# Active Directory Domain Services

# Class Objectives

By the end of today's class, you will be able to:

Explain how Active Directory is used to manage enterprise-scale environments.

Define domain controllers as servers that manage AD authentication and authorization.
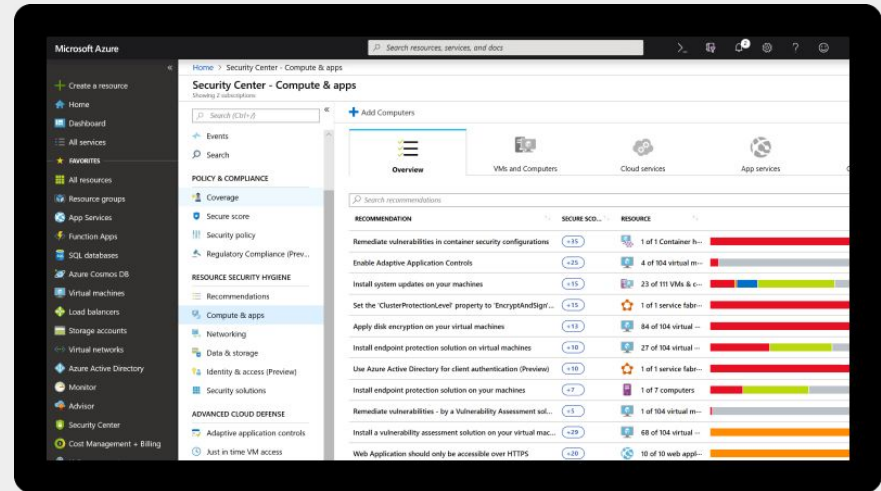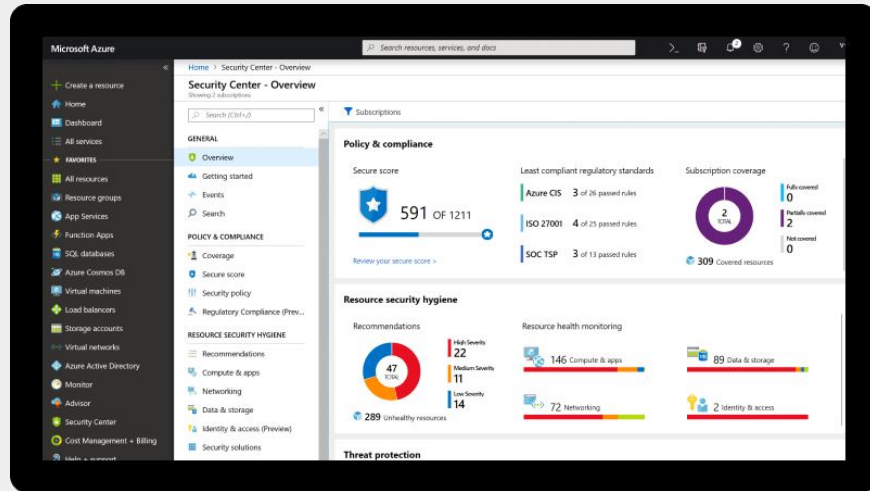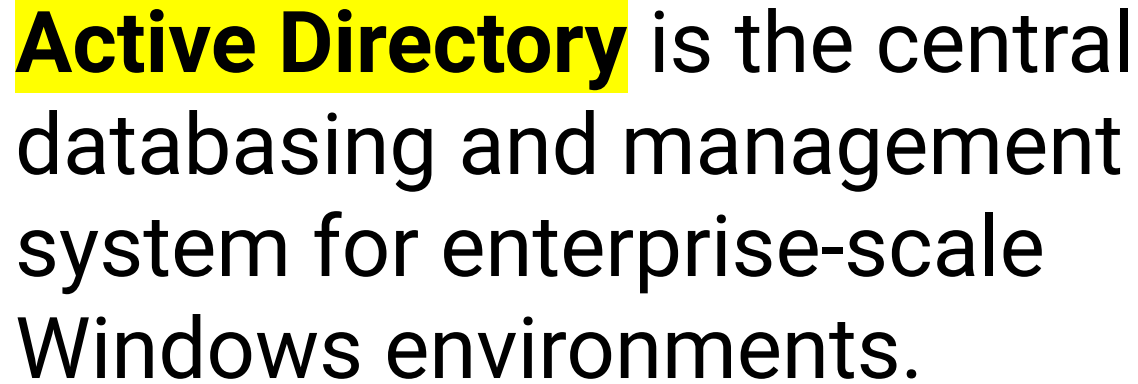
Use Active Directory tools to create organizational units, users, and groups.

Create and link Group Policy Objects that enforce domain-hardening policies.

Today, we're going to learn to manage the central databasing system for enterprise-scale Windows environments: **Active Directory Domain Services**, or **Active Directory (AD)**.

**Active Directory** is the central databasing and management system for enterprise-scale Windows environments.

Having a strong understanding of **Active Directory** is crucial for anyone working in Windows-based system administration and security.

# Active Directory

**Security analysts**

**Threat hunters**

**Forensics experts**

**Incidence responders**

Will all likely be required to know some Active Directory to be effective within their own organization or a client's.

**Penetration testing experts**

**Threat intelligence experts**

**Malware reverse engineering experts**

Will need to understand and leverage vulnerabilities to execute exploits in poorly implemented AD configurations.
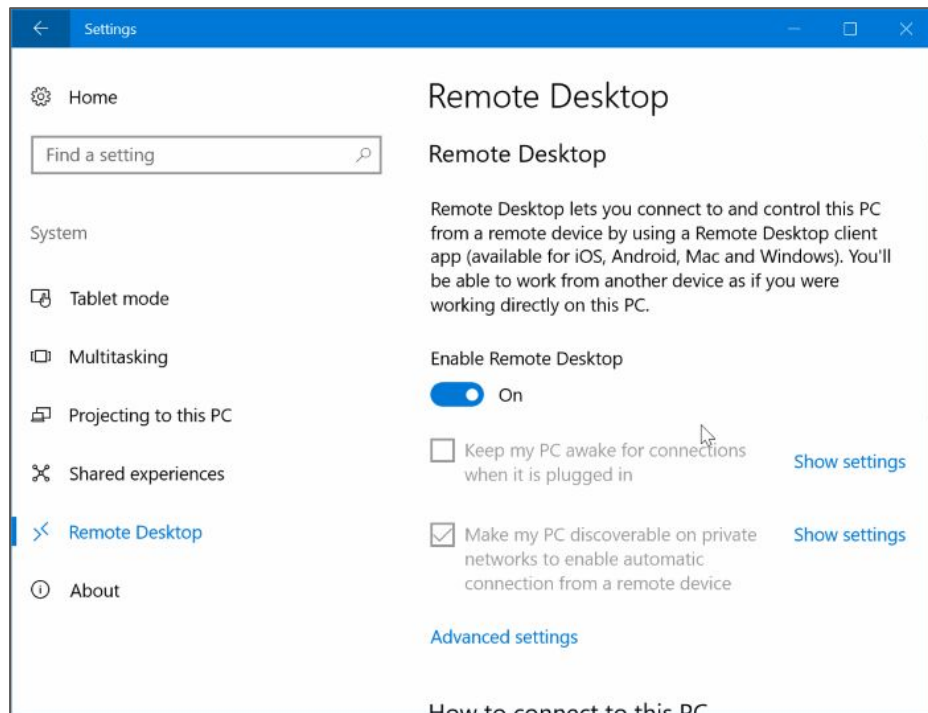
# Accessing the Lab

Before we can get started with Active Directory, we'll want to understand how it is set up and configured within our Windows Azure Lab environment.

If you have not already, take this time to log into your Windows RDP Host machine.

Then, start up and log into the nested virtual machines.
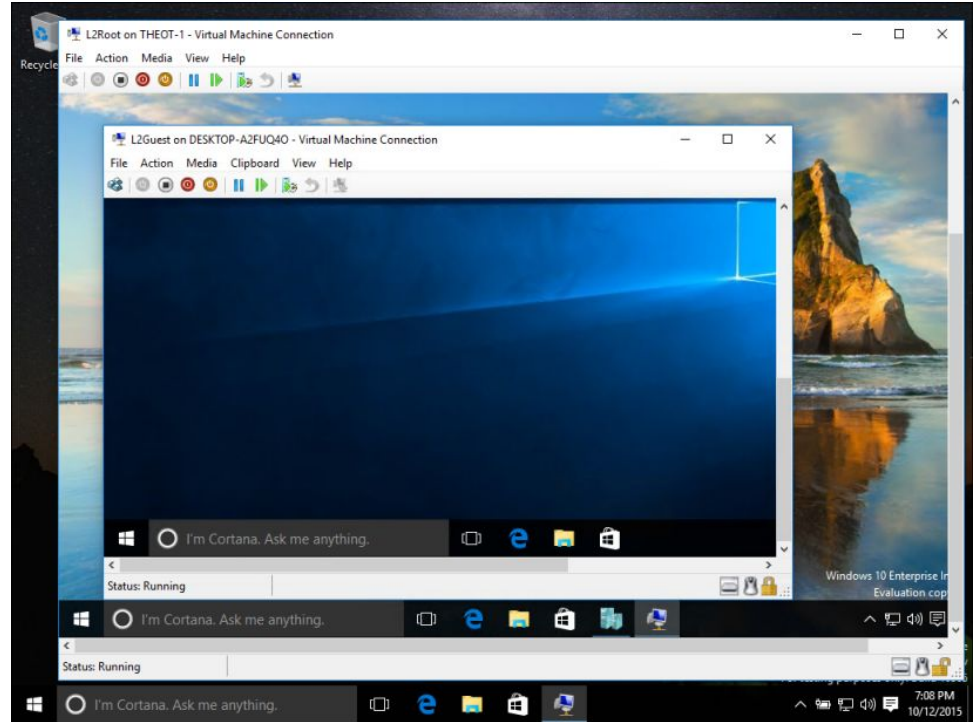
# The Machines

Within our Windows RDP Host machine we have two nested Hyper-V virtual machines:

**01** A **Windows 10 virtual machine** that has Windows 10 installed on it, just like our Windows RDP Host machine.

**02** A **Windows Server virtual machine** that has the Windows Server 2019 operating system installed.

# The Connectivity

Your Windows Azure Labs have already been set up with Active Directory Domain Services installed and configured.

The Windows Server machine has Active Directory set up on it with the domain, GoodCorp.net. This will be the domain that we will be managing.

We'll be using Active Directory to set up what are known as group policies on the Windows 10 machine.

The Windows Server machine is providing DNS for the Windows 10 machine.

# What Is Active Directory?

# What is AD?

Suppose a small startup with 20 employees receives a large amount of funding and adds 100 more employees to the company.

When the startup was small and scrappy, everyone helped each other out and had access to the same resources.

But for organizational and security reasons, the company now has to be stricter about resource access—ensuring everyone can access what they need, and not things they don't need.

| | | |
|---|---|---|
| **Accountant** | Needs access to | **Sensitive financial data** |
| **IT Team** | Needs access to | **Networking components like switches and routers** |
| **Everyone** | Needs access to | **Printers** |
| **Guests** | Should *not* have access to | **Network** |

# What is AD?

**Security principals**
are AD objects that can be authenticated, such as users and groups. Permissions can be assigned to Security Principals giving them only the access they need.

**Resources**
are the files, networking components, and printers that users need permission to access. Permissions depend on roles and responsibilities within the company.

| Security principals | | Resources |
|---|---|---|
| Accountant | Needs access to | Sensitive financial data |
| IT Team | Needs access to | Networking components like switches and routers |
| Everyone | Needs access to | Printers |
| Guests | Should *not* have access to | Network |
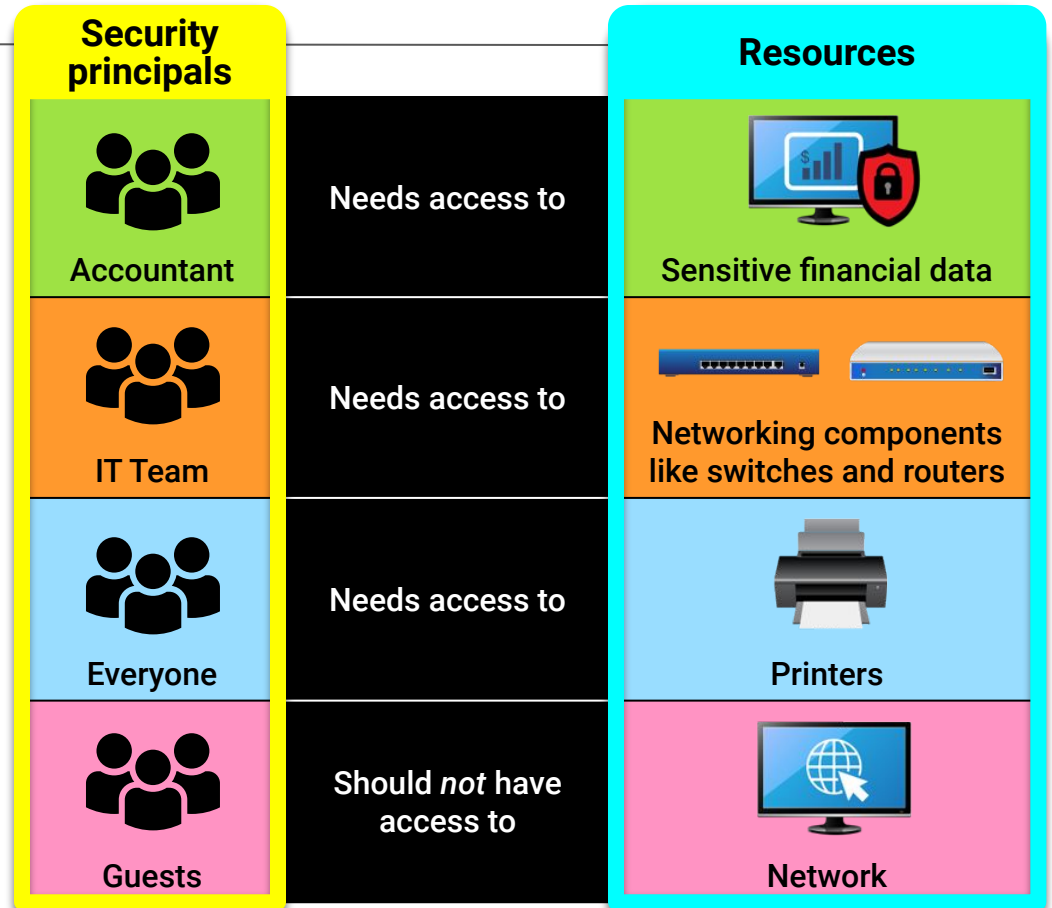
**Microsoft's Active Directory** is the system we use to manage these resources and security principals.

# What Exactly Is AD?

Active Directory is all the services that work together to manage **authentication** and **authorization** within a Windows Server network.

## Authentication

Allows users to prove their identity using a password, token, or biometric key.

## Authorization
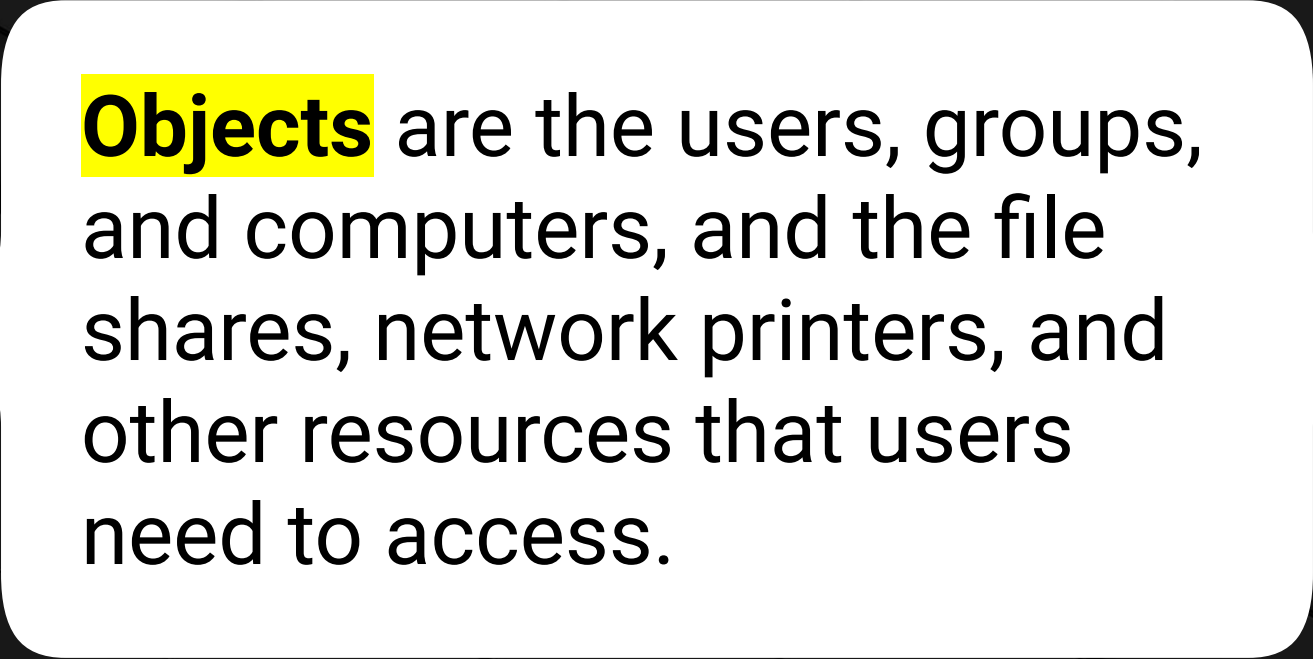
Provides or denies users permission to material.

Remember the principle of least privilege from the Linux SysAdmin units?

Active Directory understands an organization's resources and security principals as objects.

**Objects** are the users, groups, and computers, and the file shares, network printers, and other resources that users need to access.

# AD Architecture

**Active Directory** has a hierarchical structure of organizational units, users, machines, groups, domains, trees, and forests.



**Legend**

| | |
|---|---|
| ▲ | Domain |
| IT | IT Group |
| 👥 | Domain Administrator |
| ↔ | Trust |

Corp — Forest Root Domain

**Central IT Team**
- Enterprise Administrators
- Domain Administrators
- Schema Administrators

**Div 1 IT Team**
- Domain Administrators

**Div 2 IT Team**
- Domain Administrators

**Div 3 IT Team**
- Domain Administrators

Division 1

Division 2

Division 3
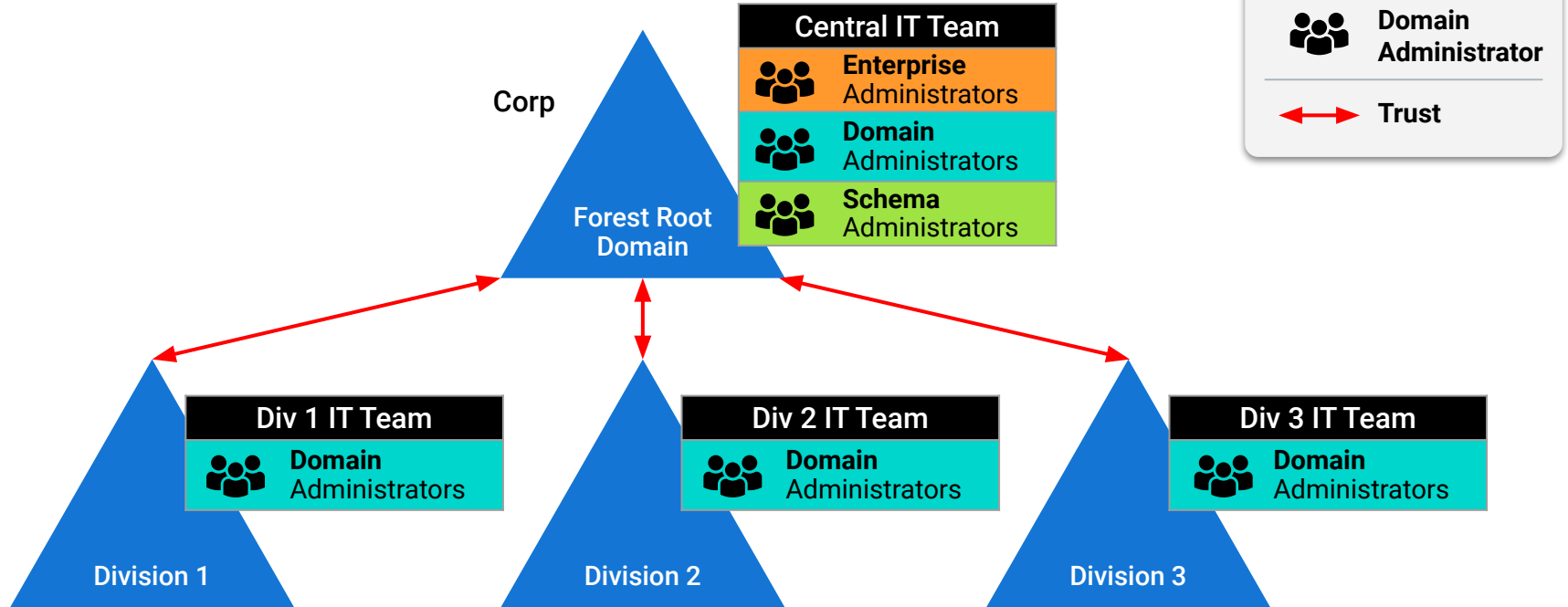
# AD Authentication

AD uses the following authentication protocols:

## LDAP
(Lightweight Directory Access Protocol)

A standardized protocol for adding, deleting, and editing objects. If Active Directory is a journal of information, LDAP is the pencil and eraser.

## Kerberos

A ticket-based authentication protocol, now the default authentication protocol for Windows Server domains. It provides direct encrypted sessions between users and networked resources.

## NTLM
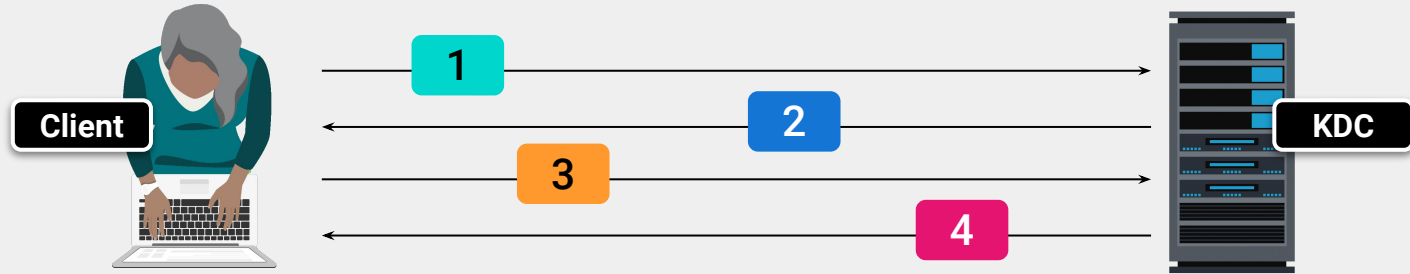(New Technology LAN Manager)

An authentication protocol that has become outdated because of pass the hash attacks.

We'll learn more about protocols in our Networking units, and will discuss these specific protocols during our Pentesting units.

# Kerberos Overview

Bob is attempting to access a networked file server:



**1**

Bob's Windows 10 machine sends a request to authenticate the **Key Distribution Center (KDC)**, seeking a **Ticket Granting Ticket (TGT)**.

A KDC has a database of valid credentials, an **Authentication Server** and a **Ticket Granting Server.**

**2**

Once his credentials are verified, Bob receives a TGT that allows him to request access to resources.

That TGT is cached and permits him to request more tickets for the current domain session.

**3**

When Bob attempts to access the file server, he sends the Ticket Granting Ticket to the Ticket Granting Server, requesting access to the file server.

**4**

The Key Distribution Center checks if the file server exists and if the TGT is valid. If it is, the KDC sends Bob an encrypted **service ticket** containing info he authenticated earlier, and a **session key**. Bob is then sent the encrypted service ticket and a copy of the session key.

# Kerberos Overview

Bob is attempting to access a networked file server:
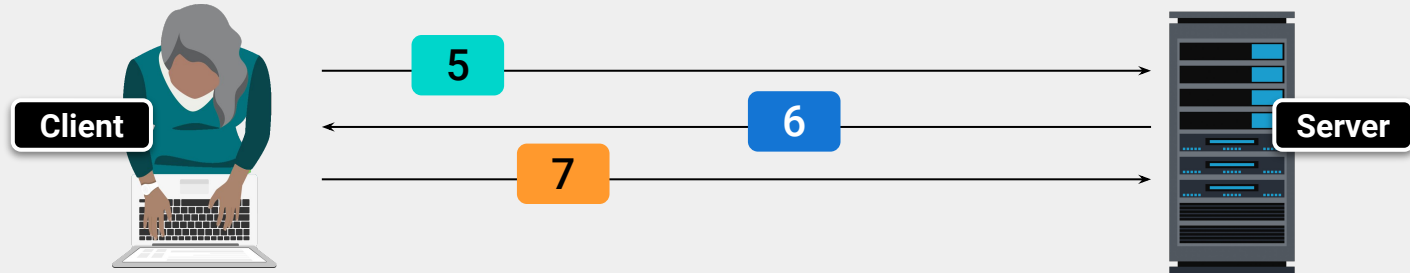


## 5

Bob then uses the session key to encrypt a new message containing his current information and send that, along with the service ticket, to the file server.

## 6

The file server then decrypts the service ticket containing the session key, and uses that session key to decrypt the message from Bob that contains his current information.

## 7

Finally, the file server uses the session key to encrypt a new message to be sent to Bob containing information about the file server.

If Bob's existing copy of the session key properly decrypts the message, the file server is verified.

# Creating OUs, Users, and Groups

Now that we've introduced Active Directory domain controller, we'll assign organizational units and groups.

**Organizational units (OUs)** are logical groupings of an organization's assets and accounts.

# Creating OUs, Users and Groups

For example:

- All of the computers in the sales department of our company should be grouped together in an organizational unit, which might be called `GC Users > Sales`.

- All of these computers would have the same policies, set by the group policies.

# Creating OUs, Users and Groups

In the following demo, we will:

**01** — Create a new domain organizational unit called GC Users.

**02** — Create a sub-OU called Marketing.

**03** — Create a user, Caroline, under the GC Users > Marketing OU.

**04** — Create a group, Marketing, under the GC Users > Marketing OU.

# Instructor Demonstration

## Creating Organizational Units

# Activity: Creating Domain OUs, Users, and Groups

For this activity, you will set up users, groups, and organizational units for your recently created domain.

Suggested Time:

20 Minutes

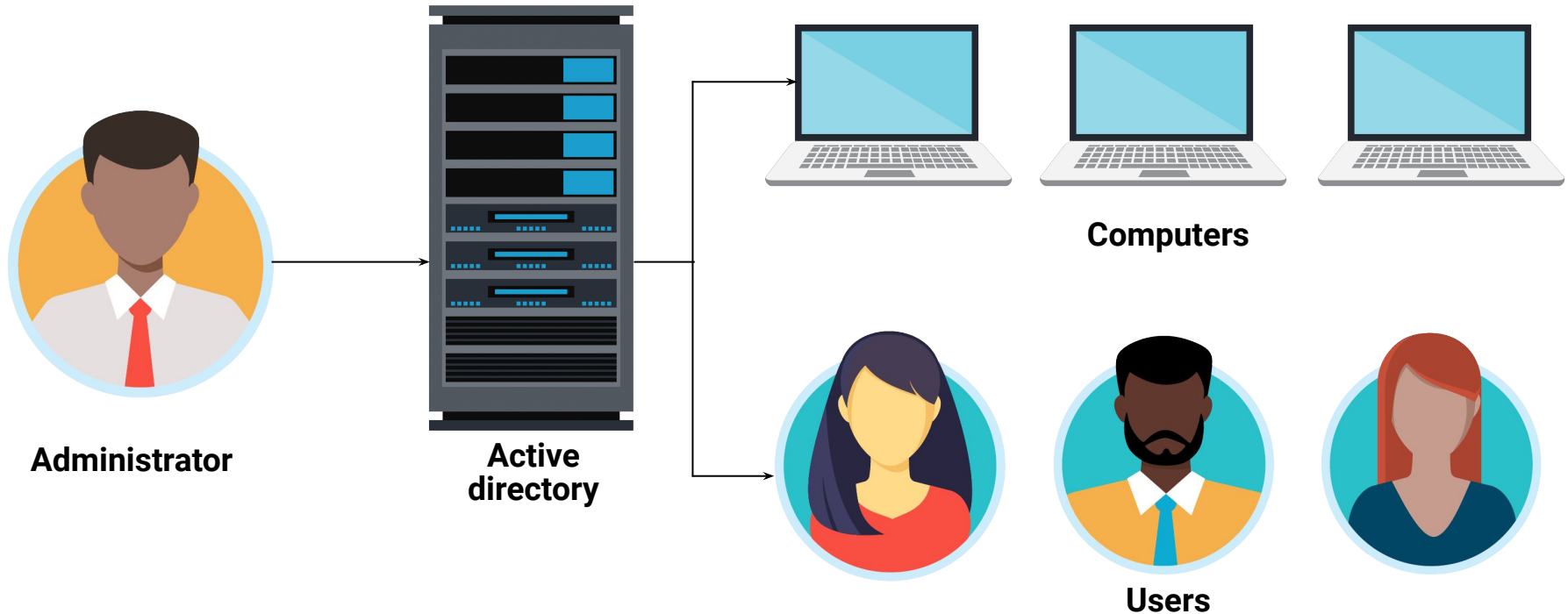# Time's Up! Let's Review.

Questions?

Countdown timer

# 15:00

(with alarm)

# Group Policy Objects

# Now that we have OUs, groups, and users, we can create **Group Policies** that enforce the principle of least privilege.



**Administrator**
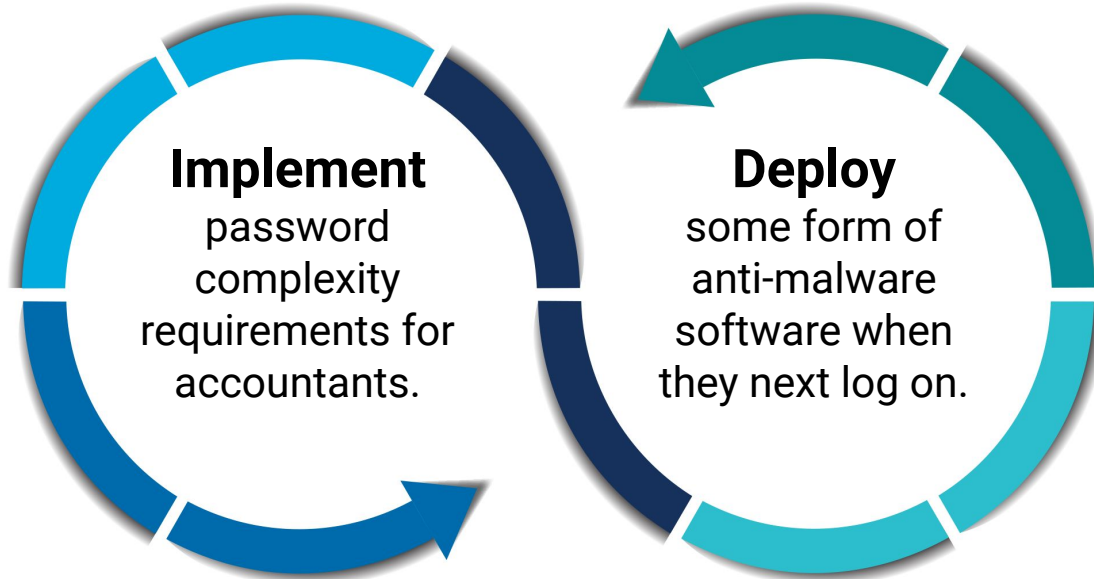
**Active directory**

**Computers**

**Users**

**Group Policy Objects (GPOs)** are packages of policy settings that contain one or more group policy.

# Group Policy Objects

GPOs are the basis of AD's policy management. For example, if we want to both:

**Implement**
password complexity requirements for accountants.

**Deploy**
some form of anti-malware software when they next log on.

We can combine these two policies into one GPO called `Better Password and Anti-Malware Setup` and apply it to all accountants in the OU.

# Group Policy Object Demo

In the following demo, we will:

**01** Create a Group Policy Object.

**02** Edit the individual policies for our Group Policy Object.

**03** Link the Group Policy Object to an organizational unit.

**04** Within the Windows 10 machine, retrieve the latest Active Directory changes.

**05** Verify if the GPO worked.

# Instructor Demonstration

## Creating Group Policy with Group Policy Objects

# Activity: Creating Group Policy with Group Policy Objects

In this activity, you will create Group Policy Objects to enforce policies for users.

Suggested Time:

25 Minutes

# Questions?

## ⚠️ Shut Down Your Machines ⚠️

Everyone must shut down their Hyper-V virtual machines and Windows RDP Host Machine.

You will need the remaining hours to complete your homework.

Questions?