AWS Directory Services

AWS provides several directory types.

The following three types currently feature on the exam and will be covered on this page:

* Active Directory Service for Microsoft Active Directory.
* Simple AD.
* AD Connector.

As an alternative to the AWS Directory service you can build your own Microsoft AD DCs in the AWS cloud (on EC2).

* When you build your own you can join an existing on-premises Active Directory domain (replication mode).
* You must establish a VPN (on top of Direct Connect if you have it).
* Replication mode is less secure than establishing trust relationships.

The table below summarises the directory services covered on this page as well as a couple of others, and provides some typical use cases:

| **Directory Service Option** | **Description** | **Use Case** |
| --- | --- | --- |
| AWS Cloud Directory | Cloud-native directory to share and control access to hierarchical data between applications | Cloud applications that need hierarchical data with complex relationships |
| Amazon Cognito | Sign-up and sign-in functionality that scales to millions of users and federated to public social media services | Develop consumer apps or SaaS |
| AWS Directory Service for Microsoft Active Directory | AWS-managed full Microsoft AD running on Windows Server 2012 R2 | Enterprises that want hosted Microsoft AD or you need LDAP for Linux apps |
| AD Connector | Allows on-premises users to log into AWS services with their existing AD credentials. Also allows EC2 instances to join AD domain | Single sign-on for on-premises employees and for adding EC2 instances to the domain |
| Simple AD | Low scale, low cost, AD implementation based on Samba | Simple user directory, or you need LDAP compatibility |

## 

## **Active Directory Service for Microsoft Active Directory**

Fully managed AWS services on AWS infrastructure.

Best choice if you have more than 5000 users and/or need a trust relationship set up.

Includes software patching, replication, automated backups, replacing failed DCs and monitoring.

Runs on a Windows Server.

Can perform schema extensions.

Works with SharePoint, Microsoft SQL Server and .Net apps.

You can setup trust relationships to extend authentication from on-premises Active Directories into the AWS cloud.

On-premises users and groups can access resources in either domain using SSO.

Requires a VPN or Direct Connect connection.

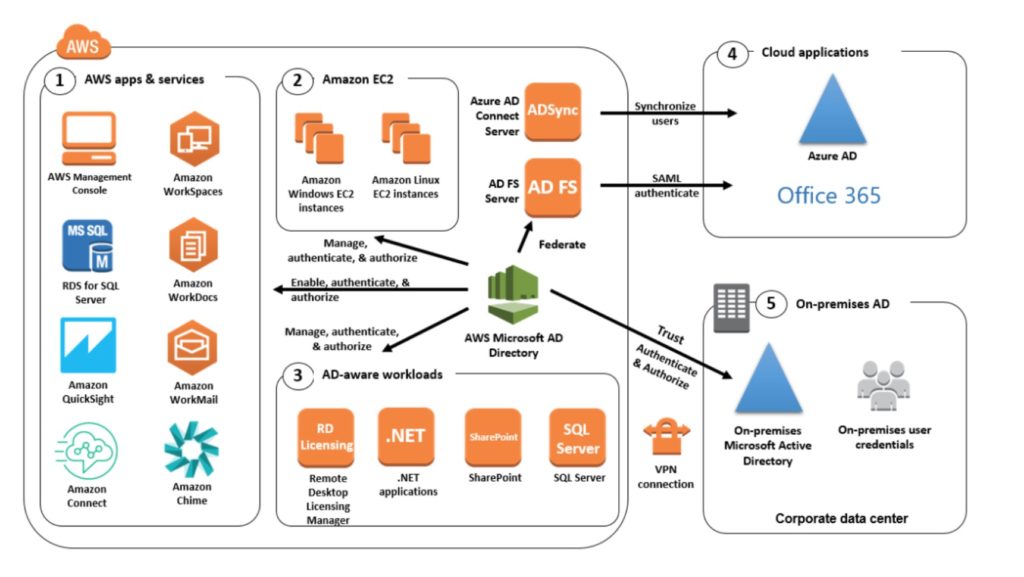
Can be used as a standalone AD in the AWS cloud.

When used standalone users can access 3rd party applications such as Microsoft O365 through federation.

You can also use Active Directory credentials to authenticate to the AWS management console without having to set up SAML authentication.

AWS Microsoft AD supports AWS applications including Workspaces, WorkDocs, QuickSight, Chime, Amazon Connect, and RDS for Microsoft SQL Server.

The following diagram shows some of the use cases for your AWS Microsoft AD directory, including the ability to grant your users access to external cloud applications and allow your on-premises AD users to manage and have access to resources in the AWS Cloud.



Includes security features such as:

* Fine-grained password policy management.
* LDAP encryption through SSL/TLS.
* HIPAA and PCI DSS approved.
* Multi-factor authentication through integration with existing RADIUS-based MFA infrastructure.

Monitoring provided through CloudTrail, notifications through SNS, daily automated snapshots.

Scalable service that scales by adding Domain Controllers.

Deployed in a HA configuration across two AZs in the same region.

AWS Microsoft AD does not support replication mode where replication to an on-premises AD takes place.

Two editions:

* Standard Edition is optimized to be a primary directory for small and midsize businesses with up to 5,000 employees. It provides you enough storage capacity to support up to 30,000 directory objects, such as users, groups, and computers.
* Enterprise Edition is designed to support enterprise organizations with up to 500,000 directory objects.

Directory Sharing:

* AWS Directory Service for Microsoft Active Directory allows you to use a directory in one account and share it with multiple accounts and VPCs.
* There is an hourly sharing charge for each additional account to which you share a directory.
* There is no sharing charge for additional VPCs to which you share a directory, or for the account in which you install the directory.

## **Simple AD**

An inexpensive Active Directory-compatible service with common directory features.

Standalone, fully managed, directory on the AWS cloud.

Simple AD is generally the least expensive option.

Best choice for less than 5000 users and don’t need advanced AD features.

Powered by SAMBA 4 Active Directory compatible server.

Can create users and control access to applications on AWS.

Provides a subset of the features provided by AWS MS AD.

Features include:

* Manage user accounts.
* Manage groups.
* Apply group policies.
* Securely connect to EC2 instances.
* Kerberos-based SSO.
* Supports joining Linux or Windows based EC2 instances.

AWS provides monitoring, daily snapshots, and recovery services.

Manual snapshots possible.

Simple AD is compatible with WorkSpaces, WorkDocs, Workmail and QuickSight.

You can also sign on to the AWS management console with Simple AD user accounts to manage AWS resources.

Available in two editions:

* Small – supports up to 500 users (approximately 2000 objects).
* Large – supports up to 5000 users (approximately 20,000 objects).

AWS creates two directory servers and DNS servers on two different subnets within an AZ.

Simple AD does not support:

* DNS dynamic updates.
* Schema extensions.
* Multi-factor authentication.
* Communication over LDAPS.
* PowerShell AD cmdlets.
* FSMO role transfer.

Not compatible with RDS SQL server.

Does not support trust relationships with other domains (use AWS MS AD).

## **AD Connector**

AD Connector is a directory gateway for redirecting directory requests to your on-premises Active Directory.

AD Connector eliminates the need for directory synchronization and the cost and complexity of hosting a federation infrastructure.

Connects your existing on-premises AD to AWS.

Best choice when you want to use an existing Active Directory with AWS services.

AD Connector comes in two sizes:

* Small – designed for organizations up to 500 users.
* Large – designed for organizations up to 5000 users.

The VPC must be connected to your on-premises network via VPN or Direct Connect.

When users log in to AWS applications AD connector forwards sign-in requests to your on-premises AD DCs.

You can also join EC2 instances to your on-premises AD through AD Connector.

You can also login to the AWS Management Console using your on-premises AD DCs for authentication.

Not compatible with RDS SQL.

You can use AD Connector for multi-factor authentication using RADIUS-based MFA infrastructure.

## 

## **AD Connector vs Simple AD**

The table below describes some of the key differences to consider when choosing AD Connector or Simple AD:

| **AD Connector** | **Simple AD** |
| --- | --- |
| Must have an existing AD | Standalone AD based on Samba |
| Existing AD users can access AWS assets via IAM roles | Supports user accounts, groups, group policies, and domains |
| Supports MFA via existing RADIUS-based MFA infrastructure | Kerberos-based SSO |
|  | MFA not supported |
|  | Trust relationships not supported |

### **Related posts:**

* ****