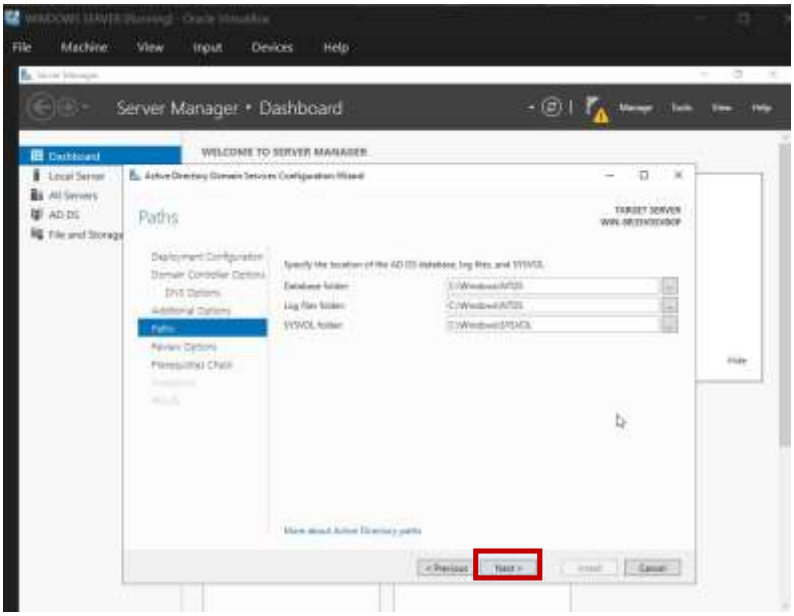

Server Manager • Dashboard

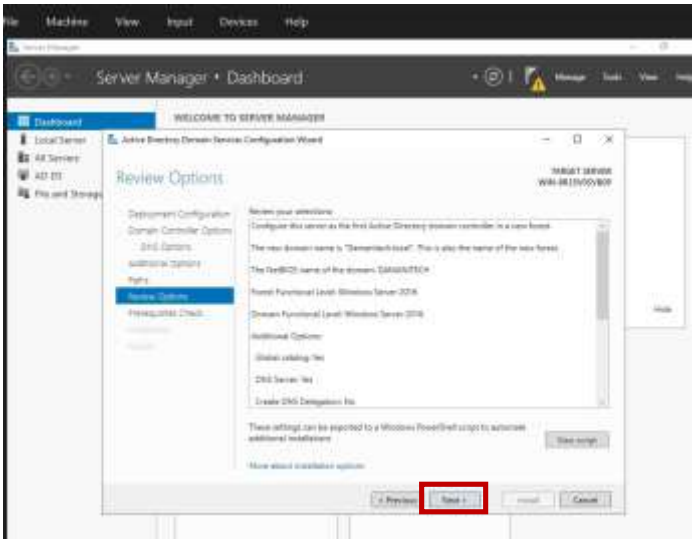

Server Manager • Dashboard
Deployment Configuration

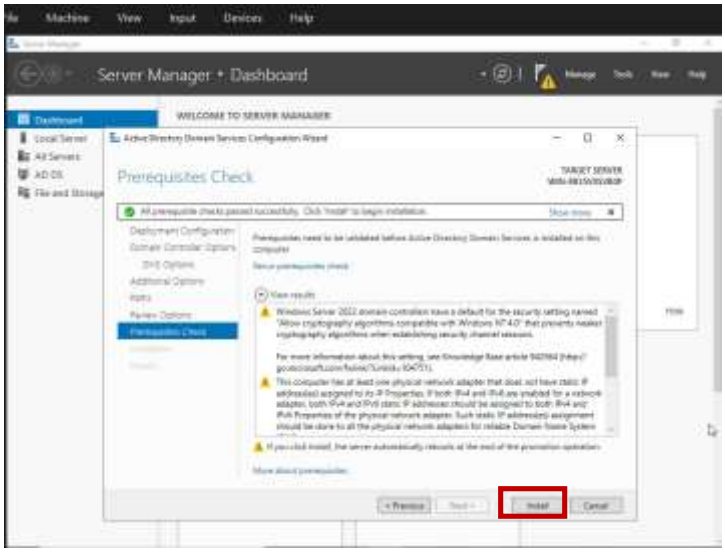

Server Manager • Dashboard
Domain Controller Options
Next >

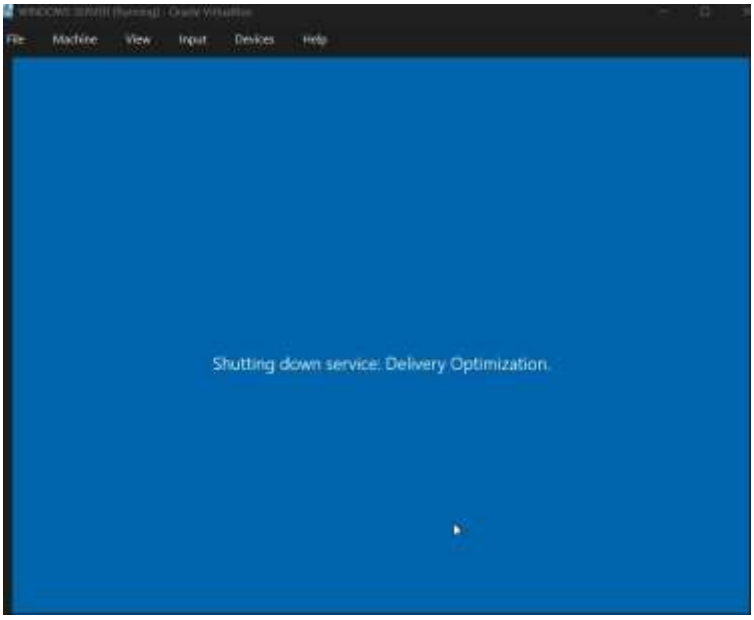

Server Manager • Dashboard
DNS Options
Next >

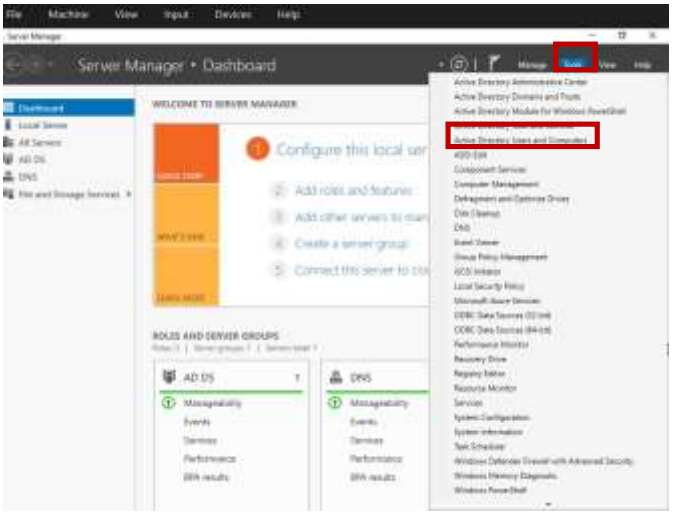

Server Manager • Dashboard
Additional Options
Next >

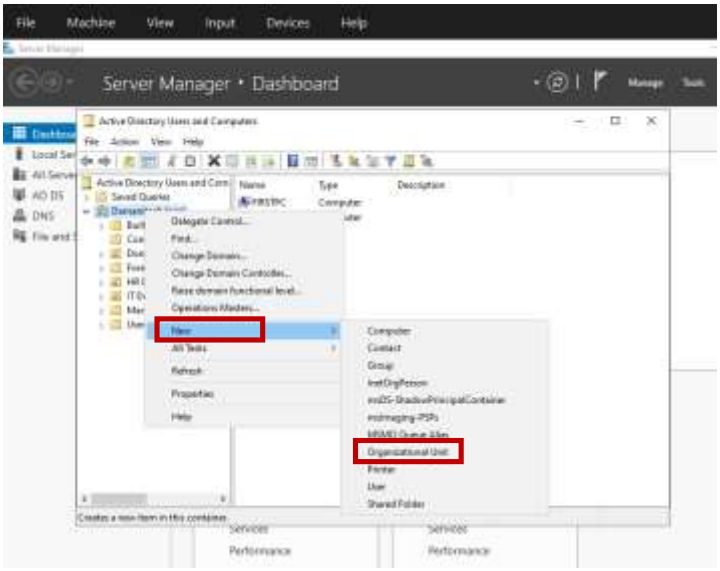

File
Machine
View
Input
Devices
Help
Server Manager • Dashboard
WELCOME TO SERVER MANAGER
Paths
Next >

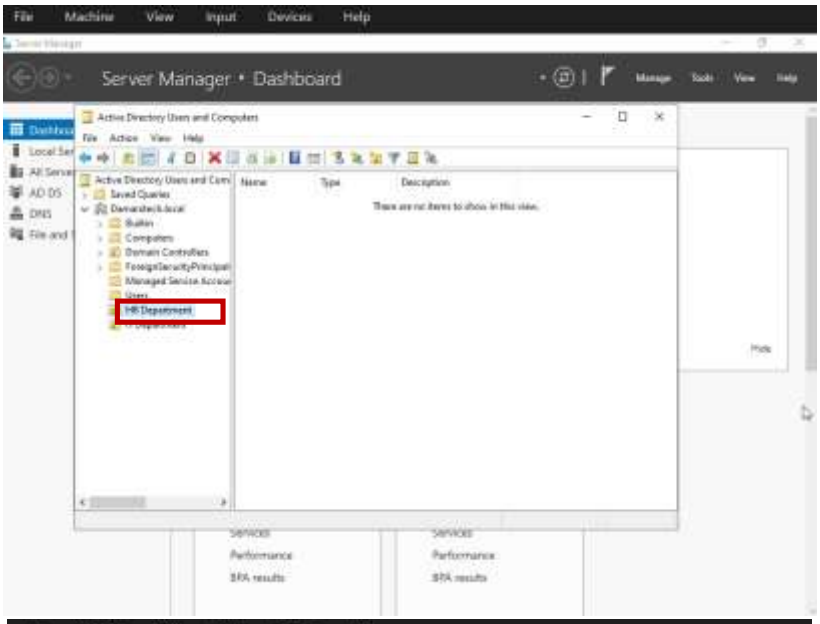

Machine
View
Input
Devices
Help
Server Manager • Dashboard
WELCOME TO SERVER MANAGER
Review Options
Next >

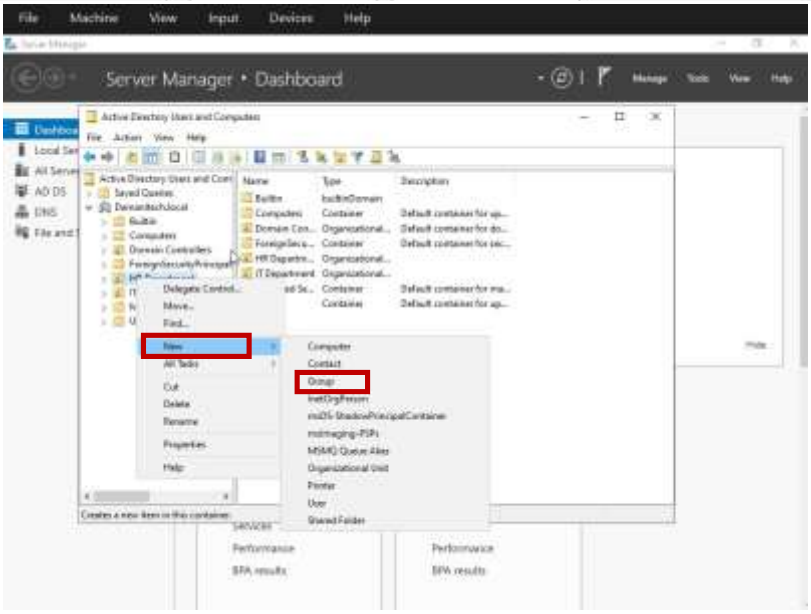

Machine
View
Input
Devices
Help
Server Manager • Dashboard
WELCOME TO SERVER MANAGER
Prerequisites Check
Install

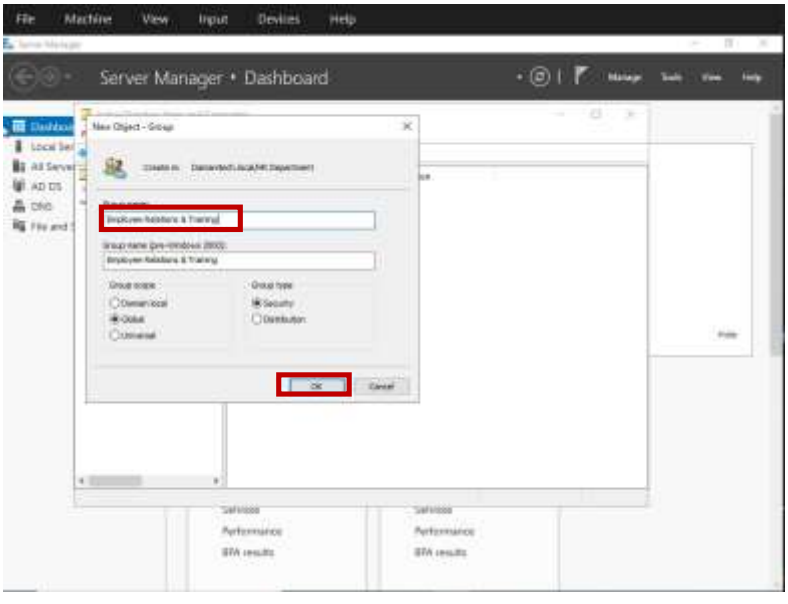

File
Machine
View
Input
Devices
Help
Shutting down service: Delivery Optimization.

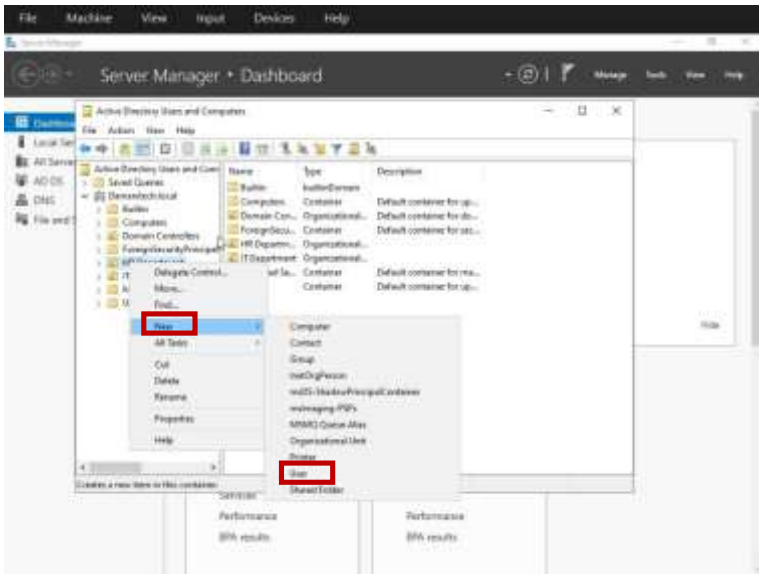

Server Manager • Dashboard
Tools
Active Directory Users and Computers
WELCOME TO SERVER MANAGER
ROLES AND SERVER GROUPS
AD DS
DNS

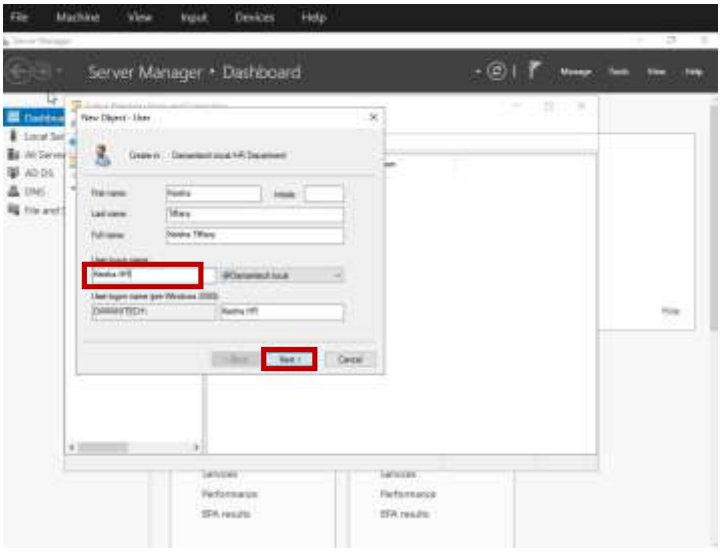

File
Machine
View
Input
Devices
Help
Server Manager • Dashboard
Active Directory Users and Computers
Delegate Control...
Find...
Change Domain...
Change Domain Controller...
Raise domain functional level...
Operations Masters...
New
All Tasks
Refresh
Properties
Help
Computer
Contact
Group
InetOrgPerson
msDS-ShadowPrincipalContainer
msImaging-PSPs
MSMQ Queue Alias
Organizational Unit
Printer
User
Shared Folder

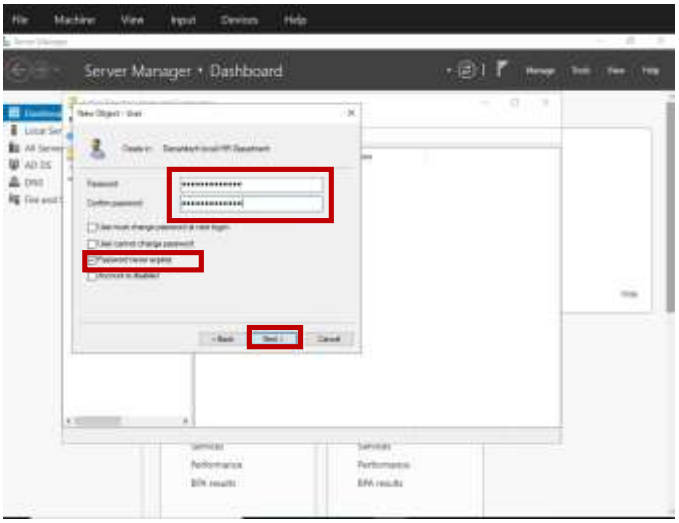

File Machine View Input Devices Help
Server Manager • Dashboard
Active Directory Users and Computers
HR Department


File Machine View Input Devices Help
Server Manager • Dashboard
Active Directory Users and Computers
New
Group


File Machine View Input Devices Help
Server Manager • Dashboard
New Object - Group
OK
Cancel


File Machine View Input Devices Help
Server Manager • Dashboard
Active Directory Users and Computers
New
User


File Machine View Input Devices Help
Server Manager • Dashboard
New Object - User
Next
Cancel


File Machine View Input Devices Help
Server Manager • Dashboard
New Object - User
Password never expires
Next
Cancel