PHASE 7: Enterprise Security & Mobility Stack

This phase consolidates multiple security and endpoint mobility technologies—enabling secure cloud-managed infrastructure with real-time protection, hybrid file access, identity-based SSO, and virtual desktop deployment.

TRACK A – File Server + OneDrive Hybrid Sync (KFM) (Phase 6C)

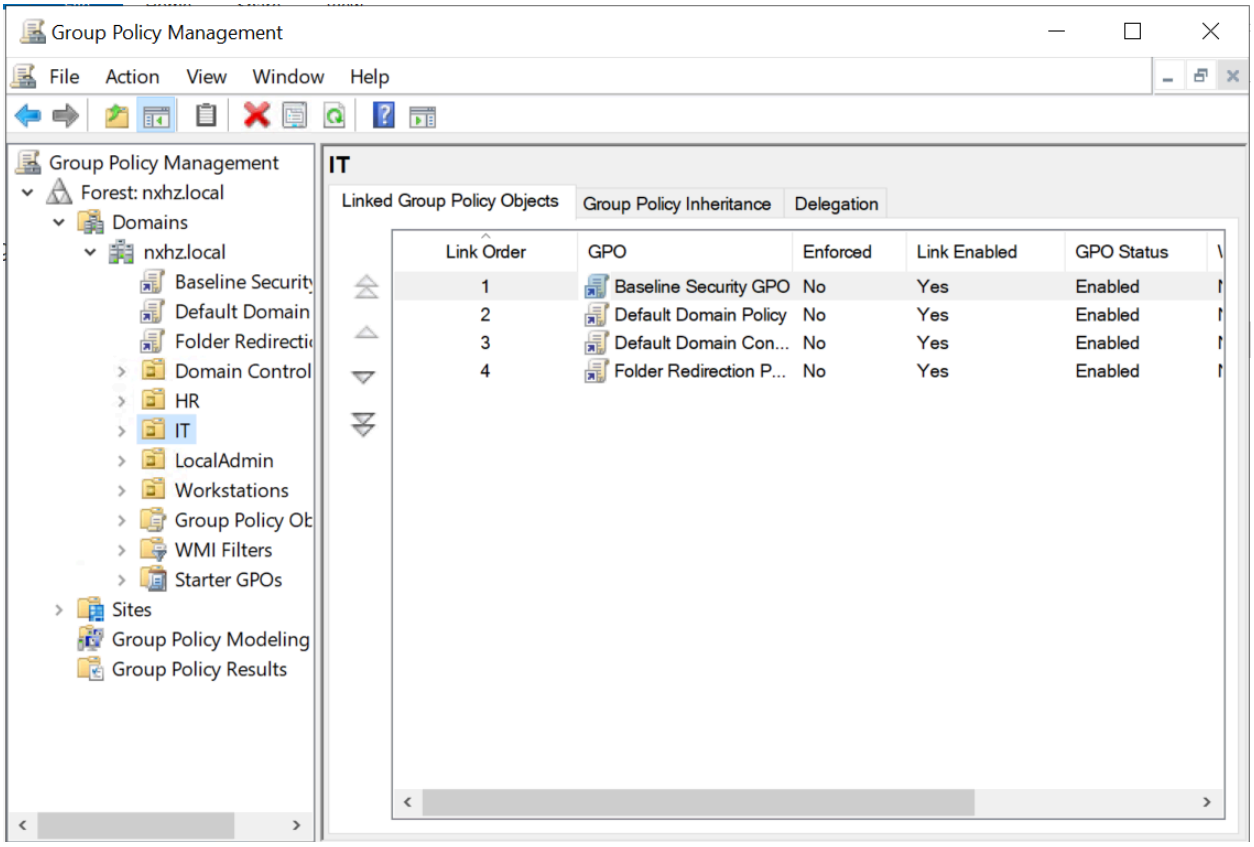
Create a traditional file server for internal folder redirection and sync redirected folders to OneDrive using Known Folder Move (KFM).

🛠️ Step-by-Step Deployment

1. On DS01: Install File Server Role
    - Server Manager → Add Roles and features → Role-based → File and Storage Services → File Server
    - Create folder: C:\CompanyShare
2. Share the folder:
    - Right-click D:\CompanyShare → Properties → Sharing → Advanced Sharing
    - Share name: CompanyShare
    - NTFS and Share Permissions: Full Control for Domain Users
3. UNC path: \DS01\CompanyShare
4. On DC01: Redirect folders via GPO
    - Group Policy Management → dipeshcorp.local → Create new GPO: “Folder Redirection Policy”
    - Edit GPO:

    User Configuration → Policies → Windows Settings → Folder Redirection
        - Documents: Right-click > Properties > Setting: Basic > Redirect following location to \FS01\CompanyShare%username%
        - Repeat for Desktop, Pictures

- Link GPO to OU (e.g., “OnPremUsers”)



5. Enabled KFM in Intune:
   - Go to: https://endpoint.microsoft.com → Devices → Configuration Profiles
   - Create profile:
     - Platform: Windows 10 and later
     - Profile type: Settings Catalog
     - Name: Enable KFM
   - Add settings:
     - Silently move known folders to OneDrive = Enabled
     - Prompt user = Disabled
     - Use OneDrive Files On-Demand = Enabled
   - Assign to: “All Cloud ices”

TRACK B – Entra ID SSO for SaaS Applications

Use Microsoft Entra ID (Azure AD) as a Single Sign-On identity provider for external SaaS platforms such as Zoom, Salesforce, or Adobe.

.🛠️ Step-by-Step Deployment

1. Registered SaaS App
    - Portal: https://entra.microsoft.com → Applications → Enterprise Applications → + New Application
    - Select SaaS app (e.g., Zoom, Salesforce)
    - Setup SSO → Choose: SAML (or OIDC)
2. Configured SSO settings:
    - Microsoft provides prefilled values (Identifier, Reply URL, etc.)
    - Download Federation Metadata (if required by SaaS app)
3. Assigned Users & Groups
    - Go to: App → Users and Groups → Add Users
    - Assign: user1@dipeshcorp.onmicrosoft.com or group “Cloud Users”
4. Optional: Created Conditional Access Policy
    - Entra ID → Conditional Access → New Policy
    - Name: MFA for SaaS
    - Users: All cloud users
    - Apps: All cloud apps
    - Grant: Require MFA

TRACK B – Windows 365 Cloud PC

Provision a secure, always-on cloud-hosted desktop using Microsoft Windows 365 (Enterprise Trial).

.🛠️ Step-by-Step Deployment

1. Assigned Trial License
    - Portal: https://admin.microsoft.com → Billing → Licenses
    - Add “Windows 365 Enterprise Trial” license
    - Assign to: device1@dipeshcorp.onmicrosoft.com
2. Created Provisioning Policy
    - Portal: https://endpoint.microsoft.com → Devices → Windows 365
    - Provisioning Profiles → Create profile:
        - Name: DipeshCorp – CloudPC
        - Image: Windows 11 Enterprise
        - Region: East US
        - Join Type: Azure AD Join
        - Network: Microsoft-hosted network
    - Assign to: “Cloud PC Users” group
3. User Access
    - Login to: https://windows365.microsoft.com
    - Sign in as: user1@dipeshcorp.onmicrosoft.com
    - Click on Cloud PC → Boot up takes ~2–3 mins
    - Use as regular Windows 11 desktop