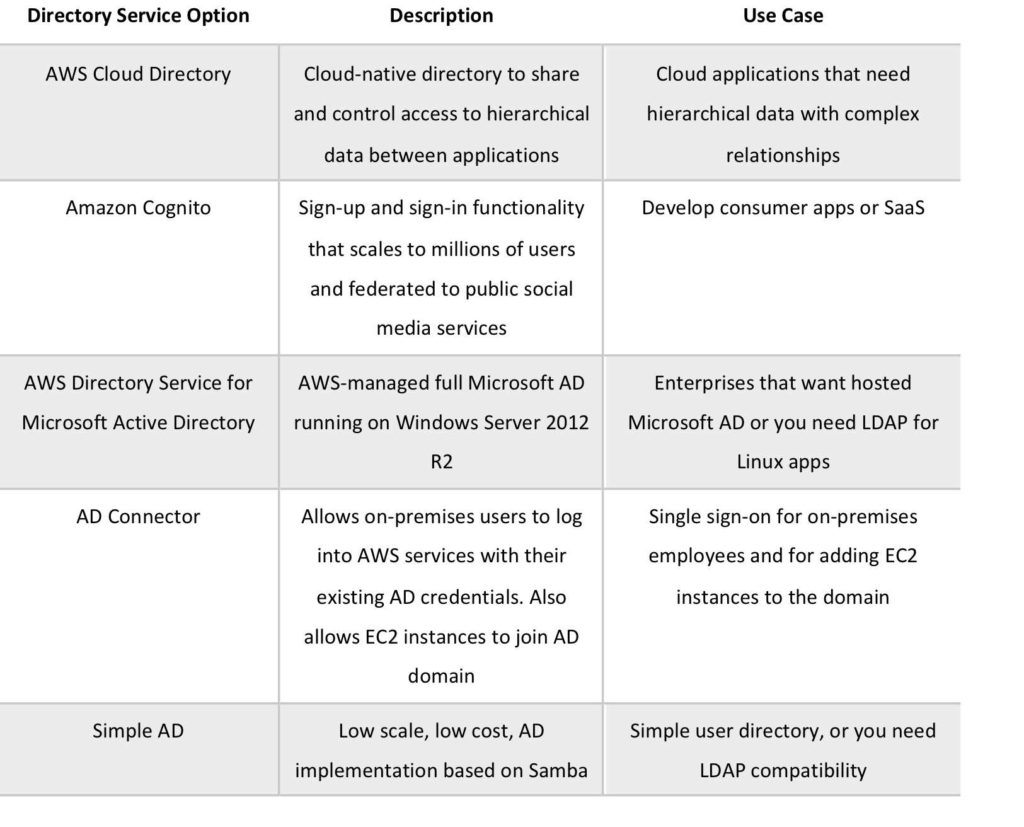
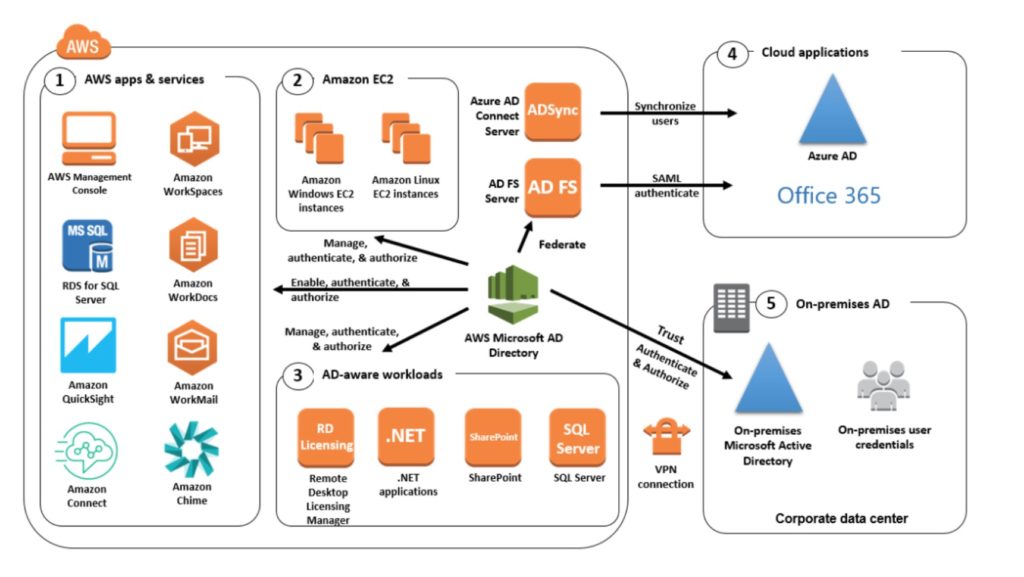
**Directory Service**

* AWS provides many directory types. Three important ones are
  + 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-premise AD domain(replication mode)
  + You must establish a VPN (on top of DC if you have it)
  + Replication mode is less secure than establishing trust relationships
* 
* **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 to 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, SQL Server and .NET apps
  + You can setup trust relationships to extend authentication from on-premises AD’s to the cloud
  + On-premise users and groups can access resources in either domain using SSO
  + Requires a VPN or DC connection
  + Can be used as a standalone AD
  + When used standalone users can access 3rd party applications such as Microsoft O365 through federation
  + You can also use AD 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 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
    - Fine-grained password policy management
    - LDQP encryption through SSL/TLS
    - HIPAA and PCI DSS approved
    - MFA through integration with existing RADIUS-based mFA infrastructure
    - Monitoring provided through CT, notifications through SNS, daily automated snapshots
    - Scalable service that scales by adding Domain Controllers
    - Deployed in HA configuration across two Azs in the same region
    - Microsoft AD does not support replication mode where replication to an on-premise 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 AD 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 AD-compatible service with common directory features
    - Standalone, fully managed, directory in the AWS cloud
    - Aimple 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 AD 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
      * Kuberos-based SSO
      * Supports joining Linux or Windows based EC2 instances
    - AWS provides monitoring, daily snapshots and recovery services. Manual snapshots possible
    - Aimple 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
      * MFA
      * 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-premise AD
    - AD Connector eliminates the need for directory synchronization and the cost of complexity of hosting a federation infrastructure
    - Connects your existing on-premise AD to AWS
    - Best choice when you want to use an exissting AD with AWS services
    - AD Connector comes in two sizes:
      * Small – designed for organizations with up to 500 users
      * Large – designed for organizations with up to 5000 users
    - The VPC must be connected to your on-premise network via VPN or Direct Connect
    - When users log into AWS applications AD connector forwards sign-in requests to your on-premise AD DCs
    - You can also join EC2 instances to your on-premise AD through AD Connector
    - You can also login to the AWS Management Console using your on-premise AD DCs for authentication
    - Not compatible with RDS SQL
    - You can use AD Connector for MFA using RADIUS-based MFA infrastructure
  + **AD Connector vs Simple AD**
* 