Student Guide

AWS Directory Service

Mentor: Naresh Adepu

https://www.linkedin.com/in/nareshgadepu/

📘 AWS Directory Service – Study Guide

(For AWS Solutions Architect Associate – SAA-C03)

---

1. 🌐 What is AWS Directory Service?

AWS Directory Service provides multiple ways to run Microsoft Active Directory (AD) in the AWS Cloud or connect AWS resources with your existing on-premises AD.

AD is used to manage **users, groups, computers, and authentication** in a centralized way.

---

2. 🏛 Why Use AWS Directory Service?

- Centralized user management for AWS workloads

- Seamless integration with **Windows EC2 instances**

- Support for **single sign-on (SSO)** with AWS IAM Identity Center

- Hybrid cloud integration (On-Prem AD + AWS)

- Enforce **security, compliance, and MFA**

---

3. ⚙️ The 3 Flavors of AWS Directory Service

1. AWS Managed Microsoft AD

- Fully managed AD in the AWS Cloud (built on Windows Server AD).

- Highly available across multiple AZs.

- Supports **multi-factor authentication (MFA)**.

- Can establish **trust relationships** with on-prem AD (but **no object sync**).

- Editions:

    o **Standard** – up to 30,000 objects

    o **Enterprise** – up to 500,000 objects

- Use case: Hybrid setups with on-prem AD, AWS workloads needing AD.

2. AD Connector

- Acts as a **proxy** between AWS services and on-prem AD.

- No directory data stored in AWS.

- All user management stays on-prem.

- Supports MFA.

- Two sizes:

    - Small (≤ 500 users)

    - Large (≤ 5,000 users)

- Use case: Reuse existing AD credentials for AWS without syncing or migrating.
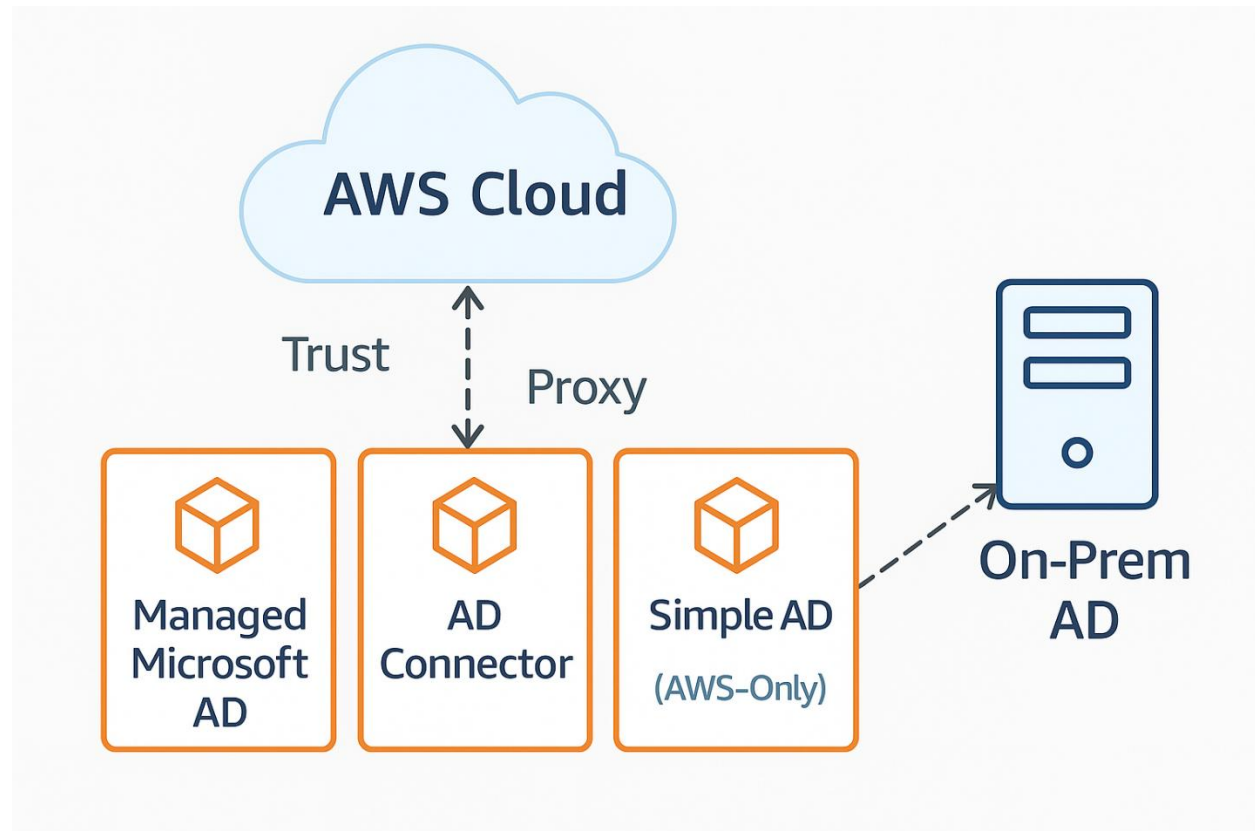
3. Simple AD

- AD-compatible directory powered by Samba.

- Standalone in AWS (not Microsoft AD).

- **No trust with on-prem AD**.

- Basic features only, lower cost.

- Use case: Small orgs, testing, when no on-prem AD exists.

4. 🔑 Key Exam Tips

- **Trust relationships**: Only AWS Managed Microsoft AD supports it.

- **Sync**: Not supported natively – use replication with self-managed AD.

- **AD Connector**: Just a proxy; nothing stored in AWS.

- **Simple AD**: Cannot integrate with on-prem; AWS-only.

- Editions matter → Standard vs Enterprise (know object limits).

5. 🖼 Visual Diagram

---

6. 🧪 Hands-On Lab (Step-by-Step)

Lab: Explore Directory Service Options

1. Login to AWS Console → Search **Directory Service**.

2. Click **Set up directory**.

3. Observe available options:

    o   AWS Managed Microsoft AD

    o   Simple AD

    o   AD Connector

    o   (Ignore Cognito user pool redirect).

4. Select **AWS Managed Microsoft AD** → Review editions (Standard vs Enterprise).

5. Explore **trust setup wizard** → See how to link with On-Prem AD.

6. Select **AD Connector** → Review size options (500 vs 5,000 users).

7. Select **Simple AD** → Note "no trust with on-prem".

✅ Outcome: You can now clearly identify the purpose and limitations of each option.

---

7. 📋 Mock Exam Questions

Q1. Which AWS Directory Service allows you to establish a trust with on-prem AD?

- A) Simple AD

- B) AD Connector

- C) AWS Managed Microsoft AD ✅

Q2. Your company wants to reuse on-prem AD credentials for AWS access without storing directory data in AWS. Which service fits?

- A) AWS Managed Microsoft AD

- B) AD Connector ✅

- C) Simple AD

Q3. Which Directory Service option is lowest cost and used when no on-prem AD exists?

- A) Simple AD ✅

- B) AD Connector

- C) AWS Managed Microsoft AD

---

8. 📝 Summary Cheat Sheet

- **Managed Microsoft AD** → Full AD in AWS + Trusts with on-prem.

- **AD Connector** → Proxy to on-prem AD, no storage in AWS.

- **Simple AD** → Lightweight standalone AD, AWS-only.