AWS Directory Service is a managed service based on the cloud that allows us to create directories and let AWS experts handle and manage the other parts like high availability, monitoring, backups, recovery, and others.

There are three important components :

- Active Directory Service with Microsoft Active Directory
- Simple AD
- AD Connector

AWS managed Microsoft Active Directory

AWS Directory Service for Microsoft Active Directory is powered by an actual Microsoft Windows Server Active Directory (AD) in the AWS Cloud.

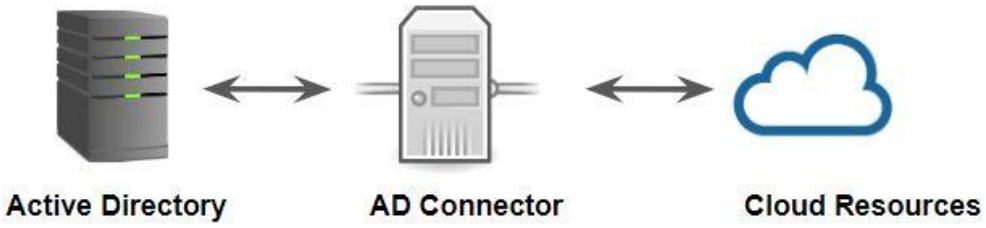
There are two types:

- Standard Edition -- For small and midsize (up to 5000 users)
- Enterprise Edition -- For larger deployments.

AD Connector

It is a proxy service that provides an easy way to connect applications in the cloud to your existing on-premise Microsoft AD.

When users log in to the applications, AD Connector forwards sign-in requests to your on-premises Active Directory domain controllers for authentication.



Simple AD

Simple AD is a Microsoft Active Directory–compatible directory from AWS Directory Service that is powered by Samba 4.

Simple AD supports basic Active Directory features such as user accounts, group memberships, joining a Linux domain or Windows-based EC2 instances, Kerberos-based SSO, and group policies. AWS provides monitoring, daily snapshots, and recovery as part of the service.

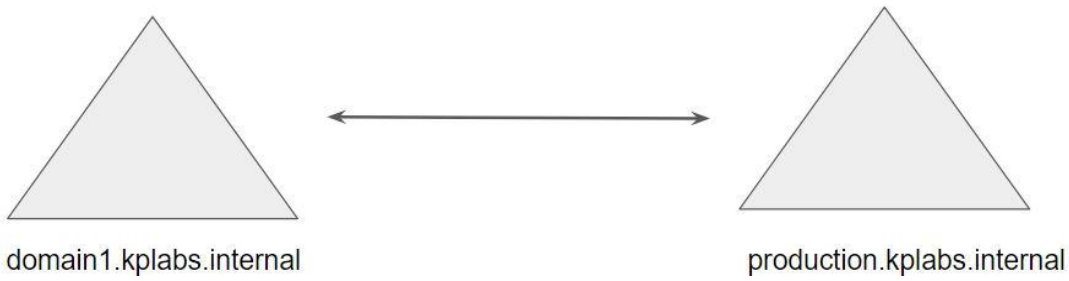
Simple AD does not support trust relationships, DNS dynamic update, schema extensions, multi-factor authentication, communication over LDAPS, PowerShell AD cmdlets, or FSMO role transfer.

Active Directory Trusts

In AD, domain to domain communication can occur through Trusts.

An AD DS trust is a secured, authentication communication channel between entities, such as AD DS domains.

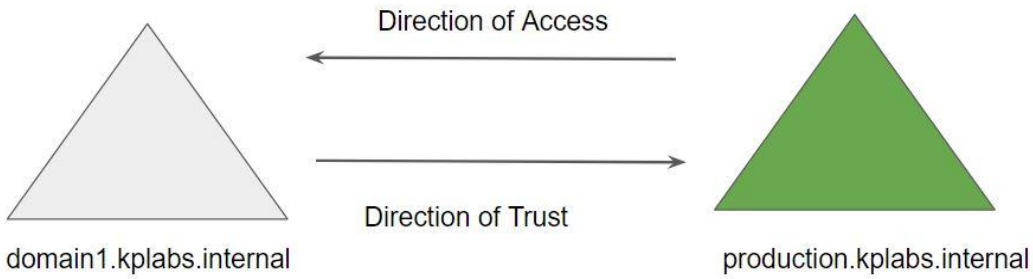
Trusts enable you to grant access to resources to users, groups, and computers across entities



Direction of Trust

Trust can either be one-way or two-way.
In a two-way trust, the domain from either side can access the other side.

In the following diagram, we have one-way trust.



Migrating AD Aware Workloads

If you already have an AD infrastructure and want to use it when migrating AD-aware workloads to the AWS Cloud, you can use AD trusts to connect AWS Microsoft AD (Standard Edition) to your existing AD.

This means your users can access AD-aware and AWS applications with their on-premises AD credentials, without needing you to synchronize users, groups, or passwords.