

# Azure Active Directory Lab

## Lab Objective

Design and deploy an enterprise-style Active Directory environment in Microsoft Azure to demonstrate identity management, redundancy, DNS configuration, and domain controller replication.

## Environment Overview

- Azure Virtual Network with custom DNS configuration
- Two Windows Server domain controllers (DC01 and DC02)
- Active Directory Domain Services with DNS and Global Catalog enabled
- Multi-Availability Zone deployment for resilience

## Step-by-Step Lab Summary (What & Why)

### 1. Resource Group Creation

Created a dedicated Azure Resource Group to logically organize all AD-related resources and simplify management and cleanup.

### 2. Virtual Network Deployment

Configured a virtual network and subnet to allow secure private communication between domain controllers.

### 3. DC01 Virtual Machine Deployment

Deployed a Windows Server VM to act as the first domain controller, establishing the identity authority.

### 4. AD DS Installation & Domain Creation

Installed Active Directory Domain Services and promoted DC01 to create a new forest and domain (corp.local).

### 5. DNS Configuration

Configured DC01 as the primary DNS server so domain resources could be properly located and authenticated.

### 6. DC02 Virtual Machine Deployment

Deployed a second Windows Server VM in a different availability zone to simulate enterprise redundancy.

### 7. DNS Alignment for DC02

Manually configured DC02 to use DC01 for DNS to ensure domain discovery and authentication.

### 8. DC02 Promotion

Promoted DC02 as an additional domain controller, enabling replication of AD, DNS, and Global Catalog services.

## **9. Replication Validation**

Confirmed that Active Directory objects replicated successfully between DC01 and DC02.

## **10. Organizational Units & User Objects**

Created OUs and sample user accounts to simulate a real corporate directory structure.

## **Skills Demonstrated**

- Active Directory Domain Services (AD DS)
- Azure Virtual Machines and Networking
- DNS troubleshooting and configuration
- Multi-domain controller replication
- Enterprise identity architecture fundamentals

## **Why This Lab Matters**

This lab mirrors real-world enterprise identity environments. Understanding how domain controllers, DNS, and replication work is foundational for SOC analysts, defenders, and blue team operations, especially when monitoring authentication events and lateral movement.