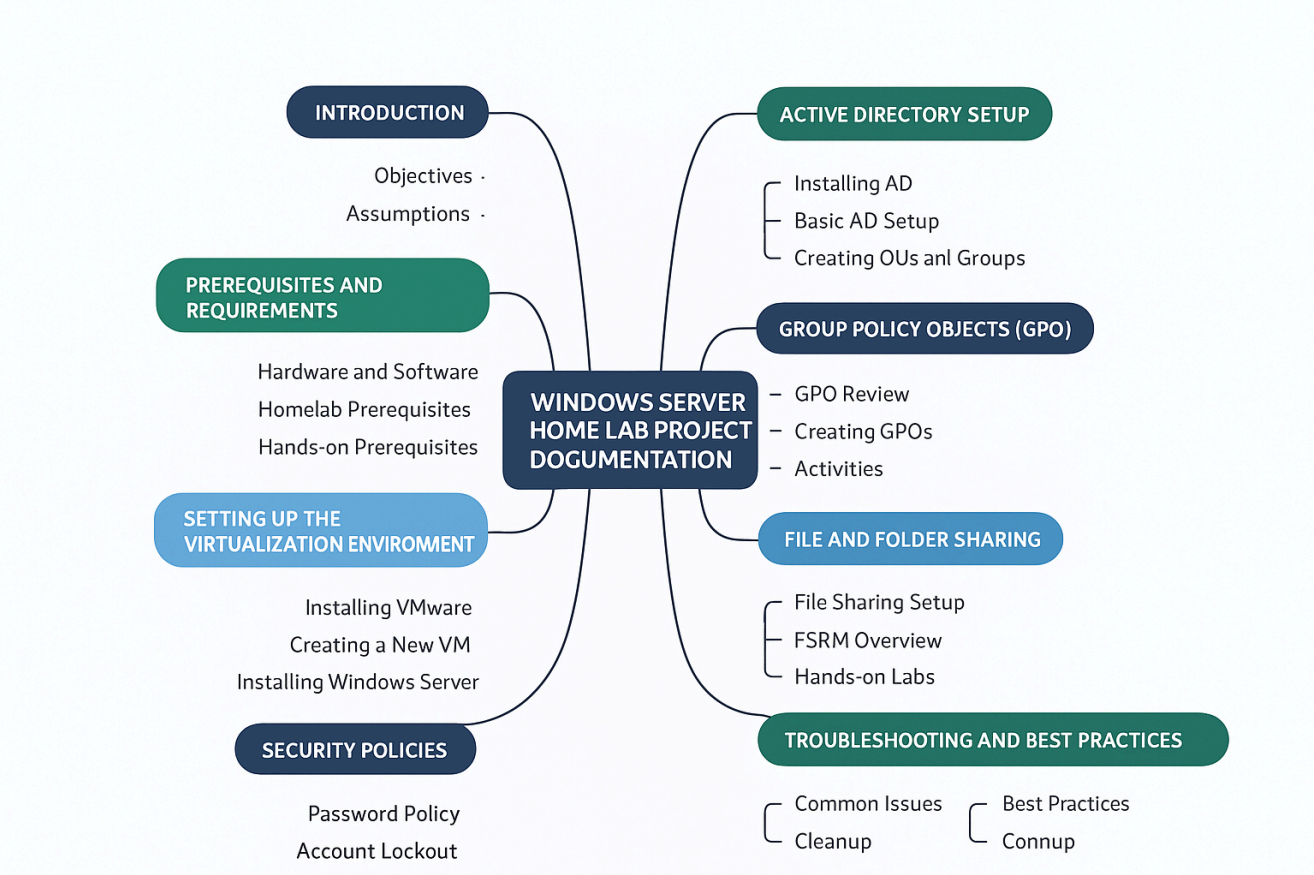
Windows Server Home Lab Project Documentation



1. Introduction

This documentation provides a comprehensive guide to setting up and managing a Windows Server Home Lab. The project is designed for IT enthusiasts, students, and professionals looking to gain hands-on experience with Windows Server technologies in a controlled, virtualized environment. Key focus areas include Active Directory (AD), Group Policy Objects (GPO), file and folder sharing, security policies, service accounts, and related configurations.

The lab simulates a small enterprise network, allowing you to practice domain management, user/group administration, policy enforcement, and file services without affecting production systems. This guide aggregates topics from various tutorial chapters to create a logical, step-by-step workflow.

Objectives:

- Build a virtualized Windows Server environment.
- Configure core services like AD, GPO, and file sharing.
- Implement security best practices.
- Test configurations through hands-on activities.

Assumptions:

- Basic knowledge of Windows OS and networking.
- Access to a host machine with sufficient resources (e.g., 16GB+ RAM, multi-core CPU).

2. Prerequisites and Requirements

Before starting, ensure you meet the following prerequisites to avoid setup issues.

Hardware and Software Requirements

- **Host Machine:** Windows 10/11 (Pro edition recommended for Hyper-V, but VMware is used here).
- **CPU:** Supports virtualization (enable in BIOS: Intel VT-x or AMD-V).
- **RAM:** Minimum 8GB (16GB+ recommended to run multiple VMs).
- **Storage:** 100GB+ free space for VMs and ISOs.
- **Software:**
  - VMware Workstation (free Player version or Pro).
  - Windows Server ISO (download from Microsoft Evaluation Center; e.g., Windows Server 2022).
  - Windows Client ISO (e.g., Windows 10/11 for client VMs).
- **Network:** Stable internet for downloads; lab uses virtual networks (NAT or bridged).

Homelab Prerequisites

- Verify BIOS virtualization settings.
- Download ISOs and store them securely.
- Plan VM resources: Allocate 2-4GB RAM and 2 vCPUs per VM initially.
- For security labs, ensure an isolated network to prevent accidental exposure.

Hands-on Prerequisites

- Familiarize yourself with basic command-line tools (PowerShell, cmd).
- Backup your host machine before proceeding.

3. Setting Up the Virtualization Environment

This section covers installing VMware Workstation and creating virtual machines (VMs) for the lab.

Installing VMware Workstation

1. Download VMware Workstation Player/Pro from the official VMware website.
2. Run the installer and follow the prompts (accept defaults unless customizing).
3. Restart the host if prompted.

4. Launch VMware and verify virtualization is enabled (Tools > Virtual Machine Settings > Hardware > Processors > Enable virtualization engine).

Downloading Windows Server ISO

1. Visit the Microsoft Evaluation Center.
2. Search for "Windows Server 2022" (or desired version) and download the ISO.
3. Save it to a dedicated folder on your host.

Creating a New VM

1. In VMware, select "Create a New Virtual Machine."
2. Choose "Installer disc image file (iso)" and browse to the Windows Server ISO.
3. Set VM name (e.g., "DC1" for Domain Controller) and location.
4. Allocate disk space (e.g., 60GB, split into multiple files for flexibility).
5. Customize hardware: 4GB RAM, 2 CPUs, network adapter set to NAT.
6. Finish and power on the VM.

Installing Windows Server on VM

1. Power on the VM; it boots from the ISO.
2. Select language, time, and keyboard preferences.
3. Choose "Windows Server Standard (Desktop Experience)" for GUI-based setup.
4. Accept license terms and select "Custom: Install Windows only."
5. Create a partition on the virtual disk and proceed with installation.
6. Set administrator password post-install.

Windows Server Setup

1. After installation, log in as Administrator.
2. Run Server Manager (starts automatically).
3. Configure server name (e.g., DC1) via System Properties.
4. Set static IP (e.g., 192.168.0.10/24) in Network Settings.
5. Update Windows via Settings > Update & Security.

4. Active Directory Setup

Active Directory (AD) forms the core of domain management. This section guides you through installation and basic configuration.

Installing Active Directory

1. In Server Manager, select "Manage > Add Roles and Features."
2. Choose "Role-based or feature-based installation."

3. Select "Active Directory Domain Services" and add required features.
4. Complete installation and promote the server to a Domain Controller (DC).
5. In the post-install wizard, choose "Add a new forest" and set root domain name (e.g., homelab.local).

Basic AD Setup

1. Open Active Directory Users and Computers (dsa.msc).
2. Verify domain structure.
3. Set up DNS (integrated with AD) and test resolution.
4. Create organizational units (OUs) for different departments:
    - USA
    - Europe
    - Asia
5. Create user accounts and groups within these OUs:
    - Add the following groups: Users, Computers, and Servers.
        - **Users:** Add 3 people for each Department (IT, Accounting, HR, Sales, Management).
        - **Computers:** IT, Accounting, HR, Sales, Management.
        - **Servers:** IT, Accounting, HR, Sales, Management.

Creating Organizational Units (OUs)

1. In AD Users and Computers, right-click domain > New > Organizational Unit.
2. Name it (e.g., "Users," "Computers," "Groups").
3. Delegate control if needed for sub-admins.

Group Scope and Type Explanation

- **Scopes:** Domain Local (permissions within domain), Global (grouping across domains), Universal (cross-forest).
- **Types:** Security (for permissions), Distribution (for email lists).

How to Create Groups

1. Right-click OU > New > Group.
2. Specify name, scope, and type.
3. Add members via group properties.

Creating Users

1. Right-click OU > New > User.
2. Enter details (name, logon name).

3. Set password (enforce complexity).
4. Assign to groups.

Hands-on Activity

- Create an OU "TestOU."
- Add 2 users and 1 group.
- Test user login from a client VM.

5. Group Policy Objects (GPO)

GPOs enforce settings across the domain. This covers review, installation, creation, and activities.

GPO Review

- GPOs link to domains, sites, or OUs.
- Processing order: Local > Site > Domain > OU (LSDOU).
- Inheritance can be blocked/enforced.

Installing Group Policy Management Console (GPMC)

1. In Server Manager, add "Group Policy Management" feature.
2. Launch gpmc.msc.

Creating GPOs

1. In GPMC, right-click domain/OUs > Create a GPO in this domain, and Link it Here.
2. Name it (e.g., "PasswordPolicy").
3. Edit via right-click > Edit.

GPO Types Explanation

- Computer Configuration: Machine settings (e.g., startup scripts).
- User Configuration: User-specific (e.g., desktop restrictions).

Applying GPOs

1. Link GPO to OU.
2. Force update: gpupdate /force on target machines.
3. Test: Log off/on or reboot.

Moving Computers to Different OU

1. In AD Users and Computers, right-click computer > Move.

2. Select target OU; GPOs apply accordingly.

Testing GPO

1. Use gpresult /r on client to view applied policies.
2. Verify settings (e.g., wallpaper change).

Activities

- **Activity 1:** A Marketing Intern needs access to the Marketing Team's shared folder "Marketing" to view content but should not modify or delete files.
- **Activity 2:** The HR Department needs a secure folder HRGroup that only HR staff can access. Other employees should not see the folder at all.
- **Activity 3:** A third-party vendor needs access to a temporary folder VendorFiles to upload reports but should not see other files.
- **Activity 4:** In the IT Department, all techs need access to the Software Repository Software but only senior IT staff should be able to access the "Licenses" subfolder.
- **Activity 5:** Configure a GPO to enforce a password policy requiring a minimum length of 8 characters and complexity.

Bonus Activity

- Link GPO to site level and test inheritance.

6. File and Folder Sharing

Set up shared resources for network access.

File and Folder Sharing Overview

- NTFS permissions for local access.
- Share permissions for network.
- Combine for least privilege.

Set Up File Sharing

1. Create folder (e.g., C:\Shares\Public).
2. Right-click > Properties > Sharing > Advanced Sharing > Share this folder.
3. Set permissions (e.g., Everyone: Read).

Set Up Client Machines

1. Create Windows Client VM (similar to server setup, but use Windows 10/11 ISO).
2. Join to domain: Settings > System > About > Join a domain > Enter domain name.

Map Network Drives

1. On client: File Explorer > This PC > Map network drive.
2. Enter \server\share; check "Reconnect at sign-in."

Network Drive GPO Setup

1. Create GPO > User Configuration > Preferences > Windows Settings > Drive Maps.
2. New > Mapped Drive > Set action (Create), location, label.

FSRM Overview

File Server Resource Manager (FSRM) for quotas and screening.

Installing FSRM

1. Server Manager > Add Roles > File and Storage Services > File Server Resource Manager.

Quota Management Setup

1. Open FSRM (fsrm.msc).
2. Quotas > Create Quota > Select folder > Set limit (e.g., 1GB soft quota).

File Screening Setup

1. File Screens > Create File Screen > Select folder > Block file groups (e.g., executables).

File Sharing Basics Tutorial

- Share a folder and test access from client.
- Apply NTFS permissions: Right-click folder > Properties > Security.

Hands-on Labs

- Lab 1: Share folder, map drive, test read/write.
- Lab 2: Implement quota and attempt to exceed it.

Bonus Question

Q: How do you troubleshoot "Access Denied" on a share? A: Check share permissions, NTFS permissions, network connectivity, and group membership.

Real-World Scenario

You're simulating a file server for the HR and IT departments. You want users from HR to only see HR-related folders and IT to only see theirs.

How Access-Based Enumeration (ABE) Works

- User logs in.
- Access shared folder.
- Permissions checked.
- ABE filters view to show only accessible folders.

Scenarios

- **Scenario 1:** Everyone has Full Control on "Common" folder. Remove "Everyone" and use NTFS to grant "Project Group" Read and Write access to "Project" and "Events" subfolders.
- **Scenario 2:** Explicit Deny - John is denied access to "Confidential" folder within "Project," while others have Read and Write permissions.

7. Security Policies

Enhance domain security through policies.

Password Policy

1. In GPMC, edit Default Domain Policy > Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy.
2. Set minimum length (8+), complexity, age (max 90 days).

Account Lockout Policy

1. Same path > Account Lockout Policy.
2. Set threshold (5 invalid attempts), duration (30 min).

User Rights Assignment

1. Security Settings > Local Policies > User Rights Assignment.
2. Assign rights (e.g., "Access this computer from the network" to specific groups).

Fine-Grained Passwords

1. For specific users/groups: Open AD Admin Center > Password Settings > New.
2. Set custom policies (e.g., longer passwords for admins).

8. Service Accounts and Advanced Configurations

Manage accounts for services and special modes.

Service Account Review

- Use managed service accounts (gMSA) for automation.
- Avoid using domain admin for services.

Homelab Overview

- Integrate all components: AD for auth, GPO for control, shares for storage.

Windows Kiosk Mode

1. On client: Create local user.
2. GPO > User Configuration > Administrative Templates > System > Set "Assigned Access."
3. Assign app (e.g., browser) for kiosk.

Service Account GPO

1. Create GPO for service accounts.
2. Link to OU with service users; set logon restrictions.

9. Troubleshooting and Best Practices

- **Common Issues:** DNS misconfiguration (flush cache: ipconfig /flushdns), GPO not applying (check event logs).
- **Best Practices:** Use least privilege, regular backups (export VMs), test in isolation.
- **Cleanup:** Delete test OUs/users after labs.

10. Conclusion and Next Steps

This home lab provides foundational skills for Windows Server administration. Expand by adding roles like DHCP, DNS, or Hyper-V nesting. For real-world application, consider certifications like MCSA/MCSE.

If issues arise, refer to Microsoft Docs or community forums. Happy labbing!

==========