DevOps

[Active Directory 2](#_Toc193686989)

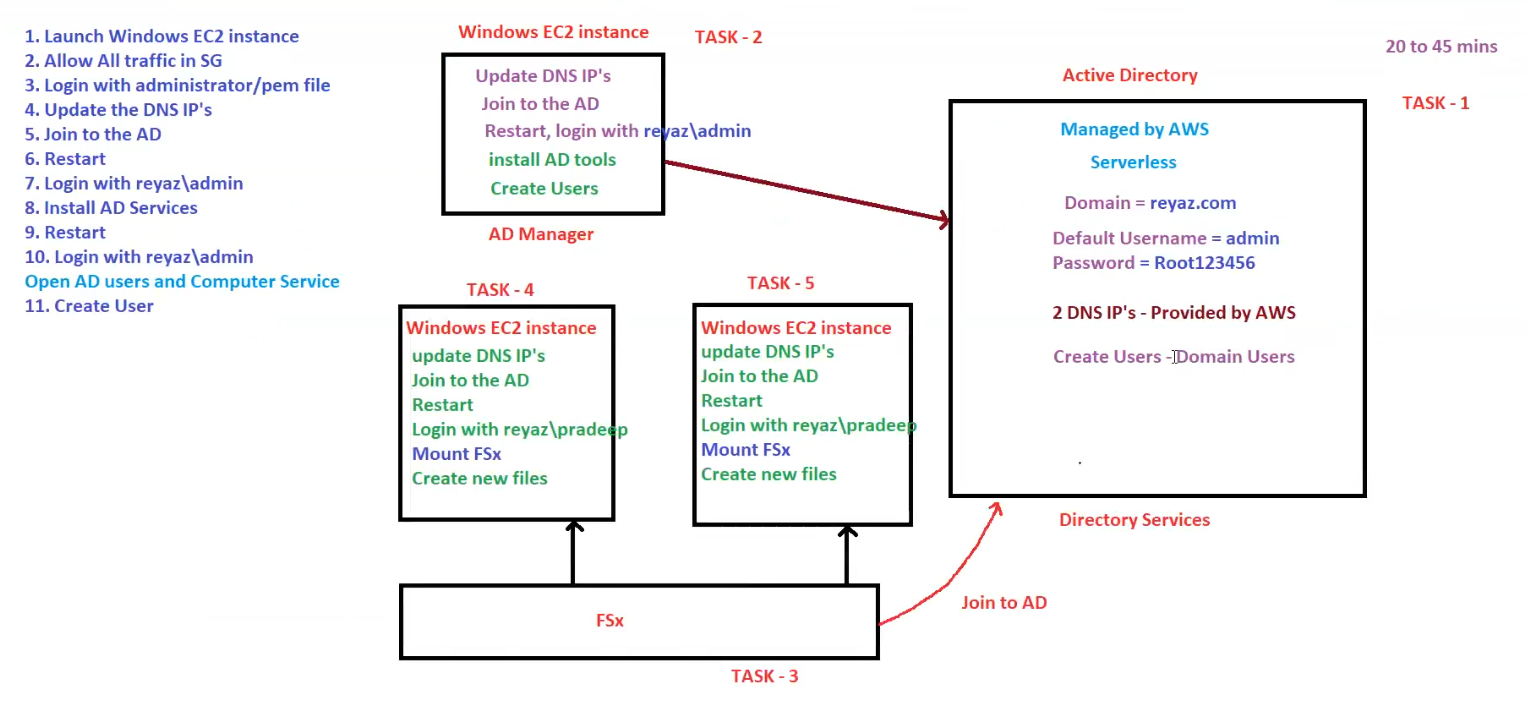
[AWS FSx and Active Directory Setup Guide 2](#_Toc193686990)

[AWS Active Directory & FSx Integration Guide 4](#_Toc193686991)

[Hybrid Active Directory 6](#_Toc193686992)

# Active Directory

## AWS FSx and Active Directory Setup Guide



Here are the structured notes based on the provided diagram:

**AWS FSx and Active Directory Setup Guide**

This guide outlines the process of integrating **AWS Managed Active Directory (AD)** with **Windows EC2 instances** and **FSx file system**, following a structured step-by-step approach.

**1. Active Directory (AD) Setup (TASK - 1)**

**AWS Managed Active Directory Configuration**

* **Managed by AWS** (Serverless)
* **Domain Name**: reyaz.com
* **Default Username**: admin
* **Default Password**: Root123456
* **DNS IPs**: Provided by AWS (2 IPs)
* **User Creation**: Domain Users

**Estimated Time:** 20 to 45 minutes

**2. Configure AD Manager Instance (TASK - 2)**

**Steps to Set Up Windows EC2 as AD Manager**

1. **Launch a Windows EC2 Instance**.
2. **Allow All Traffic** in Security Groups (SG).
3. **Login** using administrator credentials or .pem file.
4. **Update DNS IPs** (Use the AWS-provided DNS IPs).
5. **Join the Instance to the AD**.
6. **Restart the Instance**.
7. **Login** using reyaz\admin.
8. **Install AD Tools and Services**.
9. **Restart the Instance Again**.
10. **Login** using reyaz\admin.
11. **Open AD Users and Computers Service**.
12. **Create Users**.

**3. Configure FSx (TASK - 3)**

**Steps to Set Up FSx**

1. **Launch FSx Service** in AWS.
2. **Join FSx to Active Directory (AD)**.

**4. Configure Windows EC2 Instance for FSx (TASK - 4)**

**Steps to Integrate Windows EC2 with FSx**

1. **Launch a Windows EC2 Instance**.
2. **Update the DNS IPs** (Set to AWS AD-provided DNS).
3. **Join the Instance to the AD**.
4. **Restart the Instance**.
5. **Login using a domain user** (reyaz\pradeep).
6. **Mount the FSx Storage**.
7. **Create and Manage Files on FSx**.

**5. Configure Additional Windows EC2 Instances for FSx (TASK - 5)**

**Steps to Configure Additional Windows Instances**

1. **Launch another Windows EC2 Instance**.
2. **Update the DNS IPs**.
3. **Join the Instance to the AD**.
4. **Restart the Instance**.
5. **Login using reyaz\pradeep**.
6. **Mount FSx**.
7. **Create and Manage Files on FSx**.

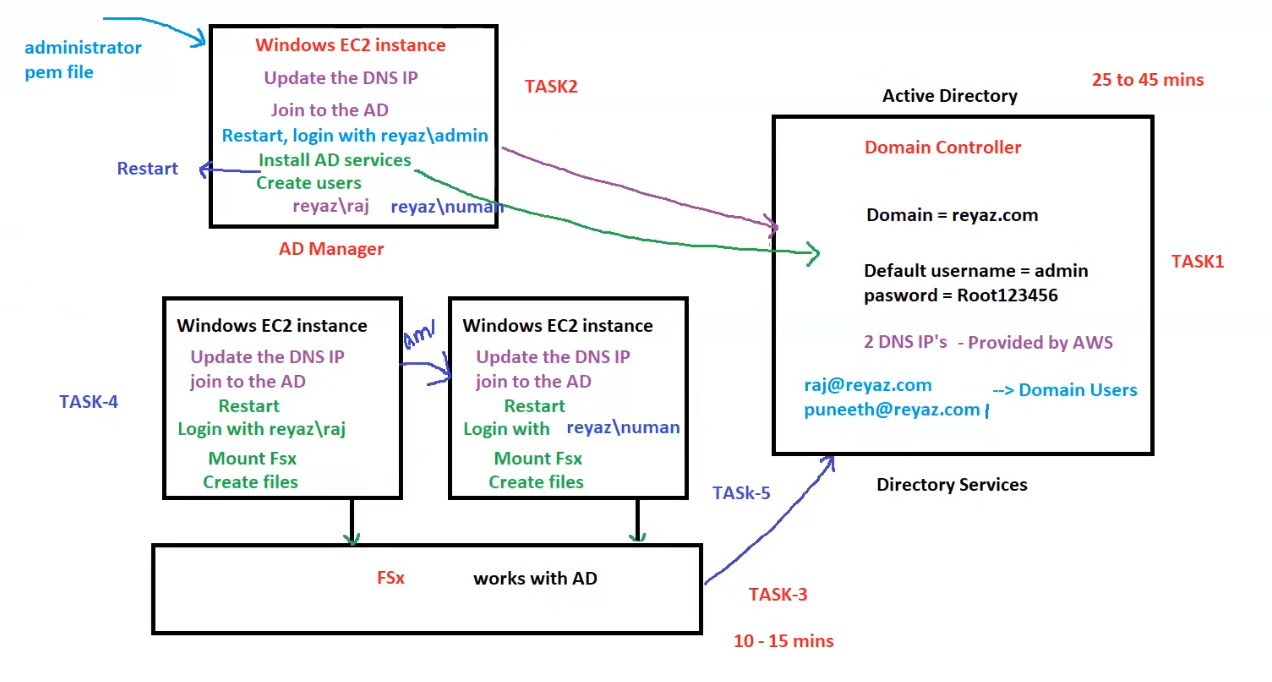
**6. Summary of Workflow**

1. **Active Directory is set up on AWS.**
2. **Windows EC2 instances are joined to the AD.**
3. **FSx is created and linked to AD.**
4. **Users and permissions are managed via AD.**
5. **Windows EC2 instances mount FSx for shared file storage.**

**Conclusion**

This setup enables a **centralized authentication system using AWS Managed Active Directory** while leveraging **AWS FSx for scalable file storage**. It ensures that **Windows instances authenticate through AD and share files using FSx**.

## AWS Active Directory & FSx Integration Guide



**AWS Active Directory & FSx Integration Guide**

This guide outlines the **integration of AWS Managed Active Directory (AD) with Windows EC2 instances and FSx** to enable centralized authentication and shared storage.

**1. Active Directory Setup (TASK - 1)**

**AWS Managed Active Directory Configuration**

* **Domain Controller**: reyaz.com
* **Default Username**: admin
* **Password**: Root123456
* **DNS IPs**: Provided by AWS (2 IPs)
* **Users Created**:
  + raj@reyaz.com
  + puneeth@reyaz.com

**Estimated Time:** **25 to 45 minutes**

**2. Configure AD Manager (TASK - 2)**

**Steps to Set Up the AD Manager Instance**

1. **Launch a Windows EC2 Instance**.
2. **Login using administrator or .pem file**.
3. **Update the DNS IPs** (Set to AWS-provided DNS).
4. **Join the Instance to AD**.
5. **Restart the Instance**.
6. **Login using reyaz\admin**.
7. **Install AD Services**.
8. **Create Users**:
   * reyaz\raj
   * reyaz\numan

**3. Set Up FSx (TASK - 3)**

**Steps to Configure FSx**

1. **Launch AWS FSx Service**.
2. **Join FSx to Active Directory**.

**Estimated Time:** **10 - 15 minutes**

**4. Configure Windows EC2 Instance for FSx (TASK - 4)**

**Steps to Integrate Windows EC2 with FSx**

1. **Launch a Windows EC2 Instance**.
2. **Update the DNS IPs**.
3. **Join the Instance to AD**.
4. **Restart the Instance**.
5. **Login using reyaz\raj**.
6. **Mount FSx Storage**.
7. **Create & Manage Files on FSx**.

**5. Configure Additional Windows EC2 Instance (TASK - 5)**

**Steps to Configure Another Windows Instance**

1. **Launch another Windows EC2 Instance**.
2. **Update the DNS IPs**.
3. **Join the Instance to AD**.
4. **Restart the Instance**.
5. **Login using reyaz\numan**.
6. **Mount FSx Storage**.
7. **Create & Manage Files on FSx**.

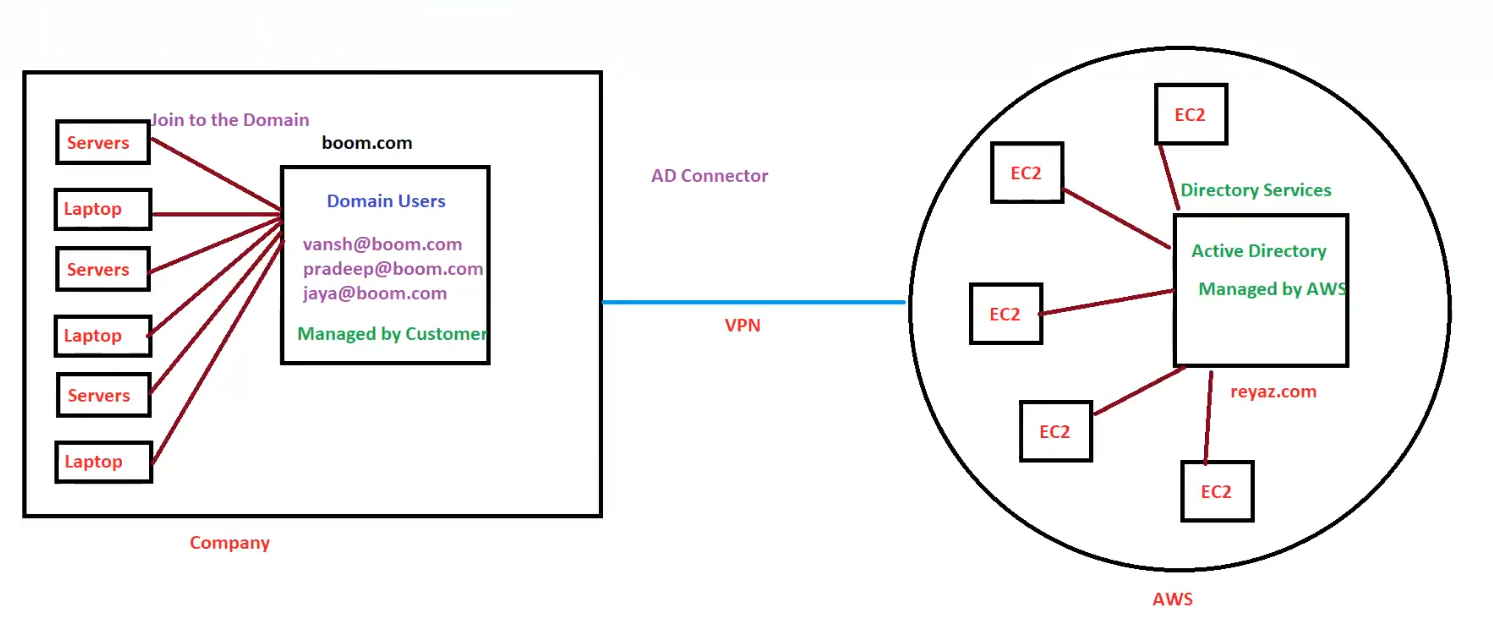
**6. Summary of Workflow**

1. **Active Directory is set up on AWS** to manage domain authentication.
2. **Windows EC2 instances are joined to the AD** to enable centralized user management.
3. **FSx is created and linked to AD** for shared storage access.
4. **Users authenticate through AD** and access FSx via domain credentials.
5. **Multiple Windows EC2 instances mount FSx for seamless file storage and collaboration.**

**Conclusion**

This setup **centralizes authentication via AWS Managed Active Directory** while enabling **shared storage with AWS FSx**, ensuring security, scalability, and ease of management.

## Hybrid Active Directory



Here are the structured notes based on the provided diagram:

**Hybrid Active Directory (AD) Setup using AWS AD Connector**

This architecture integrates **an on-premises Active Directory (AD)** with **AWS Managed Active Directory (MAD)** using an **AWS AD Connector and VPN**.

**1. On-Premises Active Directory (Company Side)**

* **Domain Name**: boom.com
* **Managed By**: Customer (On-prem IT Team)
* **Domain Users**:
  + vansh@boom.com
  + pradeep@boom.com
  + jaya@boom.com
* **Connected Devices**:
  + Multiple **Servers** and **Laptops** joined to the domain.
* **Purpose**:
  + Centralized authentication for on-premises users and devices.
  + Extends authentication to AWS resources.

**2. AWS Managed Active Directory (AWS Side)**

* **Domain Name**: reyaz.com
* **Managed By**: AWS
* **Resources Connected**:
  + Multiple **EC2 Instances** authenticate against the AWS MAD.
* **Directory Services**:
  + Provides authentication, authorization, and user management for AWS workloads.

**3. AD Connector & VPN Setup**

* **AD Connector**:
  + Acts as a bridge between **on-premises AD** (boom.com) and **AWS Managed AD** (reyaz.com).
  + Allows AWS services to authenticate users using **on-premises credentials**.
* **VPN**:
  + Establishes a **secure connection** between the on-prem network and AWS.
  + Ensures seamless communication between **on-prem servers/laptops** and **AWS resources**.

**4. Summary of Workflow**

1. **On-Prem Users (boom.com)**:
   * Employees use **on-prem AD credentials** for authentication.
   * They can log in to on-prem **laptops, servers, and applications**.
2. **AD Connector & VPN**:
   * Extends **on-prem AD authentication** to AWS.
   * Allows **AWS EC2 instances** to authenticate against the on-prem AD without duplicating identities.
3. **AWS Managed AD (reyaz.com)**:
   * Manages **AWS-specific authentication** for EC2 instances and other AWS services.

**5. Benefits of This Setup**

✅ **Single Sign-On (SSO)**: Users authenticate once and access both on-prem and AWS resources.  
✅ **No Need to Migrate AD**: Keeps existing on-prem AD while extending authentication to AWS.  
✅ **Enhanced Security**: Uses **VPN for a secure connection** and AWS **AD Connector** for authentication.  
✅ **Simplified Access Control**: Centralized user management without duplicating identities in AWS.

**Conclusion**

This **hybrid Active Directory setup** enables organizations to leverage AWS services while maintaining their existing **on-premises identity management**. It ensures **secure, seamless authentication across both environments**.