Windows Server 2016 Helpdesk Lab Documentation

Windows Server 2016 Helpdesk Lab Documentation

Tier 1 IT Support & Active Directory Administration Practice

Lab Owner: Akash Bahl
Purpose: Hands-on practice for Helpdesk support scenarios, Active Directory management, remote assistance, Group Policy configuration, and common troubleshooting workflows
Environment: Windows Server 2016 + Windows 10 Clients
Last Updated: November 2025

Table of Contents

---

1. Lab Environment Setup

Infrastructure Overview

- **Hypervisor:** VMware Workstation Pro on Kali Linux
- **Domain Controller:** Windows Server 2016

    - Domain: `deadeye5457.com`
    - NetBIOS: `DEADEYE5457`
    - Static IP: `10.1.10.2`
- **Client Machines:**
    - Desktop1 (Windows 10) - IP: `10.1.10.3`
    - Desktop2 (Windows 10) - IP: `10.1.10.4`
- **Network Configuration:** Host-Only Adapter (Isolated Lab Environment)

Initial Setup Challenge & Solution

Problem Encountered:
Windows Server 2016 installation repeatedly displayed: *"Windows Cannot Find the Microsoft Software License Terms"*

Solution Implemented:

1. Created empty VM in VMware Workstation Pro without OS pre-selection
2. Configured VM specifications: 4GB RAM, 60GB Virtual HDD, 2 vCPUs
3. **After** VM creation, mounted Windows Server 2016 ISO
4. Started VM and successfully completed installation

Why This Matters: Understanding VM provisioning workarounds is essential when deploying test environments or troubleshooting installation issues in production scenarios.

---

2. Active Directory Domain Services Configuration

Installing AD DS Role

Step-by-Step Procedure:

1. Opened **Server Manager → Manage → Add Roles and Features**
2. Selected **Role-based or feature-based installation**
3. Chose server from server pool
4. Selected **Active Directory Domain Services** role
5. Confirmed automatic addition of required features
6. Proceeded through wizard and clicked **Install**

Promoting Server to Domain Controller

Configuration Steps:

1. Post-installation: Clicked **"Promote this server to a domain controller"**
2. Deployment Configuration:
   - Selected **"Add a new forest"**
   - Root domain name: `deadeye5457.com`
3. Domain Controller Options:
   - Forest/Domain functional level: Windows Server 2016
   - DSRM Password: `Password123` *(Lab environment only)*
4. DNS Options: Automatically configured
5. NetBIOS name: `DEADEYE5457` (auto-generated)
6. Paths: Left default locations
7. Reviewed prerequisites
8. Completed promotion → Automatic server restart

PowerShell Alternative:

```
Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools
Import-Module ADDSDeployment
Install-ADDSForest `
  -DomainName "deadeye5457.com" `
  -DomainNetbiosName "DEADEYE5457" `
  -InstallDns:$true `
  -SafeModeAdministratorPassword (ConvertTo-SecureString "Password123" -
AsPlainText -Force) `
  -Force:$true
```

Verifying Domain Controller Installation

Interview Question: *"How would you verify if a computer is joined to a domain?"*

Answer:

1. On the login screen, click **"Other user"** → **"How do I sign in to another domain?"**
2. This displays the current domain controller and available domains
3. Alternatively, run: `systeminfo | findstr /B /C:"Domain"`

---

3. User Account Management Best Practices

Enabling Advanced Features in ADUC

Why This Is Critical:

- Provides access to **Attribute Editor** tab
- Shows exact Distinguished Name (DN) paths
- Reveals object metadata (creation date, modification history)
- Essential for troubleshooting complex permission issues

How to Enable:

1. Open **Active Directory Users and Computers**
2. Right-click domain root (`deadeye5457.com`)
3. Select **View** → **Advanced Features**

Enabling Active Directory Recycle Bin

Purpose: Prevents permanent accidental deletions

Activation Steps:

1. Open **Active Directory Administrative Center**
2. Select domain `deadeye5457.com` in left panel
3. Right panel: Click **Enable Recycle Bin**
4. Confirm warning (this action cannot be reversed)

Real-World Impact: Deleted user accounts can be restored within **180 days** without losing group memberships, attribute values, or security permissions.

Creating Helpdesk Administrator Account

Best Practice Method: Copy User Template

Procedure:

1. In ADUC, navigate to **Users** container
2. Locate **Administrator** account
3. Right-click Administrator → **Copy**
4. Enter new user details:
   - First name: `Helpdesk`
   - Last name: `Support`
   - User logon name: `helpdesk`
   - Password: `Password123`
5. Review inherited group memberships

MSP/Enterprise Advantage: Using template accounts ensures consistent permission sets, faster onboarding, and reduced permission drift.

Finding Users in Active Directory

Interview-Ready Response:

"To locate a user account in Active Directory, I would:

1. *Open Active Directory Users and Computers*
2. *Right-click the domain root*
3. *Select **Find***
4. *Choose **'Entire Directory'** from dropdown*
5. *Enter the user's display name, username, or email*
6. *If not found, verify spelling or check Deleted Objects container"*

---

4. Essential CMD Commands for Helpdesk

1. `ipconfig` - Basic IP Configuration

Purpose: Display current IP address and network configuration

Example Output:

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
   IPv4 Address. . . . . . . . . . . : 10.1.10.3
   Subnet Mask . . . . . . . . . . . : 255.0.0.0
   Default Gateway . . . . . . . . . : 10.1.10.1
```

What to Look For: Valid IP in expected range, correct subnet mask, gateway configured

---

2. `ipconfig /all` - Detailed Network Information

Critical Information Revealed:

- **DHCP Enabled:** Yes/No (determines static vs. dynamic IP)
- **DHCP Server:** Which server assigned the IP
- **DNS Servers:** Helps diagnose name resolution failures
- **Physical Address (MAC):** Needed for MAC filtering/network registration

---

3. `ipconfig /flushdns` - Clear DNS Cache

Troubleshooting Scenarios:

- Website not loading after DNS record changes
- Users getting "Server not found" errors
- Internal web app not resolving after migration

---

4. `net use` - Display Mapped Network Drives

Example Output:

```
C:\> net use
Status       Local     Remote                    Network
-------------------------------------------------------------------------------
---
OK           Z:        \\fileserver\shared       Microsoft Windows Network
```

Commands:

- Map drive: `net use Z: \\fileserver\shared /persistent:yes`
- Remove drive: `net use Z: /delete`

---

5. `net user [username] /domain` ⭐ CRITICAL COMMAND

Most Important Command for Tier 1 Helpdesk

Example:

```
C:\> net user helpdesk /domain
User name                    helpdesk
Account active               Yes
Password last set            11/13/2025 10:00:00 AM
Password expires             2/11/2026 10:00:00 AM
Last logon                   11/17/2025 9:30:00 AM
Global Group memberships     *Domain Users *Domain Admins
```

Critical Information Provided:

Field	Why It Matters
Account active	Check if account is disabled
Password last set	Determine password age
Password expires	Proactively notify users
Last logon	Verify if account is being used
Global Group memberships	Confirm correct permissions

---

6. `ping` - Test Network Connectivity

Basic Usage:

```
C:\> ping 10.1.10.2
Reply from 10.1.10.2: bytes=32 time<1ms TTL=128
```

Continuous Ping (Monitor Server Restart):

```
C:\> ping 10.1.10.2 -t
```

---

7. `gpupdate /force` - Force Group Policy Refresh

Usage:

```
C:\> gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

Important Distinction:

- **User-level policies:** Take effect immediately after `gpupdate`
- **Computer-level policies:** May require restart/logoff

---

8. `gpresult` - View Applied Group Policies

Commands:

- Basic report: `gpresult /r`
- Export to text: `gpresult /r > C:\results.txt`
- HTML report: `gpresult /h C:\gpreport.html`
- Check specific user: `gpresult /user anna /r`

---

9. `nslookup` - Troubleshoot DNS Issues

Example:

```
C:\> nslookup fileserver.deadeye5457.com
Server:  server2016.deadeye5457.com
Address:  10.1.10.2
Name:    fileserver.deadeye5457.com
Address:  10.1.10.5
```

---

5. Windows 10 Client Configuration & Domain Join

Setting Static IP Addresses (Lab Environment)

Why Static IPs in This Lab:

- No DHCP server in isolated environment
- Prevents unintended internet connectivity (safe testing)
- Simulates controlled network segment

Server 2016 Static IP Configuration:

```
IP Address:         10.1.10.2
Subnet Mask:        255.0.0.0
Default Gateway:    10.1.10.1
Preferred DNS:      10.1.10.2  (points to itself)
Alternate DNS:      10.1.10.1
```

Configuration Steps:

1. **Control Panel → Network and Sharing Center**
2. Click **Change adapter settings**

3. Right-click **Ethernet → Properties**
4. Select **Internet Protocol Version 4 (TCP/IPv4) → Properties**
5. Select **"Use the following IP address"**
6. Enter static configuration

VMware Network Adapter Setting: Changed from **NAT** to **Host-Only Adapter**

Joining Desktop1 to Domain

Step 1: Initial Computer Rename

1. This PC → Properties → **Change settings**
2. Computer Name tab → **Change**
3. Computer name: `Desktop1`
4. Restart

Step 2: Configure Static IP (10.1.10.3 with DNS pointing to DC)

Step 3: Verify Connectivity

```
C:\> ping 10.1.10.2
```

Step 4: Join Domain

1. This PC → Properties → **Change settings**
2. Computer Name tab → **Change**
3. Select **Domain:** `deadeye5457.com`
4. Enter credentials: `Administrator` / `Password123`
5. Success message → Restart

Step 5: Verification

- On Server 2016, open ADUC
- Check **Computers** container for **Desktop1**

Trust Relationship Error - Fix

Error Message: *"The trust relationship between this workstation and the primary domain failed."*

Resolution Steps:

1. Log in as local administrator: `.\Administrator`

2. Remove from domain → Change to **WORKGROUP**
3. Restart
4. Rejoin domain using domain admin credentials
5. Restart again

---

6. RSAT Tools Installation & Configuration

What are RSAT Tools?

Remote Server Administration Tools enable Windows 10 clients to manage Windows Server roles without full Server Manager access.

Why Helpdesk Needs RSAT

Access Control Best Practice:

- Helpdesk should **NOT** have direct access to Server Manager
- Too many overwhelming options
- Security risk (accidental misconfiguration)

RSAT Provides:

- Active Directory Users and Computers
- Group Policy Management
- DNS/DHCP management tools
- Remote Desktop Services tools

Installation Process

Path:

1. **Settings → Apps → Optional Features**
2. Click **Add a feature**
3. Search: **"RSAT"**

Tools Installed:

- RSAT: Active Directory Domain Services
- RSAT: DNS Server Tools
- RSAT: DHCP Server Tools
- RSAT: Group Policy Management Tools

- RSAT: Remote Desktop Services Tools

Post-Installation: Restart required

---

7. Organizational Units & Security Groups

Creating Organizational Units

Created OUs:

- **HR** - Human Resources department users
- **IT** - IT department and helpdesk staff

Creation Steps:

1. Open ADUC
2. Right-click domain root
3. **New → Organizational Unit**
4. Enter name
5. ☑ **Protect container from accidental deletion**

Creating Security Groups

Security Group vs Distribution Group:

Security Group	Distribution Group
Used for permissions (folder access, VPN, MFA)	Used for email distribution lists
Can be assigned file/folder ACLs	Cannot be assigned permissions

Created Security Groups:

1. **HR** - For HR department shared resources
2. **Personal** - For personal drive access

Setting Group Manager (Best Practice):

- **Managed By** tab → Select manager
- ☑ **Manager can update membership list**

Why This Matters: Quickly identify who approves access requests

8. Shared Drive Management & Permissions

Creating Shared Folders

Folders Created:

1. **HR** - Department shared folder
2. **Personal** - Individual user home folders

Creation Steps:

1. Server Manager → **File and Storage Services** → **Shares**
2. Right-click **Shares** → **New Share**
3. Share Profile: **SMB Share - Quick**
4. Share name: `HR`
5. Create

Physical Location: `C:\Shares\HR` and `C:\Shares\Personal`

Configuring NTFS & Share Permissions

Security Principle: Only grant access to specific security groups, not "Everyone"

Permissioning HR Folder:

Step 1: Disable Inheritance

- Right-click folder → Properties → Security → Advanced
- Click **Disable inheritance**
- Select **"Convert inherited permissions into explicit permissions"**

Step 2: Remove Unnecessary Groups

- Remove **Users** group
- Leave SYSTEM and Administrators

Step 3: Add Security Groups

- Add **Helpdesk** account with **Modify** permissions
- Add **HR** security group with **Modify** permissions

Step 4: Configure Share-Level Permissions

- Properties → Sharing → Advanced Sharing → Permissions

- Remove **Everyone**
- Add **HR** group → **Read/Write**
- Add **Helpdesk** → **Read/Write**

Mapping Network Drives

Method 1: Manual Mapping

1. File Explorer → This PC → Map network drive
2. Drive letter: `Z:`
3. Folder: `\\SERVER2016\HR`
4. ☑ **Reconnect at sign-in**

Method 2: Automatic via Active Directory

1. ADUC → User Properties → **Profile** tab
2. Home folder: Connect `P:` to `\\SERVER2016\Personal\%username%`
3. Auto-creates folder and maps at logon

---

9. Remote Desktop & Remote Assistance

Enabling Remote Desktop

On Desktop2:

1. File Explorer → This PC → Properties
2. Advanced system settings → **Remote** tab
3. Select **"Allow remote connections"**
4. Add **helpdesk** account to Remote Desktop Users

Connecting via Remote Desktop

From Desktop1:

1. Press **Windows Key + R** → Type: `mstsc.exe`
2. Computer: `Desktop2` or `10.1.10.4`
3. Enter credentials: `deadeye5457\helpdesk`

Accessing Administrative Shares

C$ Share Access:

```
\\Desktop2\C$
```

Use Cases:

- Copy files to/from user's computer
- Delete temp files remotely
- Check installed software
- Review system logs

Windows Remote Assistance

Purpose: View user's screen with their permission

Advantages:

- User remains logged in
- User must approve control
- Chat functionality
- Better for training scenarios

Initiating Session:

1. Run `msra.exe` on helpdesk computer
2. Select **"Help someone who has invited you"**
3. User saves invitation file to desktop
4. Access via `\\Desktop2\C$\Users\anna\Desktop\invitation.msrcIncident`

---

10. Group Policy Management

Understanding Group Policy

Common Helpdesk Use Cases:

- Password complexity requirements
- Account lockout policies
- Drive mappings
- Desktop restrictions
- Software installation

Configuring Account Lockout Policy

Configuration:

1. Group Policy Management Console
2. Default Domain Policy → Edit
3. Computer Configuration → Policies → Windows Settings → Security Settings
4. Account Policies → **Account Lockout Policy**
5. Set **Account lockout threshold:** 4 invalid logon attempts
6. Set **Account lockout duration:** 30 minutes

Modifying Password Policy

Changes Made:

- Maximum password age: **90 days**
- Minimum password length: **8 characters**

Creating Custom GPO (Task Manager Restriction)

Objective: Disable Task Manager for HR department users

Steps:

1. Create new GPO: **Task Manager - Restricted**
2. Link to **HR** OU
3. Edit GPO:
   - User Configuration → Policies → Administrative Templates
   - System → Ctrl+Alt+Del Options
   - Enable **"Remove Task Manager"**
   - Enable **"Remove Change Password"**
4. Enforce GPO

Applying Policy:

```
C:\> gpupdate /force
```

Testing: Task Manager and Change Password options removed for HR users

---

11. Common Helpdesk Scenarios & Resolutions

Scenario 1: Account Locked Out

User Report: "I can't log in. It says my account is locked."

Resolution:

1. Verify: `net user anna /domain` → Confirm lockout
2. ADUC → Find user → Properties → Account tab
3. ☑ **Unlock account**
4. Verify fix and call user

Scenario 2: Password Reset Required

Resolution:

1. Verify user identity
2. ADUC → Reset Password
3. ☑ **User must change password at next logon**
4. Communicate temp password to user
5. Document in ticket

Scenario 3: Account Expired

User Report: "Just came back from maternity leave, can't log in."

Resolution:

1. Check: `net user anna /domain` → See expiration date
2. ADUC → Account tab → Account expires: **Never**
3. Verify and test login

Scenario 4: Computer Fallen Off Domain

Error: *"The trust relationship between this workstation and the primary domain failed."*

Resolution:

1. Log in as `.\Administrator`
2. Remove from domain → WORKGROUP
3. Restart

4. Rejoin domain
5. Restart

Scenario 5: Cannot Access Network Drive

User Report: "My Z: drive has a red X."

Resolution:

1. Verify network connectivity: `ping 10.1.10.2`
2. Check mappings: `net use`
3. Test direct access: `\\SERVER2016\HR`
4. Remove stale mapping: `net use Z: /delete`
5. Recreate: `net use Z: \\SERVER2016\HR /persistent:yes`

Scenario 6: Group Policy Not Applying

User Report: "I can still open Task Manager."

Resolution:

1. Verify GPO is linked and enforced
2. Check user is in correct OU
3. Force update: `gpupdate /force`
4. Verify: `gpresult /r`
5. User must log off and back on

---

12. Advanced Troubleshooting Techniques

Remote Registry Access

Enabling Remote Registry Service:

```
C:\> sc config RemoteRegistry start= auto
C:\> sc start RemoteRegistry
```

Enabling Firewall Rules:

```
Enable-NetFirewallRule -DisplayGroup "Remote Service Management"
```

Connecting:

1. Run `regedit` on helpdesk computer
2. File → Connect Network Registry → `Desktop2`
3. Navigate to `HKEY_CURRENT_USER\Network` to see mapped drives

Continuous Ping Monitoring

Monitor server during restart:

```
C:\> ping 10.1.10.2 -t
```

Watch connection drop and return

Group Policy Result Reports

Generate HTML report:

```
C:\> gpresult /h C:\GPReport_Anna_%date%.html
```

---

13. Interview Preparation

Common Interview Questions with Lab-Based Answers

Q: "How would you unlock a locked user account?"

"I would first verify the lockout by running `net user [username] /domain` to confirm the account status. Then I'd open Active Directory Users and Computers, search for the user, open their properties, go to the Account tab, and check the 'Unlock account' checkbox. After unlocking, I'd verify with the command again and confirm with the user."

Q: "A user can't access a shared network drive. Walk me through troubleshooting."

"First, I'd verify network connectivity with ping. Then check their drive mappings using `net use` to see status. I'd verify they're in the appropriate security group using `net user [username] /domain`. If the mapping shows 'Unavailable,' I'd delete it with `net use [drive]: /delete`

and recreate it with /persistent:yes. If it's permissions, I'd verify group membership and ensure they've logged off and back on."

Q: "How do you check when a user's password expires?"

"I use `net user [username] /domain` which shows password last set date, expiration date, and if the account is locked out."

Q: "Computer has fallen off the domain. How do you fix it?"

"I would log in as local administrator using .\Administrator, remove the computer from the domain by changing it to a workgroup, restart, then rejoin the domain using domain admin credentials, and restart again."

Q: "What are RSAT tools and when would you use them?"

"RSAT stands for Remote Server Administration Tools. They allow helpdesk technicians to manage Active Directory, reset passwords, unlock accounts, and manage Group Policy from Windows 10 workstations without needing Server Manager access. I install them through Settings → Apps → Optional Features."

Q: "Explain the difference between security groups and distribution groups."

"Security groups are used for permissions like folder access, VPN, and MFA. Distribution groups are only for email distribution lists in Exchange/Office 365. You cannot assign file permissions to distribution groups."

---

14. Lab Completion & Next Steps

Lab Completion Checklist

Infrastructure:

- ✅ Windows Server 2016 installed and configured
- ✅ AD DS role installed and DC promoted

- ✅ Static IP addresses configured
- ✅ DNS functioning correctly
- ✅ Two Windows 10 clients joined to domain

Active Directory:

- ✅ Advanced Features enabled
- ✅ Recycle Bin enabled
- ✅ OUs created (HR, IT)
- ✅ User accounts created
- ✅ Security groups configured

File Services:

- ✅ Shared folders created
- ✅ NTFS and share permissions configured
- ✅ Drive mappings tested

Group Policy:

- ✅ Password policy configured
- ✅ Account lockout policy configured
- ✅ Custom GPO created and enforced

Remote Management:

- ✅ RSAT tools installed
- ✅ Remote Desktop tested
- ✅ Remote Assistance tested
- ✅ Administrative shares tested

Troubleshooting:

- ✅ Account lockout resolution
- ✅ Password reset procedures
- ✅ Domain trust issues resolved
- ✅ Network drive mapping
- ✅ Group Policy application

Skills Gained

- ✅ Active Directory administration

- ✅ User account management
- ✅ Group Policy configuration
- ✅ File server permissions
- ✅ Remote support techniques
- ✅ Troubleshooting workflows
- ✅ Professional documentation

Next Steps for Advanced Learning

1. **Office 365 Integration**
   - Install Azure AD Connect
   - Sync on-premises AD with cloud
2. **Advanced Group Policy**
   - Software deployment via GPO
   - Folder redirection
   - Printer deployment
3. **Monitoring & Reporting**
   - Event log analysis
   - Performance monitoring
   - Compliance reporting
4. **Disaster Recovery**
   - Backup and restore procedures
   - System state recovery
   - FSMO role management
5. **Automation**
   - PowerShell script library
   - Automated user provisioning
   - Report generation

Appendix: Quick Reference

Essential CMD Commands

```
ipconfig                              # Basic IP info
ipconfig /all                         # Detailed network info
ipconfig /flushdns                    # Clear DNS cache
ping [IP/hostname]                    # Test connectivity
```

```
ping [IP] -t                            # Continuous ping
nslookup [hostname]                     # DNS lookup
net use                                 # Show mapped drives
net use Z: \\server\share /persistent:yes  # Map drive
net user [username] /domain          # User account info
gpupdate /force                         # Force GP update
gpresult /r                             # Show applied policies
```

Troubleshooting Quick Reference

Symptom	Command	Action
Can't reach server	`ping [IP]`	Check network connectivity
Name not resolving	`nslookup [hostname]`	Check DNS configuration
Account issues	`net user [username] /domain`	Verify account status
Policy not applying	`gpresult /r`	Check applied GPOs
Drive mapping issue	`net use`	Verify mapping status

Lab Environment: Isolated/Host-Only Network
Safety: No production systems affected
Cost: Free (using trial/evaluation software)
Time Investment: 20-30 hours
Documentation Date: November 2025

End of Documentation