# Module 01

## IntroductiontoAWS Identity and Access Management (IAM)

# IAM
# OV ERVIEW



rajendra0968jangid

# Business Scenario: Sara is hired!

# Sara’s responsibilities

01

Create an manage AWS Accounts

02

Create Users and Groups

03

Access control Management

04

Authentication and Authorization

05

Follow the Principle of Least Privilege

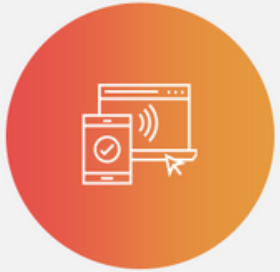
06

Audit User Access

# AWS Account

# Manager Request: Create an AWS Account

01



Access AWS and Cloud res ou rces

02

Pay as you go model (No upfront investment)

03

Communication between accounts is pos s ibl e

04

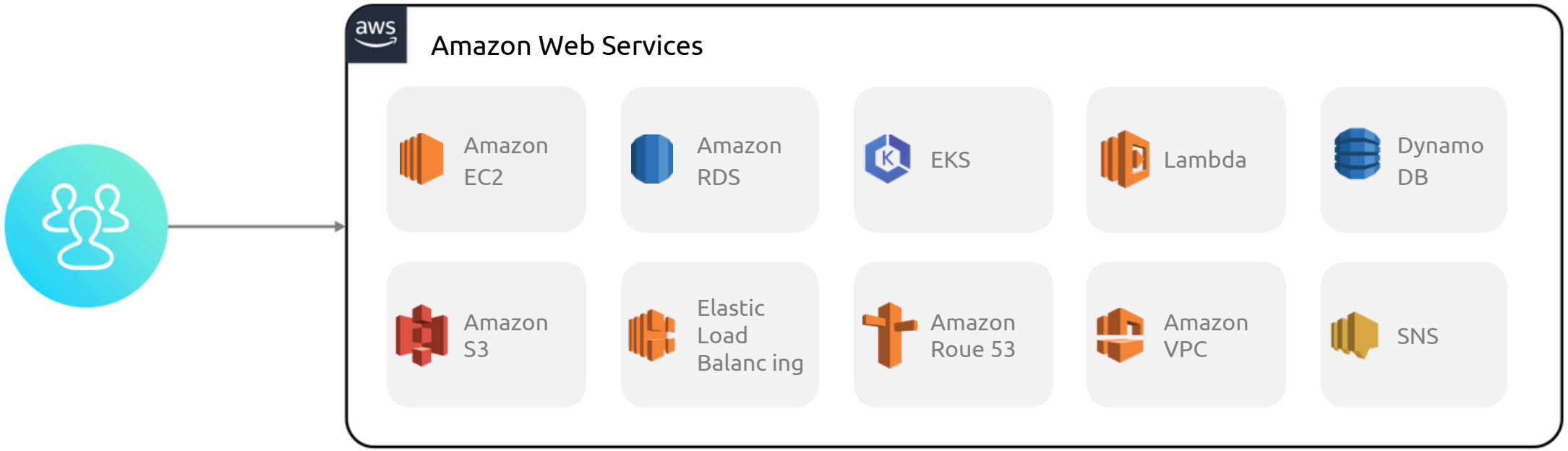
Consolidate billing for many accounts

05

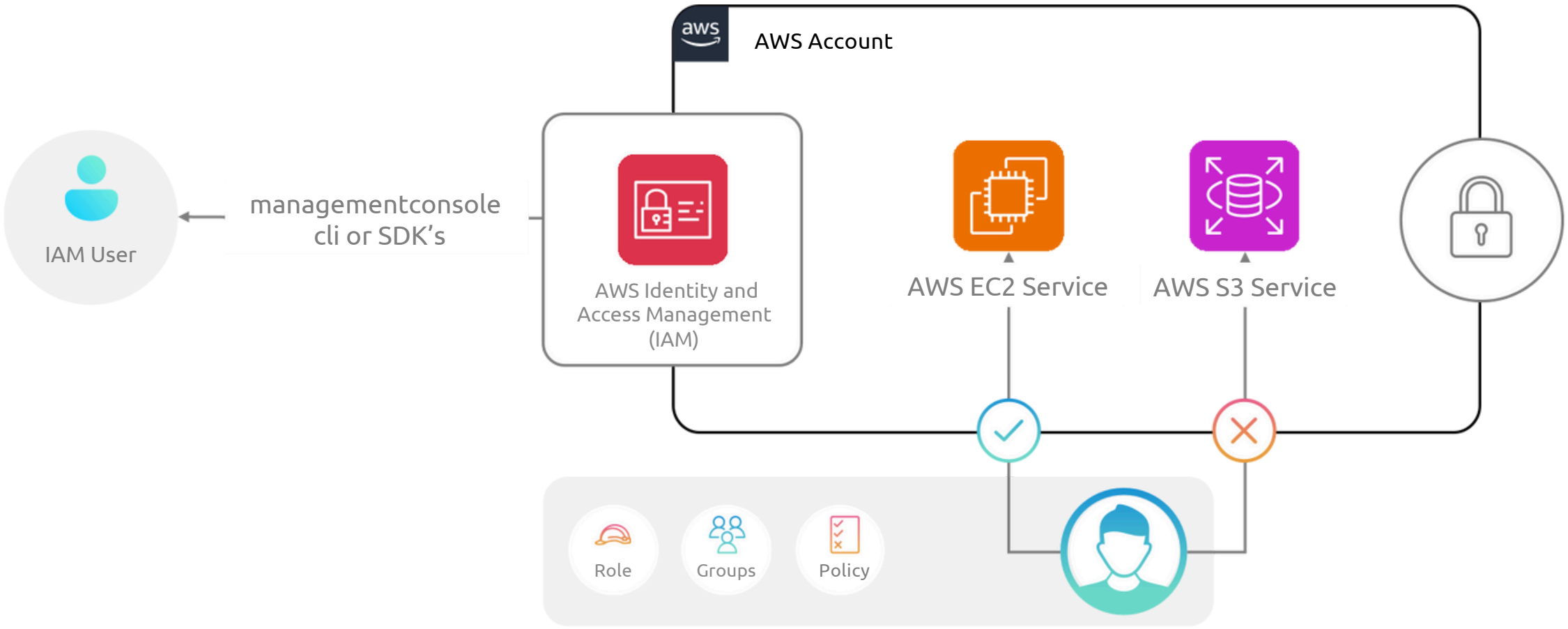
Create accounts for every department or organization unit

# IAM Users

# Allow AWS Access for Users

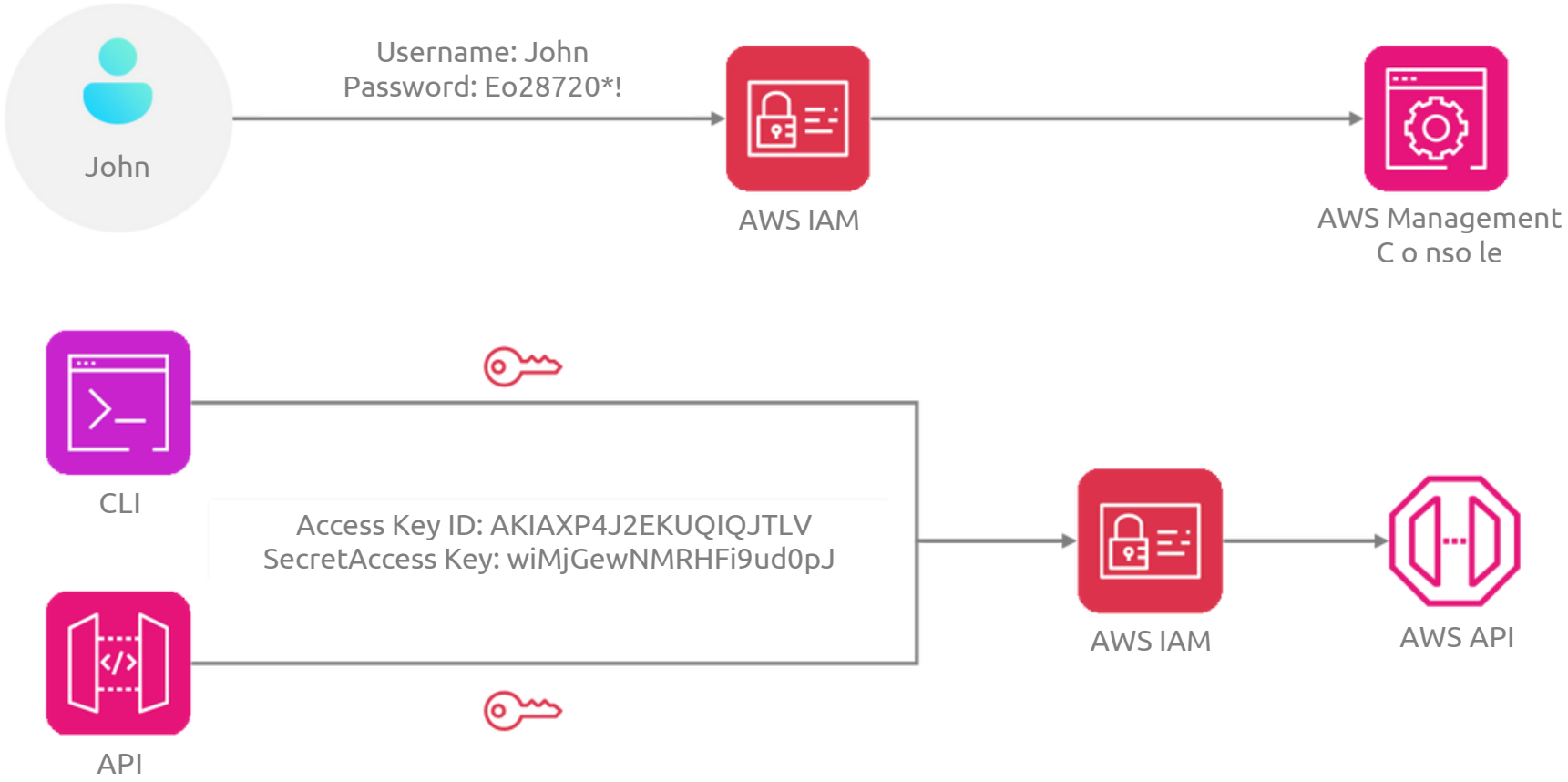


# IAM User


aws
AWS Account
IAM User
managementconsole
cli or SDK's
AWS Identity and
Access Management
(IAM)
AWS EC2 Service
AWS S3 Service
Role
Groups
Policy

# AWS CLIand SDK

# IAM User Access Keys

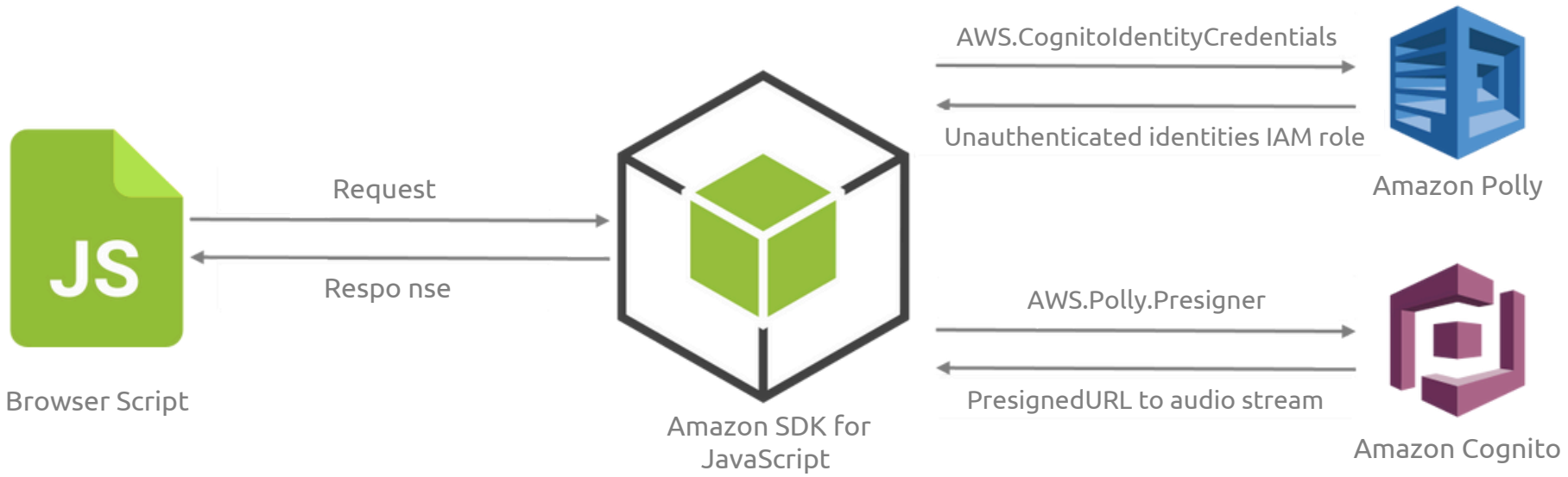


# AWS CLI

aws cli

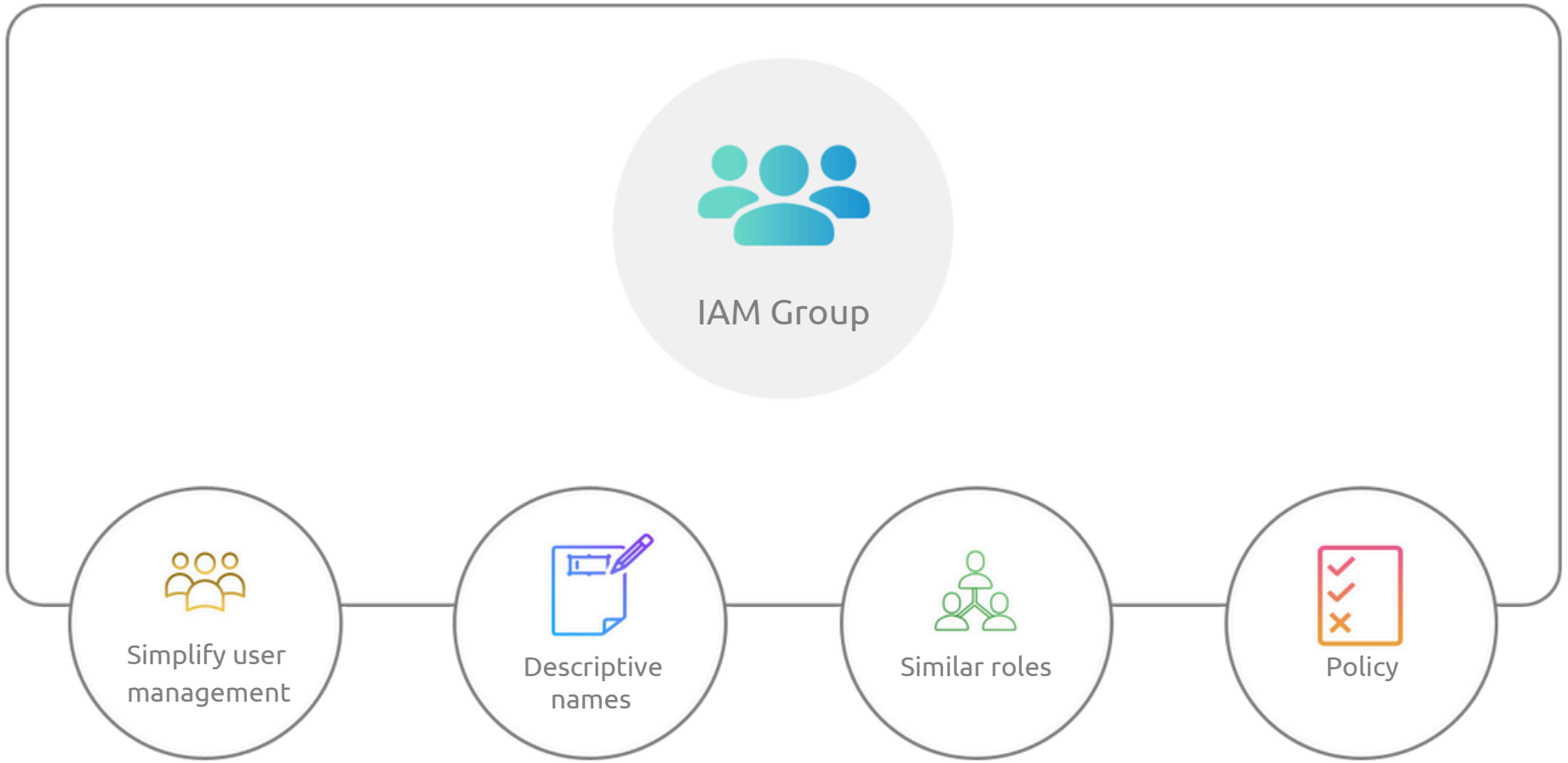
```
→ ~ awsconfigure
AWS Access Key ID [None]: AKIAS7790KQGK63WUK6T5
AWS Secret Access Key [None]: kkQEiBjJSKrDkWBLO9G/JJKQWIOKL/CpHjMGyoiJWW
Default region name [None]: us-east-1
Default output format [None]:
```

# AWS SDK


AWS.CognitoIdentityCredentials
Unauthenticated identities IAM role
Amazon Polly
Request
Respo nse
JS
Browser Script
Amazon SDK for JavaScript
AWS.Polly.Presigner
PresignedURL to audio stream
Amazon Cognito

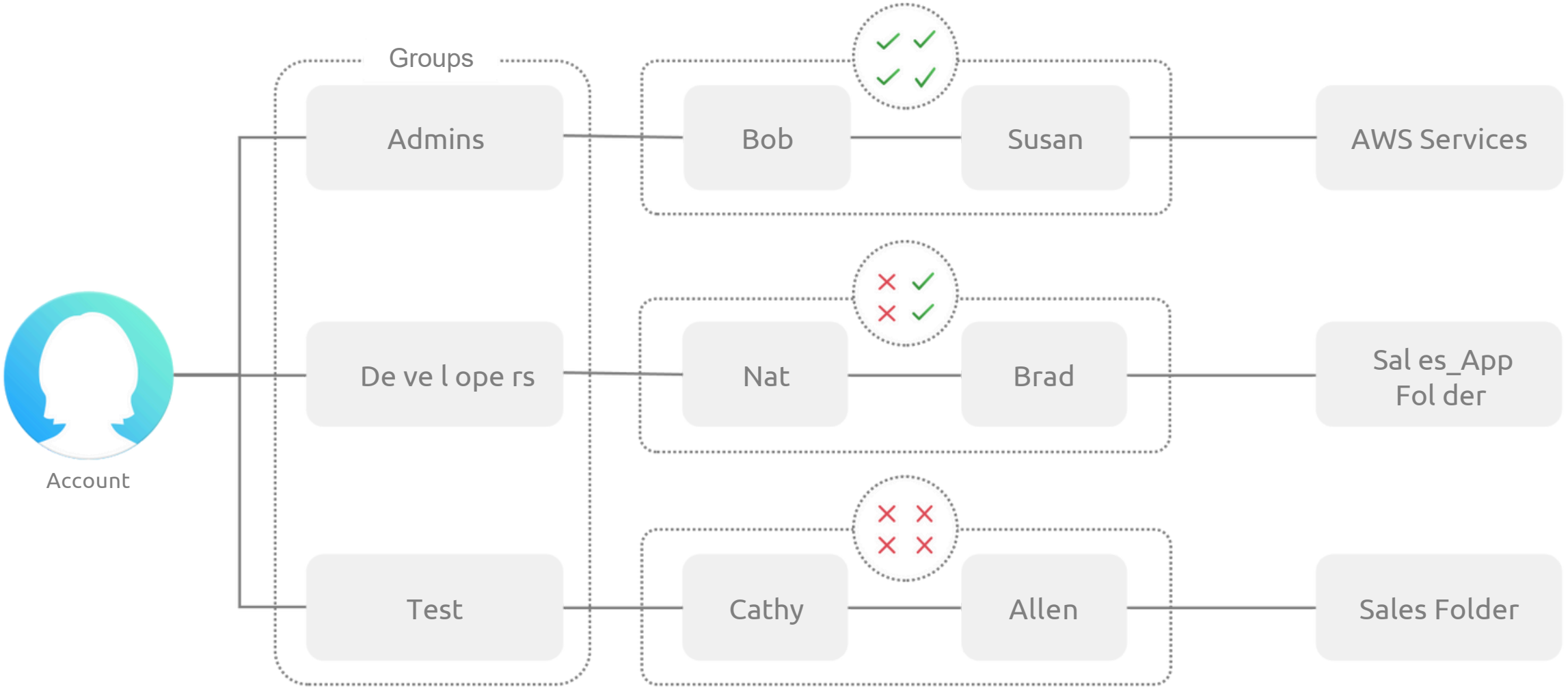
# IAM Groups

# IAM Groups



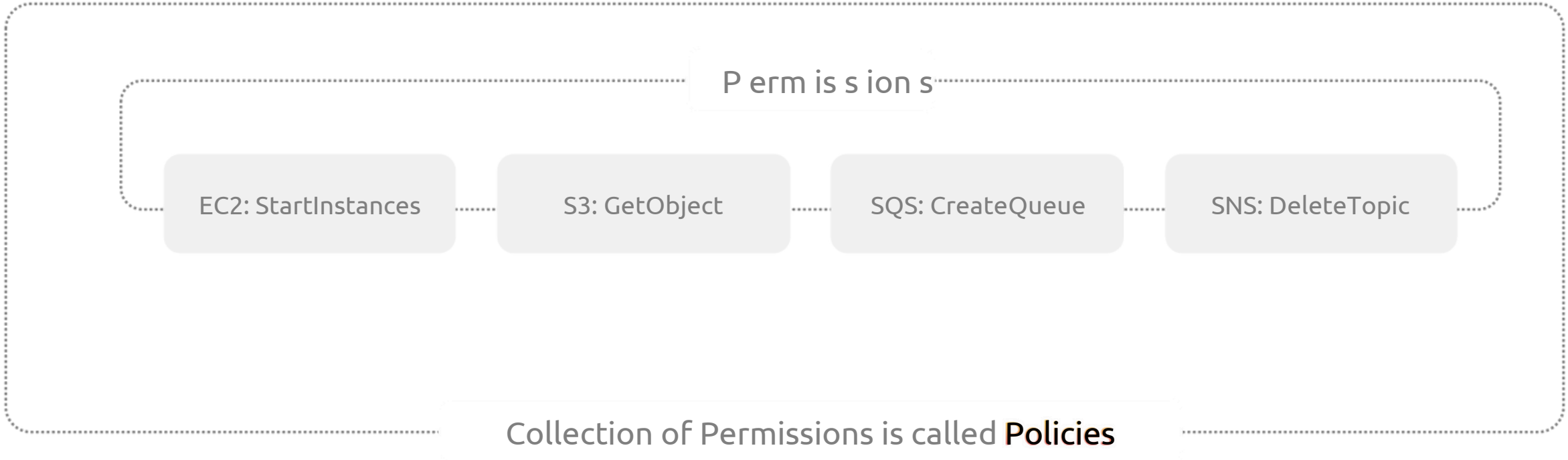
# IAM Policies and Permissions

# Implement the Principle of Least Privilege



# IAM Permissions

IAMpermissionsprovidefine-grained control over the actions performed on AWS resources.



# IAM Policy

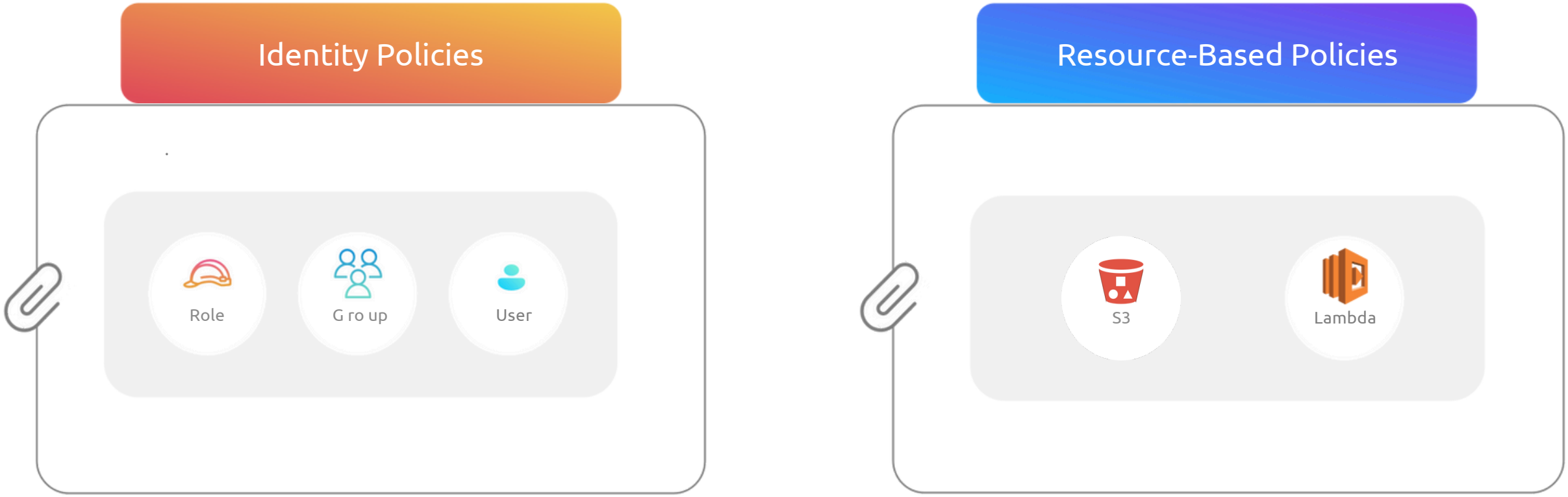
IAM policies manage access and permissions in AWS

A policy defines the permissions and actions for an identity, group or resource

Rules that define what resources an entity can access and what operations they can perform .

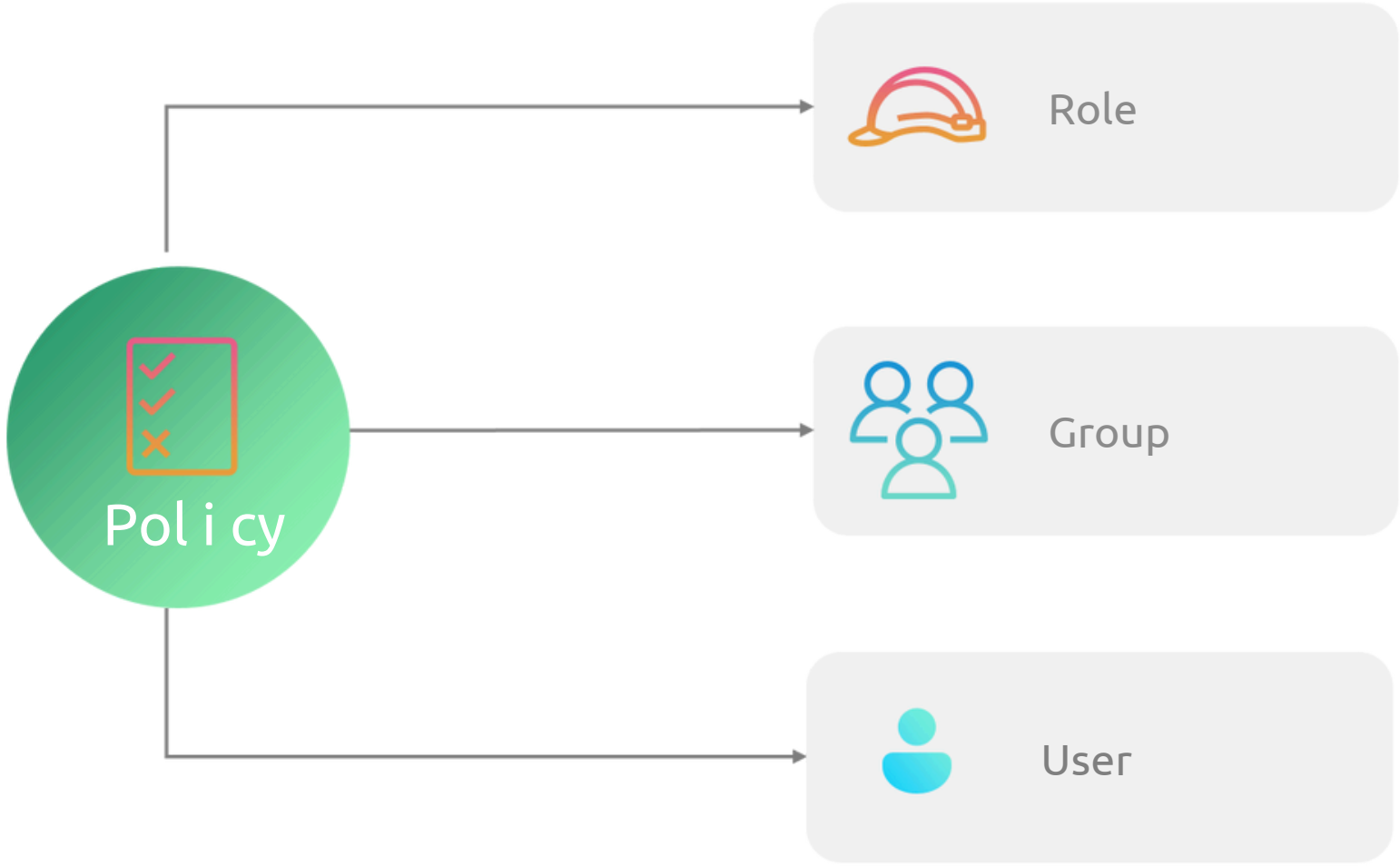
IAM policies provide fine-grained access control for resources and services.

# AWS IAM Policies



# IAM Identity Policies

# AWS Identity Policy

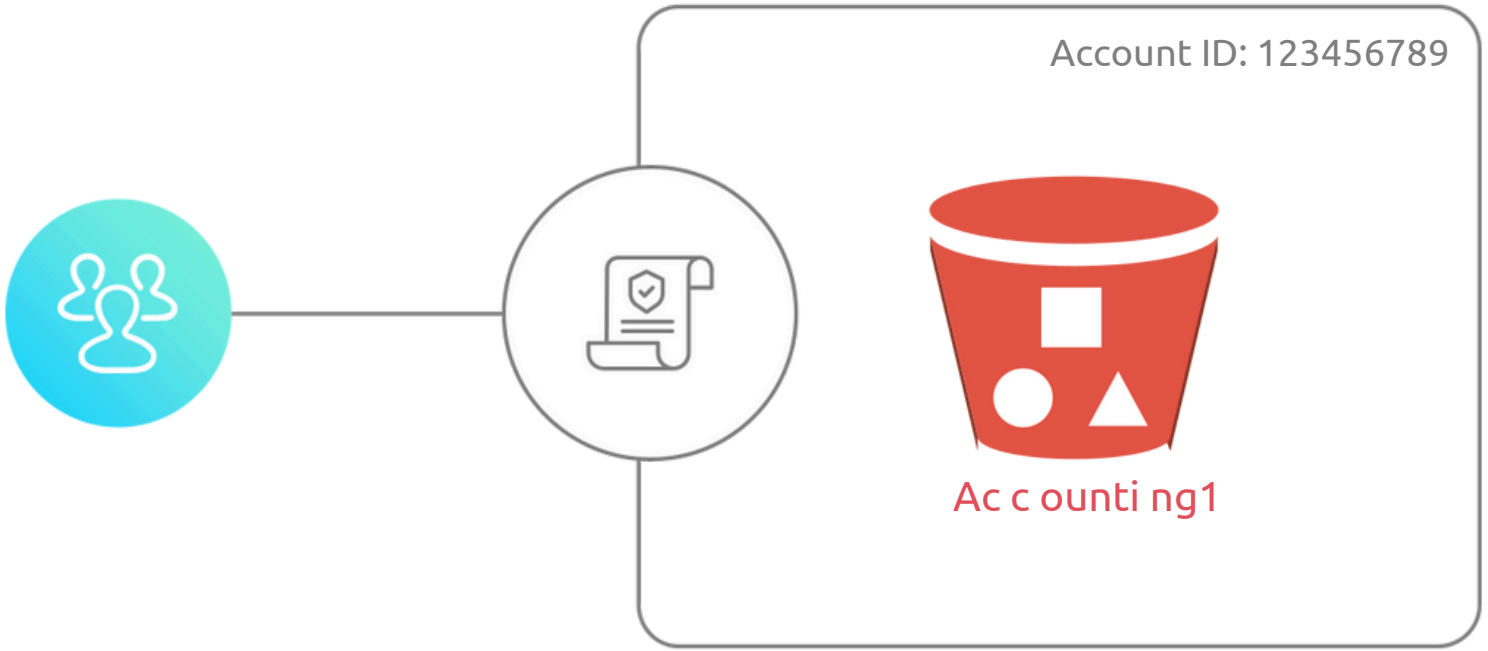


# AWS Identity Policy Example

```
{
    “Version” : “2012-10-17”,
    “Statement”:   [
    {
          “Effect” : “Allow”,
          “Action”:   [
               “s3: *”
          ],
          “Resource”:   [
              “arn: aws:s3 :::<bu cket-n ame>”
          ]
    },
    {
          “Action”:   [
                “ec2 :Start Instan ce”
    ],
    Effect”:  “Allow”,
    “Resource”: “arn:aws:ec2:::<Instance-Id>”
     }
    ]
  }
```

# IAM resource-Based Policies

# AWS Resource Based Policy

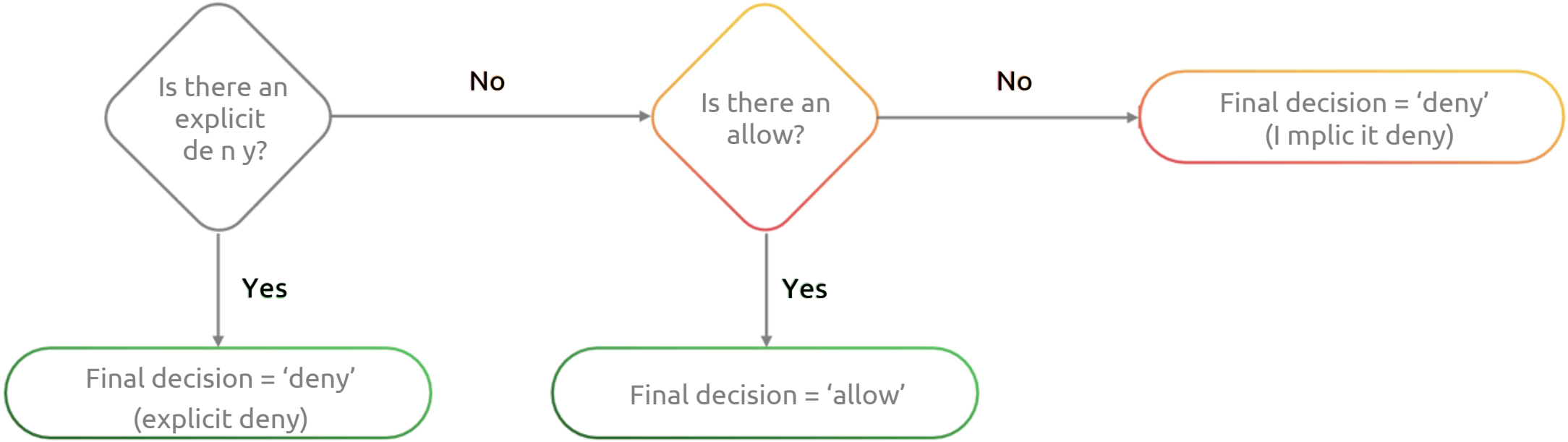


# AWS Resource Policy Example

exam ple

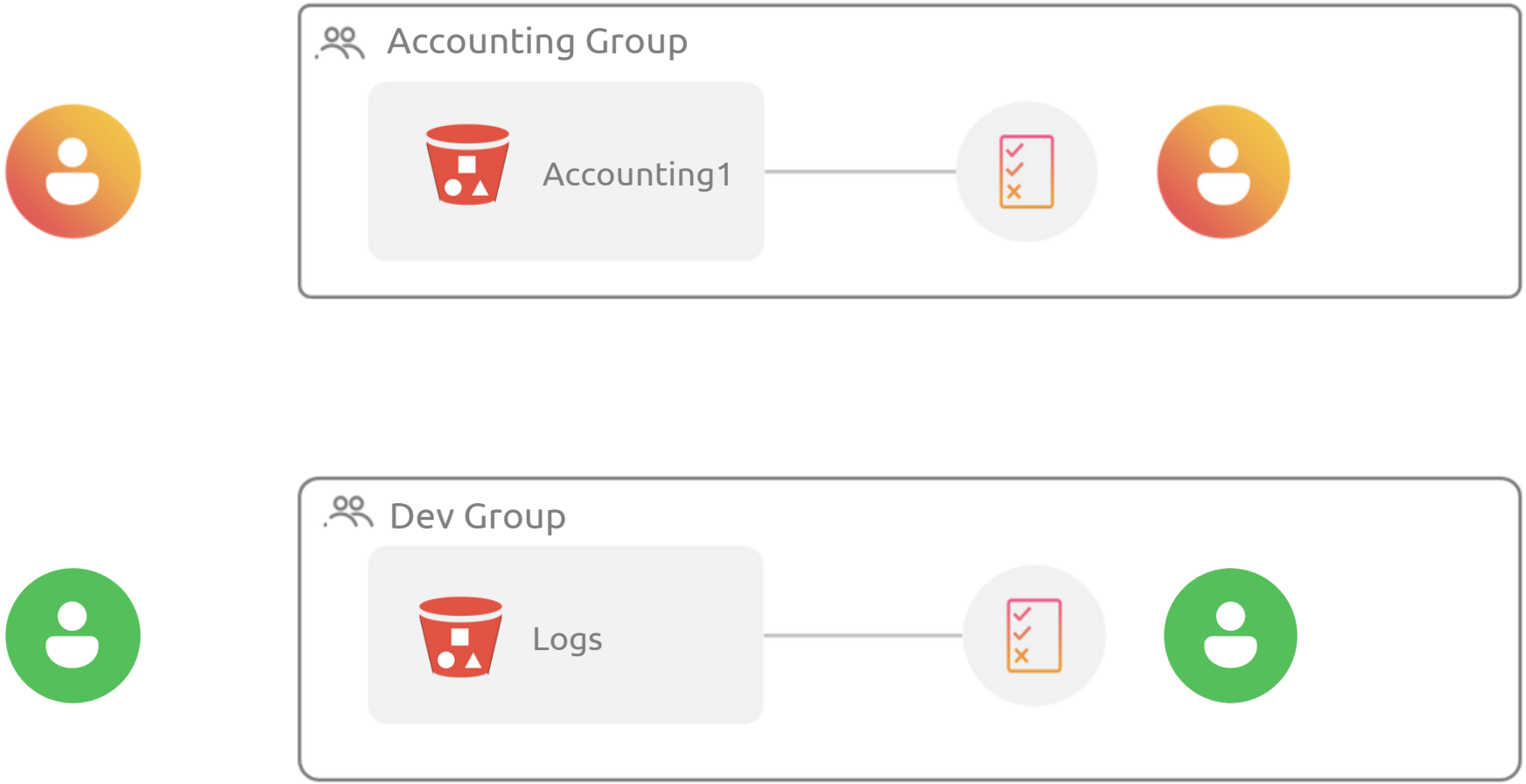
```
{ "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789:group/accounting"
            },
            "Action": "s3:*",
            "Resource": [
                "ar n:a ws: s3: ::a cco unt ing 1",
                "ar n:a ws: s3: ::a cco unt ing 1/* "
            ]
        }
    ]
}
```

# How Are IAM Policies Evaluated?



# IAM Permission Boundaries

# Manager Request: We are hiring interns



# Permission Boundary

Sets the maximum permissions an IAM entity (such as a user or role) can be granted

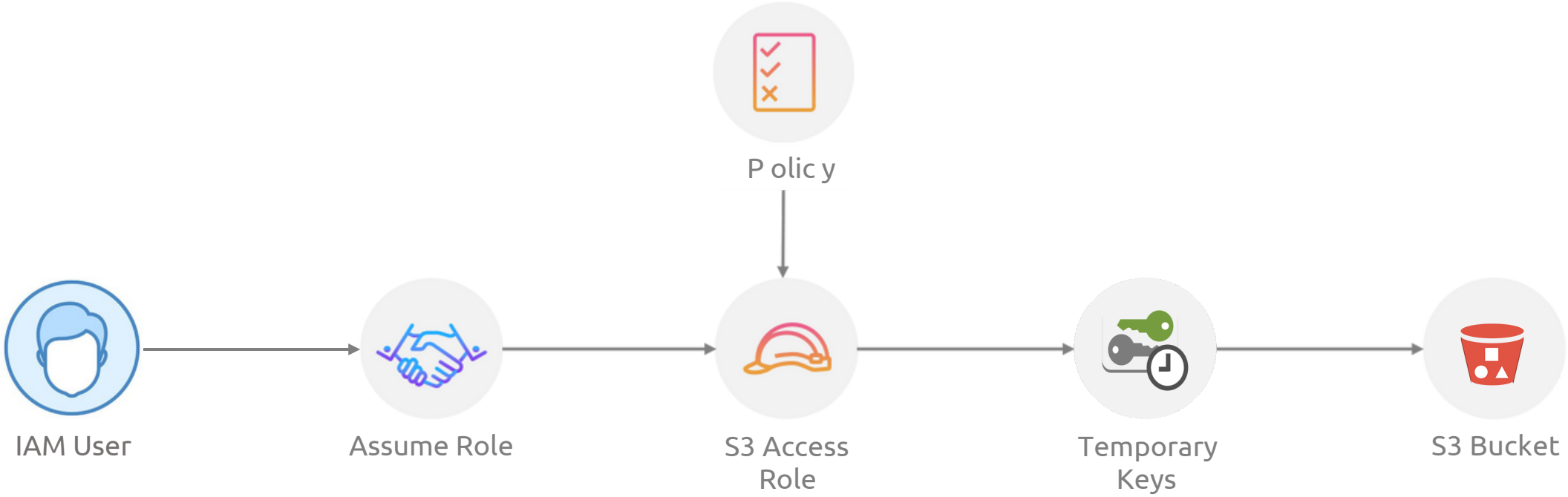
A guardrail to prevent unintended access to resources and enforce the principle of least privilege.

Restricts the entity's IAM policies, ensuring they cannot exceed the defined boundary.

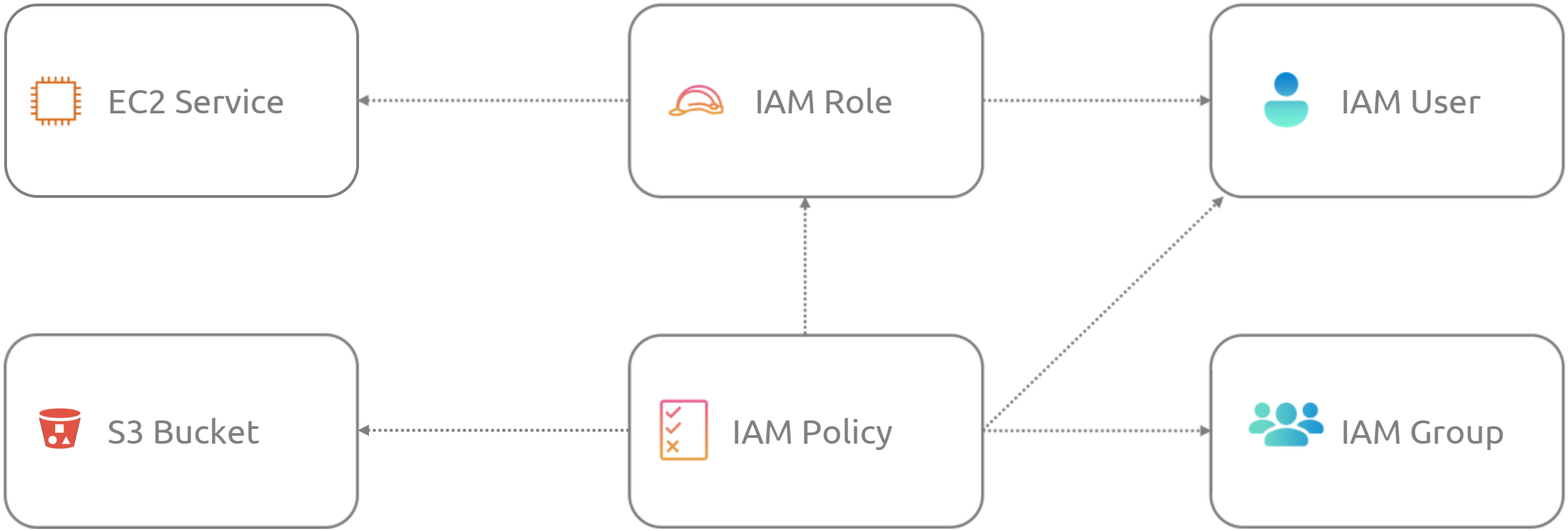
Control and limit the scope of permissions for different users and rol es

# IAM Roles

# Increase security by using IAM roles

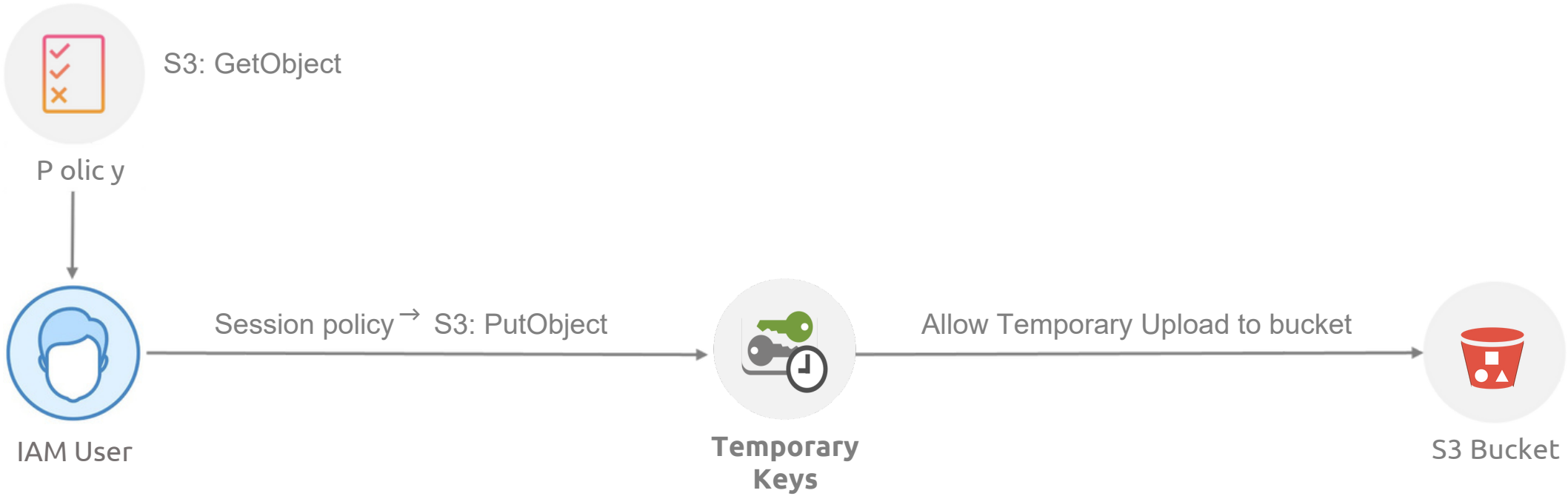


# AWS IAM Role



# IAM Session Policies

# Manager request: Allow temporary upload to S3 bucket



# Session policies

Session policies define the maximum permissions granted to IAM users when they assume an IAM role.

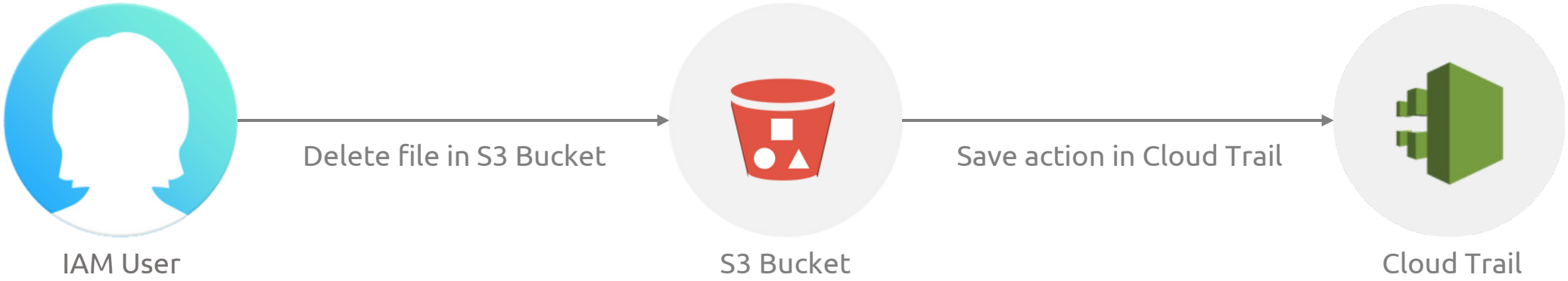
They are used in conjunction with IAM roles to further restrict the permissions an IAM user has.


Session policies are temporary, ensuring that users have the necessary access only when needed.

You can implement granular access controls for various users and scenarios.

# Auditing with CloudTrail

# Manager Request: Audit user access to S3 objects



# Cloudtrailand User Access Audit

Log API calls to AWS services, for example stop an ec2 instance.

Audit actions taken by users, services and AWS resourc es.

Track and review API calls made by AWS IAM users, for example access an S3 buc ket.

Detect successful and unsuccessful login attempts and detect security threats.

# Module 02

## IAM Policies,Federation, STS and MFA

# Sara must handle the following

**01 |** AWS Managed Policies

**02 |** Customer Managed Policies

**03 |** Inline Policies

**04 |** Multi-Factor Authentication (MFA) and password policies

**05 |** Fe de ra ti on

**06 |** SSO and STS

**07 |** RAM

**08 |** VPC Endpoints

# Sara’s Task List

01

Document employee department and respo nsibilit ies

02

Create a list of resourcesand access level per employee

03

Create policies by grouping proper permissions

04

Create groups with similar responsibilities and attach policies to gro ups

05

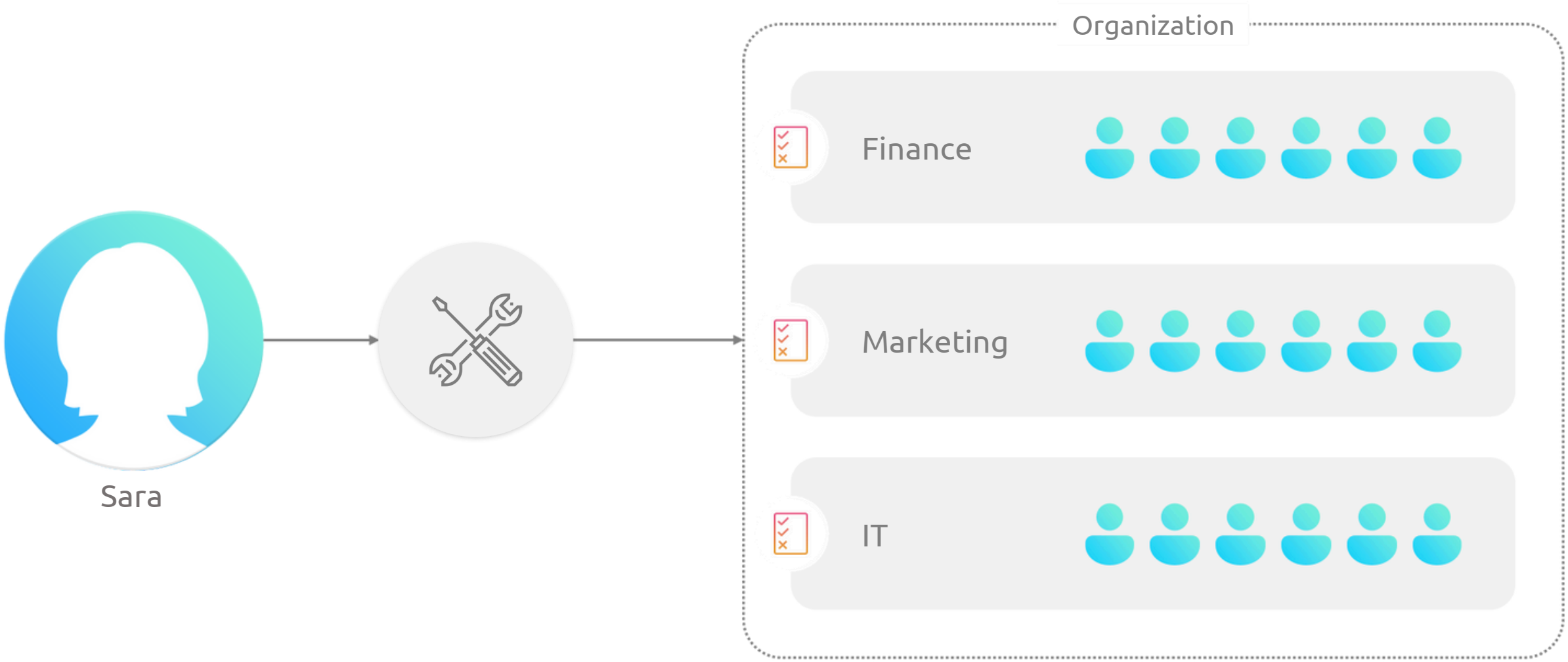
Add users to groups and attach inline policies as needed

06

Configure resources with resource-based po lic ie s

# IAM Access Control

# Manager Request: Sara must configure access control for all employees



# Identity Policy Options

## AWS Managed policies

Pros

- Quick and easy to use

Cons

- May not cover all use cases

## Customer Managed policies

Pros

- More customizable and can be re-used.

Cons

- Require more management overhead

## Inline policies

Pros

- Attaches directly to an entity

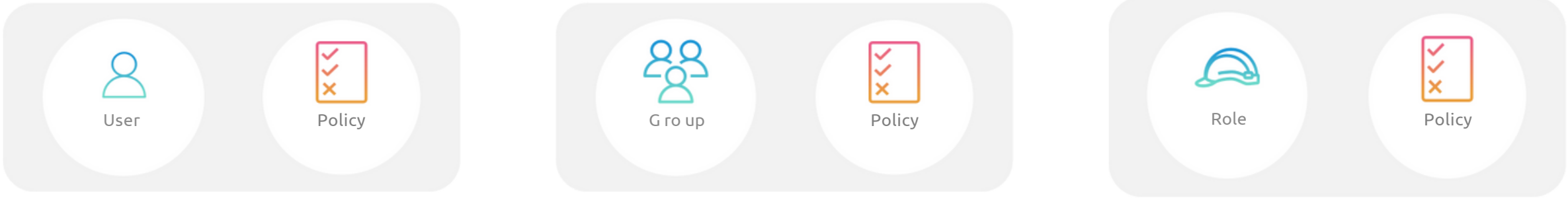
Cons

- Can't be re-used
- Require more management overhead.

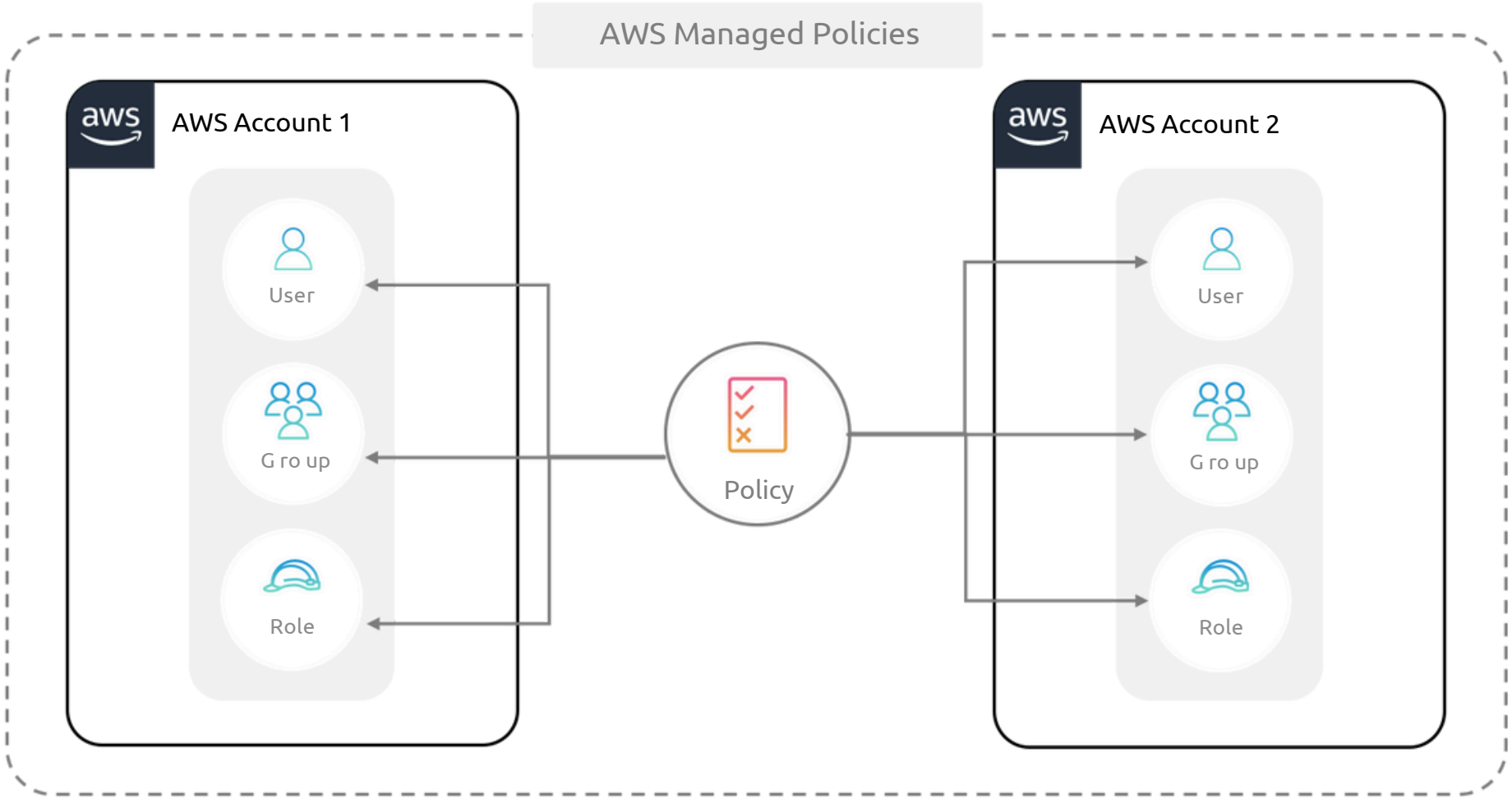
# Inline vs Managed Policies

# Inline Policies

Inlinepoliciesarecreated and attached directly to an IAM entity.



# AWS Managed Policies




Managed policiesallowyoutodefinepoliciesonceandapplythemtomultiple entities,
making it easier to manage and update policies at scale.

# IAM Policy Building Blocks

IAM Policies


**E ffect**
Allow,Deny

**Actions**
S3:GetObject, EC2:StartInstance

**Resources**
arn:aws:s3:::my-bucket/*, arn:aws:ec2:us-east-1:123456789012:i n sta n ce/i-0123456789a b cd ef0

**Conditions**
timeofday,source IP address

**P rincipa l**
Entitythatthe policy applies to

# IAM Conditions

Used to define additional constraints or requirements

Conditions are Key-Value pairs definingstate or value

# IAM Conditions Examples

1

Time Based

2


IP Based

3

Geo Based

4

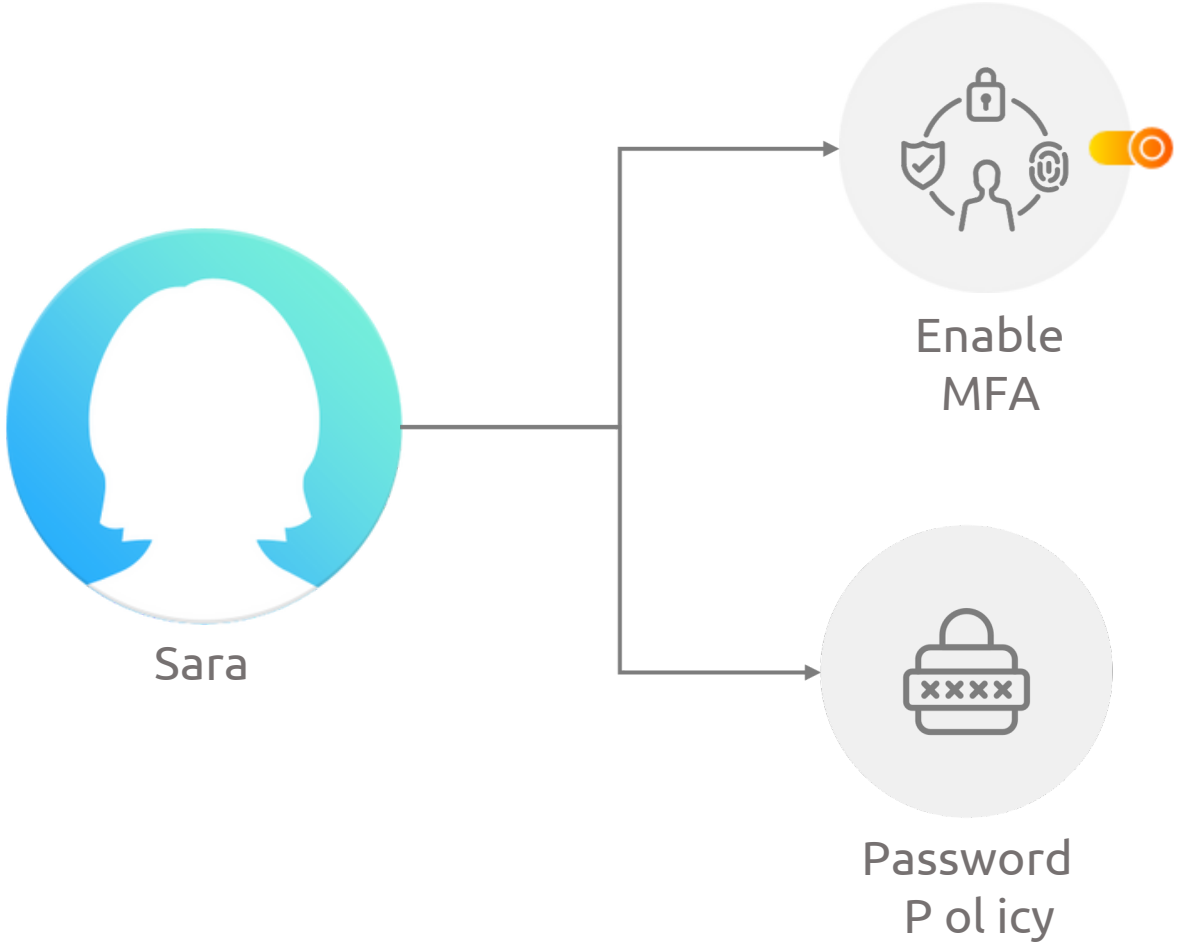
User Based

# AWS Resource Policy Example

exam ple

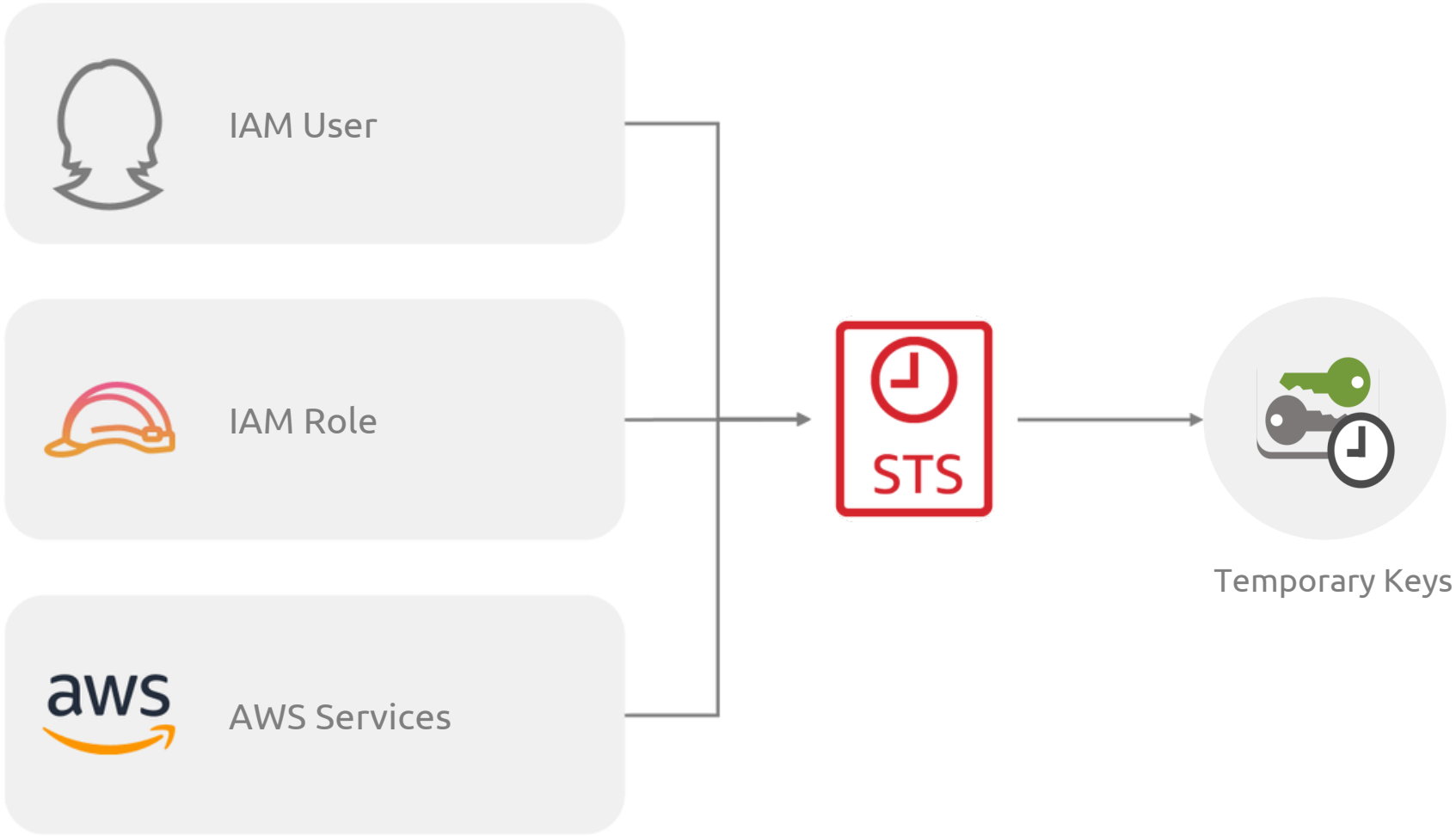
```
{  "Version": "2012-10-17",
      "Statement": [
            {
               "Effect": "Deny",
               "Action":    "*",
               "Resource": "*",
               "Condition": {
                     "NotIpAddress": {
                           "aws:SourceIp": [
                                 "tr ust ed- ip- ran ge- 1",
                                  "trusted-ip-range-2"
                                       ]
                                    },
                     "NumericLessThan": {
                           "aws:CurrentTime": "09:00"
                        },
                     "NumericGreaterThan": {
                           "aws:CurrentTime": "17:00"
                        }
                     }
               }
 ] }
```

# Manager Request: Enable MFA and password policies for IAM users

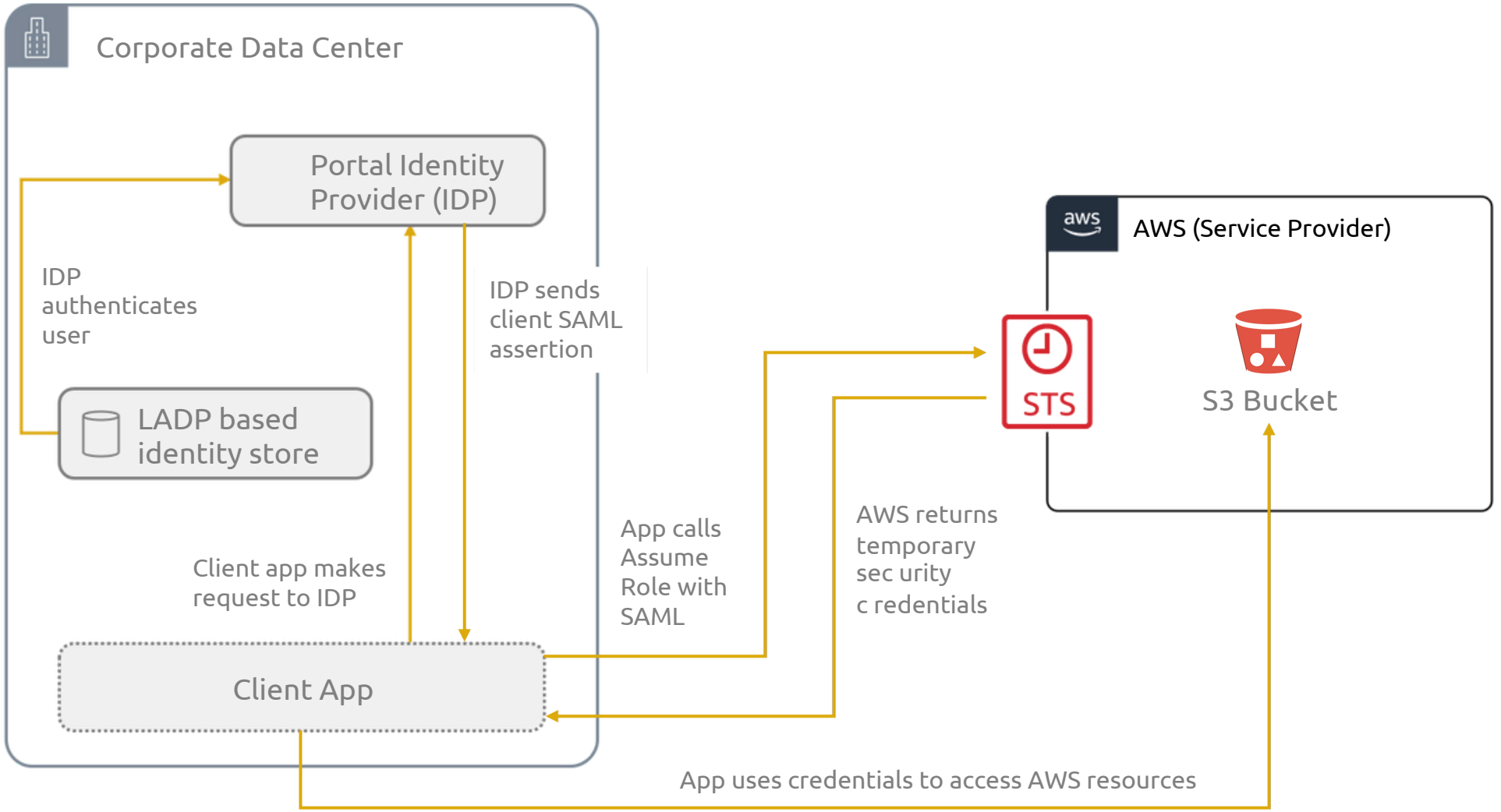


# Security Token Service (STS)

# Security Token Service (STS)

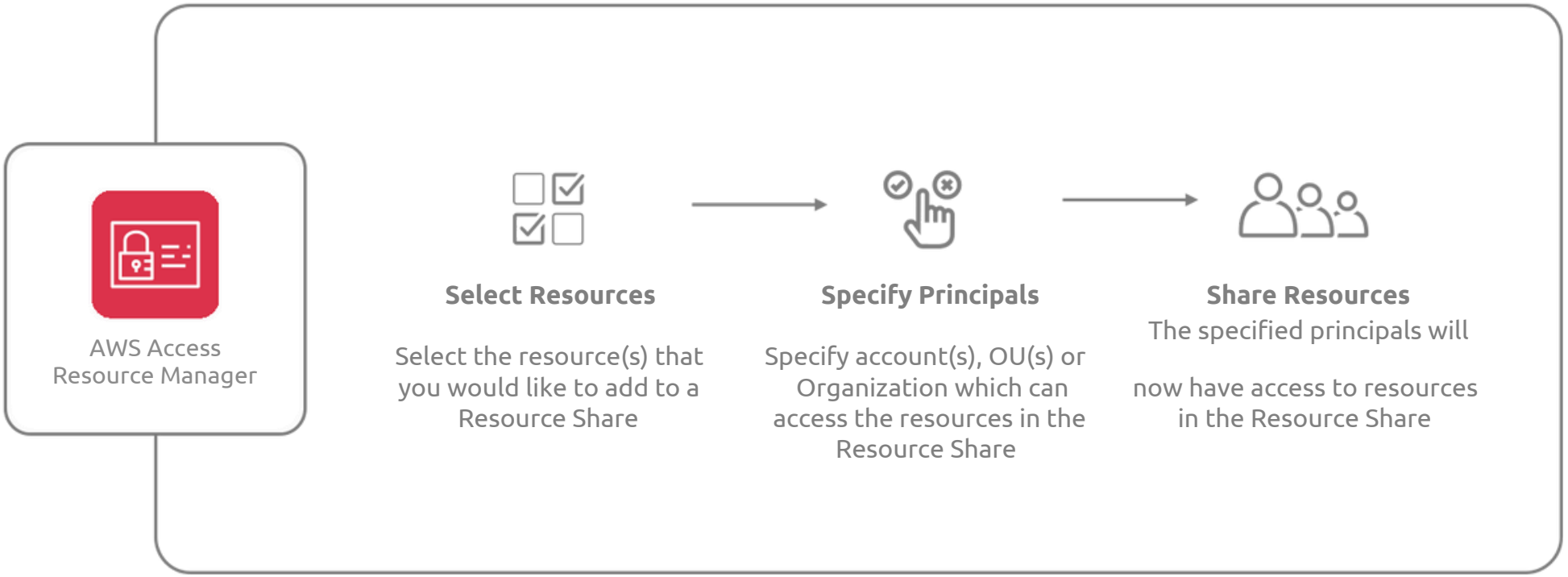


# STS Example


Corporate Data Center
Portal Identity Provider (IDP)
IDP authenticates user
LADP based identity store
IDP sends client SAML assertion
Client app makes request to IDP
Client App
App calls Assume Role with SAML
AWS returns temporary sec urity c redentials
aws
AWS (Service Provider)
STS
S3 Bucket
App uses credentials to access AWS resources

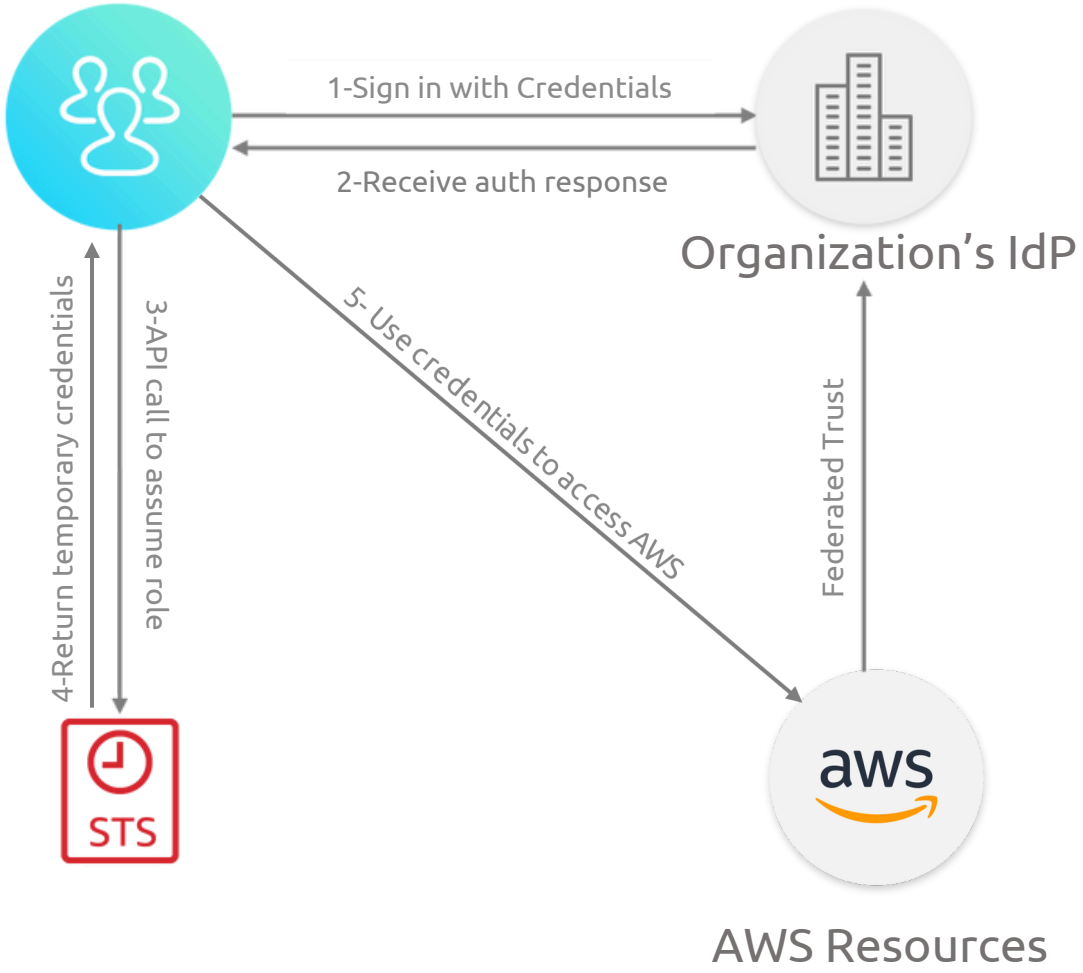
# AWS Resource Access Manager (RAM)

# Share resources with RAM

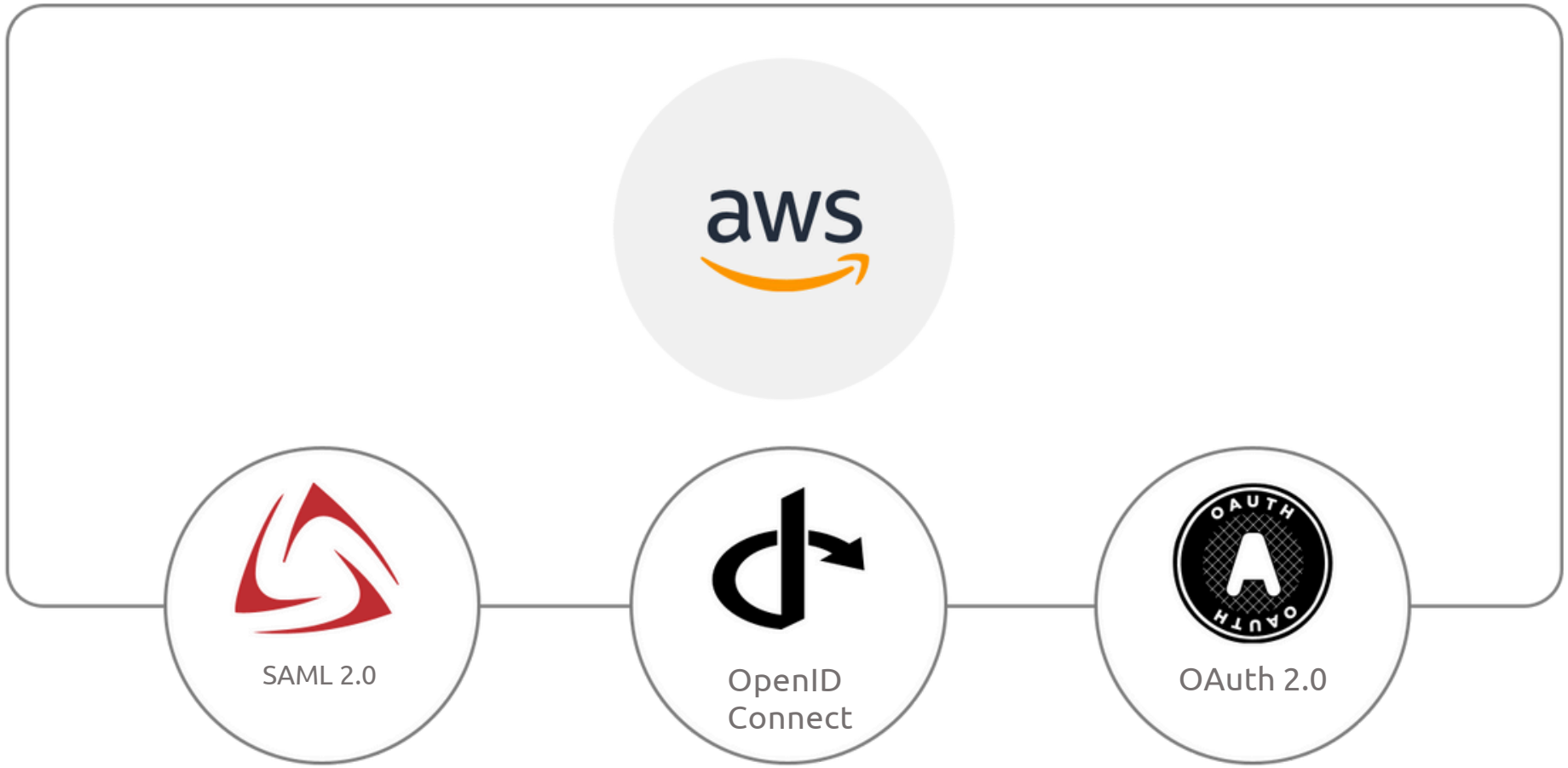


# Identity federation in AWS

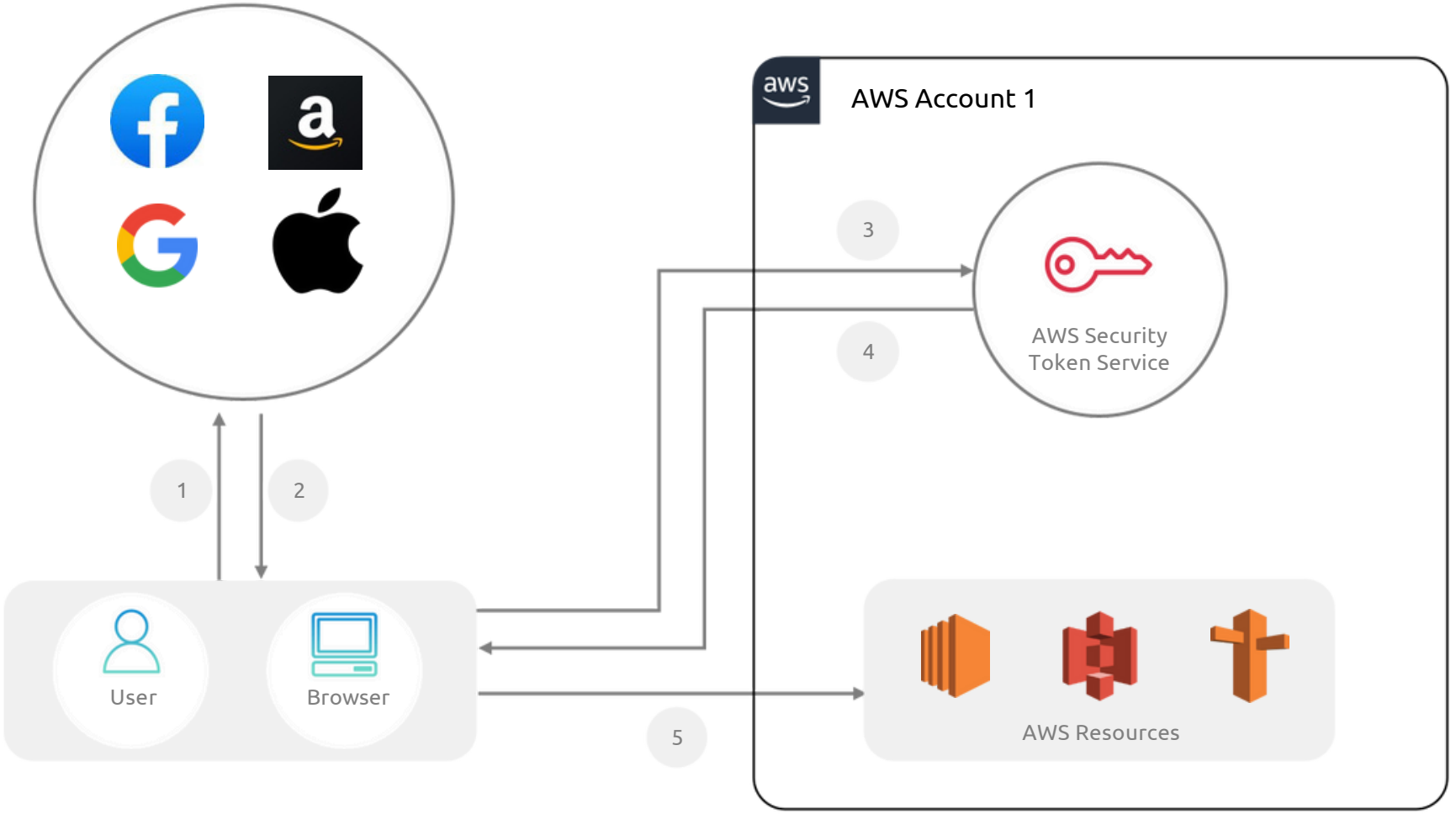
# Identity Federation in AWS



# Identity Federation Standards



# Web Identity Federation



# Benefits of Identity Federation in AWS

01

## Simplified User Management

Users can access AWS resources using their existing organizational credentials.

02

## Centralized Authentication

Administrators can manage user access through a central location.

03

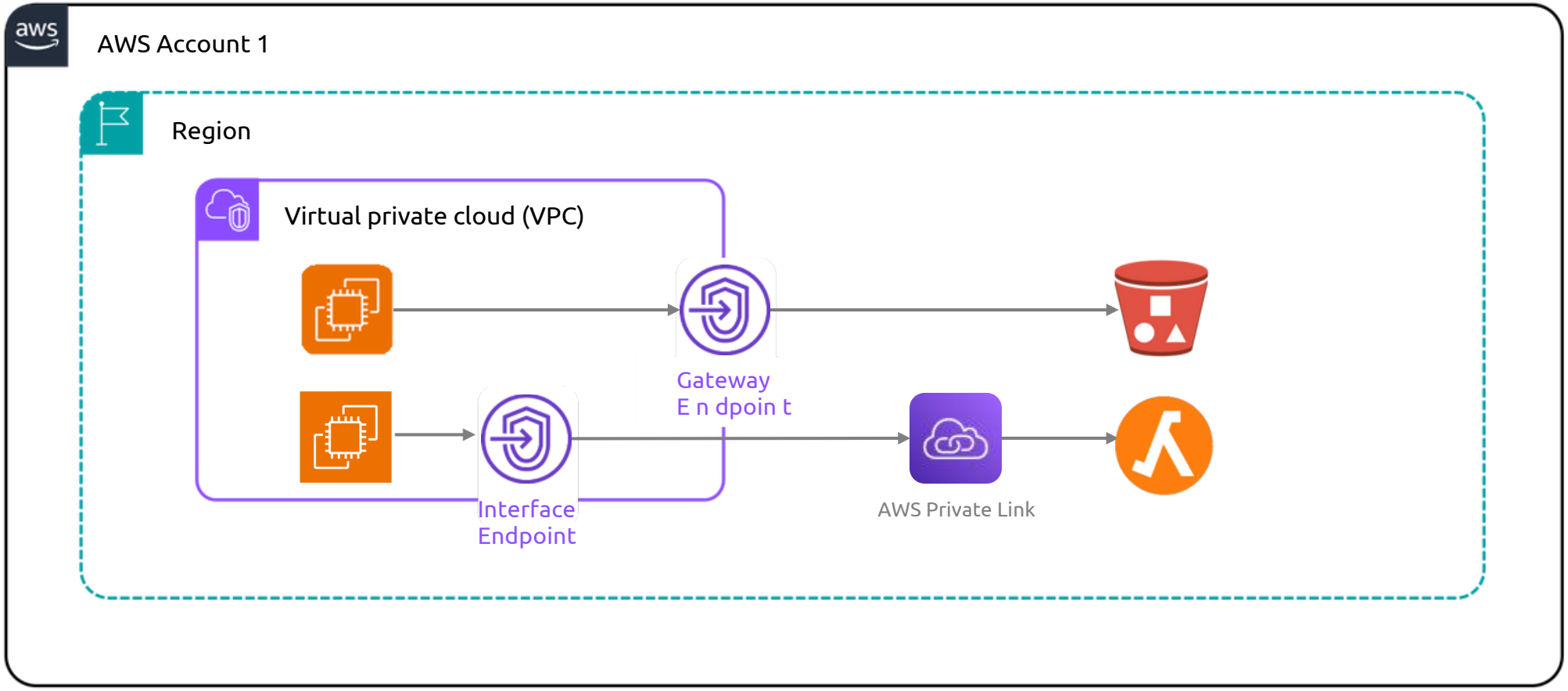
## Improved Security

Reducing the risk of errors and improving overall security posture.

# AWS Private Link

# AWS Private Link and VPC Endpoints

AWSPrivateLinkallowsyoutosecurelyaccessAWSserviceswithoutexposing your traffic to the internet.



# Module 03

## ConfigureAWSIAM at Scale

# Sara must plan for expansion

01 | Create AWS accounts for each department

02 | Enable Centralized IAM management using AWS Organizations

03 | Configure IAM cross account ac c ess

04 | Monitoring user access using Cloudtrail

05 | Setting alarms for resource usage using Cloudwatch

06 | Implement security, governance and compliance measures using AW S Config

07 | IAM Anywhere

08 | IAM Identity Center

# Manager Request:

## Create Accounts For Every Department

01

Isolation and Resource Management

02

Security and C o mplianc e

03

Cost Allocation and Budgeting

04

Resource Scaling P erfo rmanc e

05

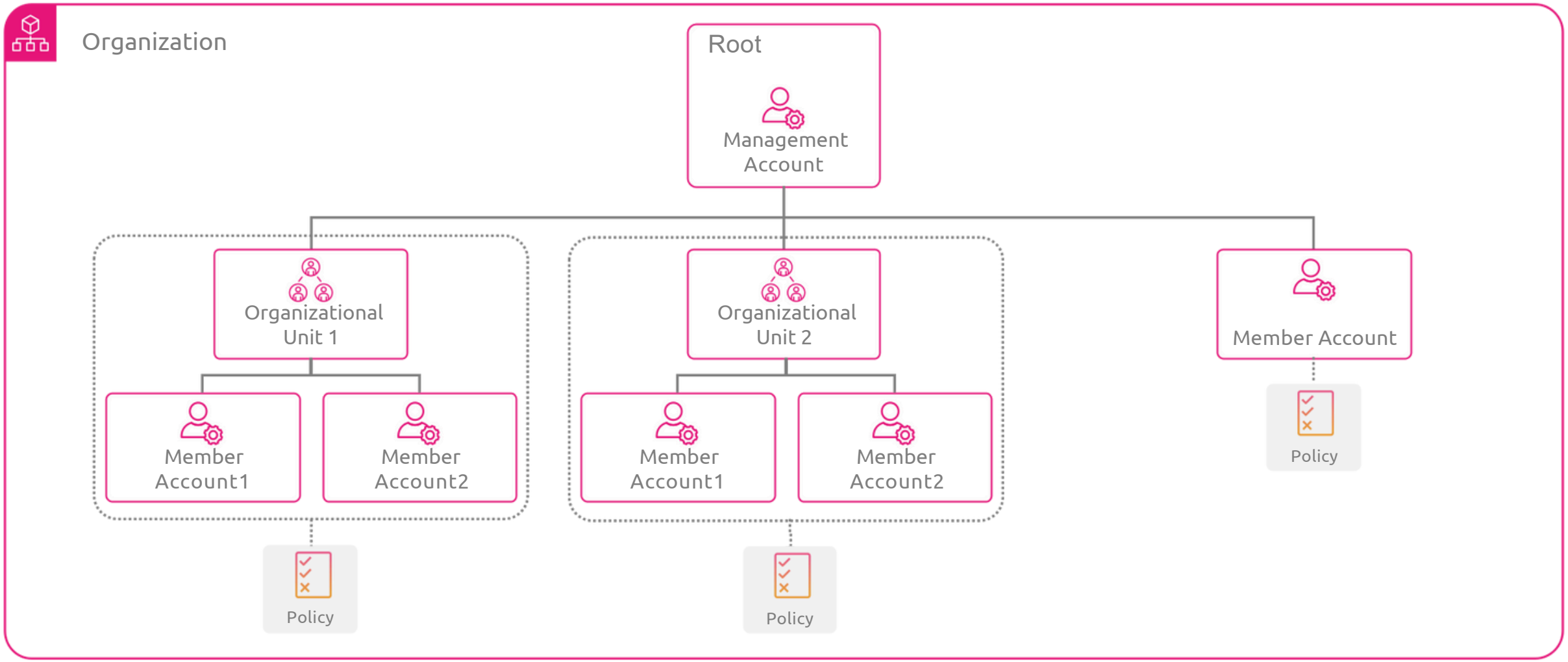
Development and Testing

06

Agility and Innovation

# AWS Organizations

# AWS Organizations



# AWS OrganizationsBenefits

**01**

Centralized Billing

**02**

Resource Sharing

**03**

Access Ma na gem ent

**04**

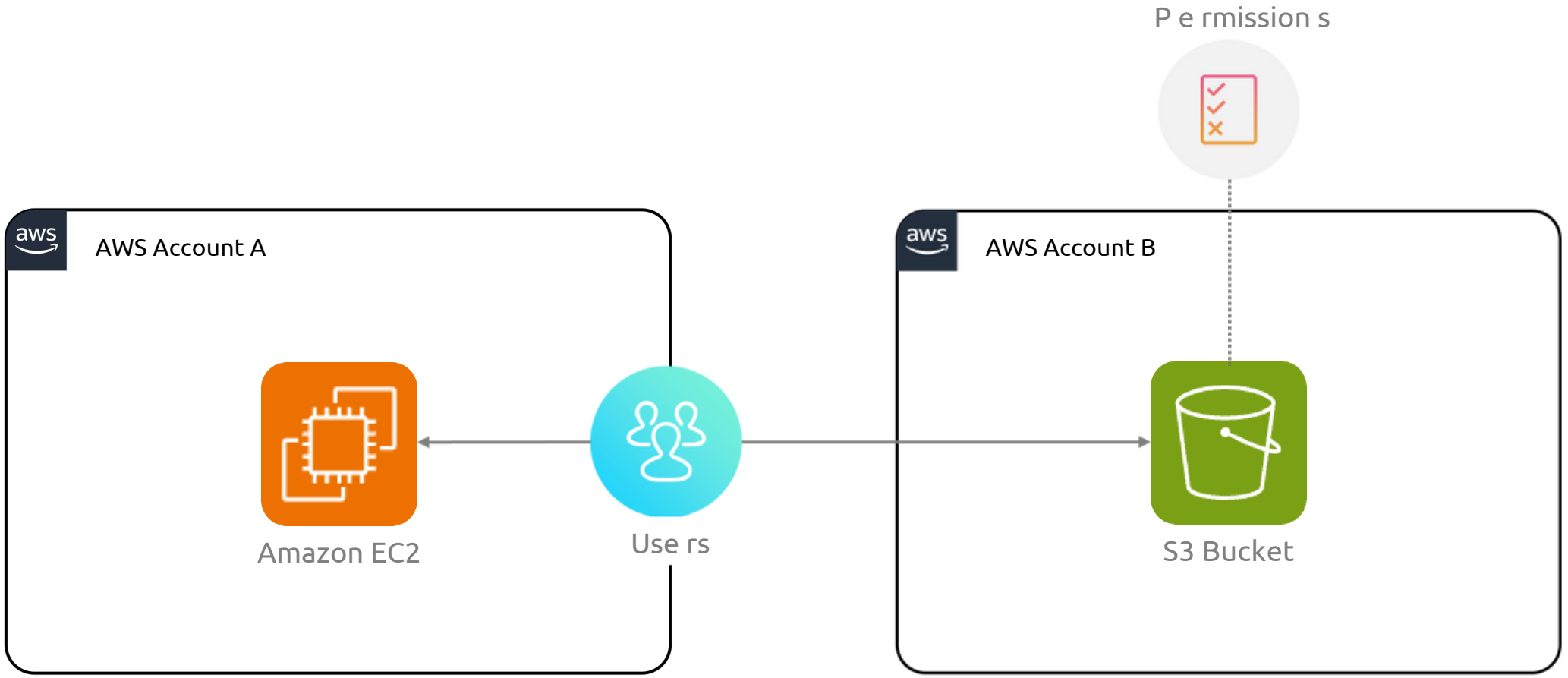
Com pl ia nce

**05**

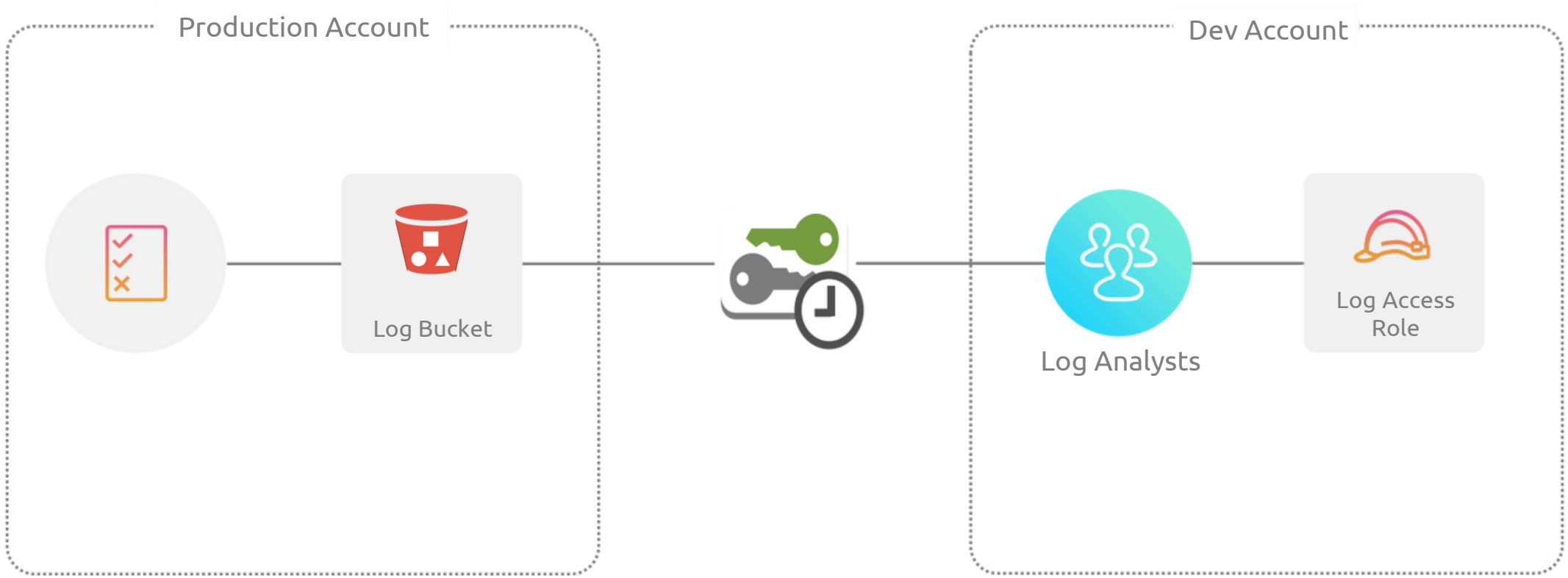
Simplified Account Management

# IAM cross account access

# IAM Cross Account Access



# Manager Request : Provide log access to Log Analysts group



# Centralized logging and m onitoring

# Centralized Logging and Monitoring

01

CloudTrail

CaptureAPICalls

02

C loudW atc h

Capture Metrics and Logs

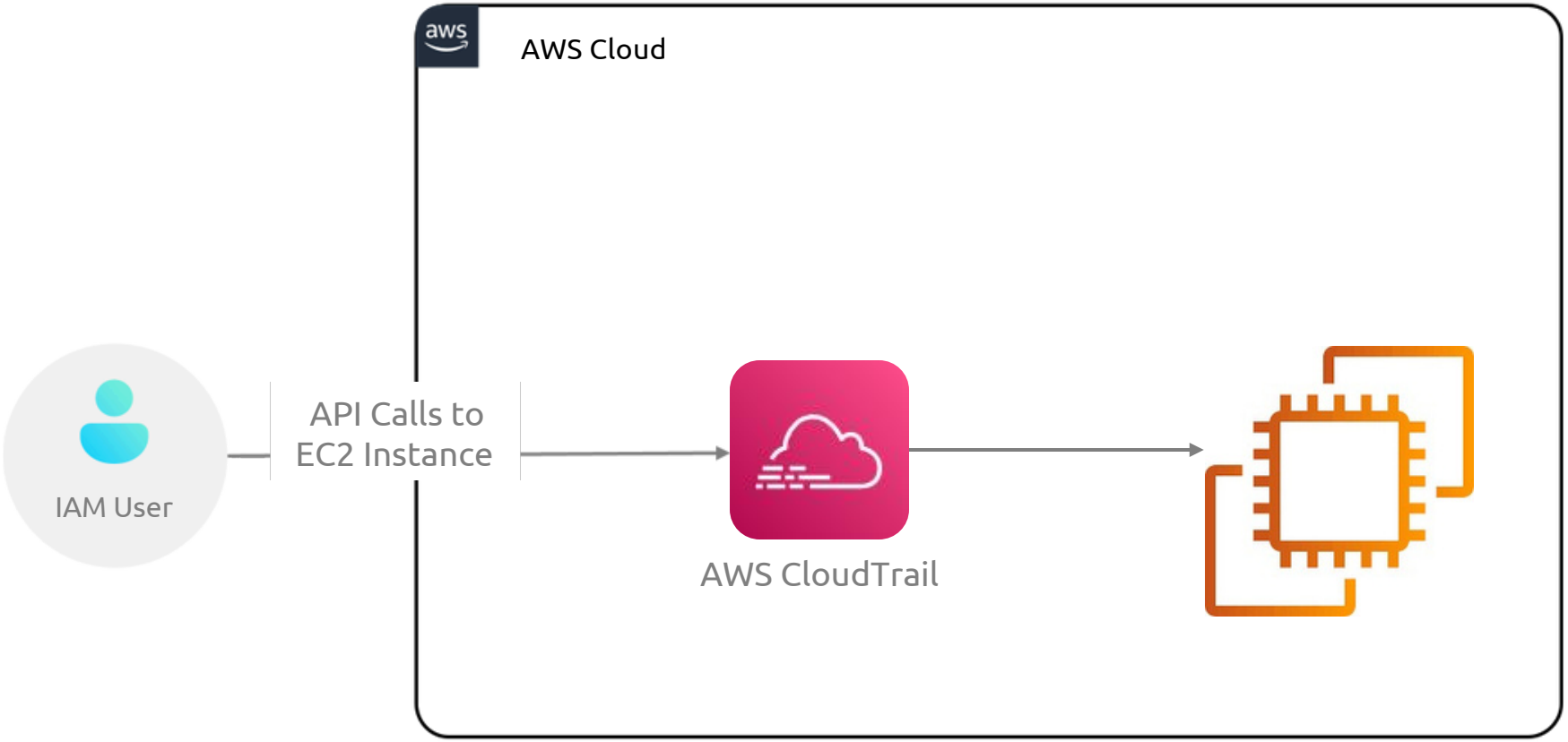
03

AWS Config

Enforce Governance Policies

# Monitoring user access using Cloudtrail

# Manager Request : Investigate who shutdown an EC2 instance



# AWS CloudTrail

AWS CloudTrail

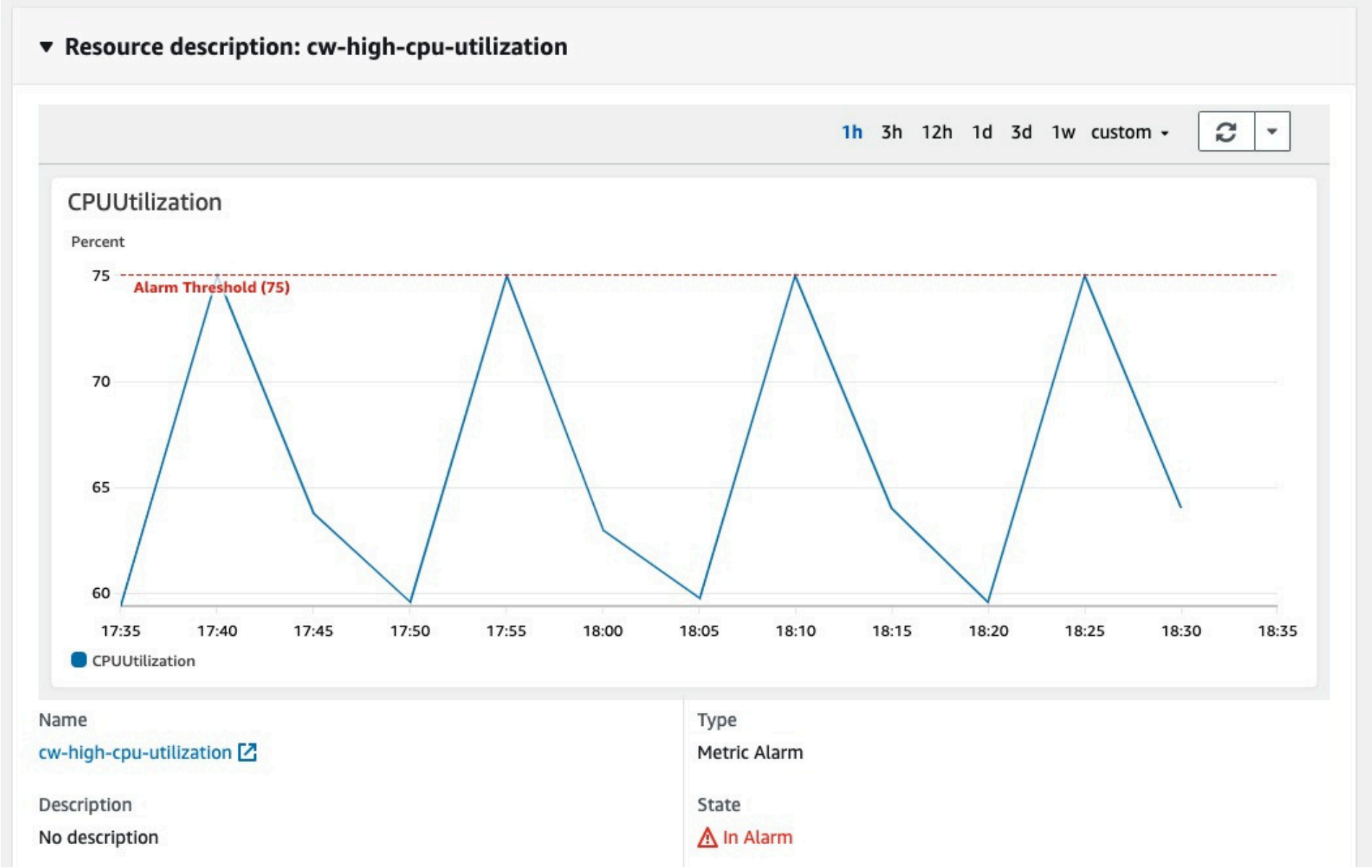
Tracks and logs API

Auditing and C om plian c e

# Setting alarms for resource usageusingCloudWatch

# Manager Request:

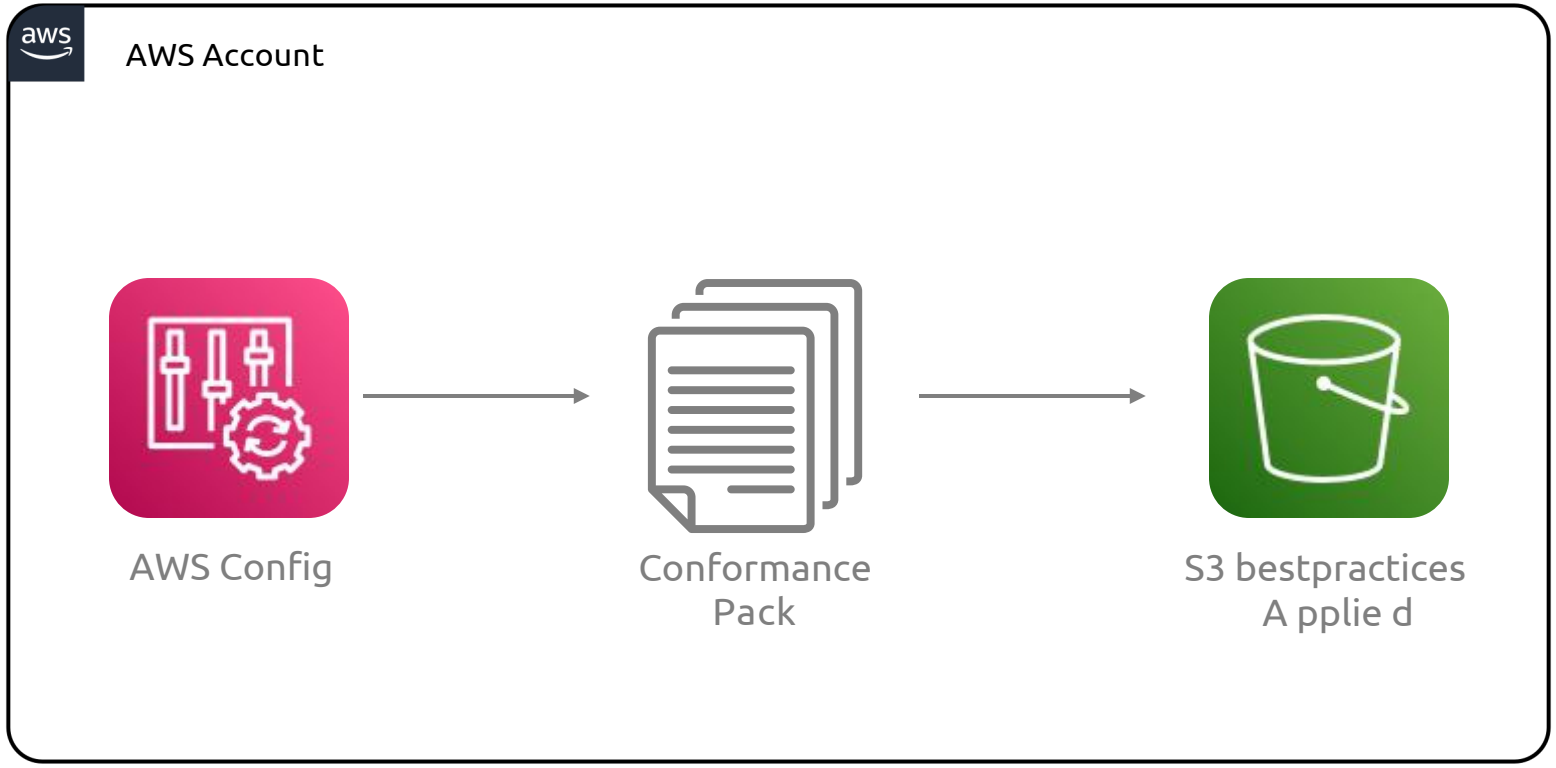
Generate analarmfor excessive CPU usage



# AWS CloudWatch

# AWS Config

# Manager Request : Make sure we are PCI compliant



# Manager Request : Make sure we are PCI compliant

AWS Config

Monitors

Rec ords

Ac c ess

Au dit

Evaluate

Config changes

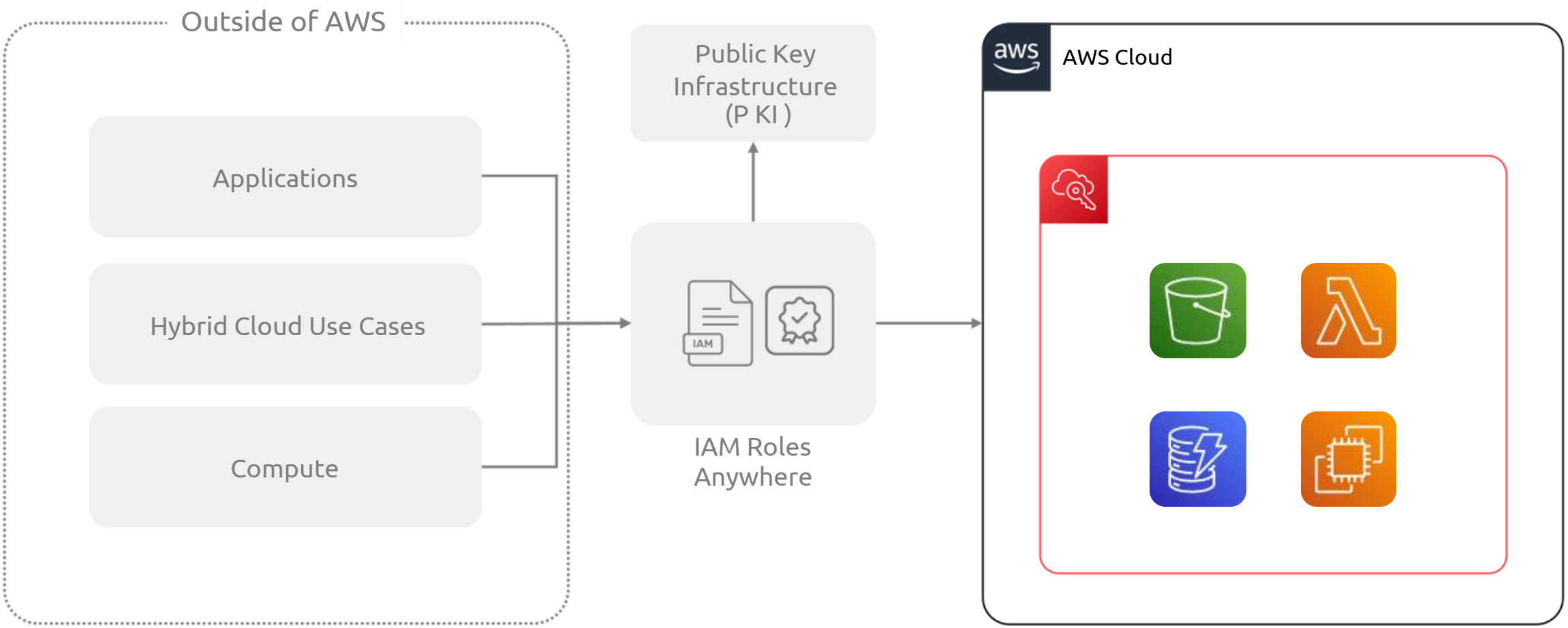
Updates

N/W Config

Installed App

# IAM Anywhere

# Manager Request : Allow servers outside of AWS, access to AWS resources



# IAM Anywhere provides several benefits to customers

1

Centralized Access Management

2

Improved S ecu rit y

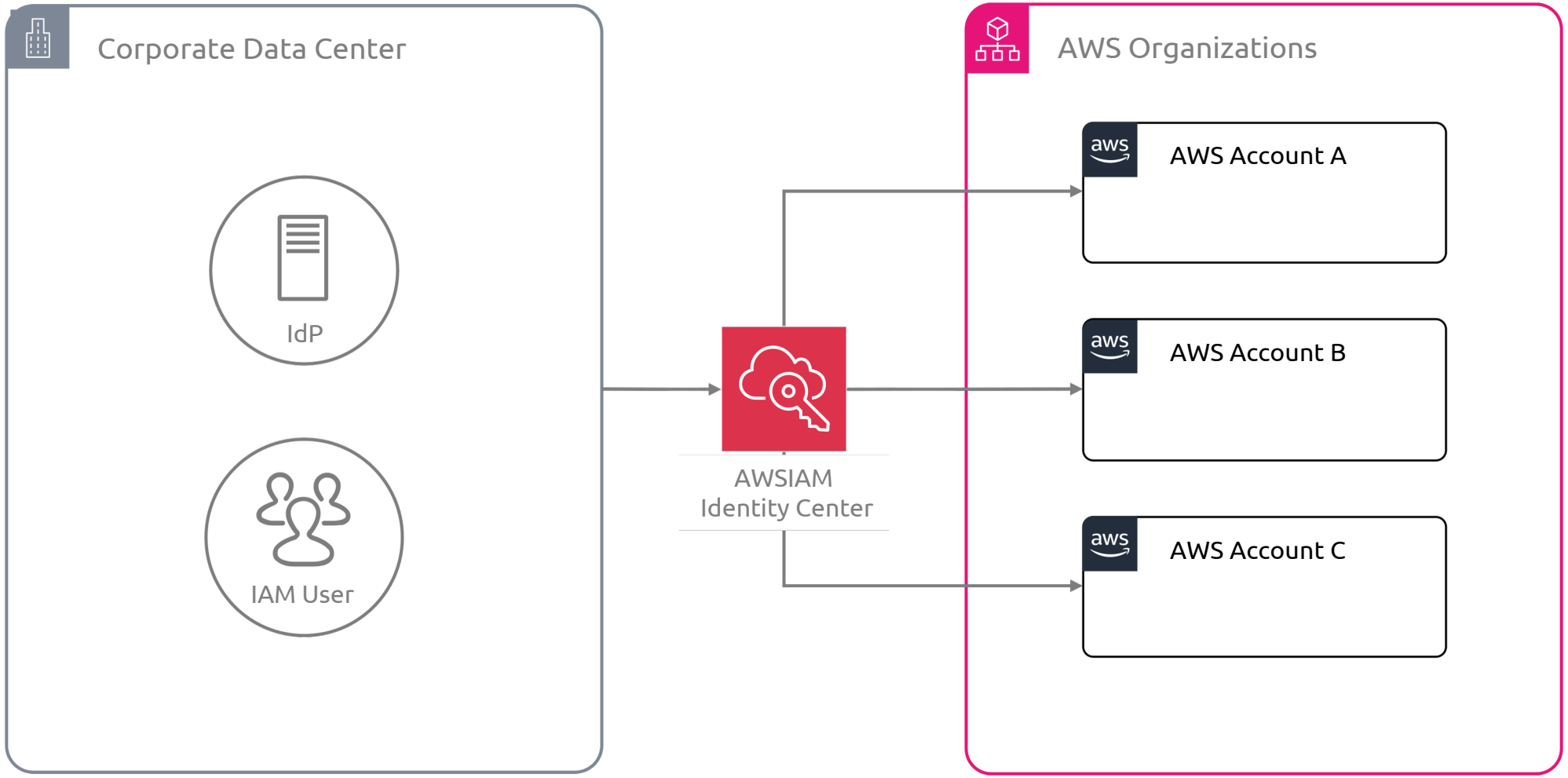
3

Simplified Access

4

Fl exibil it y

# IAM Identity Centre



AWS IAM Identity Center

- Manage sign-in security for your workforce identities
- Manage the access of your workforce across AWS accounts
- Managetheaccess of your workforce to integrated appl i c ati ons
- Recommended approach for workforce authentication and authorization on AWS for organizations of any size and type