Lab 2 – Identity & Directory Services (Active Directory Domain Services)

Course: NET-2220 Server Management
Student: Clayton Holden
Date Completed:

1. Purpose

The purpose of this lab was to install Active Directory Domain Services (AD DS), promote a Windows Server 2022 system to a domain controller, configure a basic organizational structure, and create sample identity objects. This lab introduced centralized authentication and the fundamentals of directory-based identity management.

2. AD DS Installation and Domain Controller Promotion

AD DS was installed using Server Manager:

1. Add Roles and Features
2. Select **Active Directory Domain Services**
3. Complete installation

The server was then promoted to a domain controller:

- Created a new forest: **corp.local**
- Accepted default functional levels
- Set DSRM password
- Restarted to complete domain controller configuration

After reboot, the system allowed domain login using:

```
corp\Administrator
```

---

3. Directory Structure and Identity Configuration

Using **Active Directory Users and Computers (ADUC)**, the following objects were created:

Organizational Units

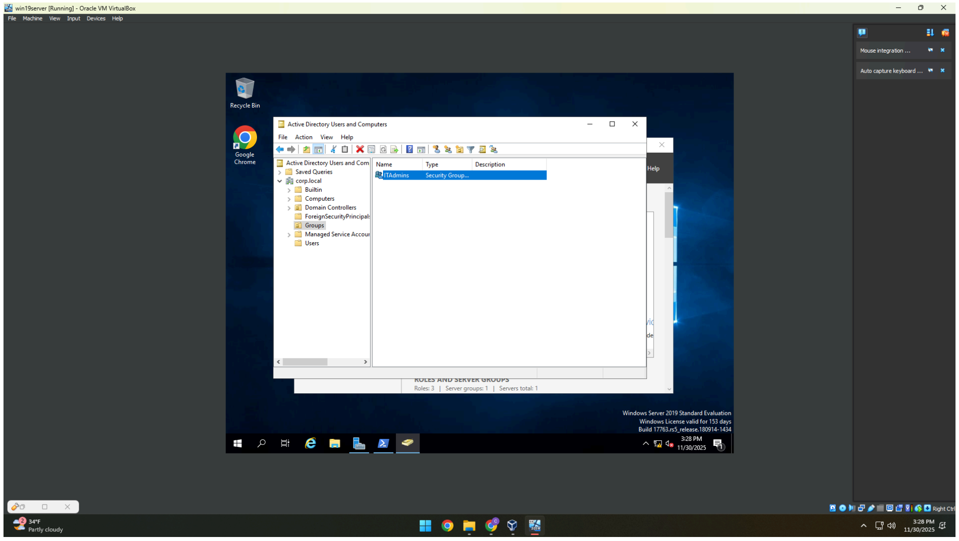
- **Users**
- **Groups**

Identity Objects

- **User:** `jsmith`
  - Password: `ComplexPwd123!`
- **Group:** `ITAdmins`
  - Security group, Global scope

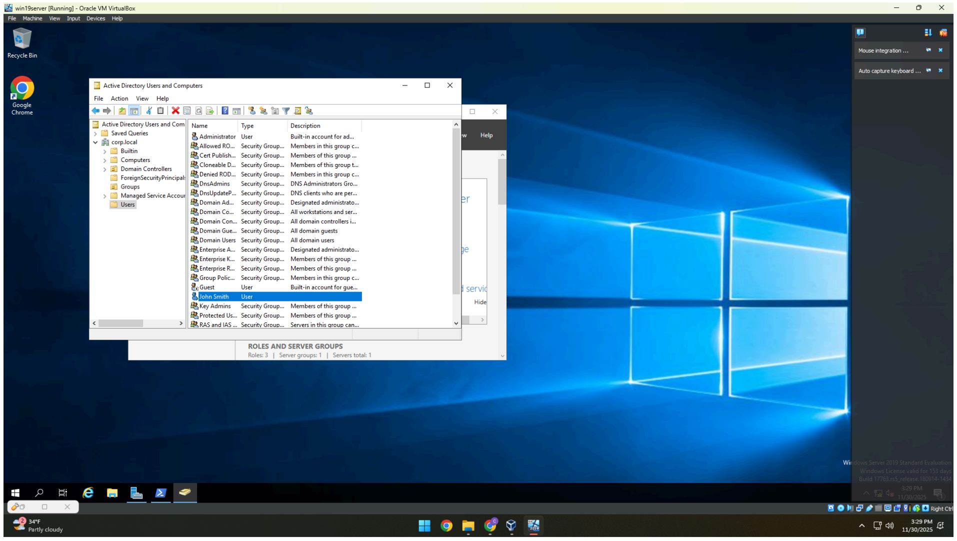
The user **jsmith** was added to the **ITAdmins** group to demonstrate group-based access control.

Evidence:



win19server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
corp.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Groups
Managed Service Accour
Users
ROLES AND SERVER GROUPS
Roles: 3 | Server groups: 1 | Servers total: 1
Windows Server 2019 Standard Evaluation
Windows License valid for 153 days
Build 17763.rs5_release.180914-1434
3:28 PM
11/30/2025

Name	Type	Description
ITAdmins	Security Group...	



win19server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
corp.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Groups
Managed Service Accour
Users
ROLES AND SERVER GROUPS
Roles: 3 | Server groups: 1 | Servers total: 1
3:29 PM
11/30/2025

Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
Denied ROD...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise K...	Security Group...	Members of this group ...
Enterprise R...	Security Group...	Members of this group ...
Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
John Smith	User	
Key Admins	Security Group...	Members of this group ...
Protected Us...	Security Group...	Members of this group ...
RAS and IAS ...	Security Group...	Servers in this group can...

---

4. Hybrid Identity Notes

Hybrid directory synchronization is used when organizations have traditional on-prem Active Directory but also use cloud services such as Microsoft 365 or Azure. Azure AD Connect enables unified identities across both environments, allowing single sign-on, MFA enforcement, conditional access, and seamless mobility for users. Hybrid identity supports phased cloud migration and strengthens authentication security.

---

5. Reflection

Centralized authentication is critical in server environments because it provides one authoritative location for managing user accounts, passwords, and permissions across all systems. When each server relies on standalone local accounts, access becomes inconsistent, difficult to audit, and more vulnerable to attack. Weak identity controls increase risks such as password reuse, privilege escalation, and lateral movement by attackers. Active Directory Domain Services mitigates these issues by centralizing identity and policy management, enabling group-based access, and enforcing consistent security policies throughout the organization.