TECHNICAL RECORD

Active Directory Infrastructure & Ubuntu Domain Integration

Windows Server 2022 • AD DS • DNS • DHCP • GPO • SMB • Kerberos • Samba • Winbind

Enterprise identity, policy, endpoint and cross-platform authentication lab

PROJECT VALUE

Designed and implemented a Windows Server Active Directory environment, centrally managed Windows endpoints through DNS/DHCP/GPO, enforced role-based resource access, and extended the identity environment to Ubuntu using Kerberos, Samba and Winbind for cross-platform domain interoperability.

What I Built

- Deployed Windows Server 2022 in Oracle VM VirtualBox and promoted it to a Domain Controller for internal.awesconsults.site.
- Configured AD-integrated DNS and Windows DHCP so domain clients could discover the DC, obtain network configuration, authenticate and process policy.
- Designed an OU and security-group structure for Head Office and Branch Office functions, enabling role-based administration and policy targeting.
- Created and validated Group Policy controls, including password/security policy and firewall configuration.
- Joined Windows 10 Pro endpoints to the domain and verified centralized policy application using gpupdate and gpresult.
- Implemented SMB resource access using AD security groups rather than per-user permissions.
- Integrated Ubuntu Server with the Active Directory identity environment using Kerberos, Samba and Winbind, then validated domain user/group discovery.
- Prepared Ubuntu for domain-aware authentication/resource access using PAM/Winbind and Windows file-sharing utilities.

Core Environment

Area	Implementation
Domain	internal.awesconsults.site
Domain Controller	Windows Server 2022; recorded FQDN: AwesconsultsDC.internal.awesconsults.site
Original lab network	192.168.56.0/24 Host-only network; DC address 192.168.56.106
Windows endpoints	Windows 10 Pro domain-joined clients
Directory services	AD DS + DNS + DHCP + Group Policy
Ubuntu integration	Kerberos realm INTERNAL.AWESCONSULTS.SITE; Samba + Winbind; PAM/resource-access components
Virtualization	Oracle VM VirtualBox; original AD lab scope only

Active Directory & Policy Engineering

Built the directory around organizational roles rather than a flat user structure. Recorded OUs included Head Office (Admins, Users, Managers, Finance, IT) and Branch Office (Sales, Marketing, HR, Maintenance). Role-based security groups were used to support policy targeting and resource authorization.

Control	Recorded Configuration / Validation
Password policy	Minimum 12 characters; complexity enabled; maximum age 90 days; remember last 5 passwords.
Group Policy	Example policy: Awesconsults Security Policies; targeted security/firewall configuration.
Policy validation	gpupdate /force; gpresult /r; gpresult /h C:\Temp\gpresult.html
SMB authorization	Admins: Full Control; Managers: Change; Users: Read.
Domain client DNS	Clients configured to use the Windows Server/DC DNS service for AD discovery.

Ubuntu–Active Directory Integration

Extended the Windows identity environment to Ubuntu so the Linux system could participate in the same domain-oriented authentication and resource model instead of operating as an isolated local-account server.

Integration Layer	Implementation / Evidence
Kerberos	Realm configured as INTERNAL.AWESCONSULTS.SITE; KDC/admin server recorded as AwesconsultsDC.internal.awesconsults.site.
Samba	Installed/configured to provide Windows/AD interoperability.
Winbind	Used for domain identity resolution on Ubuntu.
Identity validation	wbinfo -u used to enumerate domain users; wbinfo -g used to enumerate domain groups.
PAM integration	PAM/Winbind components prepared for domain-aware Linux authentication.
Windows resource access	cifs-utils and libpam-mount included for access/mounting of Windows resources where required.

Cross-Platform Authentication Flow

```
Windows Server / AD DS
internal.awesconsults.site
        |
        +-- DNS locates domain services
        |
        +-- Kerberos provides domain authentication context
        |
        v
Ubuntu Server
Kerberos + Samba + Winbind
        |
        +-- resolves AD users/groups
```

```
        +-- supports domain-aware authentication
        +-- accesses Windows/SMB resources as configured
```

DNS, DHCP & Client Join Workflow

```
Windows Server 2022
   |-- AD DS
   |-- AD DNS
   |-- DHCP
   |
   +--> Windows client receives network settings
   +--> Client uses DC DNS
   +--> Client locates internal.awesconsults.site
   +--> Client joins/authenticates to domain
   +--> GPO applies centrally managed settings

Ubuntu
   +--> resolves AD/DC services
   +--> uses Kerberos/Samba/Winbind
   +--> discovers domain identities and Windows resources
```

Troubleshooting & Validation

- Resolved/validated domain-client behavior by checking addressing, DNS selection and domain discovery rather than treating authentication failures as isolated AD issues.
- Used gpupdate /force and gpresult output to distinguish GPO creation from successful client-side policy processing.
- Validated Ubuntu's AD visibility with wbinfo -u and wbinfo -g after configuring the Kerberos/Samba/Winbind stack.
- Recognized DNS as a dependency for AD and Kerberos: clients and Ubuntu must resolve the domain controller and internal AD namespace correctly.
- Kept VirtualBox's role separate from Windows DHCP so enterprise services, rather than the hypervisor, controlled domain-client configuration.

Selected Administrative Commands

```
Windows
gpupdate /force
gpresult /r
gpresult /h C:\Temp\gpresult.html
ipconfig /all
nslookup <domain-or-host>

Ubuntu
wbinfo -u
wbinfo -g
kinit <domain-user>        # Kerberos validation where configured
klist                      # Inspect Kerberos tickets
getent passwd              # Identity/NSS validation where configured
```

Skills Demonstrated

Capability	Evidence from Project
Windows Server administration	Installed/configured Windows Server 2022 roles and promoted a new AD forest/domain.
Identity & access management	Structured OUs/groups, domain users, role-based SMB permissions and centralized

	policy.
DNS/DHCP engineering	Connected addressing and name resolution to domain discovery/authentication requirements.
Group Policy	Created security controls and verified effective policy on Windows endpoints.
Linux/Windows integration	Configured Kerberos, Samba and Winbind so Ubuntu could resolve and interact with AD identities.
Troubleshooting	Validated each layer independently: IP, DNS, domain join, GPO, Kerberos, Winbind and resource access.
Virtualization	Built the original Windows/Linux enterprise lab in Oracle VM VirtualBox.

Summary

Built a cross-platform enterprise identity lab combining Windows Server 2022 Active Directory with Ubuntu integration. Implemented AD DS, DNS, DHCP, OU/security-group design, Group Policy, Windows domain joining and role-based SMB permissions, then integrated Ubuntu using Kerberos, Samba and Winbind for domain identity discovery and Windows-resource interoperability. The project demonstrates practical systems administration across Windows and Linux, with particular strength in identity dependencies, centralized endpoint management, authentication, access control and structured troubleshooting.

Scope note: This record intentionally covers AD DS environment and Ubuntu–Active Directory integration only. It excludes a later WireGuard/VPN integration and later segmented .56/.57 routing redesign.