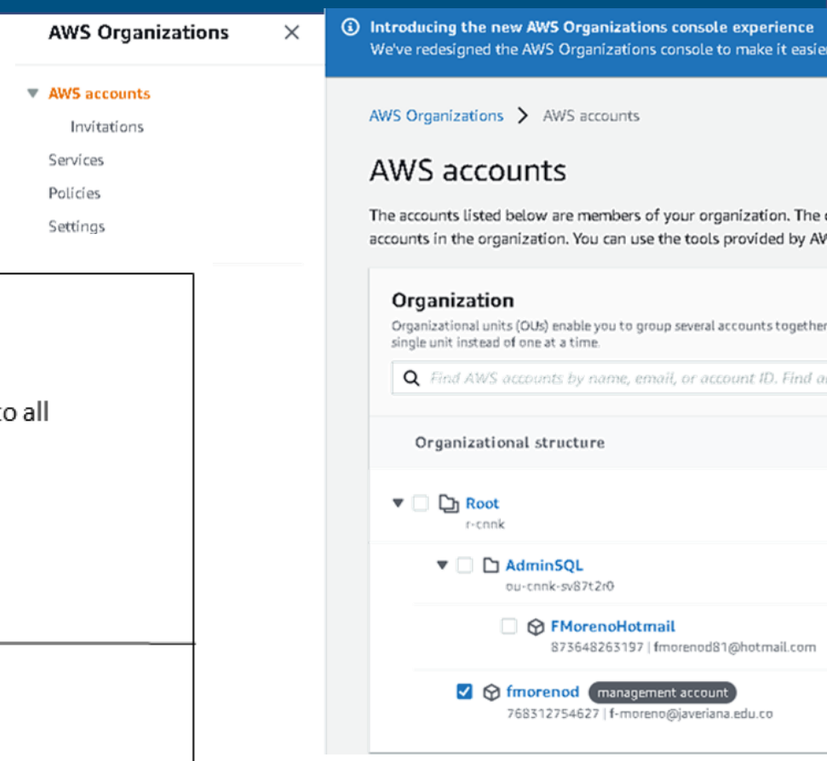
AWS Solutions Architect Associate

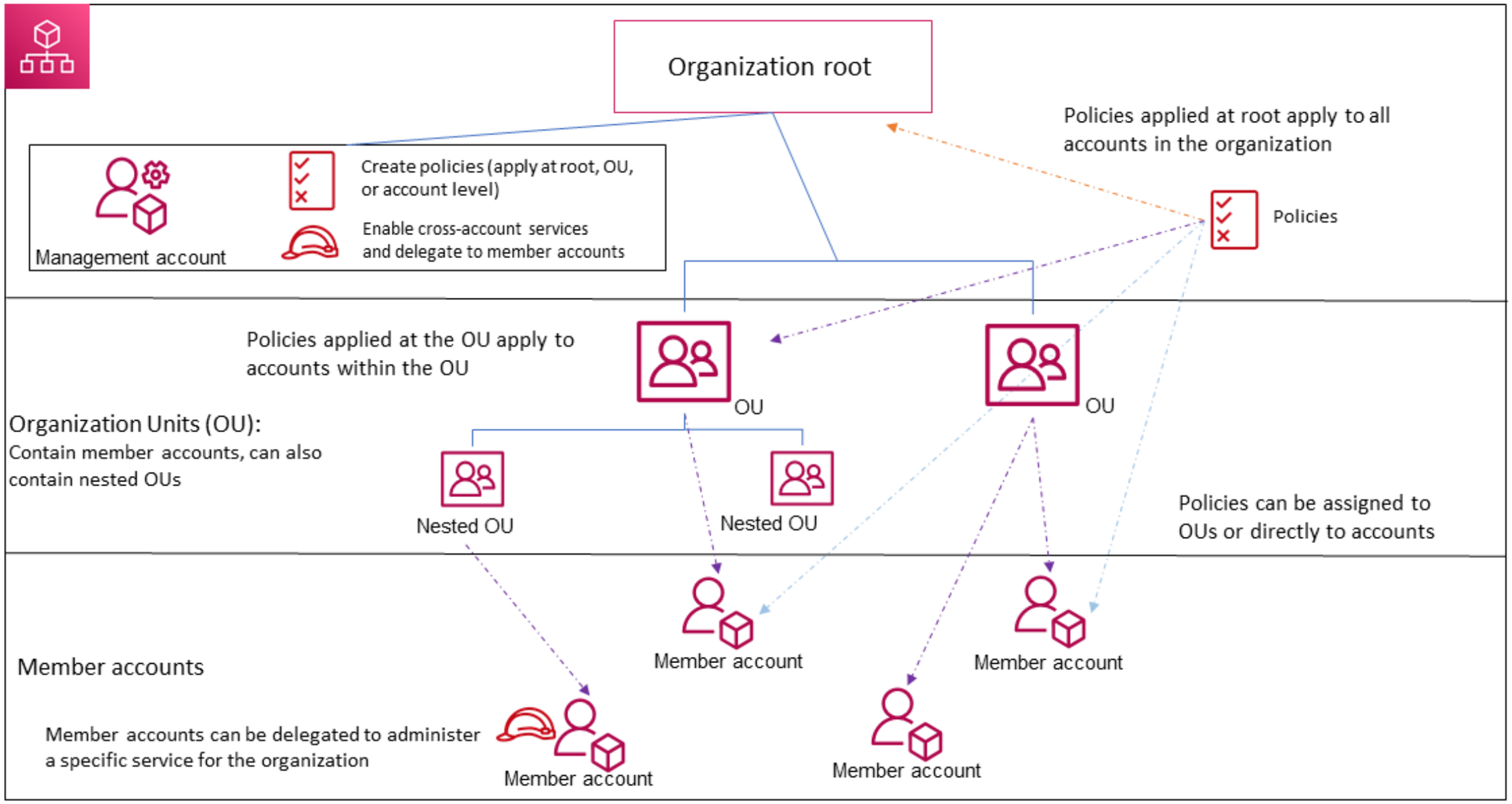
Session 202

Security, Id &Compliance: Organizations, Directory Services, Single SignOn and Cognito

July/2024

AWS Organizations



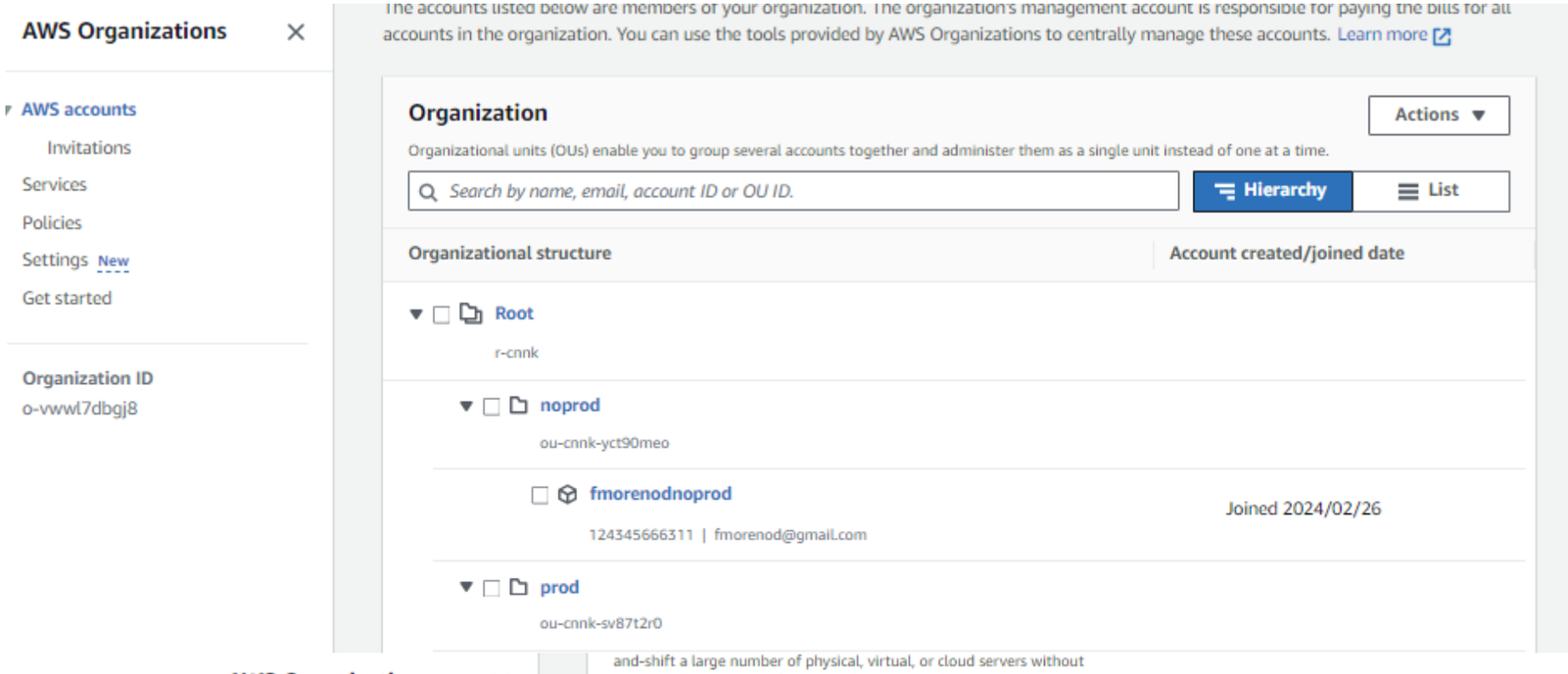


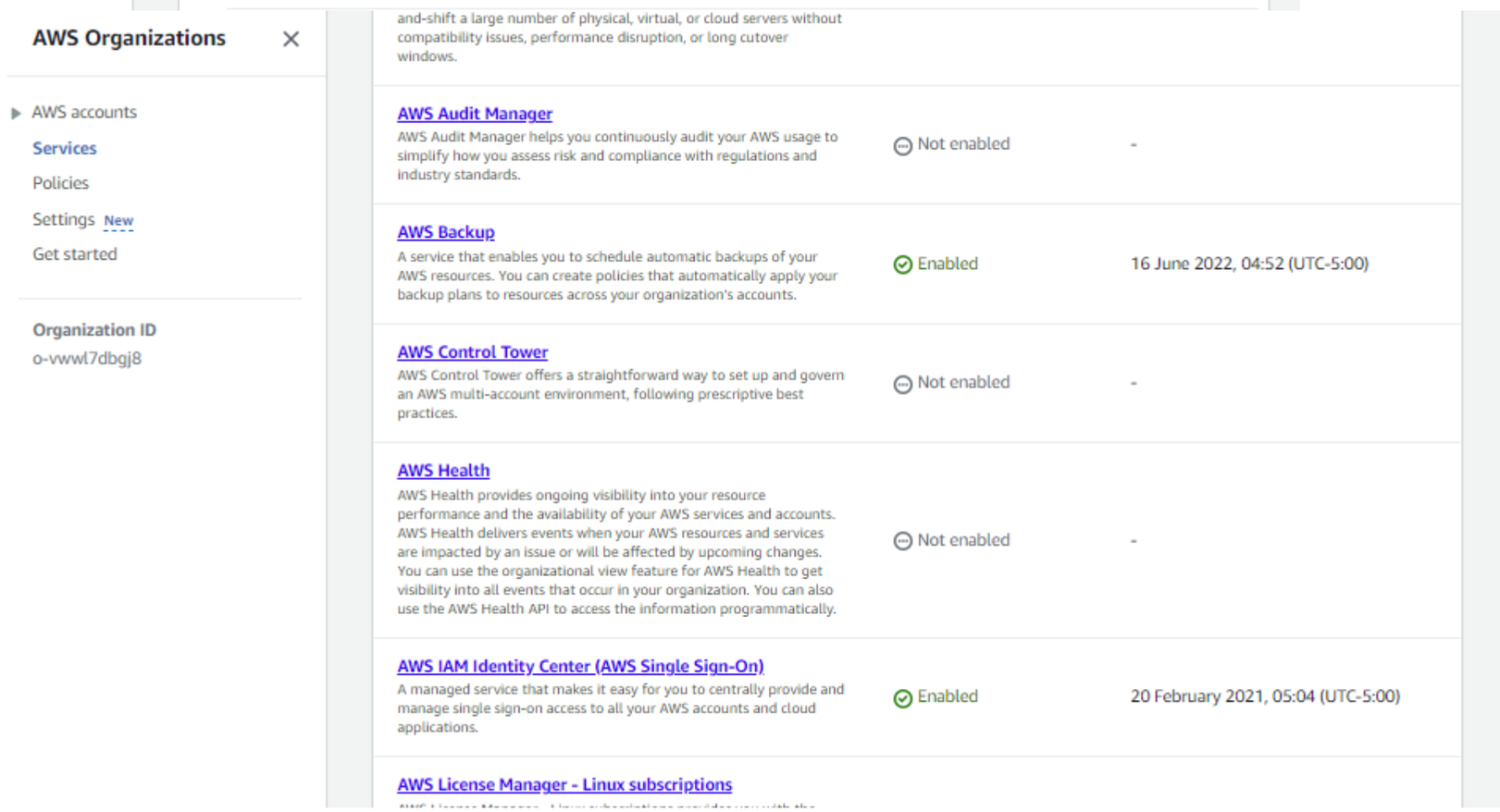
Centralized Government/2 Modes: Billing Only and ALL Features (Billing and SCP). **Inheritance.**
Invitations: Handshake.
Relation Member-to-Organization is 1:1
Free! You only pay by consumed resources on Accounts.

Services:
AI services opt-out policy
Tag Policies
Backup Policies
Service Control Policy - SCP

Taken from https://docs.aws.amazon.com/organizations/latest/userguide/orgs_getting-started_concepts.html (12/07/2024)

Services through AWS Organizations





Like 15 services that works on all accounts.
For instance:
RAM – Resource Manager Access
Cloudtrail – To detect API Calls
Config
Identity Center (Former AWS SSO)
Directory Services

SCP vs IAM

Centralization
Organizations offers centralized management of cloud environments, providing flexibility and seamless alignment with business processes.

Governance
Organizations can secure and audit your environment by controlling access to accounts, AWS Regions, and services.

Compliance
With Organizations, you can strengthen your security posture by enforcing policies, monitoring activities, and helping with compliance across accounts.

Resource sharing
You can use Organizations to share resources across developer teams rapidly and securely.

Apply for Accounts, and for Users/Roles created on that account following the Policy Evaluation. No apply for Resource-Based Policies, Service-Linked Roles or External Users of the Organization.
Best Practices:

- Manage your accounts within a single organization
- Use a strong password for the root user
- Document the processes for using the root user credentials
- Enable MFA for your root user credentials
- Apply controls to monitor access to the root user credentials
- Keep the contact phone number updated
- Use a group email address for root accounts
- Group workloads based on business purpose and not reporting structure
- Use multiple accounts to organize your workloads
- Enable AWS services at the organizational level using the service console or API/CLI operations
- Use billing tools to track costs and optimize resource usage
- Plan the tagging strategy and enforcement of tags across your organization resources
- Best practices for the management account
- Best practices for member accounts

Taken from https://docs.aws.amazon.com/prescriptive-guidance/latest/transitioning-to-multiple-aws-accounts/set-up-organization.html (12/07/2024)

Deny List vs Allow List

Deny List

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAllActions",
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        },
        {
            "Sid": "DenyDynamoDB",
            "Effect": "Deny",
            "Action": "dynamodb:*",
            "Resource": "*"
        }
    ]
}
```

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "dynamodb:*",
            "Resource": "*"
        }
    ]
}
```

Allow List

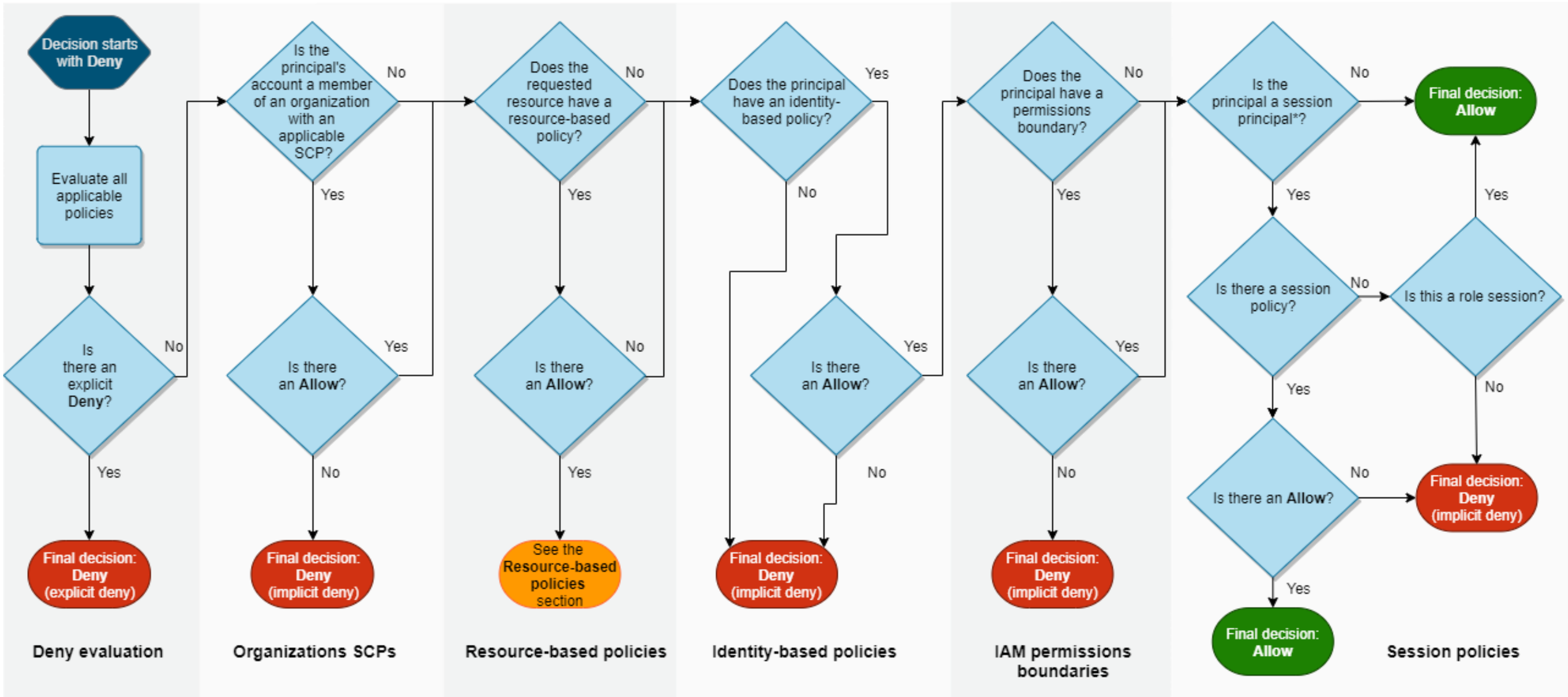
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*"
            ],
            "Resource": "*"
        }
    ]
}
```

2 Strategies: Deny List and Allow List.

Deny List: Allow on ancestors (by Default, AWS Managed Policy – FullAWSAccess) and apply explicit deny on childs. – Shorter (<5120 bytes on Policy) and Recommend.
Allow List: Specifying Resources on Ancestors and its implicit a Deny.

Taken from https://www.aws.training/Details/Video?id=16451 (02/06/2021)

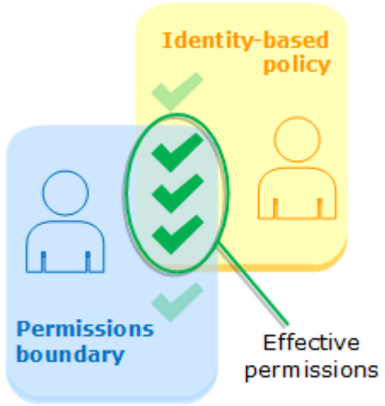
Policy Evaluation, including SCP and IAM



*A session principal is either a role session or an IAM federated user session.

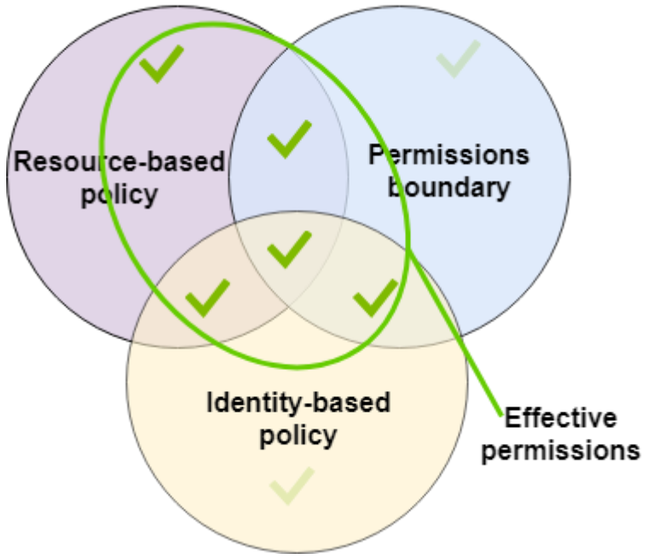
Taken from https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html#policy-eval-denyallow (16/07/2024)

Permissions Boundaries

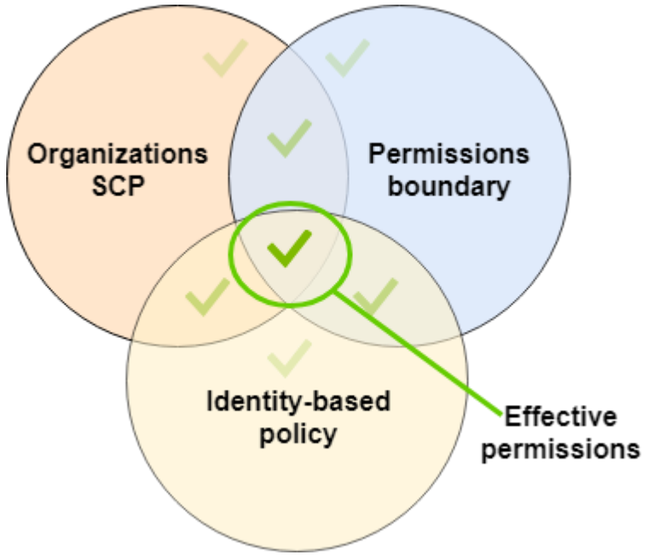


Identity-Based Permission with Boundaries (Only one per Entity)

Limit Permissions to delegate administrators to create IAM Entities. Take care to avoid overpass permissions, delete permissions.
In addition, you can use tags to control actions.



Resource-based policies



Organizations SCPs

Taken from https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html and https://docs.aws.amazon.com/IAM/latest/UserGuide/access_iam-tags.html (15/07/2024)

AWS Resource Access Manager

Service that allow share shareable resources-and actions- with AWS Accounts in side your AWS Organization or External Accounts.

Advantage:

- Centralized Government
- Low costs
- Security using Advanced IAM policies
- Free!

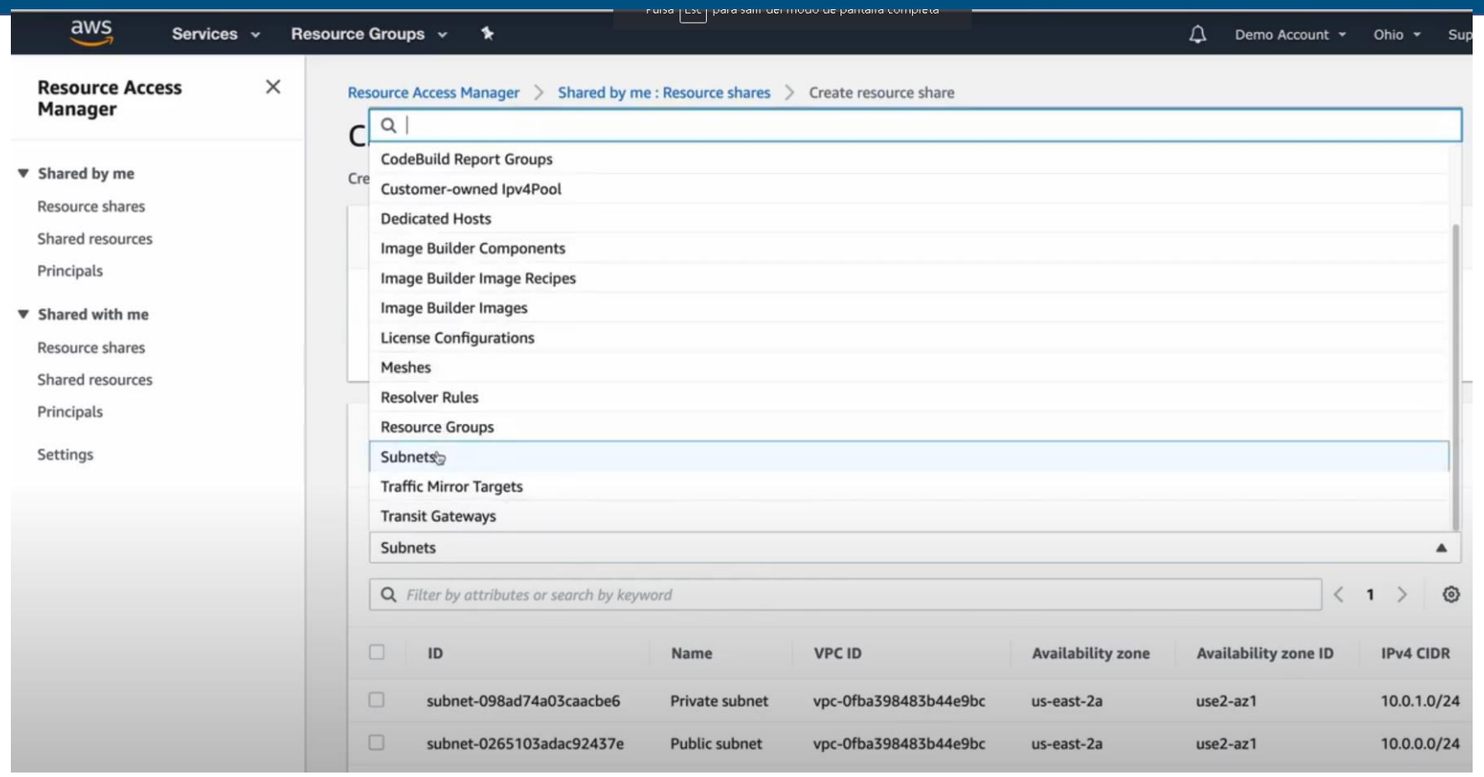
More info at: https://docs.aws.amazon.com/ram/latest/userguide/iam-examples.html and https://aws.amazon.com/ram/ (12/07/2024)

Services that work with AWS RAM

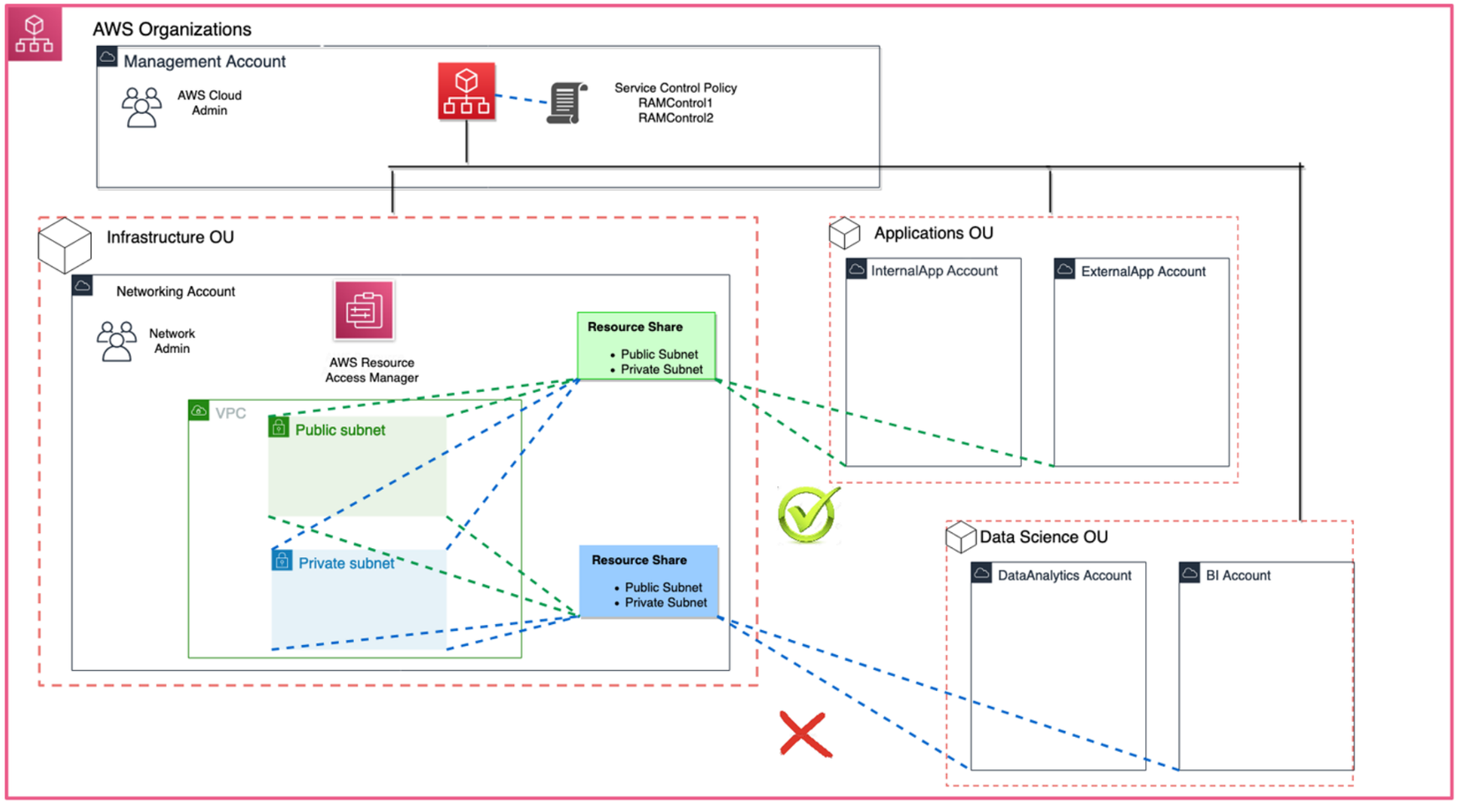
- AWS App Mesh
- Amazon Aurora
- AWS Certificate Manager Private Certificate Authority
- AWS CodeBuild
- Amazon EC2
- EC2 Image Builder
- AWS Glue
- AWS License Manager
- AWS Network Firewall
- AWS Outposts
- AWS Resource Groups
- Amazon Route 53
- AWS Systems Manager Incident Manager
- Amazon VPC

Taken from https://docs.aws.amazon.com/ram/latest/userguide/shareable.html (10/06/2021)

RAM

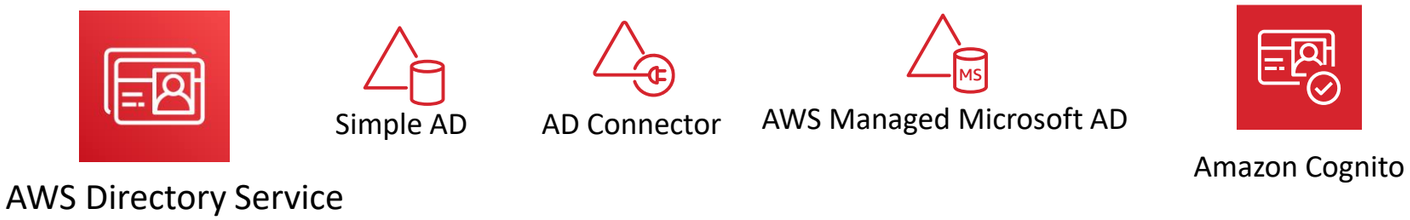


Steps:
Acc A. Activate AWS Organizations on RAM
Acc A. Create Shared Resource
Acc A. Modify IAM / SCP Policies
Acc B. Accept Shared Invitation.
Acc B. Working with Shared Resourced.

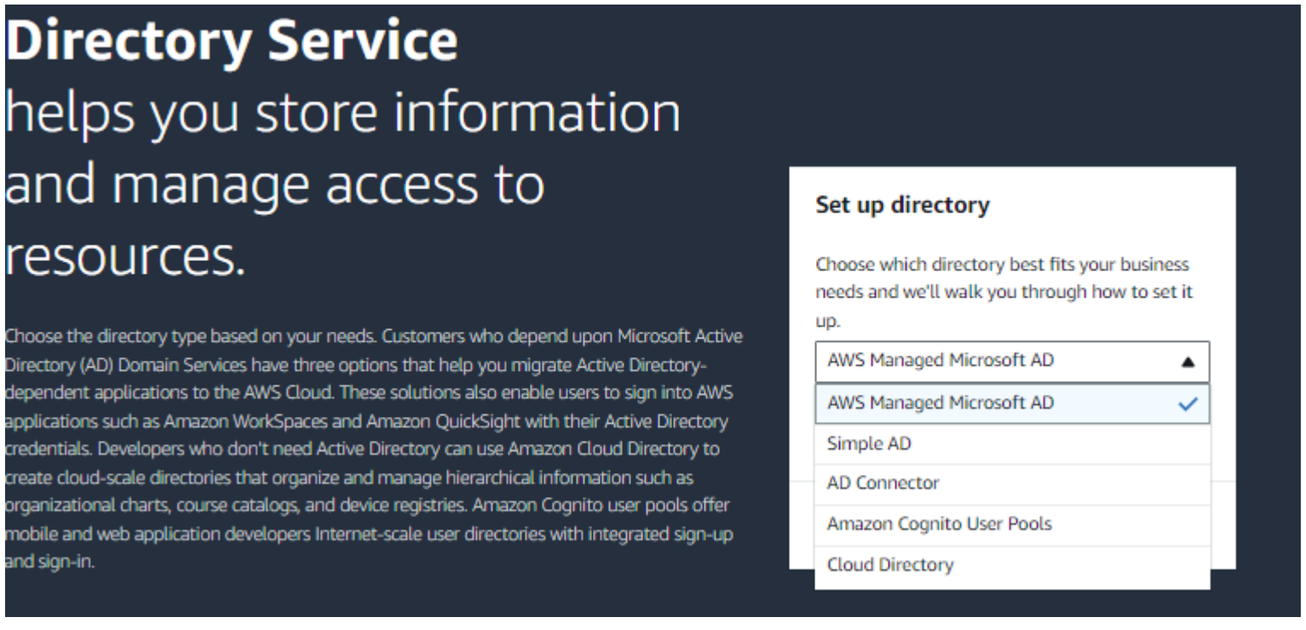


Taken from https://www.youtube.com/watch?v=KL9SICG52zY and https://aws.amazon.com/blogs/security/control-vpc-sharing-in-an-aws-multi-account-setup-with-service-control-policies/ (16/07/2024)

Directory Service for MS Active Directory



AWS Directory Service provides multiple ways to use AD with other AWS services.
Directories store information about users, groups, and devices, and administrators use them to manage access to information and resources.
AWS Directory Service provides multiple directory choices for customers who want to use existing Microsoft AD or Lightweight Directory Access Protocol (LDAP)–aware applications in the cloud.



Take care of:
MFA (No on Simple AD)
Ports (DNS, LDAP, Kerberus Auth, Radius-MFA)
Users (<5k use Simple AD, >5k Users Managed AD).
AWS Integration (Workspaces, Workdocs use Managed AD).
Subnet Netmasks and AZs

More info:
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/what_is.html#choosing_an_option and https://youtu.be/8xhHEtekgZ4 (12/07/2024)

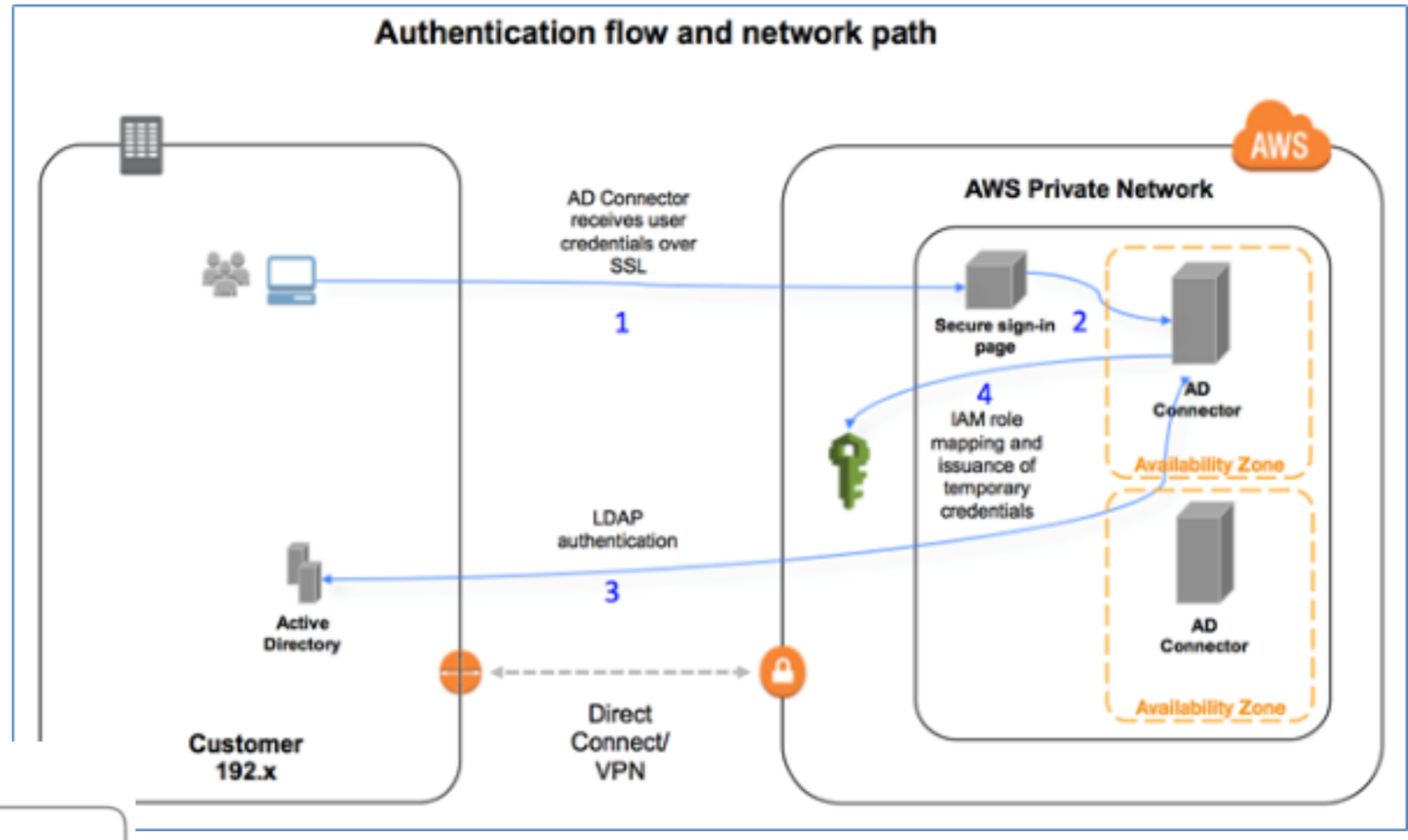
Taken from https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html#policy-eval-denyallow (02/06/2021)

AD Connector for Microsoft Active Directory

AD Connector is a proxy that enables you to use identities from your existing self-managed Microsoft Active Directory (AD) with compatible AWS applications. You can also use AD Connector to join Amazon EC2 instances to your AD domain and manage these instances using your existing group policy objects. This makes it easier to deploy AD-aware applications on these Amazon EC2 instances and use your self-managed AD for user and group authorization.

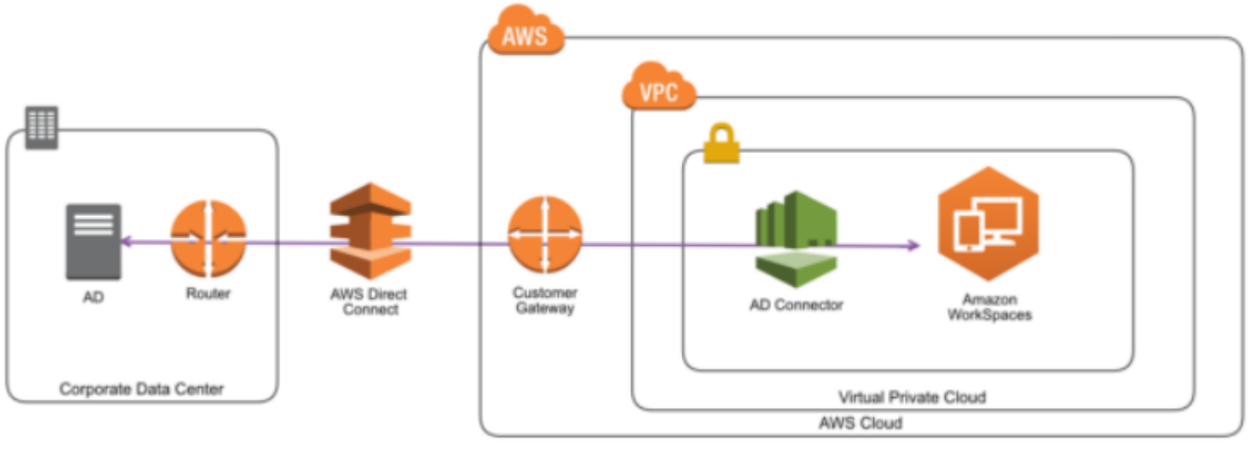
AD Connector

Notes to implement:
2 Subnets in different AZ.
Assure your subnet netmask (Reserved Netmask, 2 ENIs)
No Single Level Domain, Windows 2003 Server and up.



When to use

AD Connector is your best choice when you want to use your existing on-premises directory with compatible AWS services.



Taken from https://docs.aws.amazon.com/directoryservice/latest/admin-guide/what_is.html (16/07/2024) and https://aws.amazon.com/blogs/security/how-to-connect-your-on-premises-active-directory-to-aws-using-ad-connector/ (12/07/2024)

Simple AD for Microsoft Active Directory

Simple AD is a standalone managed directory that is powered by a Samba 4 Active Directory Compatible Server.

- Small - Supports up to 500 users (approximately 2,000 objects including users, groups, and computers).
- Large - Supports up to 5,000 users (approximately 20,000 objects including users, groups, and computers).

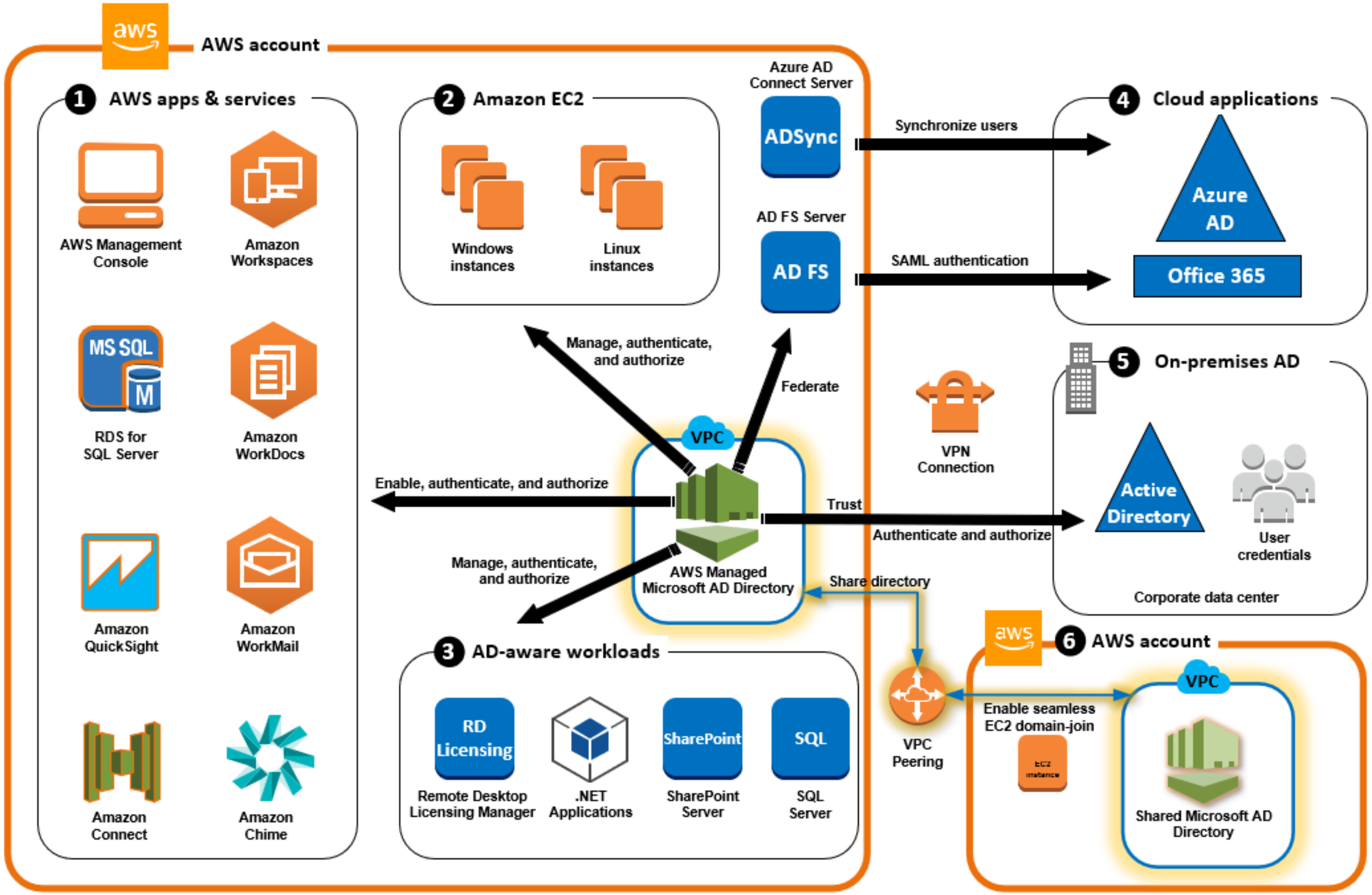
Simple AD provides a subset of the features offered by AWS Managed Microsoft AD, including the ability to manage user accounts and group memberships, create and apply group policies, securely connect to Amazon EC2 instances, and provide Kerberos-based single sign-on (SSO). Some limits on AWS Services (https://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_simple_ad.html)

When to use

You can use Simple AD as a standalone directory in the cloud to support Windows workloads that need basic AD features, compatible AWS applications, or to support Linux workloads that need LDAP service.

Taken from https://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_simple_ad.html (02/06/2021)

AWS Managed Microsoft AD



Full Ecosystem using AD, trust relationships, etc.

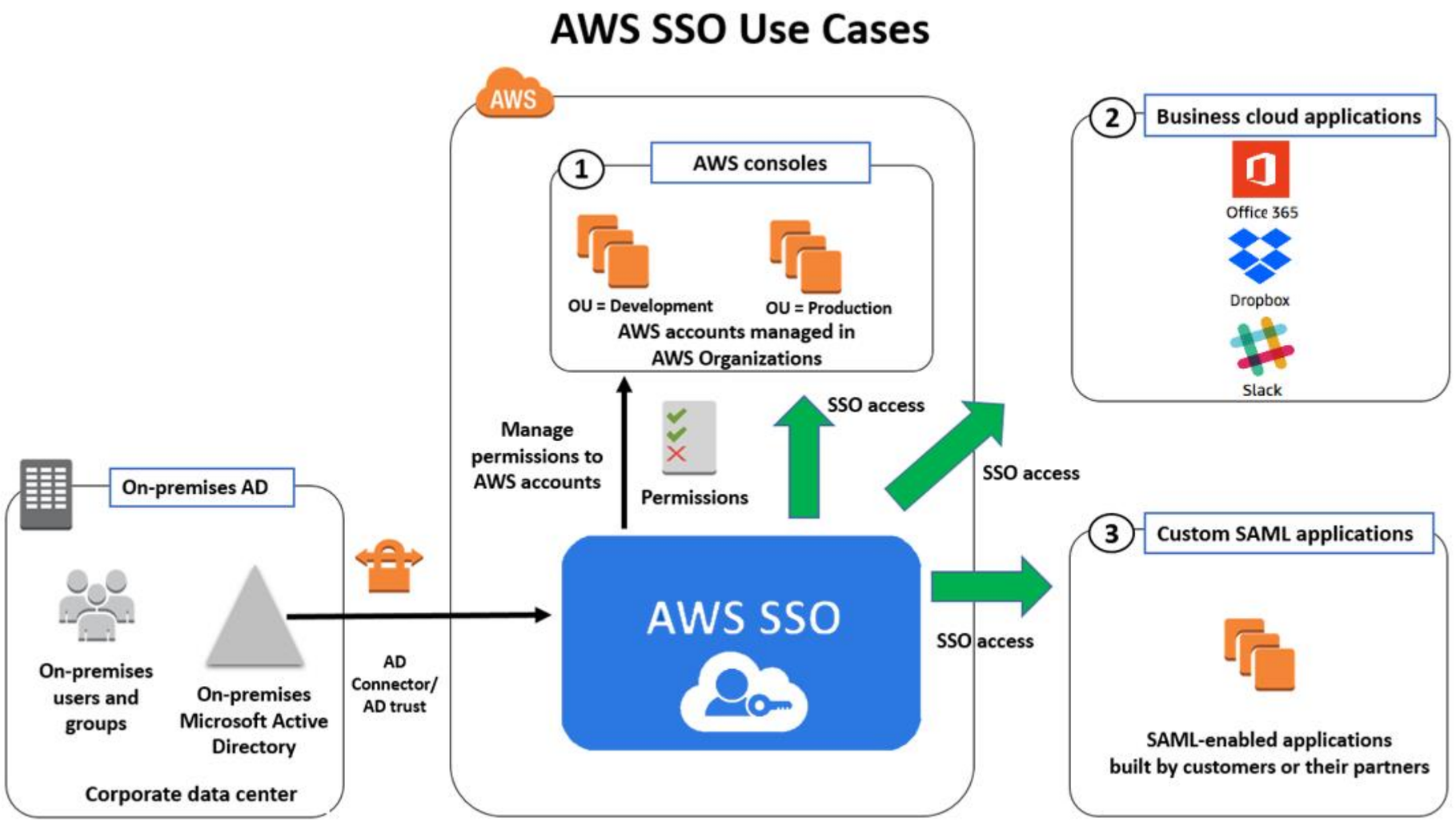
Taken from https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_use_cases.html (12/07/2024) and https://youtu.be/nuPjljOVZmU for use case #4 (12/07/2024)

AWS Identity Center (former SSO)

(…) is a cloud-based single sign-on (SSO) service that makes it easy to centrally manage SSO access to all of your AWS accounts and cloud applications.

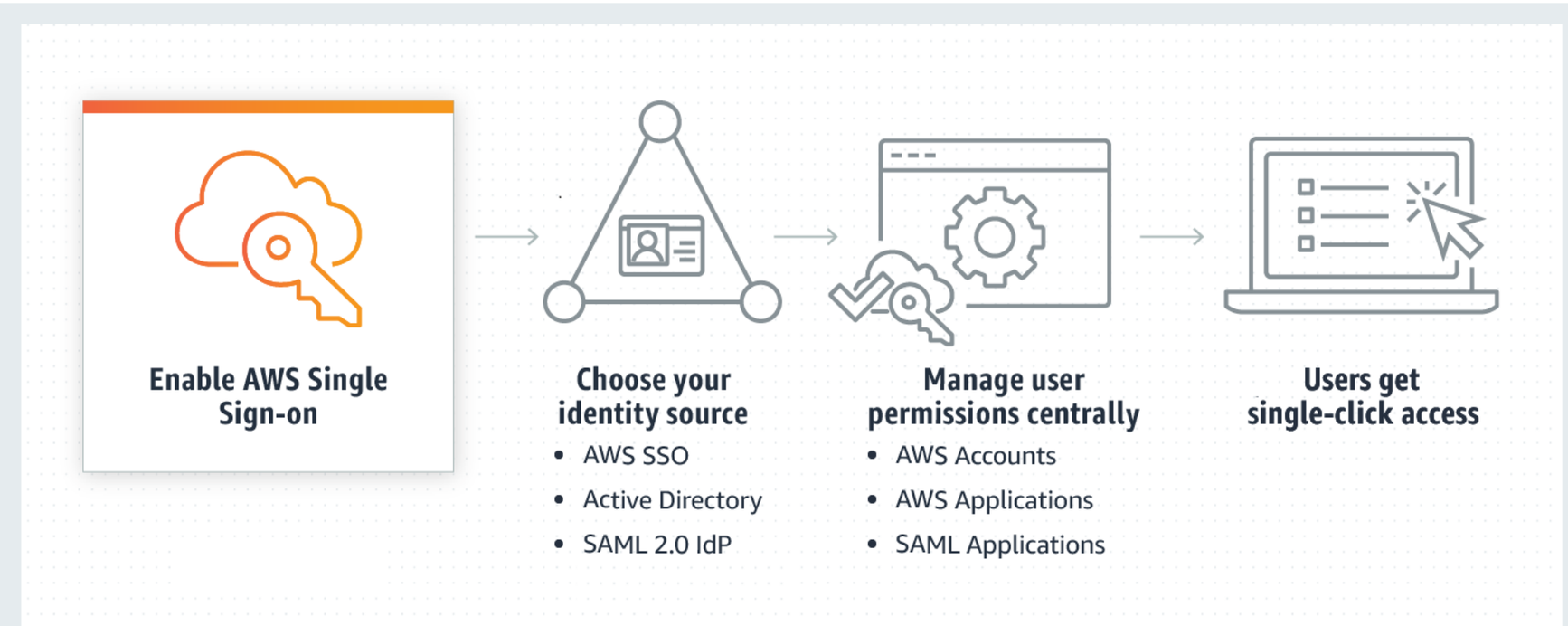
Key Concepts:

- User, Groups and Provisioning (for External Sources, i.e. AD)
- AWS SSO-Integration Enabled Application
- SAML Federation
- User Auth and Permission Sets (MFA)

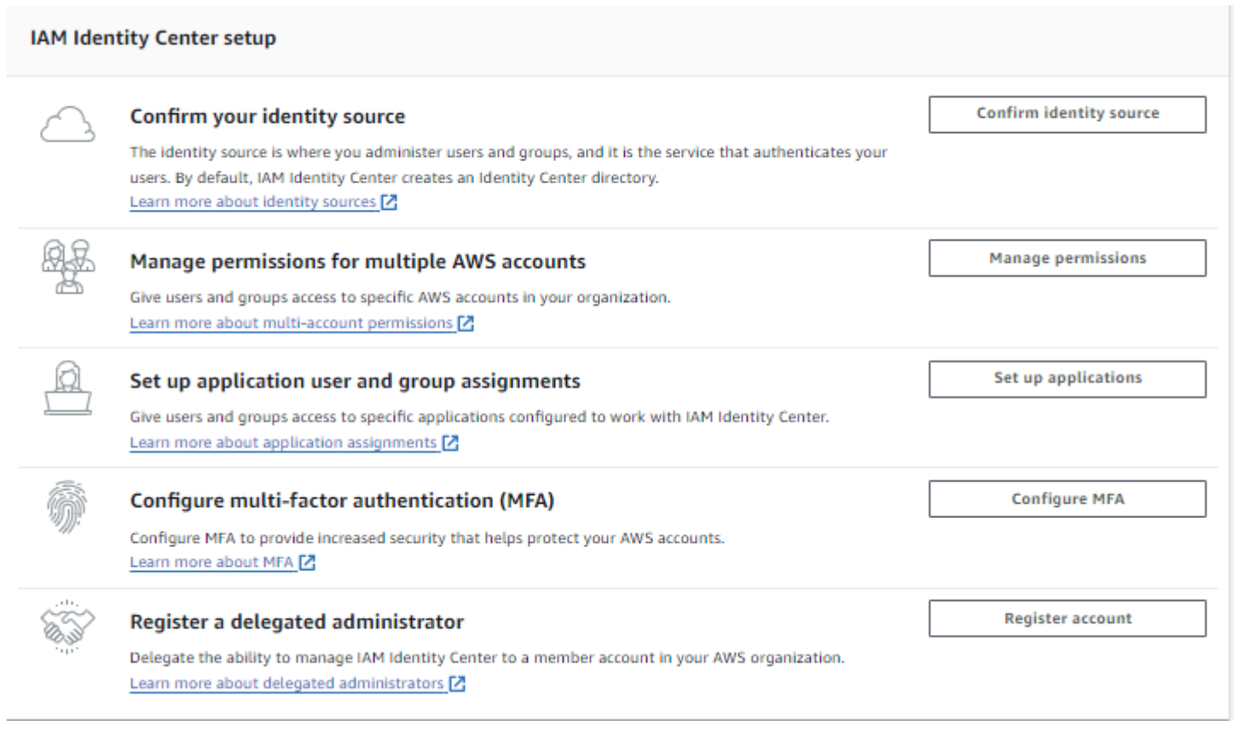


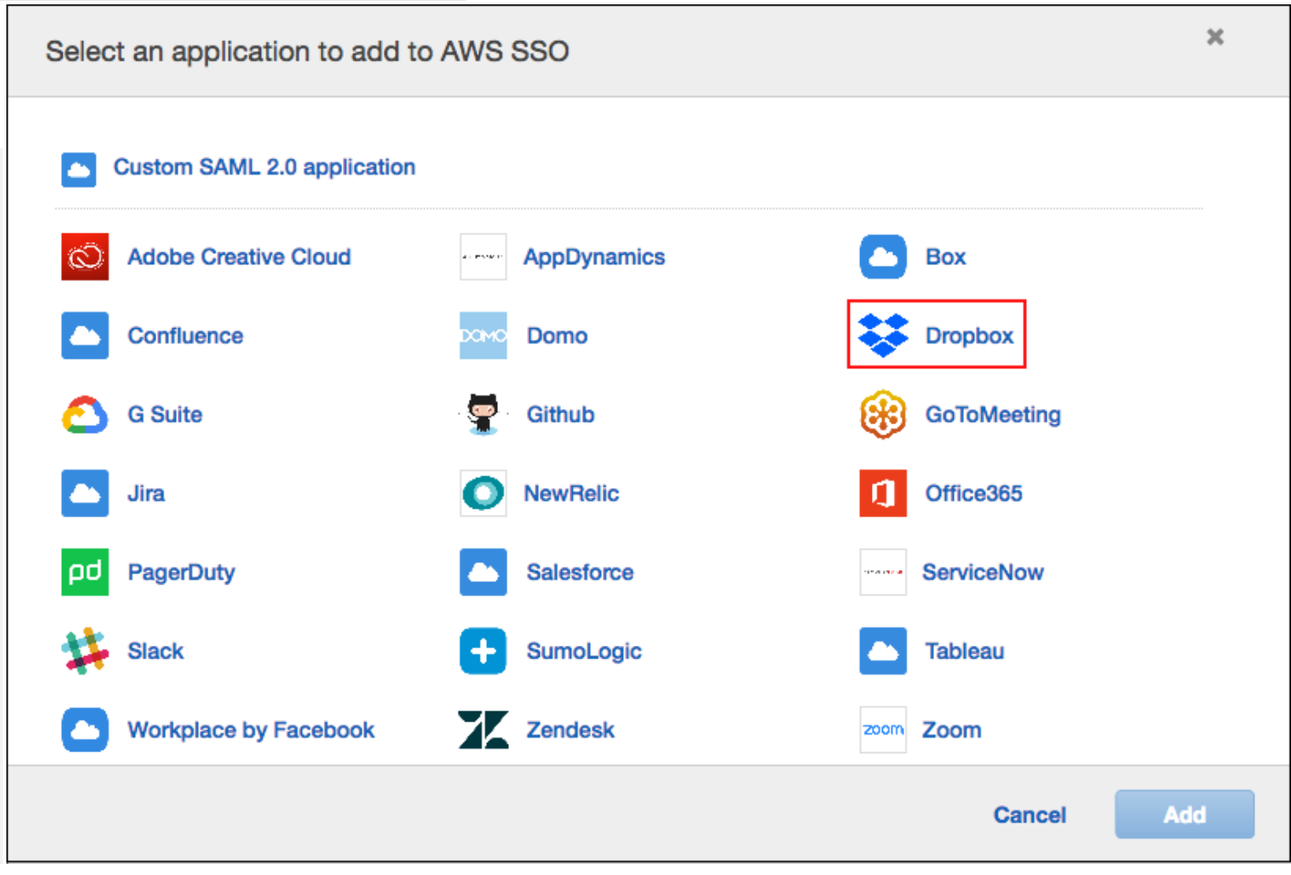
Taken fro m https://aws.amazon.com/blogs/security/introducing-aws-single-sign-on/ (17/07/2024)

AWS SSO - Steps



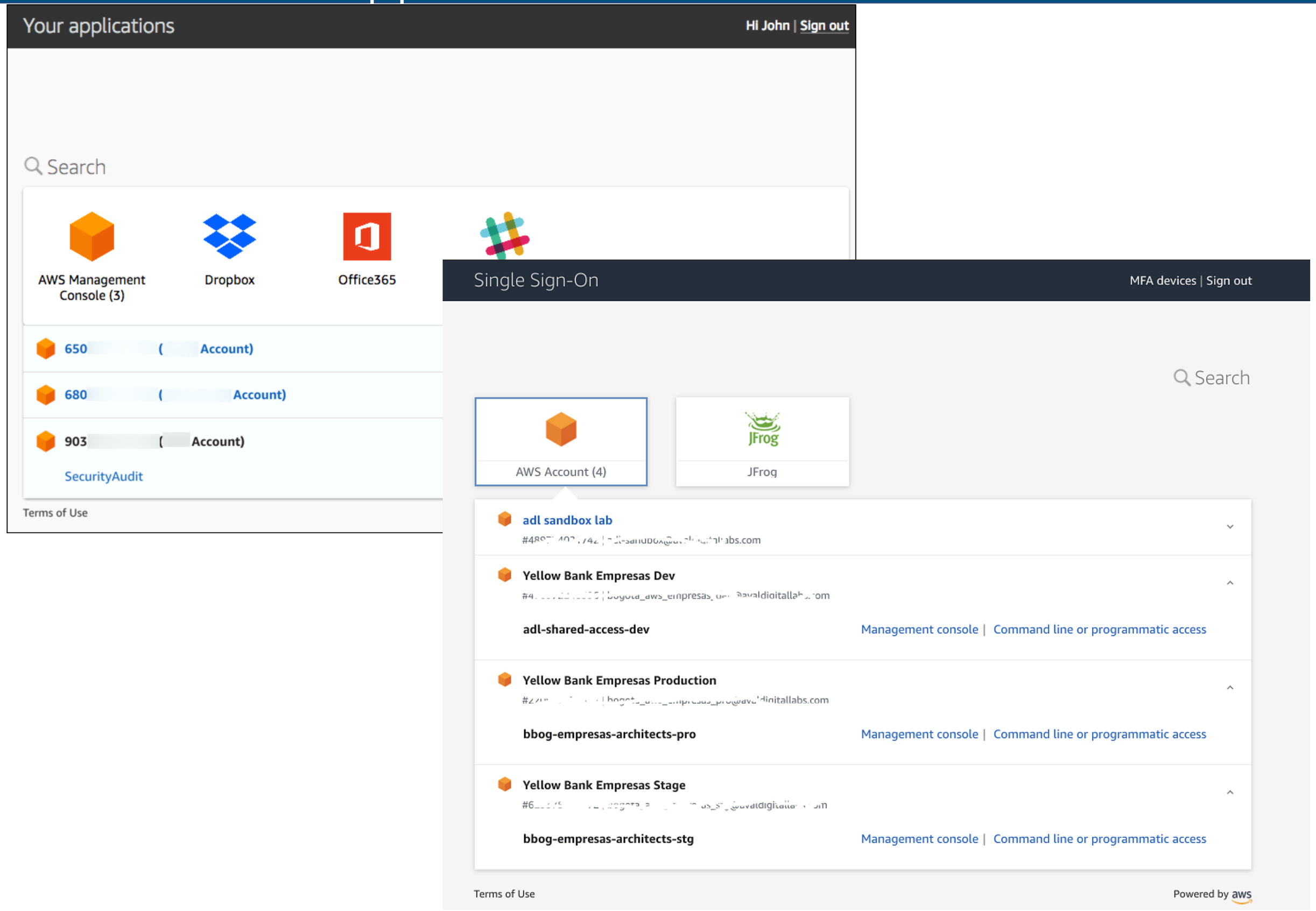
You ca use AWS SSO stored as default, to create users, groups and assign permissions.
Check Id Provider, i.e. Okta Universal Directory.
Created personalized subdomain.
Stablish Token Duration.
Apply roles.





Taken from https://aws.amazon.com/iam/identity-center/ (17/07/2024)

AWS SSO - Applications



Taken from https://aws.amazon.com/blogs/security/introducing-aws-single-sign-on/ (16/07/2024)

AWS Cognito User Pool

Secure and scalable user directory

Social and enterprise identity federation

Standards-based authentication

Security for your apps and users

Access control for AWS resources

Easy integration with your app

…lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily.

It really is this easy

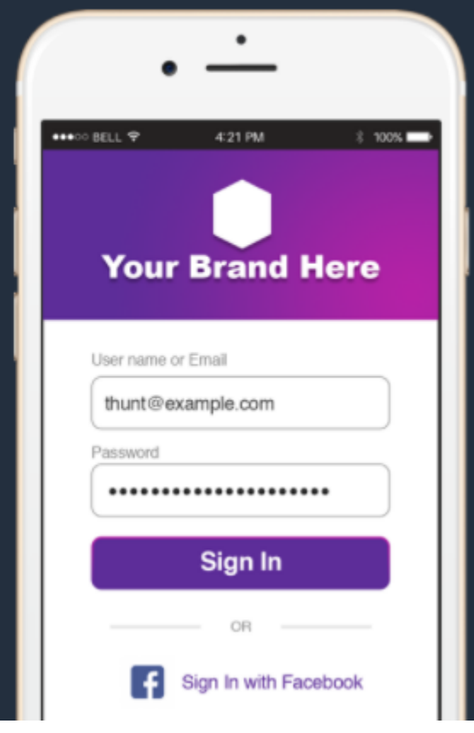
iOS Objective C | Android | iOS Swift | React Native | Web Apps

Sign in users and get back tokens using the SDKs and a few lines of code.

JavaScript

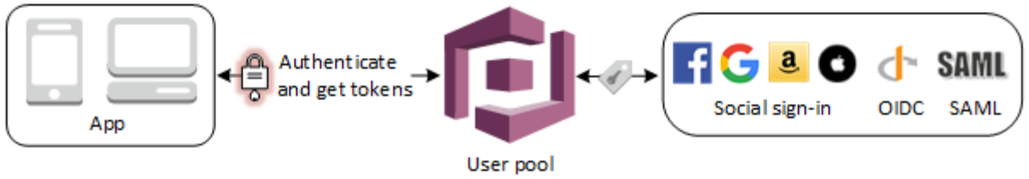
```javascript
// Add 'aws-amplify' and 'aws-amplify-react-native' libraries into your a

// Configure Auth category with your Amazon Cognito credentials
Amplify.configure({
    Auth: {
        identityPoolId: 'XX-XXXX-X:XXXXXXXX-XXXX', // Amazon Cognito Ider
        region: 'XX-XXXX-X', // Amazon Cognito Region
    }
});
```

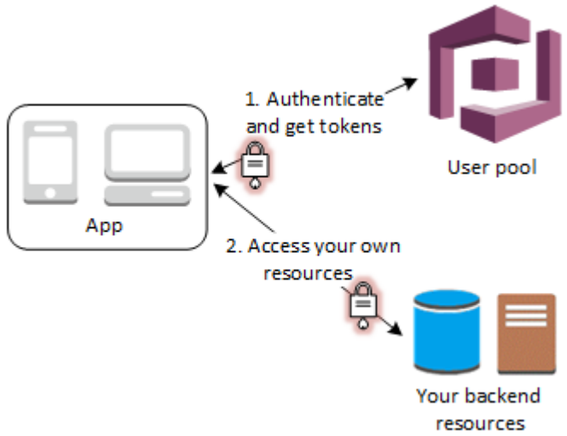


Taken fro https://aws.amazon.com/cognito/

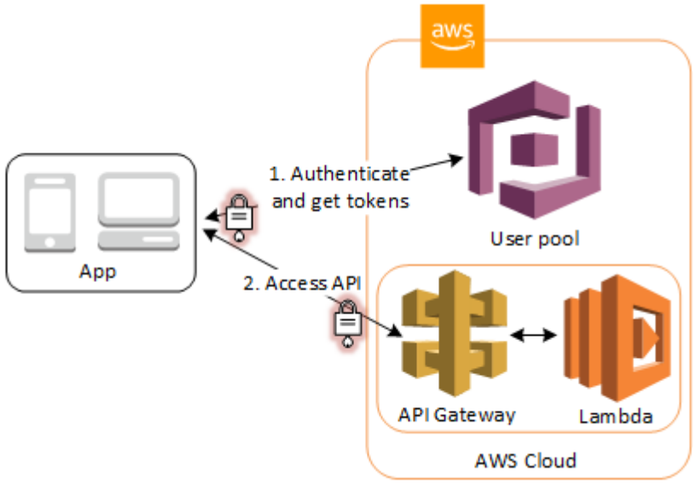
AWS Cognito: Common Cases



Authenticate with a User Pool

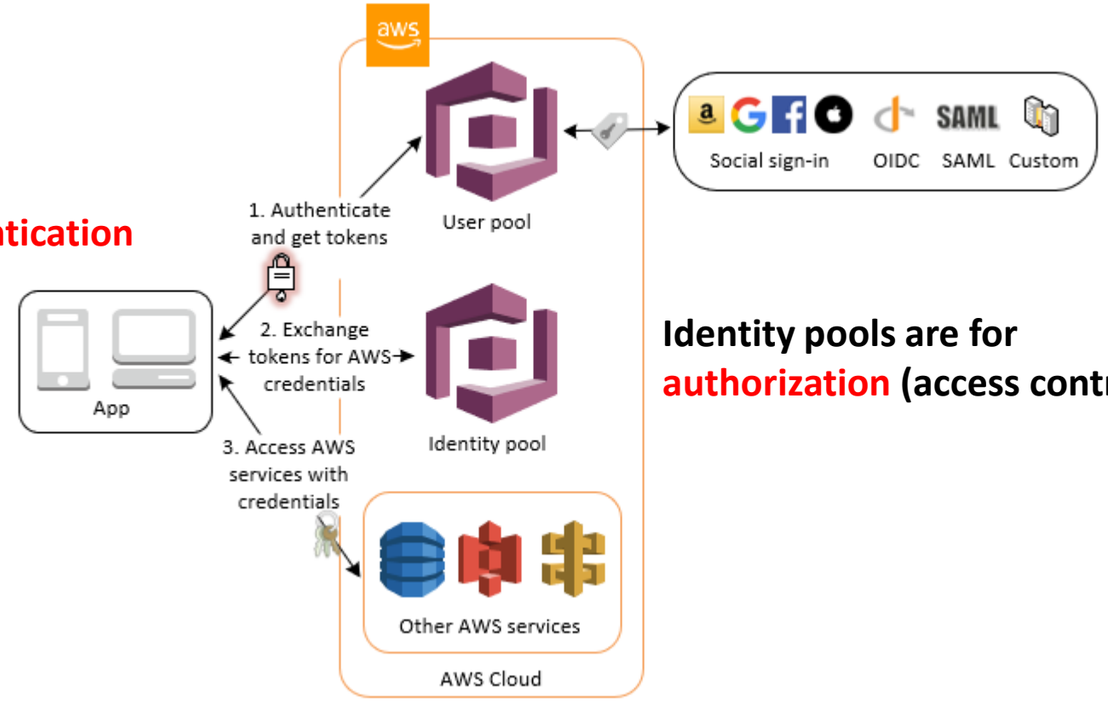


Access Your Server-side Resources with a User Pool



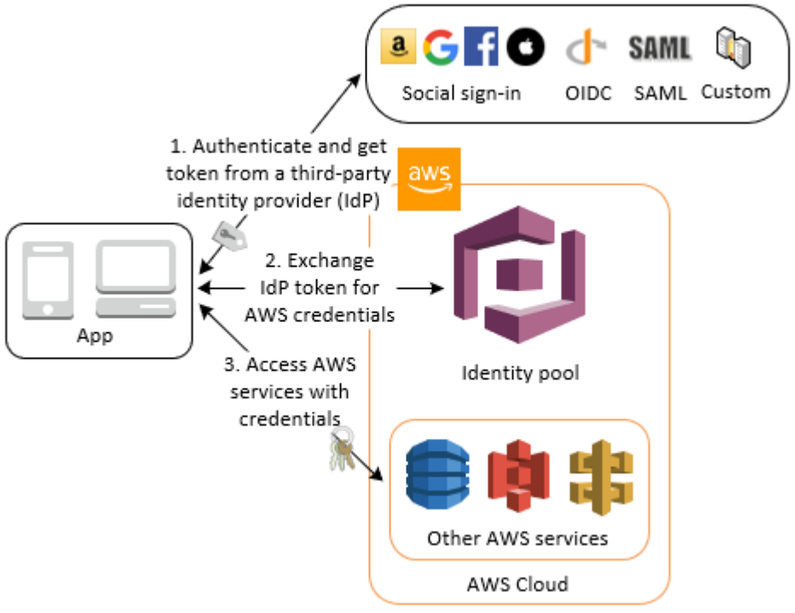
Access Resources with API Gateway and Lambda with a User Pool (Amazon Cognito authorizer Lambda function)

User pools are for authentication (identify verification)



Identity pools are for authorization (access control)

Access AWS Services with a User Pool and an Identity Pool



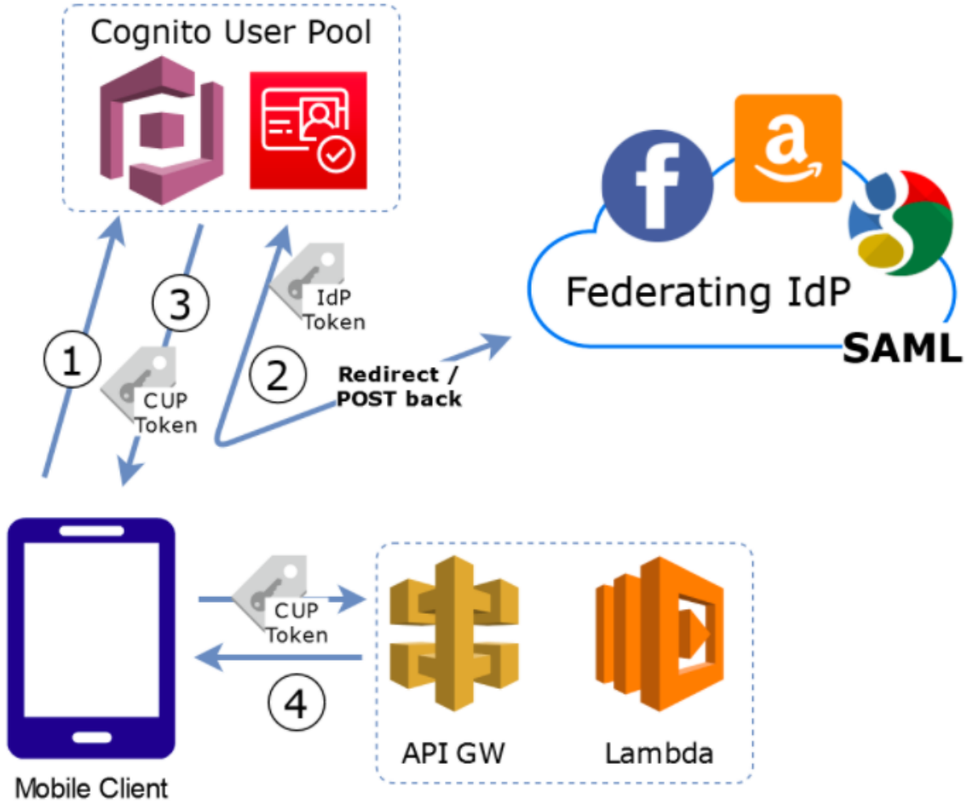
Authenticate with a Third Party and Access AWS Services with an Identity Pool

Additional Case: Using AWS AppSync

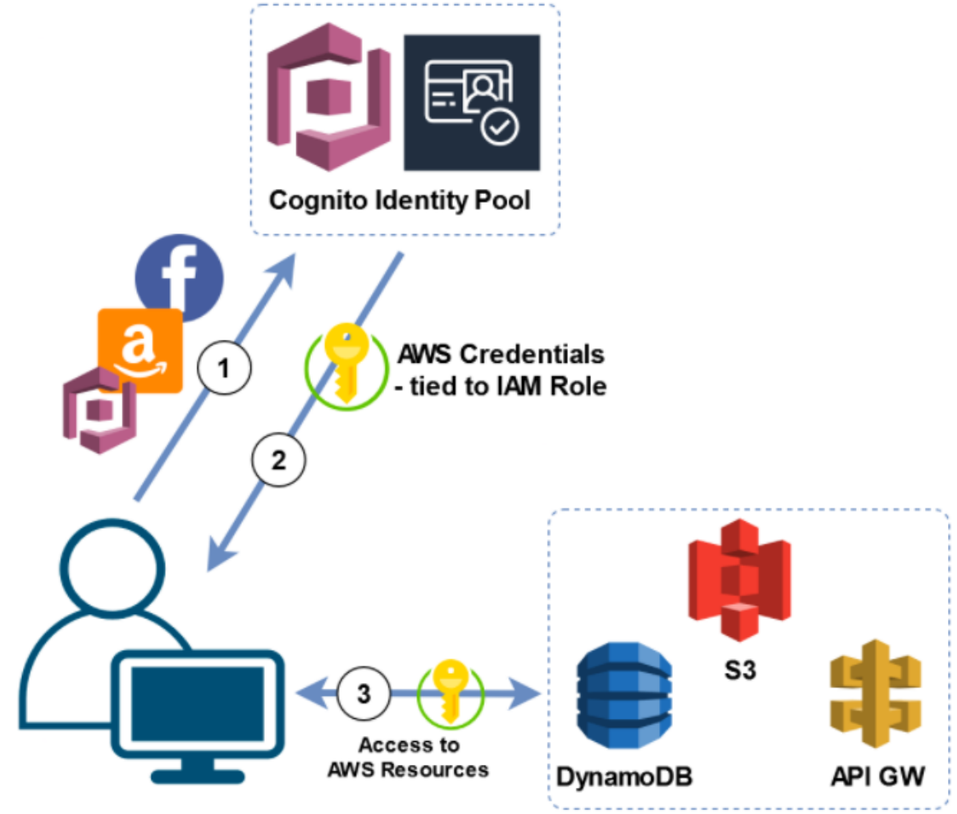
Taken from https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-scenarios.html (09/06/2021)

AWS Cognito Review and Pricings

Cognito User Pool



Cognito Identity Pool



Cognito User Pools	Cognito Identity Pools
Handles the IdP interactions for you	Provides AWS credentials for accessing resources on behalf of users
Provides profiles to manage users	Supports rules to map users to different IAM roles
Provides OpenID Connect and OAuth standard tokens	Free
Priced per monthly active user	

Pricing Tier (MAUs)	Price per MAU
First 50,000	Free
Next 50,000	$0.00550
Next 900,000	$0.00460
Next 9,000,000	$0.00325
Greater than 10,000,000	$0.00250

If you are using Amazon Cognito Identity to create a User Pool, you pay based on your monthly active users (MAUs) only.

Taken from https://tutorialsdojo.com/amazon-cognito-user-pools-and-identity-pools-explained/ (09/06/2021)