Lab Project: Customizing MDT to Enforce Domain-Only Logins

Introduction

In this lab, I went beyond a basic Windows deployment using Microsoft Deployment Toolkit (MDT). The goal was not just to install Windows, but to enforce a domain-only authentication model. After deployment, the client machines cannot be activated or accessed with a local user account - they only function when authenticated against the Active Directory domain (haki.lab).

Objectives

- Build a domain environment named haki.lab.
- Configure DHCP and WDS for PXE boot and IP distribution.
- Prepare MDT with boot/install images and a deployment share.
- Modify three core configuration files: Bootstrap.ini, CustomSettings.ini, Unattend.xml.
- Achieve semi-automated deployment where:
  * Devices join the domain automatically.
  * Local user creation during OOBE is bypassed.
  * Clients can only log in using domain accounts.

Step-by-Step Implementation

1. Server Preparation

- Installed AD DS, DNS, DHCP, WDS roles.
- Promoted the server to a Domain Controller for haki.lab.
- Created an OU for computer accounts.

2. DHCP Configuration

- Configured DHCP scope (192.168.65.0/24).
- Set DNS options to point to the DC.
- Verified clients received IP addresses.

3. WDS Setup

- Configured WDS integrated with AD.
- Added Boot Image (LiteTouchPE_x64) from MDT.

- Added Install Image (Windows 10).
- Verified PXE boot readiness.

4. MDT Deployment Share

- Created Deployment Share in MDT.
- Added Task Sequence for Windows 10/11.
- Prepared drivers if needed.

5. Core File Customization

Bootstrap.ini

Configured automatic connection to the deployment share:

```
[Settings]
Priority=Default
[Default]
DeployRoot=\\MDT-SERVER\DeploymentShare$
SkipBDDWelcome=NO
```

CustomSettings.ini

Controlled wizard pages and domain join:

```
[Settings]
Priority=Default
Properties=MyCustomProperty
[Default]
OSInstall=Y
JoinDomain=haki.lab
DomainAdmin=administrator
DomainAdminDomain=HAKI
DomainAdminPassword=YourPasswordHere
SkipDomainMembership=YES
SkipTaskSequence=NO
SkipComputerName=NO
SkipUserData=YES
SkipLocaleSelection=YES
```

```
SkipTimeZone=YES
SkipSummary=YES
SkipFinalSummary=YES
```

Unattend.xml

Configured domain join and bypassed local account creation:

```
<JoinDomain>haki.lab</JoinDomain>
<HideLocalAccountScreen>true</HideLocalAccountScreen>
```

6. Deployment Process

- Client boots PXE, receives IP from DHCP.
- Loads LiteTouchPE_x64 from WDS.
- MDT Wizard runs with minimal interaction.
- Windows installs and joins domain.
- Login screen shows: "Sign in to: HAKI".

Results

- Windows deployed automatically with minimal interaction.
- Clients auto-joined haki.lab domain.
- Local accounts bypassed, domain logins enforced.
- Mirrors enterprise deployment scenarios.

Conclusion

By modifying Bootstrap.ini, CustomSettings.ini, and Unattend.xml, MDT was transformed into a semi-automated deployment solution.

Key outcome: Endpoints cannot function without a domain account.

This lab bridges MDT with SCCM (Zero Touch) and Intune/Autopilot (Cloud) scenarios.