PHASE 2: Deployment of On-Premises Active Directory Domain Services (AD DS) & Azure AD Connect

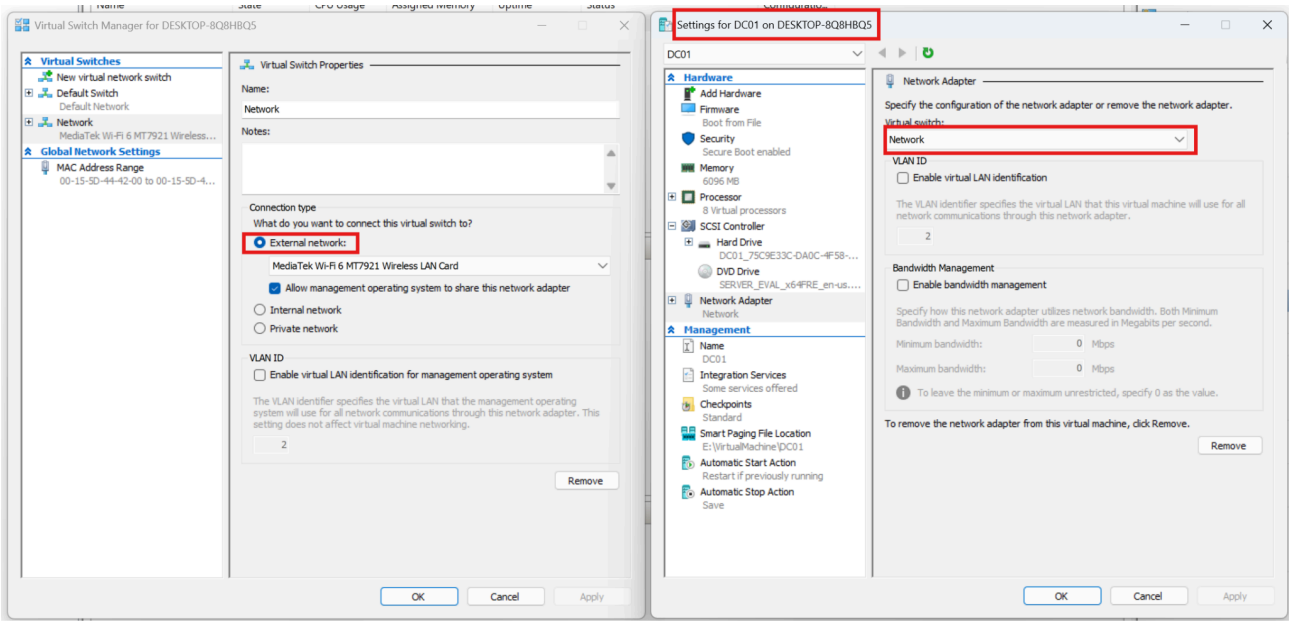
This report documents the planning, deployment, and validation of a hybrid identity infrastructure for DipeshCorp (*Alias of* ***nxhz***) through the installation of a Windows Server 2022 domain controller (DC01), configuration of Active Directory Domain Services (AD DS), and synchronization of the on-premises identity directory with Microsoft Entra ID using Azure AD Connect. This phase simulates the typical enterprise process of federating internal directory services with cloud-based identity platforms to support secure hybrid environments.

I. Provisioning of Windows Server 2022 Virtual Machine

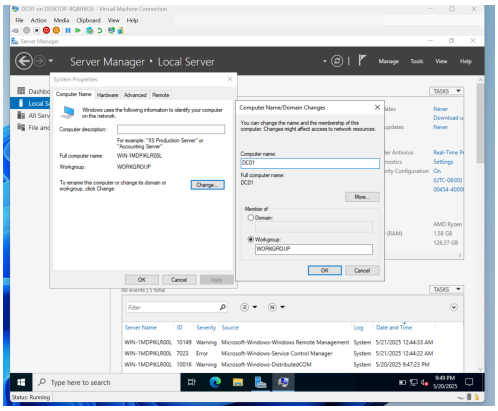
Establish a stable, dedicated server (DC01) to host Active Directory Domain Services (AD DS) and function as the core of the hybrid identity infrastructure.

Actions Completed:

1. Downloaded the Windows Server 2022 Evaluation ISO from Microsoft's official evaluation center. URL: https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2022
2. Installed Hyper-V on the local Windows 11 Pro host system via Control Panel → Turn Windows features on or off → Enabled Hyper-V Platform and Hyper-V Management Tools → Restarted system.
3. Configured an External Virtual Switch in Hyper-V Manager:
    - This step ensures the VM can access the internet or communicate with your Microsoft 365 tenant for syncing.
    - Open Hyper-V Manager → Virtual Switch Manager → Create New Virtual Switch → Type: External
    - Select the physical network adapter of your host machine → Save



4. Created a Generation 2 virtual machine with the following configuration:
   - VM Name: DC01
   - Memory: 6096 MB
   - vCPUs: 8
   - Disk Size: 126.98 GB (dynamically expanding)
   - Network Adapter: Connected to the newly created External Virtual Switch
   - Bootable Media: Windows Server 2022 ISO attached as an installation source
5. Disabled Enhanced Session Mode (to resolve keyboard input issues inside VM):
   - Hyper-V Manager > Right-click host name > Hyper-V Settings
   - Under “Enhanced Session Mode Policy” and “User” sections, unchecked “Allow enhanced session mode”

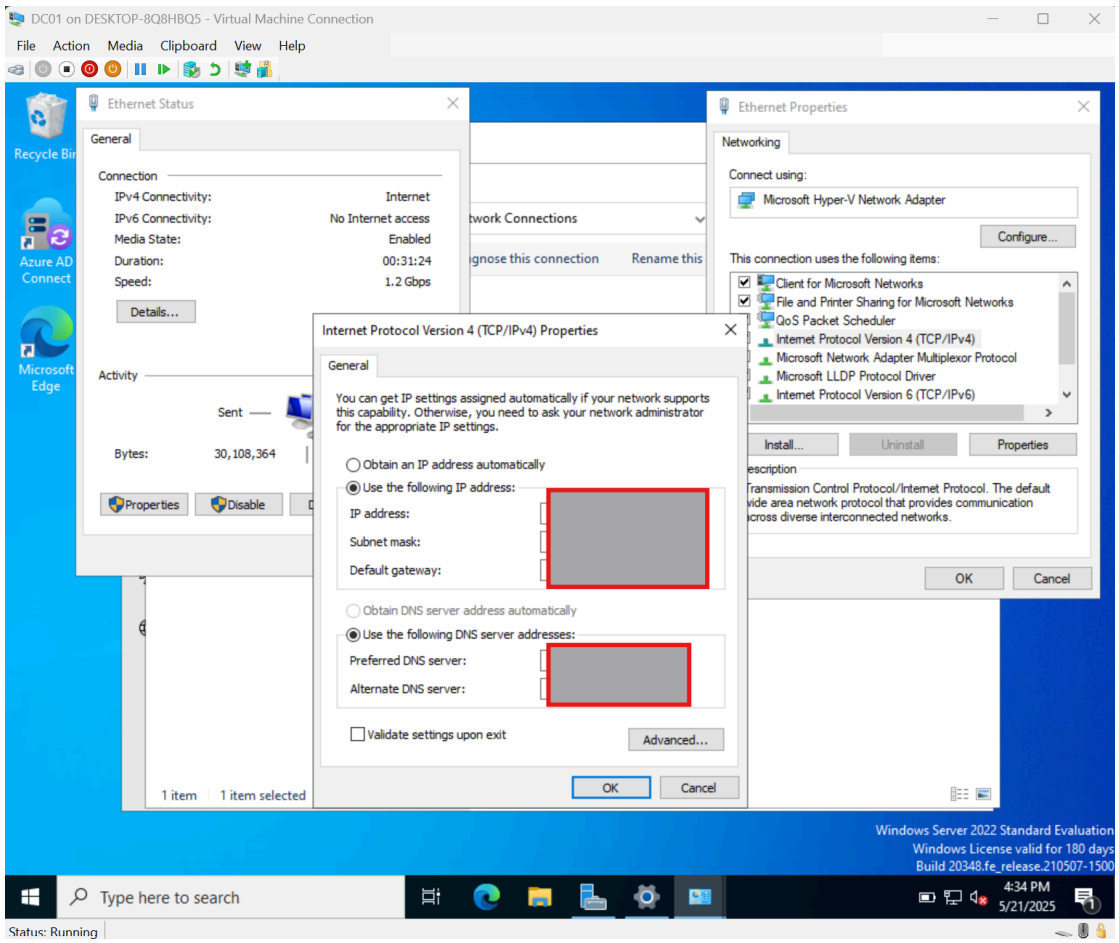


6. Booted the VM and performed OS installation:
   - Selected “Desktop Experience” edition
   - Set local administrator credentials
   - Completed setup and initial updates
7. Renamed the server to DC01 and performed a system restart.
8. Assigned a static IP configuration:
   - First, confirm the host’s physical adapter settings via:

- Control Panel → Network and Sharing Center → Adapter Settings → Ethernet/Wi-Fi > Properties > IPv4

- Based on the host adapter subnet, set the following in the VM:
  - IP Address: 192.168.1.10
  - Subnet Mask: 255.255.255.0
  - Gateway: (e.g., 192.168.1.1 — match your home router)
  - Preferred DNS: 127.0.0.1 (point to self, required for AD DS/DNS role)

⚠️ **Note:** This step is crucial for ensuring successful internet access and Azure AD Connect sync. Misconfigured IP settings can cause outbound traffic failures during synchronization.

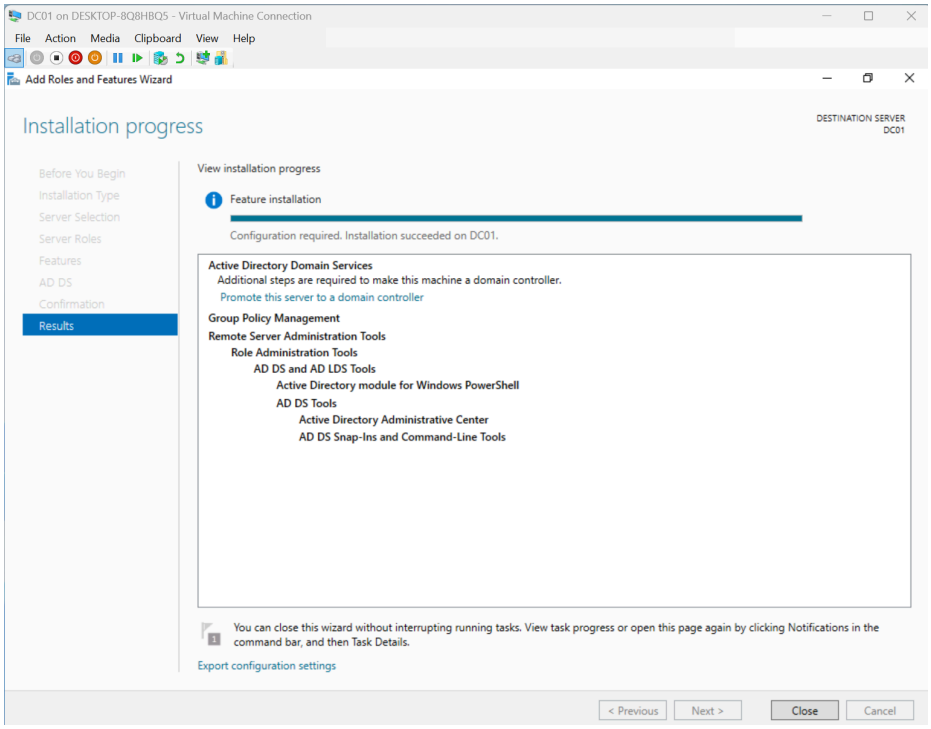


II. Active Directory Domain Services (AD DS) Installation and Configuration

Deploy a local directory service to manage user and device identities, forming the foundation of hybrid identity management.

Actions Completed:

1. Launched Server Manager → Add Roles and Features Wizard
2. Selected Role-Based Installation > Local Server (DC01)
3. Enabled role: Active Directory Domain Services
4. Completed installation and initiated domain controller promotion
    - Deployment Configuration: Add new forest
    - Root domain: dipeshcorp.local
    - Enabled DNS and Global Catalog roles
    - Defined Directory Services Restore Mode (DSRM) password
    - Verified NetBIOS name: DIPESHCORP (auto-filled)
    - Restarted DC01 to finalize domain controller promotion



Post-Promotion Configuration:

5. Logged into DC01 with domain credentials: Administrator@dipeshcorp.local

6. Launched Active Directory Users and Computers (ADUC) and verified domain presence: dipeshcorp.local

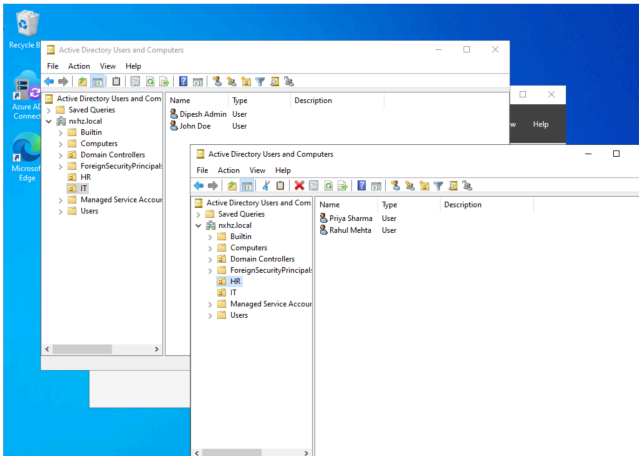
   Created Organizational Units (OUs) for department-based user separation: right-click Domain → New → OU → Configure OU settings.

   - OU: IT
   - OU: HR

User Creation:

To model a realistic user environment, standard users were added to their respective departments using a consistent naming pattern.

7. In IT OU:
   - dipesh.admin (Dipesh Admin) — UPN: dipesh.admin@dipeshcorp.local (Optionally added to Domain Admins group for setup tasks)
   - john.doe (John Doe) — UPN: john.doe@dipeshcorp.local



8. In HR OU:
   - priya.sharma (Priya Sharma) — UPN: priya.sharma@dipeshcorp.local
   - rahul.mehta (Rahul Mehta) — UPN: rahul.mehta@dipeshcorp.local

⚠️ **Note**: The same standardized process used for one OU was repeated for the others—right-click OU → New → User → Configure profile and password settings.

III. Azure AD Connect Installation and Directory Synchronization

Synchronize on-premises directory identities (dipeshcorp.local) with Microsoft Entra ID (nxhz.onmicrosoft.com) to enable hybrid identity and centralized authentication.

Actions Completed:

1. Downloaded Azure AD Connect from Microsoft: URL: https://www.microsoft.com/en-us/download/details.aspx?id=47594
2. Transferred the installer to DC01 and launched the setup
3. Accepted license terms → Selected “Customize” for granular control
4. Sign-in Method: Password Hash Synchronization
    - Skipped Single Sign-On (SSO) setup in this phase
5. Connected to Microsoft 365 Tenant:
    - Admin credentials: admin@dipeshcorp.onmicrosoft.com
    - Successfully authenticated
6. Connected to local Active Directory (dipeshcorp.local):
    - At this step, Azure AD Connect attempted to bind with the detected forest using current credentials (Domain Admin on DC01).
    - Encountered an error: "The specified account does not have the required permissions to access directory services."

🛑 **Root Cause:** Although the account was a Domain Admin, the installation wizard flagged permission inheritance or ACL mismatch in the forest root.

✔️ **Resolution:** Instead of using the detected AD account, I manually selected “Create new AD account” during the wizard.

- Azure AD Connect then automatically created and delegated a dedicated sync service account in dipeshcorp.local with the appropriate permissions.

- This approach ensured compatibility with fine-grained directory permissions and removed dependency on the original admin account.

⚠️ **Note:** This is a recommended best practice in hybrid deployments to ensure the sync account is scoped and managed by Azure AD Connect.

7. Configured OU Filtering:
    - Selected only the IT OU for initial synchronization
8. Left optional features as default:
    - Password Writeback: Enabled
    - Device Writeback: Skipped
9. Completed initial sync and verified success

View sync scheduler configuration:

```
# PowerShell script execution for the current session
Get-ADSyncScheduler
```

Trigger delta sync manually:

```
# Enable PowerShell script execution for the current session
Start-ADSyncSyncCycle -PolicyType Delta
```

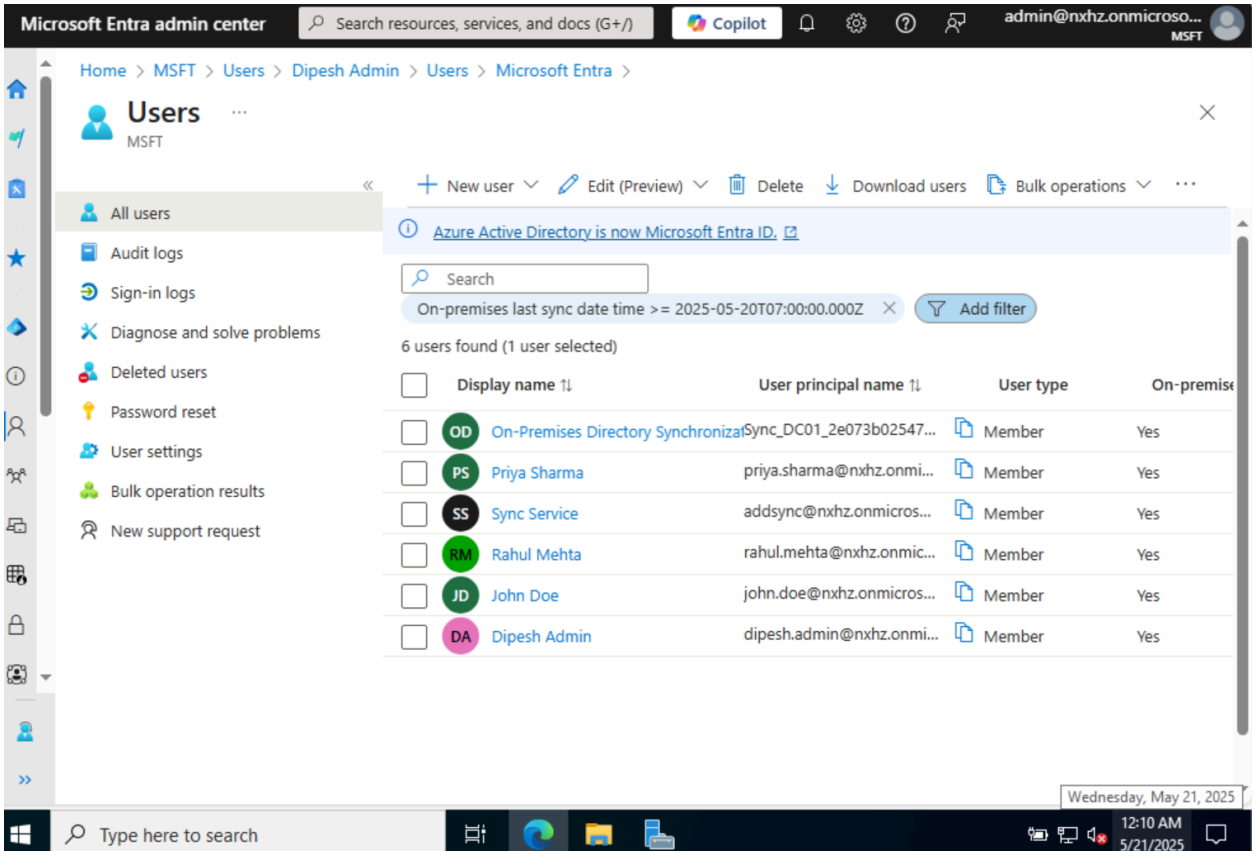
```
PS C:\Users\Administrator> Get-ADSyncScheduler


AllowedSyncCycleInterval            : 00:30:00
CurrentlyEffectiveSyncCycleInterval : 00:30:00
CustomizedSyncCycleInterval         :
NextSyncCyclePolicyType             : Delta
NextSyncCycleStartTimeInUTC         : 5/21/2025 7:22:31 AM
PurgeRunHistoryInterval             : 7.00:00:00
SyncCycleEnabled                    : True
MaintenanceEnabled                  : True
StagingModeEnabled                  : False
SchedulerSuspended                  : False
SyncCycleInProgress                 : False
```

IV. Sync Validation via Microsoft Entra ID

Validate the success of user sync and ensure proper hybrid integration.

Actions Completed:

- Logged into Microsoft Entra Admin Center: https://entra.microsoft.com
- Navigated to Identity > Users
- Confirmed the presence of the following synced identities from on-prem AD:
  - dipesh.admin@dipeshcorp.local
  - john.doe@dipeshcorp.local
- Verified that “Source” shows: Windows Server AD



V. Completion Outcome:

At the end of Phase 2, DipeshCorp (*Alias of **nxhz**)* operates a fully functional hybrid identity system with secure user provisioning across on-premises and cloud directories. This setup is a prerequisite for endpoint management using Microsoft Intune and Autopilot, as well as conditional access policies for enterprise security enforcement.