



AWS Solutions Architect Associate

Session 202

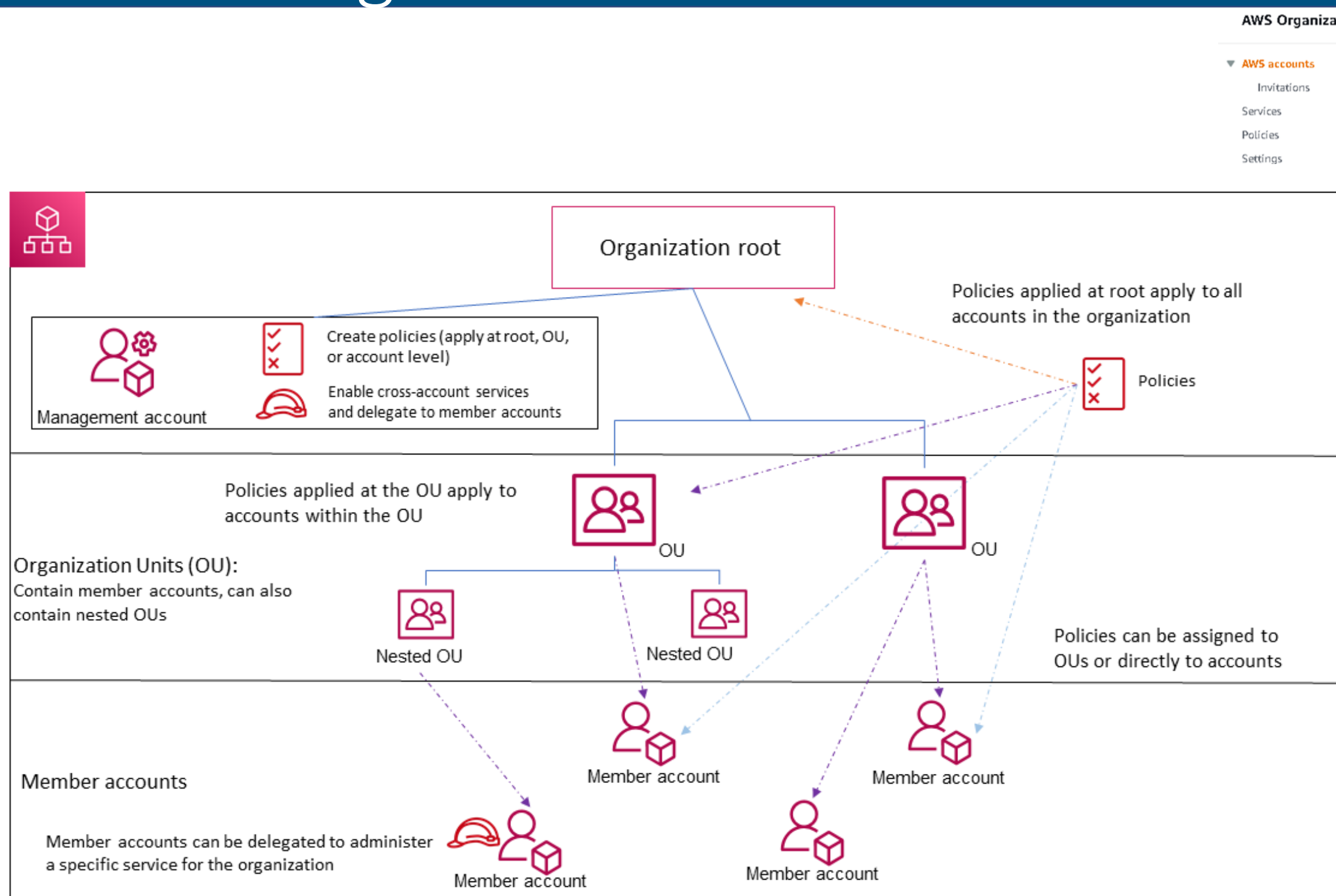
Security, Id & Compliance:
Organizations, Directory Services,
Single SignOn and Cognito

July/2024



AWS Organizations

fmorenod.co
©2024



AWS Organizations ×

Introducing the new AWS Organizations console experience. We've redesigned the AWS Organizations console to make it easier to manage your organization.

AWS Organizations > AWS accounts

AWS accounts

The accounts listed below are members of your organization. The accounts in the organization. You can use the tools provided by AWS Organizations to manage your organization.

Organization

Organizational units (OUs) enable you to group several accounts together as a single unit instead of one at a time.

Find AWS accounts by name, email, or account ID. Find an account.

Organizational structure

- Root
 - AdminSQL
 - FMorenoHotmail
 - fmorenod (management account)

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



AWS Organizations

×

AWS accounts

Invitations

Services

Policies

Settings New

Get started

Organization ID

o-wwwl7dbgj8

The accounts listed below are members of your organization. The organization's management account is responsible for paying the bills for all accounts in the organization. You can use the tools provided by AWS Organizations to centrally manage these accounts. [Learn more](#)

Organization

Actions

Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.

Search by name, email, account ID or OU ID.

Hierarchy

List

Organizational structure

Account created/joined date

▼ □ 📁 Root

r-cnnk

▼ □ 📁 noprod

ou-cnnk-yct90meo

□ 📦 fmorenodnoprod

124345666311 | fmorenod@gmail.com

Joined 2024/02/26

▼ □ 📁 prod

ou-cnnk-sv87t2r0

For instance:

RAM – Resource Manager Access

Cloudtrail – To detect API Calls

Config

Identity Center (Former AWS SSO)

Directory Services

AWS Organizations
X

► AWS accounts

Services

Policies

Settings New

Get started

Organization ID

o-vwwl7dbgj8

Service	Status	Last Updated
AWS Audit Manager AWS Audit Manager helps you continuously audit your AWS usage to simplify how you assess risk and compliance with regulations and industry standards.	Not enabled	-
AWS Backup A service that enables you to schedule automatic backups of your AWS resources. You can create policies that automatically apply your backup plans to resources across your organization's accounts.	Enabled	16 June 2022, 04:52 (UTC-5:00)
AWS Control Tower AWS Control Tower offers a straightforward way to set up and govern an AWS multi-account environment, following prescriptive best practices.	Not enabled	-
AWS Health AWS Health provides ongoing visibility into your resource performance and the availability of your AWS services and accounts. AWS Health delivers events when your AWS resources and services are impacted by an issue or will be affected by upcoming changes. You can use the organizational view feature for AWS Health to get visibility into all events that occur in your organization. You can also use the AWS Health API to access the information programmatically.	Not enabled	-
AWS IAM Identity Center (AWS Single Sign-On) A managed service that makes it easy for you to centrally provide and manage single sign-on access to all your AWS accounts and cloud applications.	Enabled	20 February 2021, 05:04 (UTC-5:00)
AWS License Manager - Linux subscriptions		



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



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.

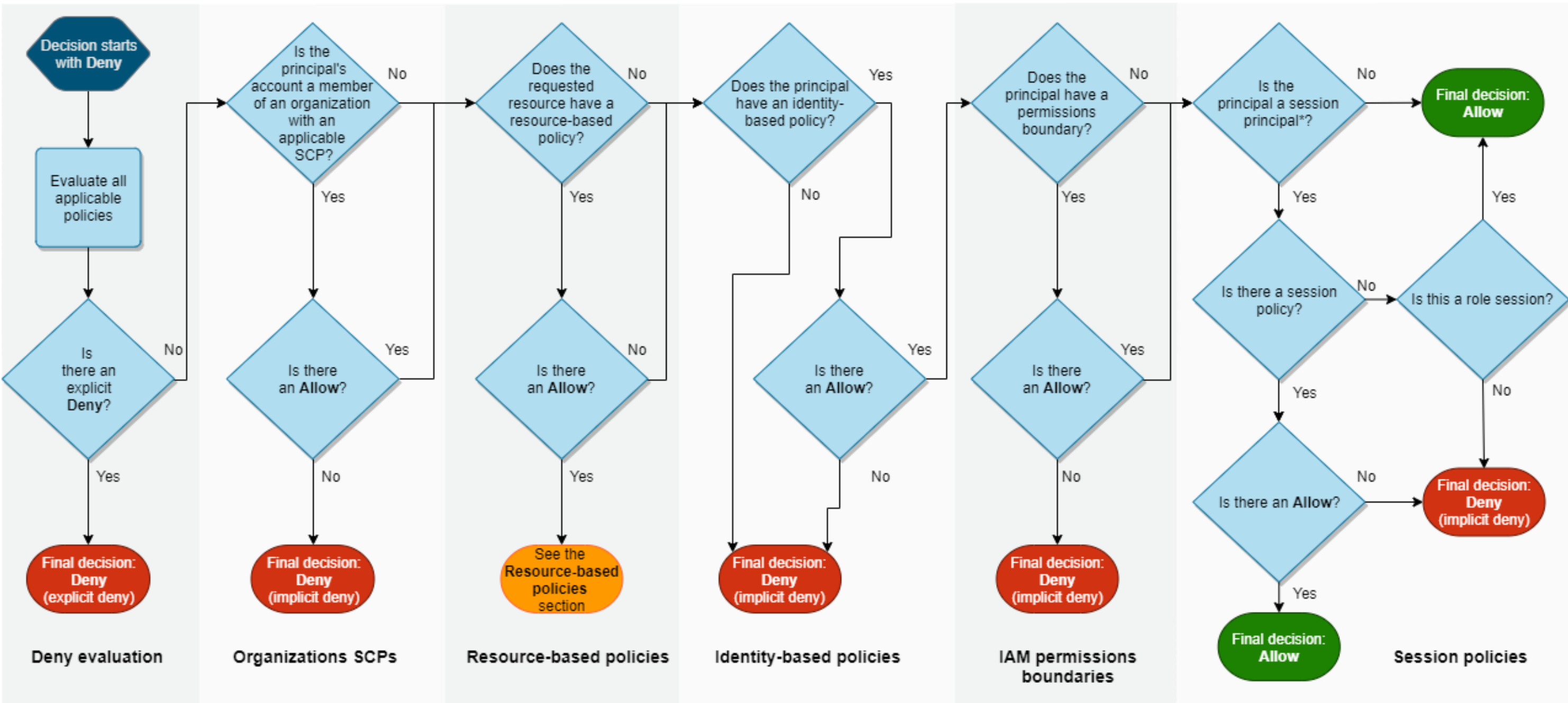
Deny List: Allow on ancestors (by Default, AWS Managed Policy – FullAWSAccess) and apply explicit deny on childs. – Shorter (<5120 bytes on Policy) and Recommend.

Allow List: Specifying Resources on Ancestors and its implicit a Deny.

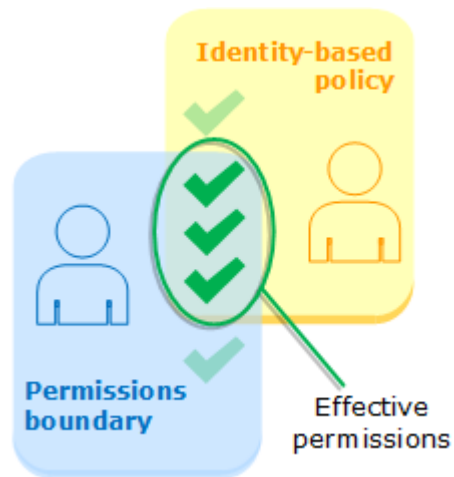


Policy Evaluation, including SCP and IAM

fmorenod.co
©2024

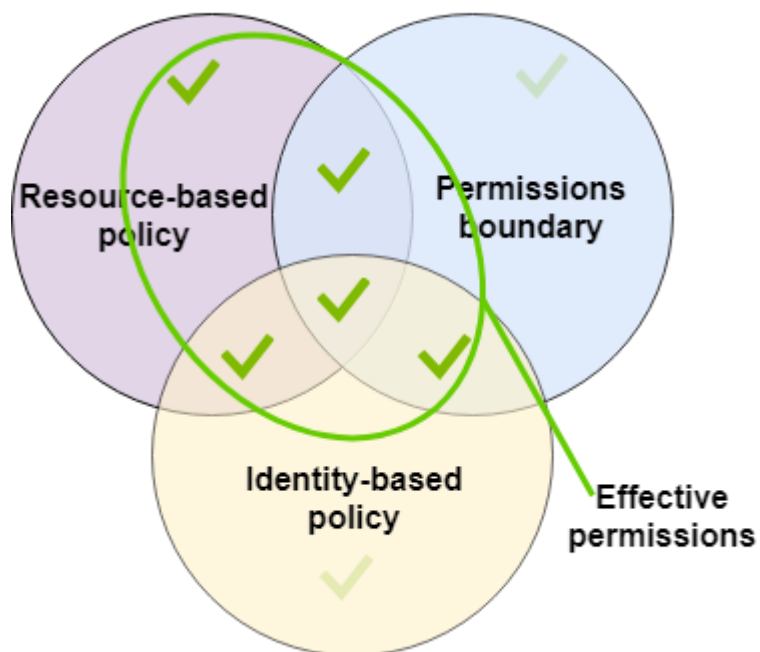


*A session principal is either a role session or an IAM federated user session.

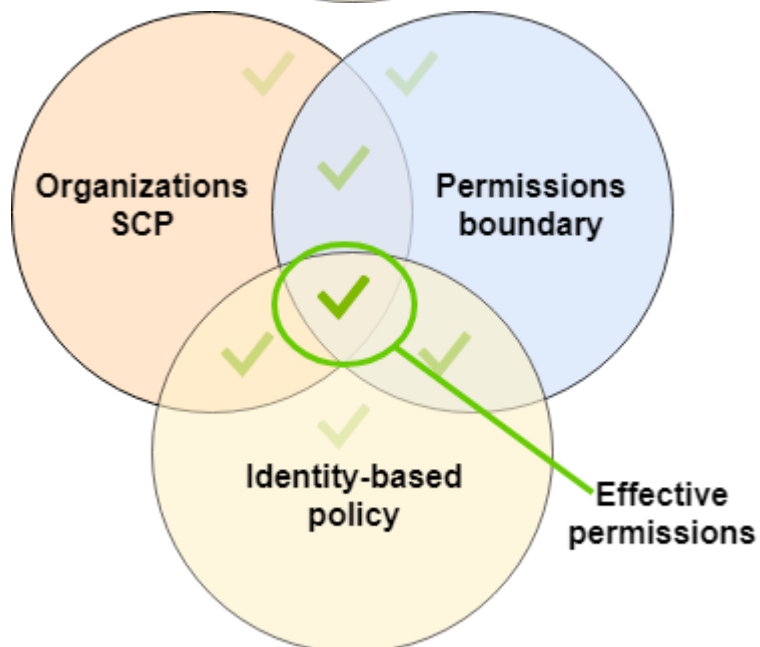


Identity-Based Permission with Boundaries (Only one per Entity)

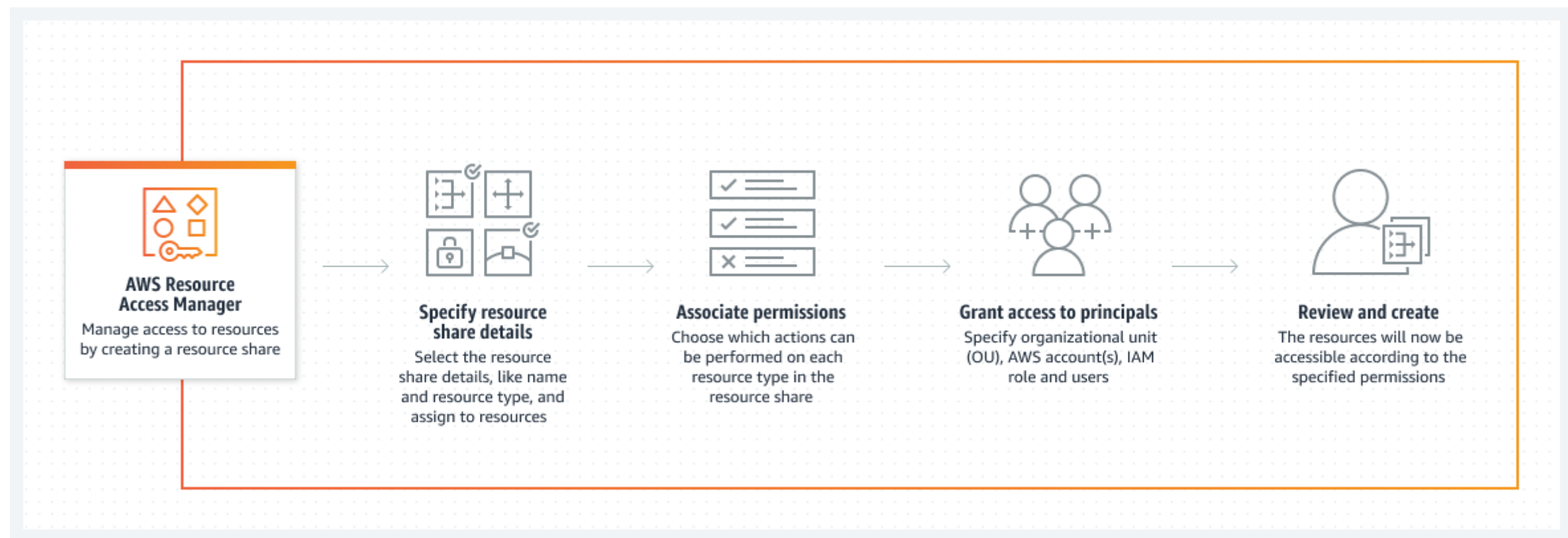
Limit Permissions to delegate administrators to create IAM Entities. Take care to avoid overpass permissions, delete permissions.
In addition, you can use tags to control actions.



Resource-based policies



Organizations SCPs



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

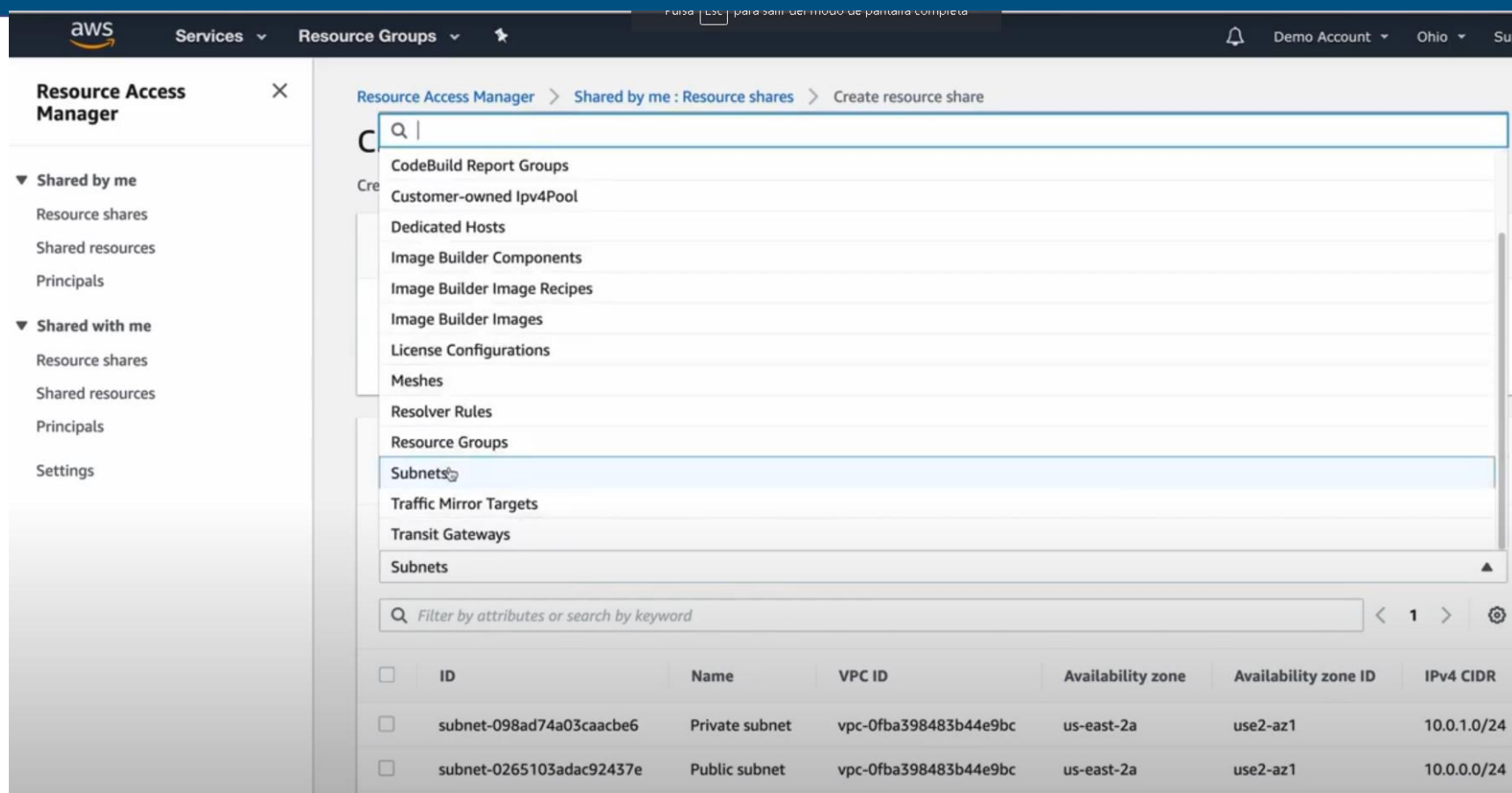
Advantage:

- 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)

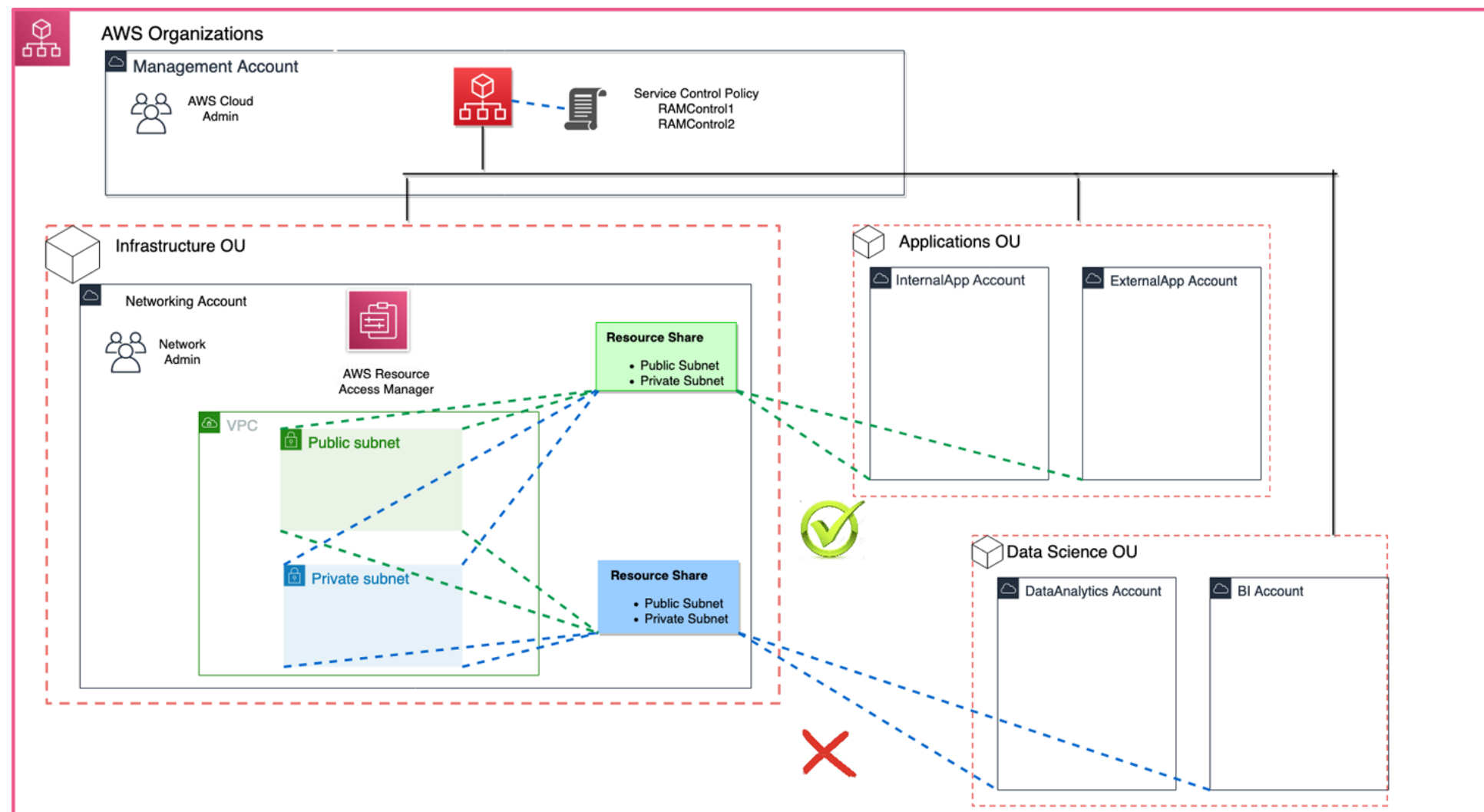
Services that work with AWS RAM

- [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](#)



Steps:

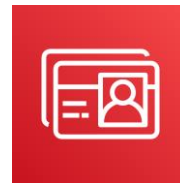
- Acc A. Activate AWS Organizations on RAM
- Acc A. Create Shared Resource
- Acc A. Modify IAM / SCP Policies
- Acc B. Accept Shared Invitation.
- Acc B. Working with Shared Resourced.





Directory Service for MS Active Directory

fmorenod.co
©2024



AWS Directory Service



Simple AD



AD Connector



AWS Managed Microsoft AD



Amazon Cognito

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.

Directory Service

helps you store information and manage access to resources.

Choose the directory type based on your needs. Customers who depend upon Microsoft Active Directory (AD) Domain Services have three options that help you migrate Active Directory-dependent applications to the AWS Cloud. These solutions also enable users to sign into AWS applications such as Amazon WorkSpaces and Amazon QuickSight with their Active Directory credentials. Developers who don't need Active Directory can use Amazon Cloud Directory to create cloud-scale directories that organize and manage hierarchical information such as organizational charts, course catalogs, and device registries. Amazon Cognito user pools offer mobile and web application developers Internet-scale user directories with integrated sign-up and sign-in.

Set up directory

Choose which directory best fits your business needs and we'll walk you through how to set it up.

AWS Managed Microsoft AD	▲
AWS Managed Microsoft AD	✓
Simple AD	
AD Connector	
Amazon Cognito User Pools	
Cloud Directory	

Take care of:

MFA (No on Simple AD)

Ports (DNS, LDAP, Kerberos 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)



AD Connector for Microsoft Active Directory



AD Connector

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.

Notes to implement:

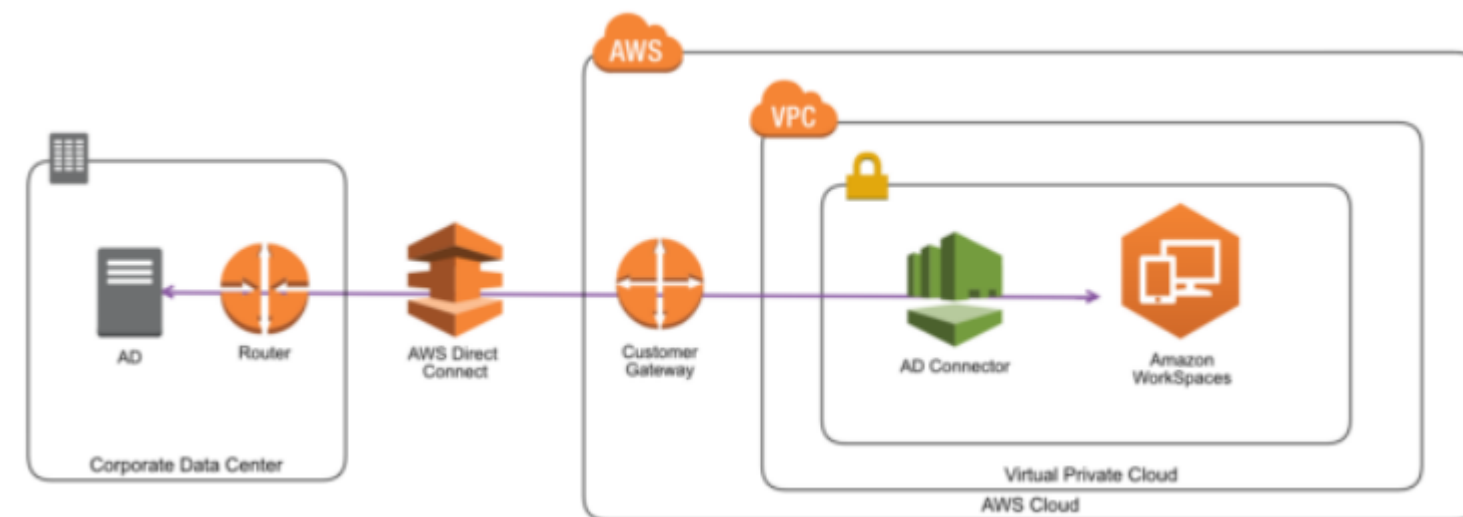
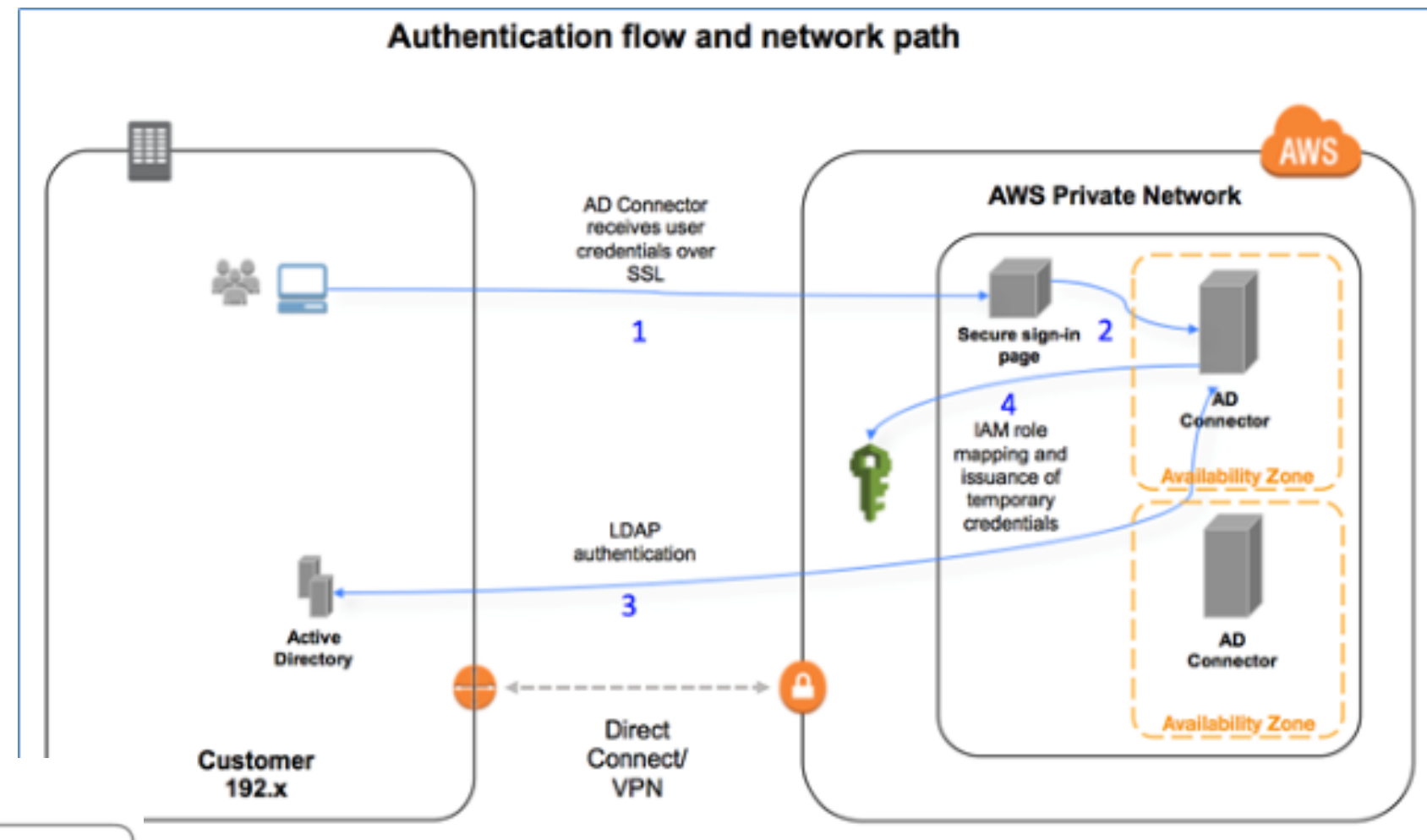
2 Subnets in different AZ.

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.





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).

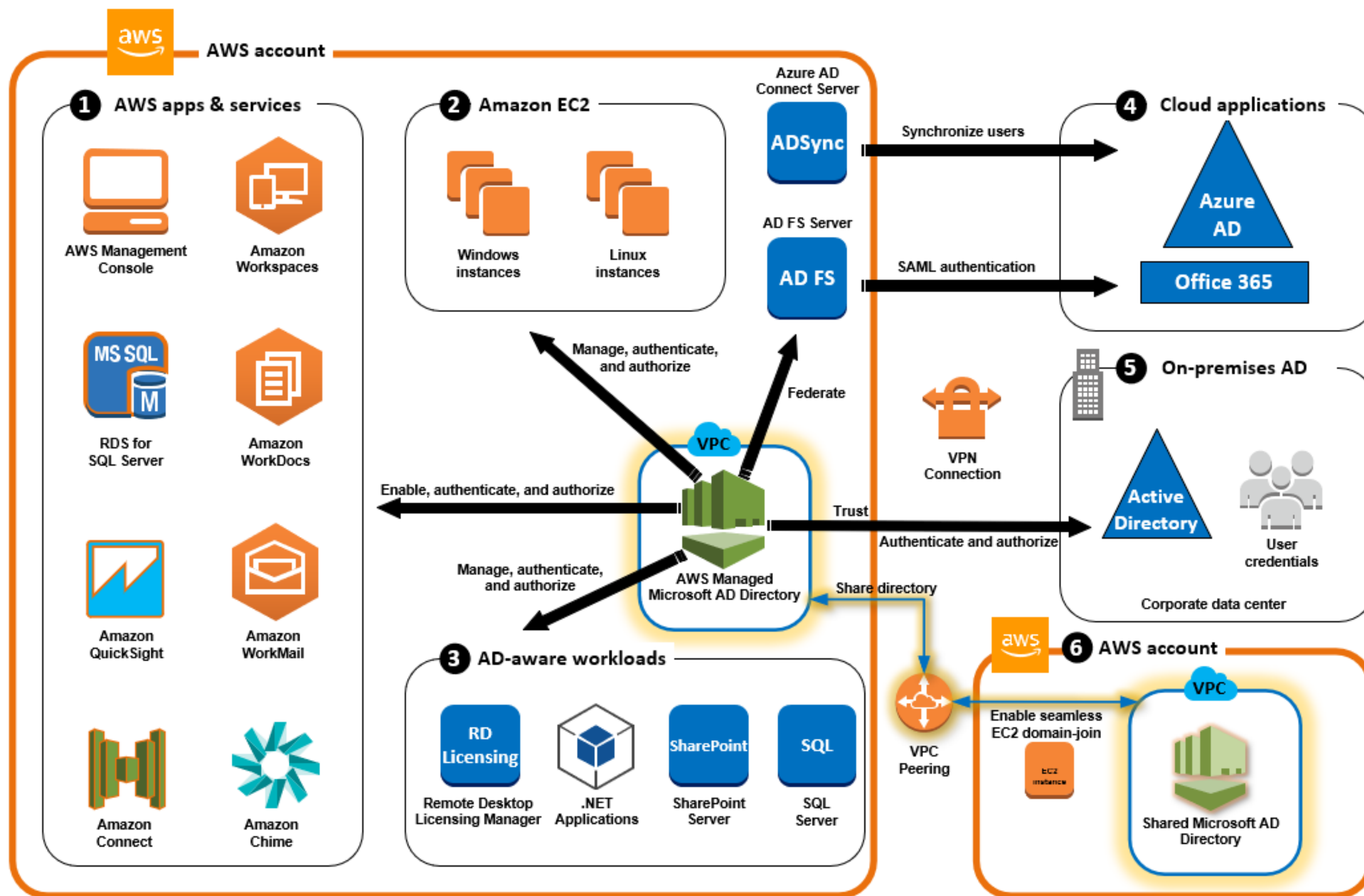
Simple AD provides a subset of the features offered by AWS Managed Microsoft AD, including the ability to manage user accounts and group memberships, create and apply group policies, securely connect to Amazon EC2 instances, and provide Kerberos-based single sign-on (SSO). Some limits on AWS Services (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.



AWS Managed Microsoft AD



Full Ecosystem using AD, trust relationships, etc.

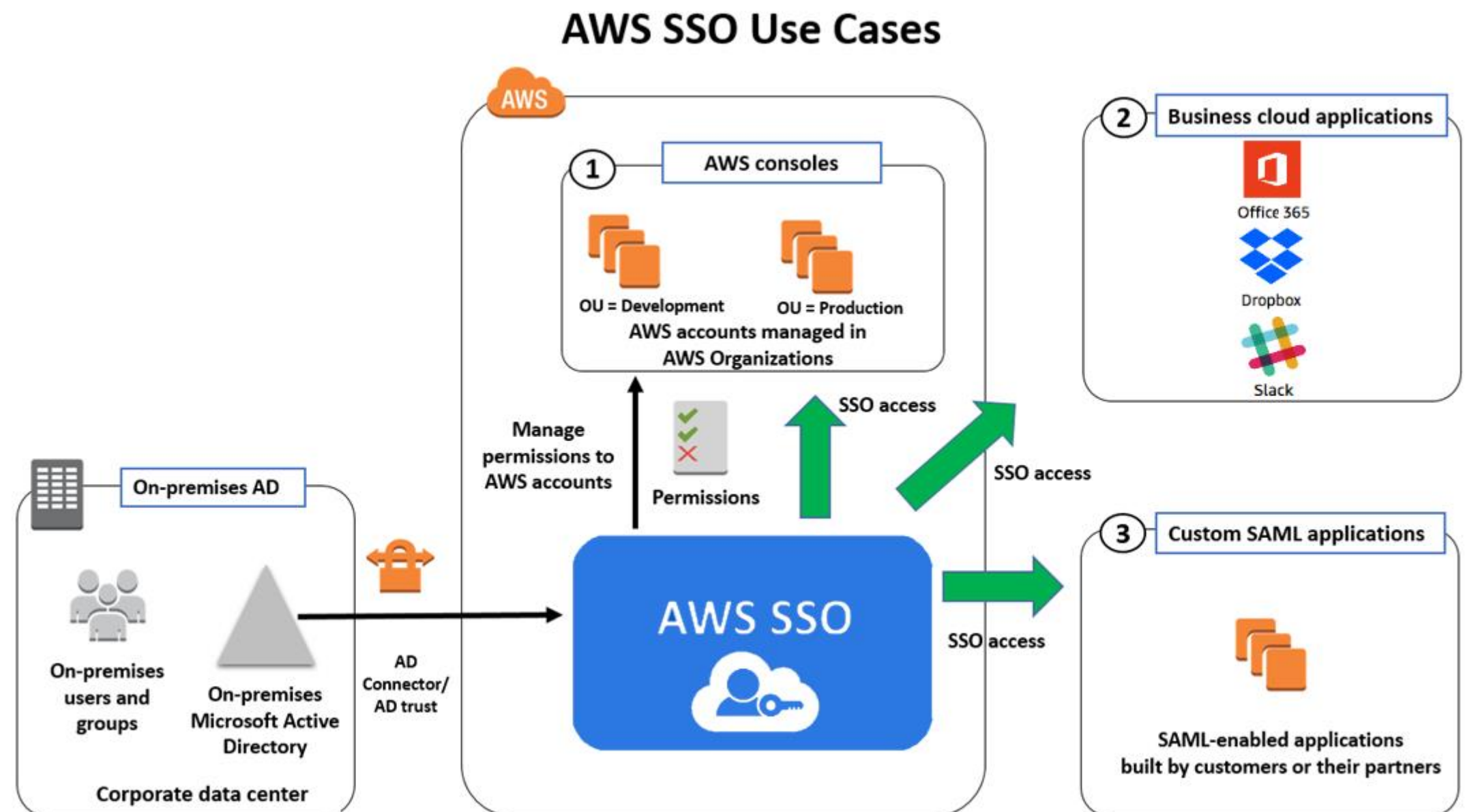


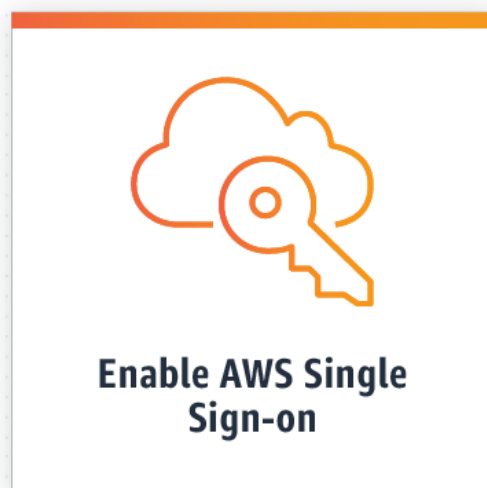
AWS Identity Center (former SSO)

(...) 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.

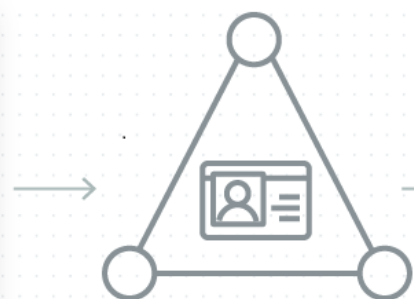
Key Concepts:

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





Enable AWS Single Sign-on



Choose your identity source

- AWS SSO
- Active Directory
- SAML 2.0 IdP



Manage user permissions centrally

- AWS Accounts
- AWS Applications
- SAML Applications



Users get single-click access

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

IAM Identity Center setup



Confirm your identity source

The identity source is where you administer users and groups, and it is the service that authenticates your users. By default, IAM Identity Center creates an Identity Center directory.

[Learn more about identity sources](#)

Confirm identity source



Manage permissions for multiple AWS accounts

Give users and groups access to specific AWS accounts in your organization.

[Learn more about multi-account permissions](#)

Manage permissions



Set up application user and group assignments

Give users and groups access to specific applications configured to work with IAM Identity Center.

[Learn more about application assignments](#)

Set up applications



Configure multi-factor authentication (MFA)

Configure MFA to provide increased security that helps protect your AWS accounts.

[Learn more about MFA](#)

Configure MFA



Register a delegated administrator

Delegate the ability to manage IAM Identity Center to a member account in your AWS organization.

[Learn more about delegated administrators](#)

Register account

Select an application to add to AWS SSO

Custom SAML 2.0 application



Adobe Creative Cloud



AppDynamics



Box



Confluence



Domo



Dropbox



G Suite



Github



GoToMeeting



Jira



NewRelic



Office365



PagerDuty



Salesforce



ServiceNow



Slack



SumoLogic



Tableau



Workplace by Facebook



Zendesk



Zoom

Cancel


Add




Your applications

Hi John | [Sign out](#)


Search




AWS Management Console (3)



Dropbox



Office365



JFrog

650 (Account)

680 (Account)

903 (Account)


SecurityAudit

[Terms of Use](#)


Single Sign-On

MFA devices | [Sign out](#)


Search



AWS Account (4)




JFrog



adl sandbox lab

#489714021742 | adlsandbox@ava.digitalabs.com




Yellow Bank Empresas Dev

#4111221110 | bogota_aws_empresas_dev@avaldigitalabs.com

adl-shared-access-dev

Management console | Command line or programmatic access




Yellow Bank Empresas Production

#2211111111 | bogota_aws_empresas_prod@avaldigitalabs.com

bbog-empresas-architects-pro

Management console | Command line or programmatic access




Yellow Bank Empresas Stage

#6111111111 | bogota_aws_empresas_stage@avaldigitalabs.com

bbog-empresas-architects-stg

Management console | Command line or programmatic access

[Terms of Use](#)

Powered by 



AWS Cognito User Pool

fmorenod.co
©2024



Secure and scalable user directory



Social and enterprise identity federation



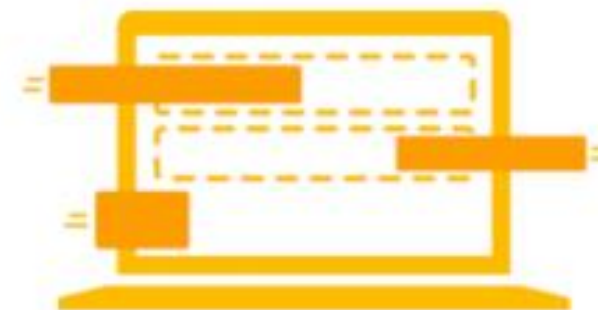
Standards-based authentication



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

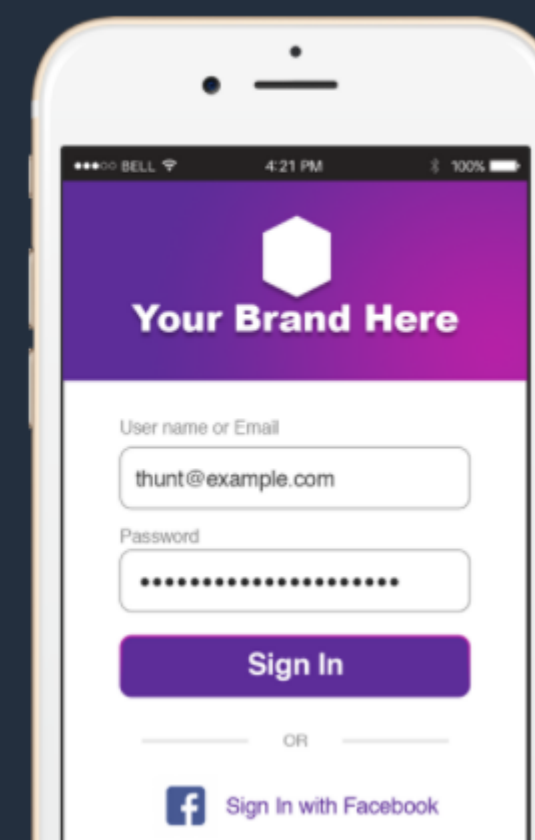


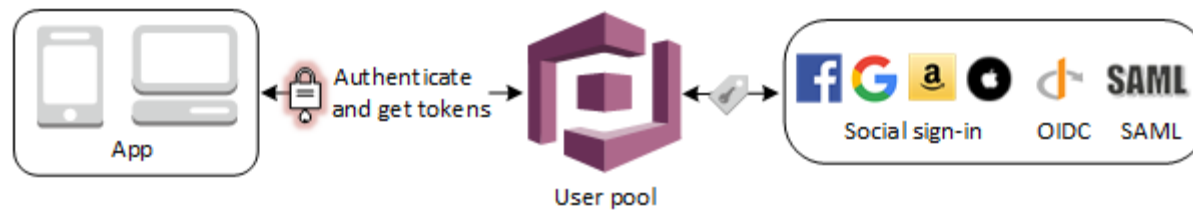
iOS Objective C Android iOS Swift **React Native** Web Apps

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

JavaScript

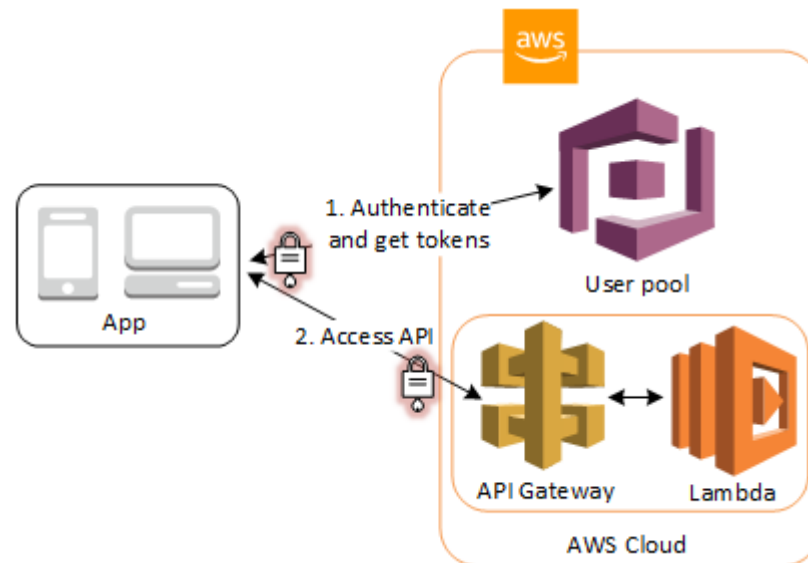
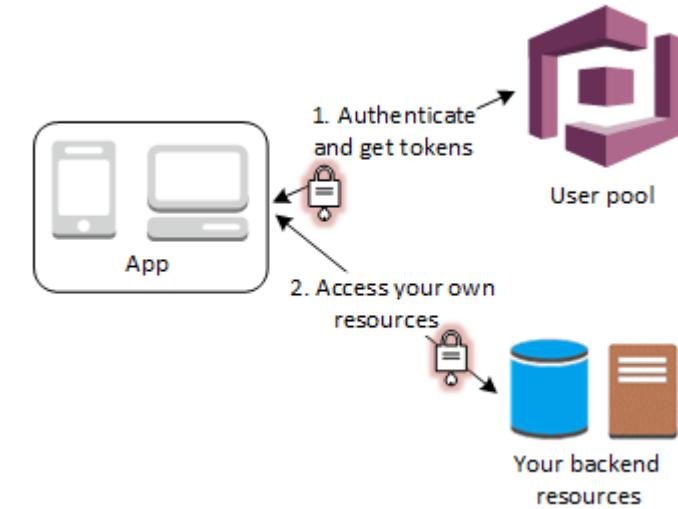
```
1 // Add 'aws-amplify' and 'aws-amplify-react-native' libraries into your app
2
3 // Configure Auth category with your Amazon Cognito credentials
4 Amplify.configure({
5   Auth: {
6     identityPoolId: 'XX-XXXX-X:XXXXXXXX-XXXX', // Amazon Cognito Identity Pool ID
7     region: 'XX-XXXX-X', // Amazon Cognito Region
8   }
9 });
```





Authenticate with a User Pool

Access Your Server-side Resources with a User Pool

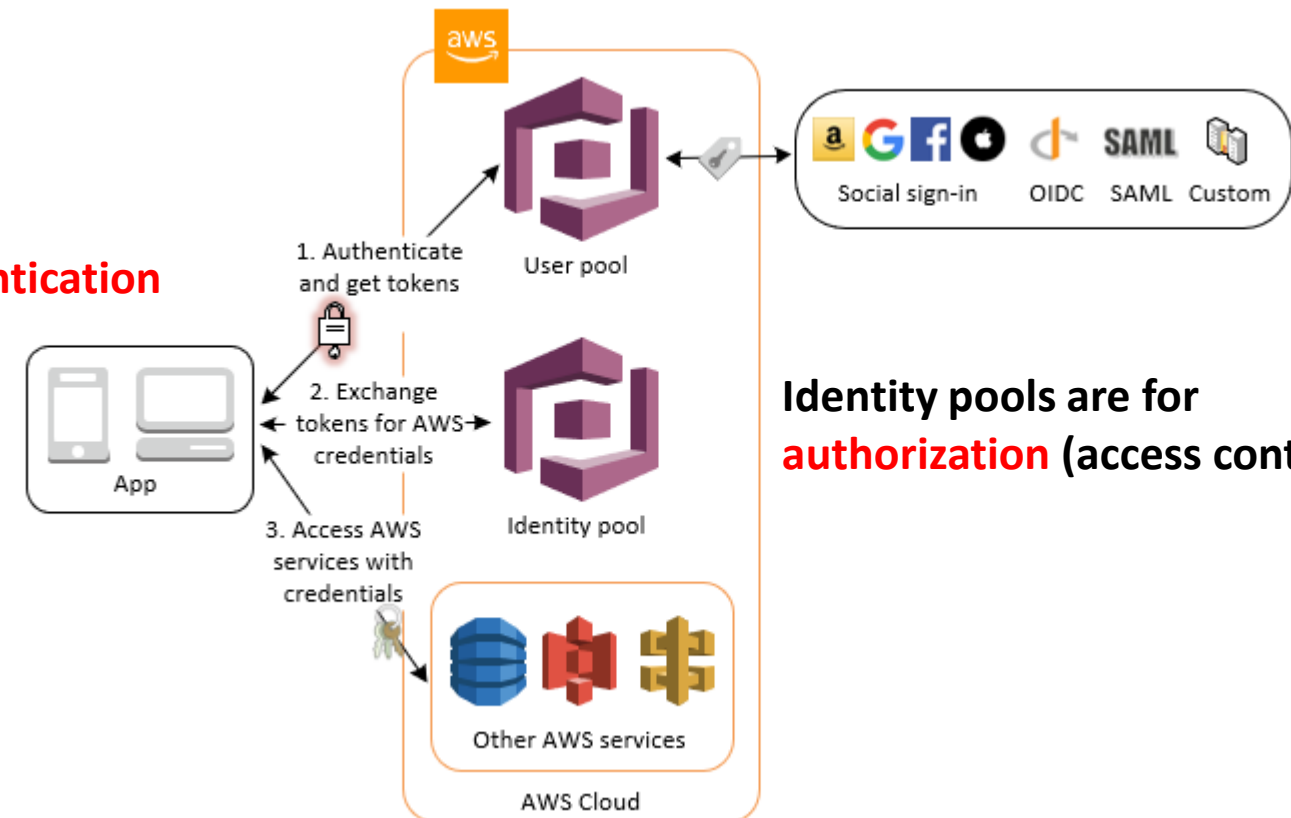
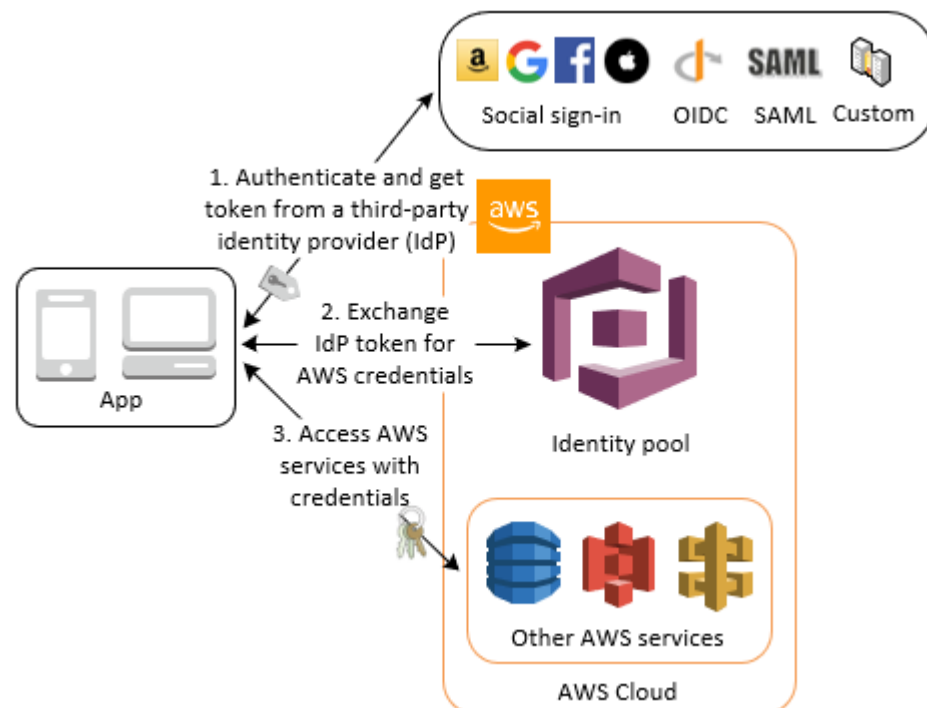


Access Resources with API Gateway and Lambda with a User Pool
(Amazon Cognito authorizer Lambda function)



User pools are for **authentication**
(identify verification)

Access AWS Services with a User Pool and an Identity Pool



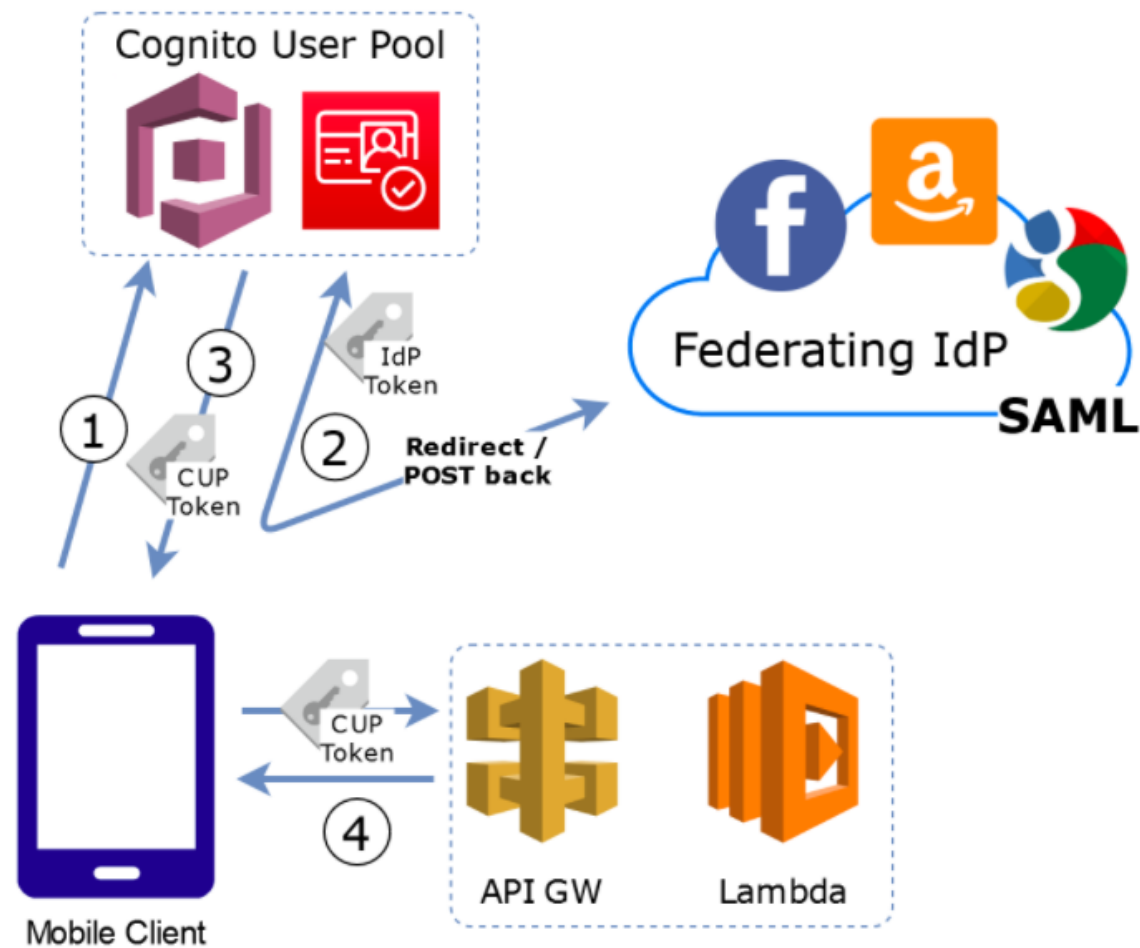
Identity pools are for **authorization** (access control)

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

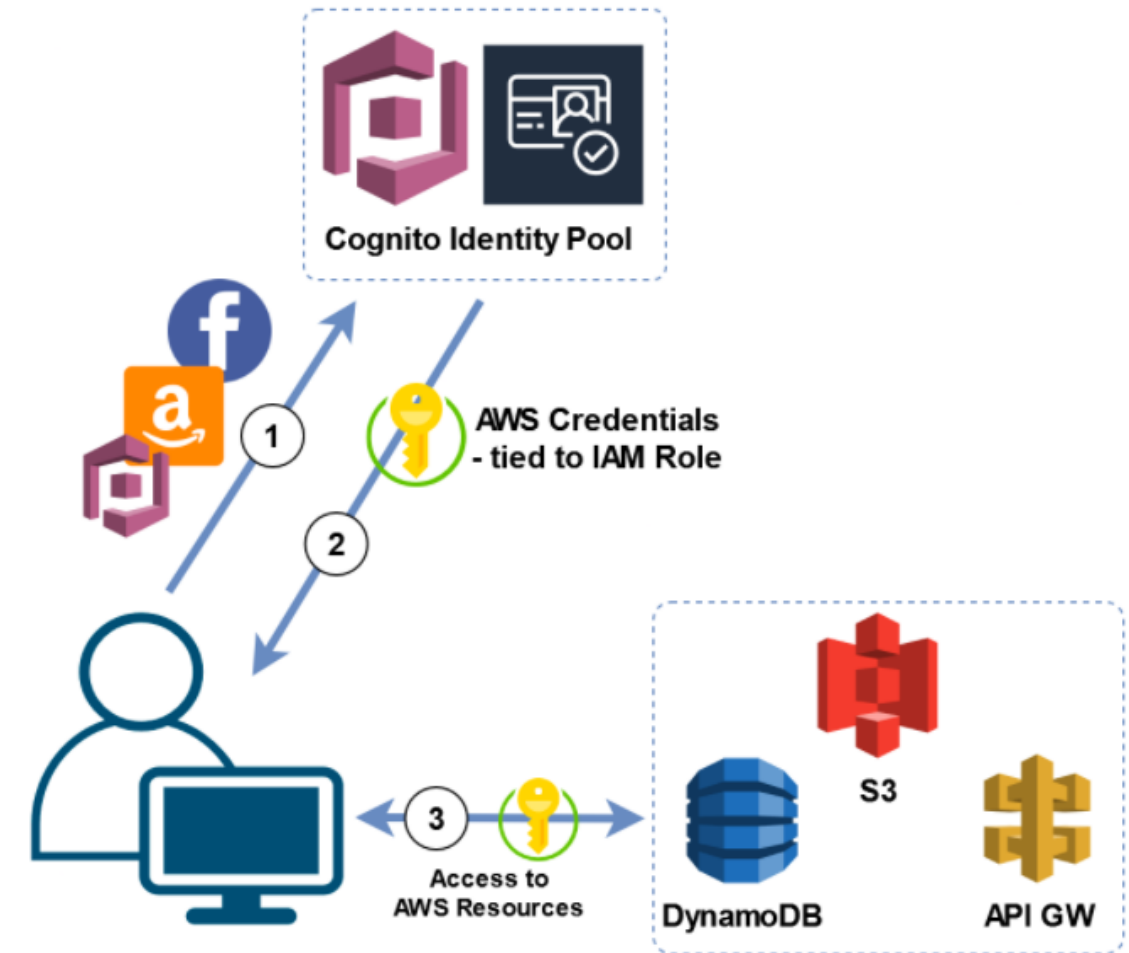
Additional Case: Using AWS AppSync



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.