Agenda

⑧ IAM VS Identity Center.

① Recap S3

② Event notification in S3

③ Hosting a website using multiple ways

④ GitOps and S3 hosting

⑤ CDN
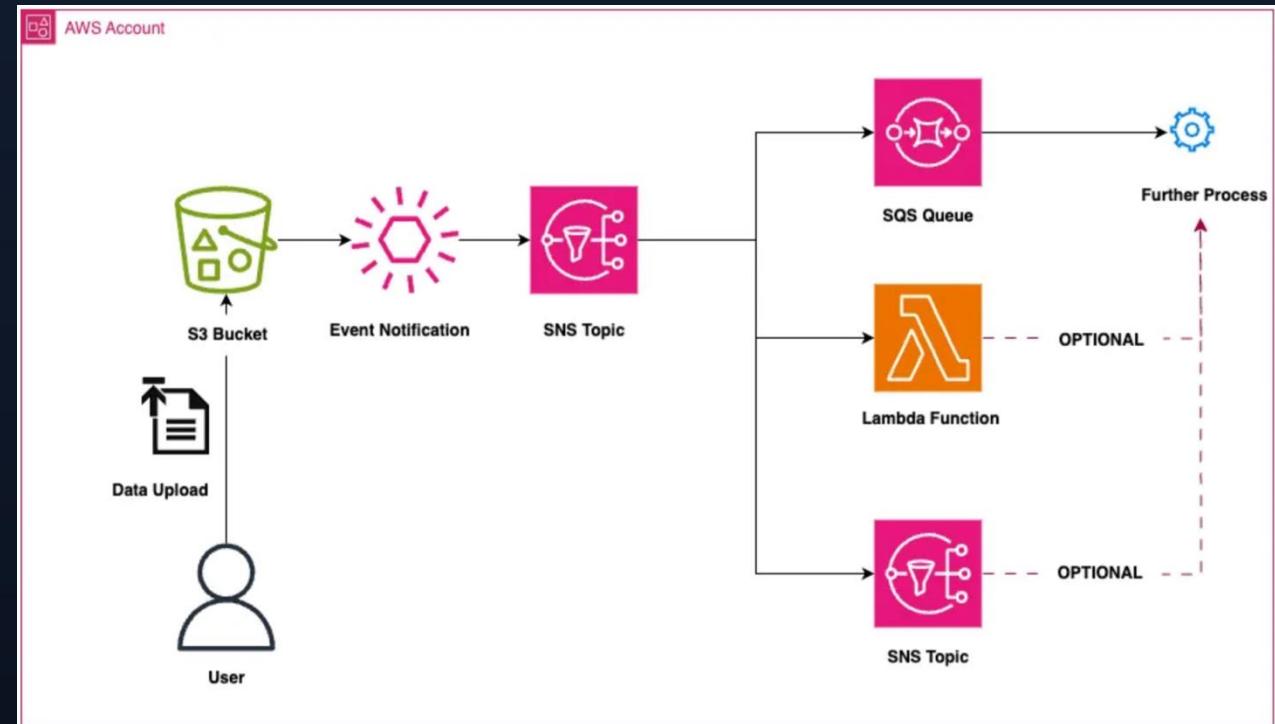
⑥ Cloudfront

⑦ Identity center

Quick Recap of S3

Event Notifications

Amazon S3 Event Notifications allow you to configure event-driven workflows by triggering various AWS services whenever specific actions occur in an S3 bucket. However, a common challenge arises when you need to configure multiple event notifications for the same event type but with different destinations.

Hosting a website using Amazon S3
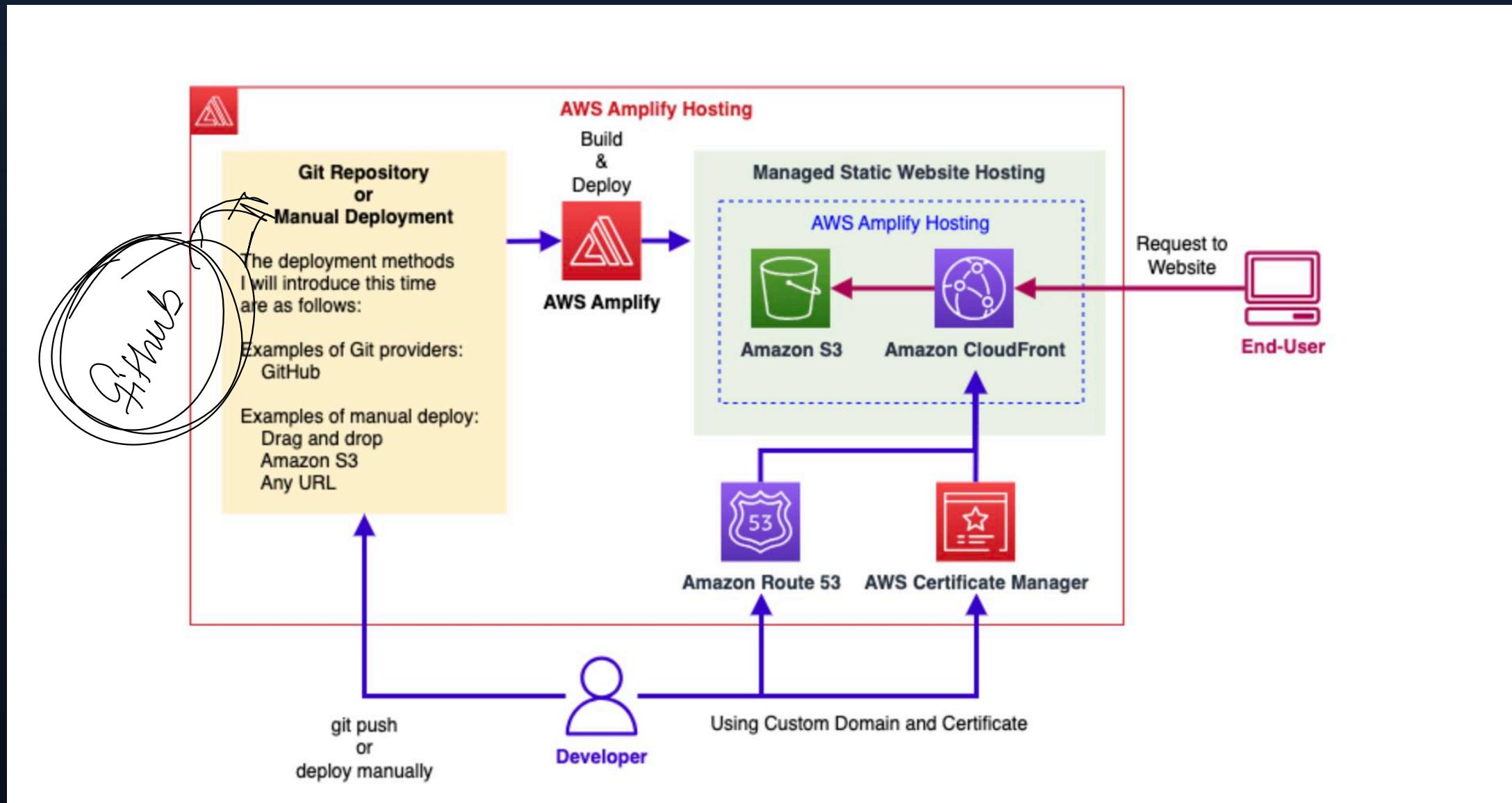
Method 0 – Directly exposing the website

Method 1 – Maintaining the website using AWS Amplify

Method 2 – Hosting the website using Amazon Cloudfront
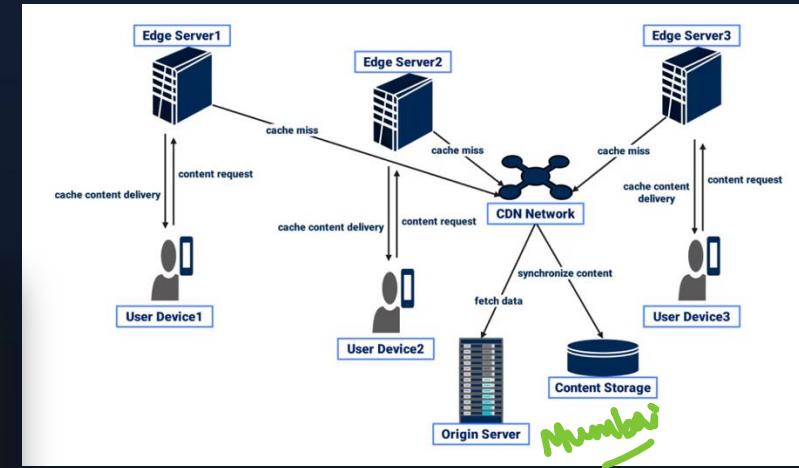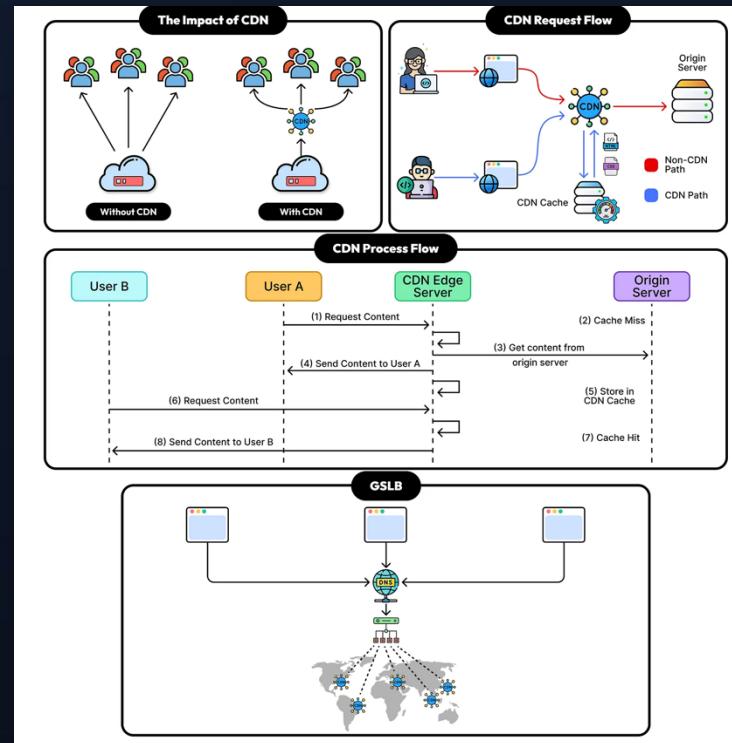
GitOps and S3 Hosting

Content Delivery Network
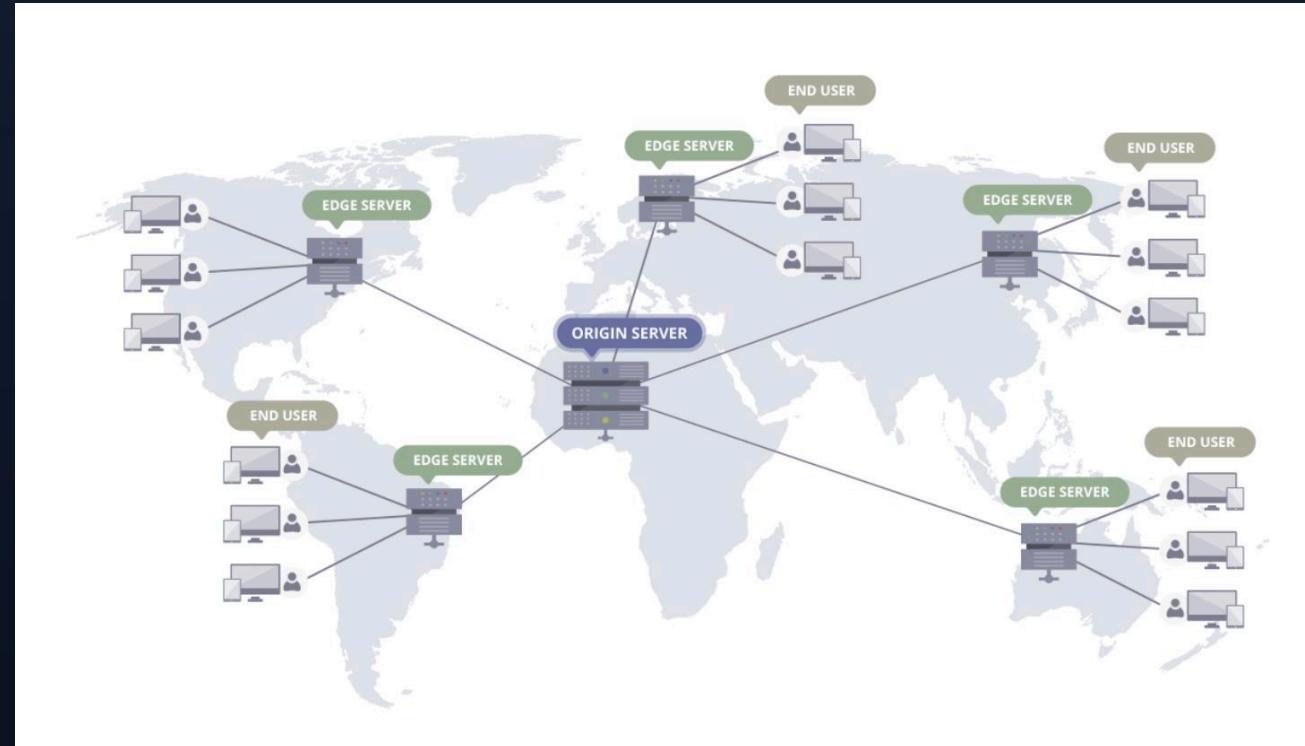
What is an Content Delivery Network?

A Content Delivery Network (CDN) is a geographically distributed network of servers that delivers web content like images, videos, and files to users from the server closest to their location, minimizing latency and speeding up load times. CDNs are needed because they improve website performance, reduce server load, and enhance user experiences by caching and distributing content efficiently and reliably across the globe.
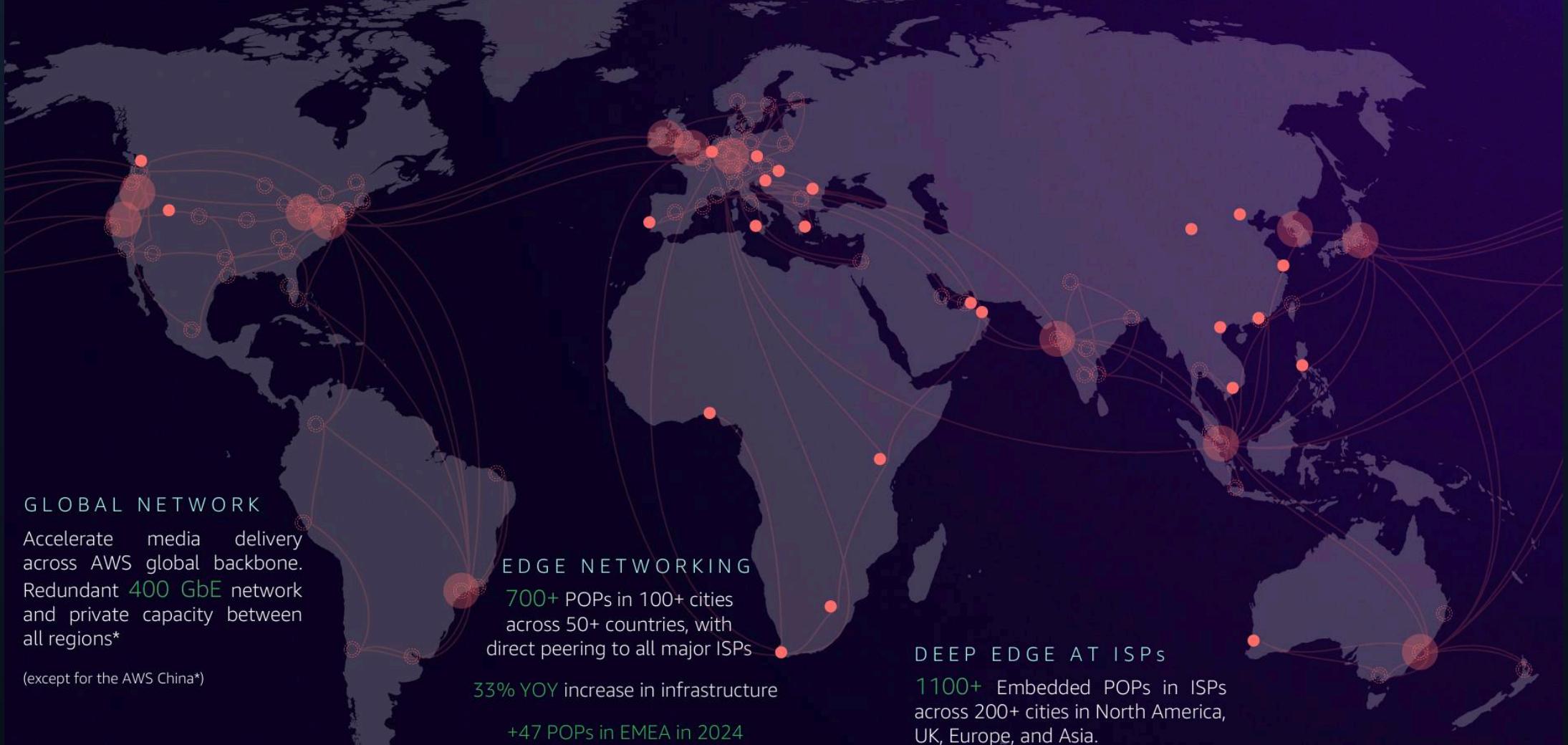
Introduction to Amazon CloudFront

Amazon CloudFront is a global content delivery network (CDN) service from AWS that accelerates the delivery of static and dynamic web content to users by caching and serving content from edge locations worldwide. It delivers data with low latency and high transfer speeds by routing requests to the nearest edge server for optimal performance.
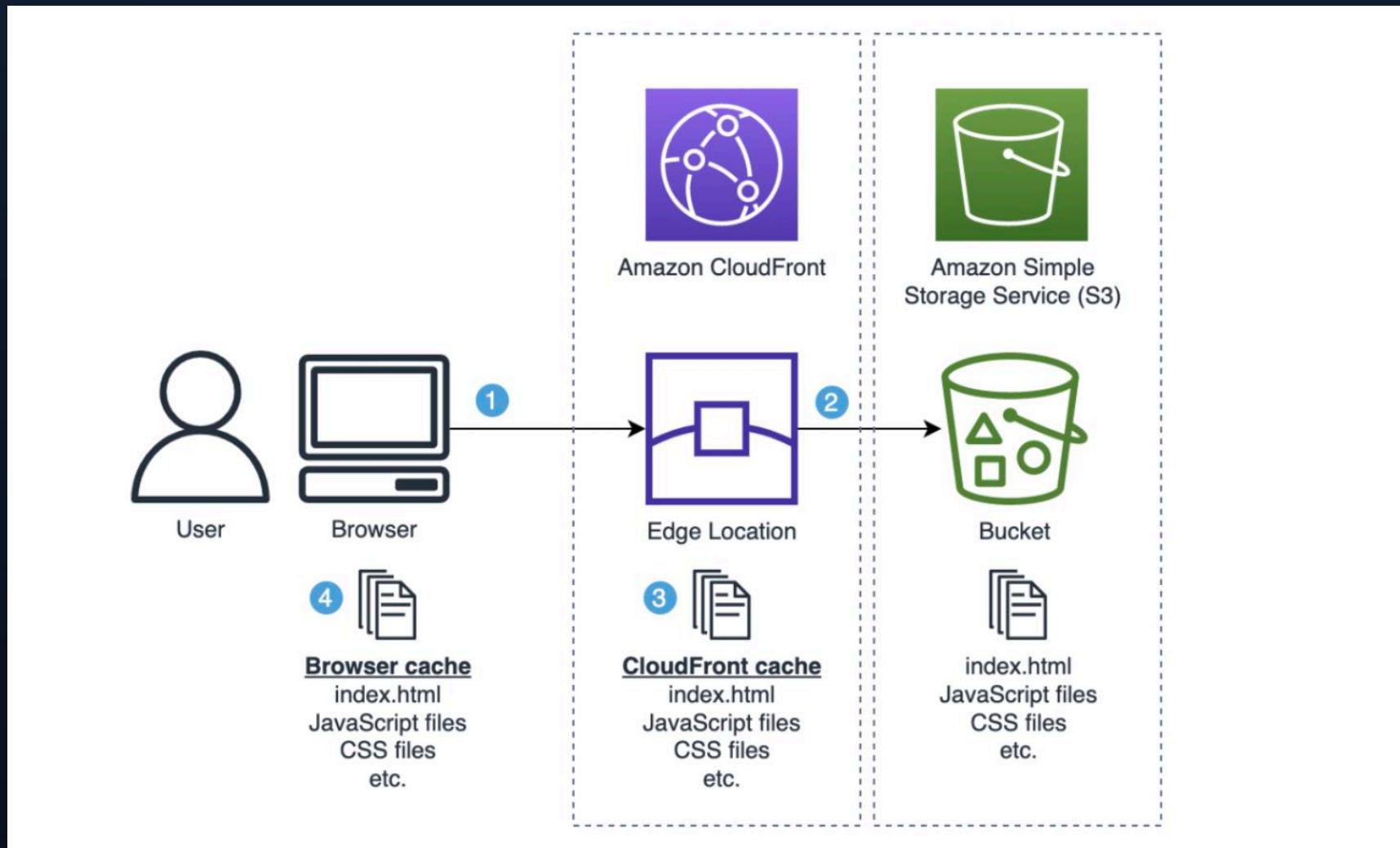
Overview
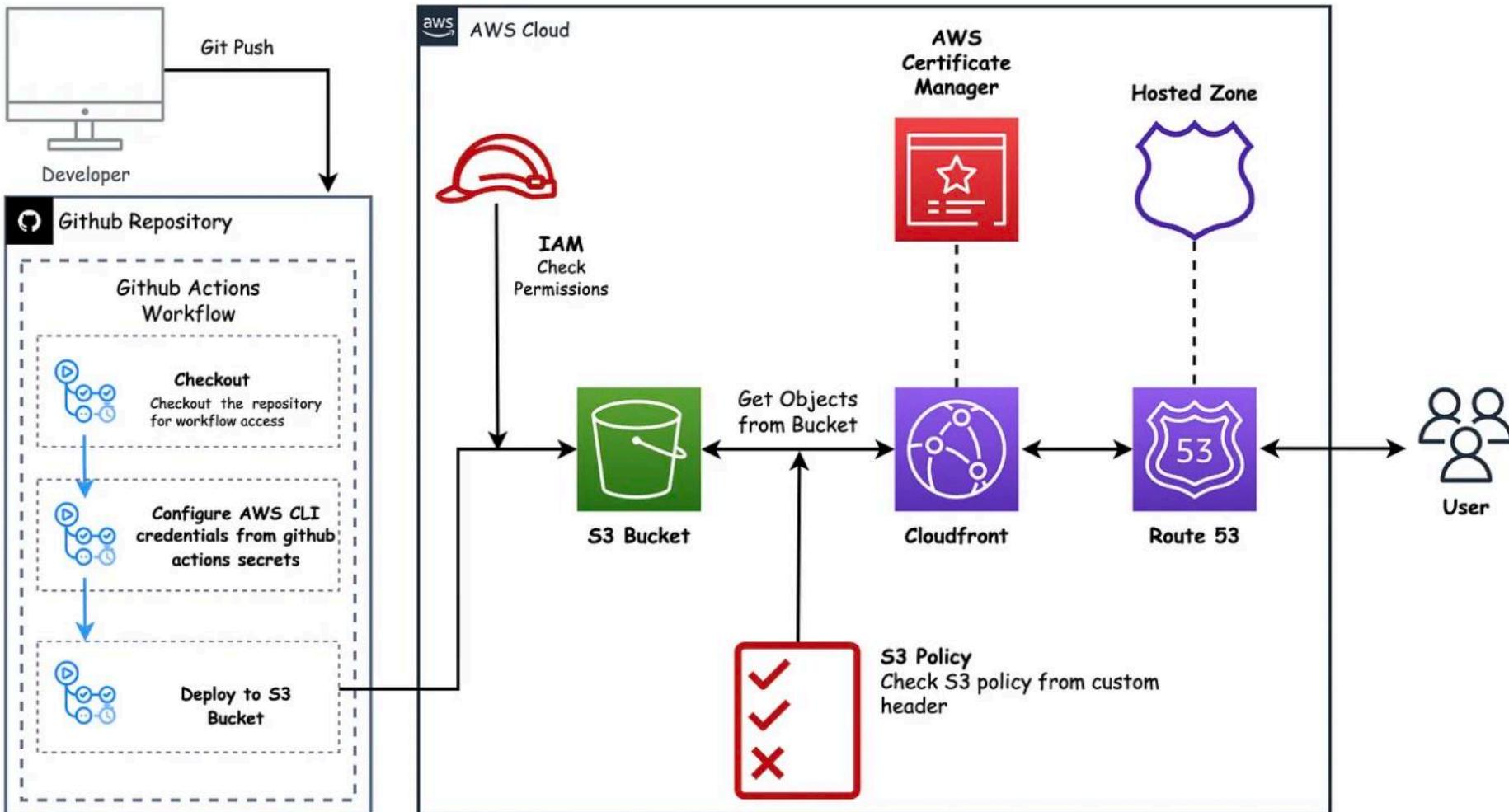
HTTP 200: Lets load the CloudFront overview

GLOBAL NETWORK

Accelerate media delivery across AWS global backbone. Redundant 400 GbE network and private capacity between all regions*

(except for the AWS China*)

EDGE NETWORKING

700+ POPs in 100+ cities across 50+ countries, with direct peering to all major ISPs

33% YOY increase in infrastructure

+47 POPs in EMEA in 2024

DEEP EDGE AT ISPs

1100+ Embedded POPs in ISPs across 200+ cities in North America, UK, Europe, and Asia.

CloudFront S3 Architecture

GitOps and S3 Hosting

IAM Identity Centre: Overview

Use IAM Identity Center to connect your workforce to AWS

User store for your AWS organization

Sync users and groups from any directory that supports SCIM; do this once for your AWS environment
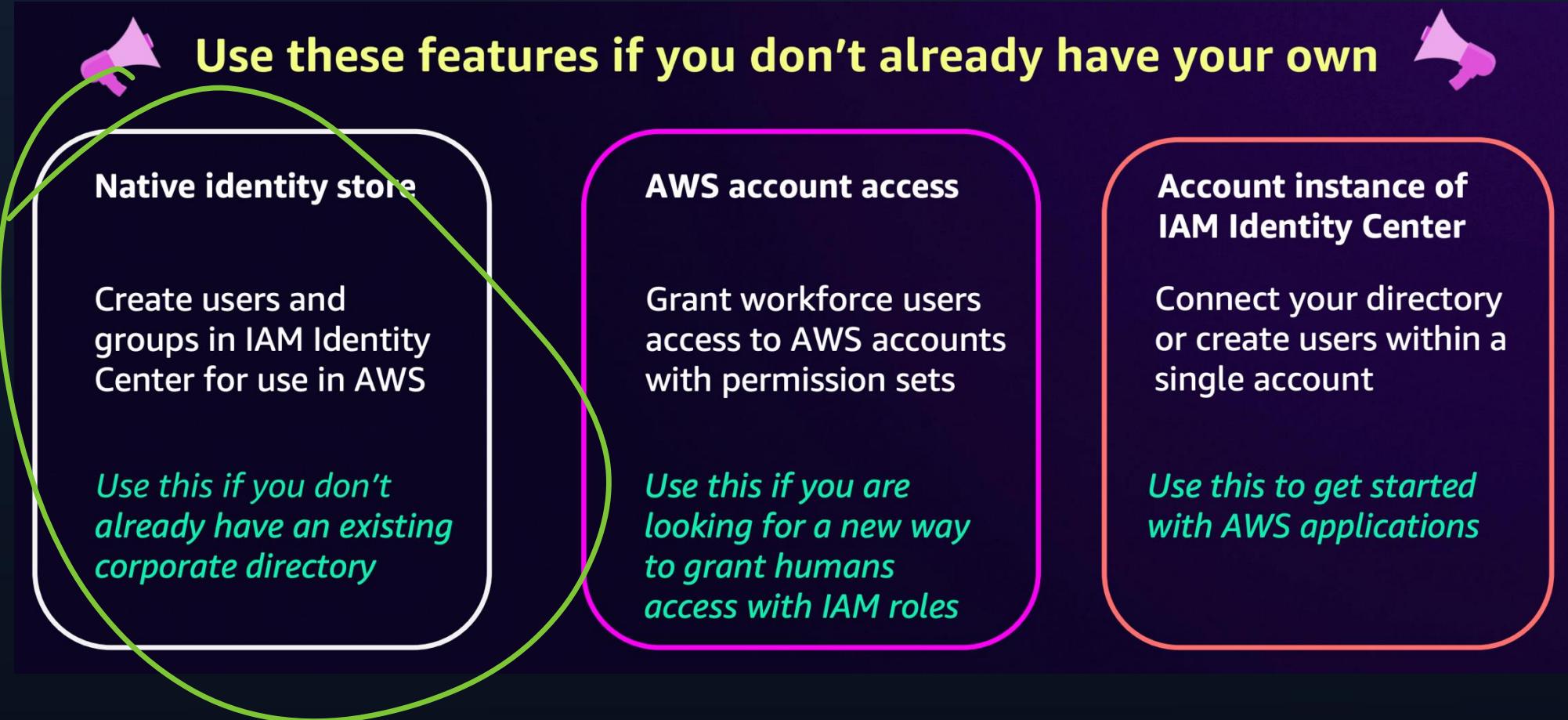
AWS application access

Allow your workforce to authenticate to AWS applications, such as Amazon QuickSight
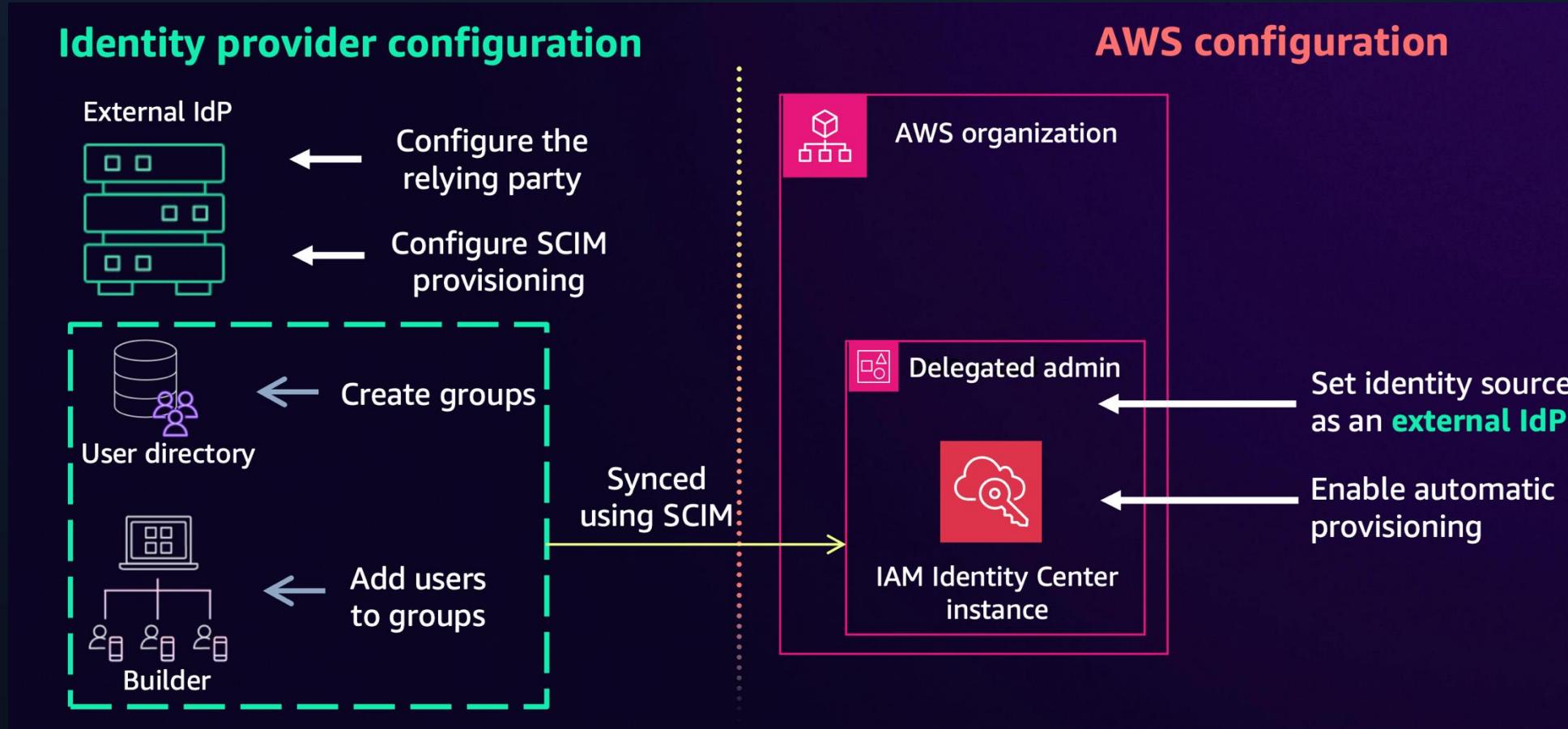
Trusted identity propagation (TIP)
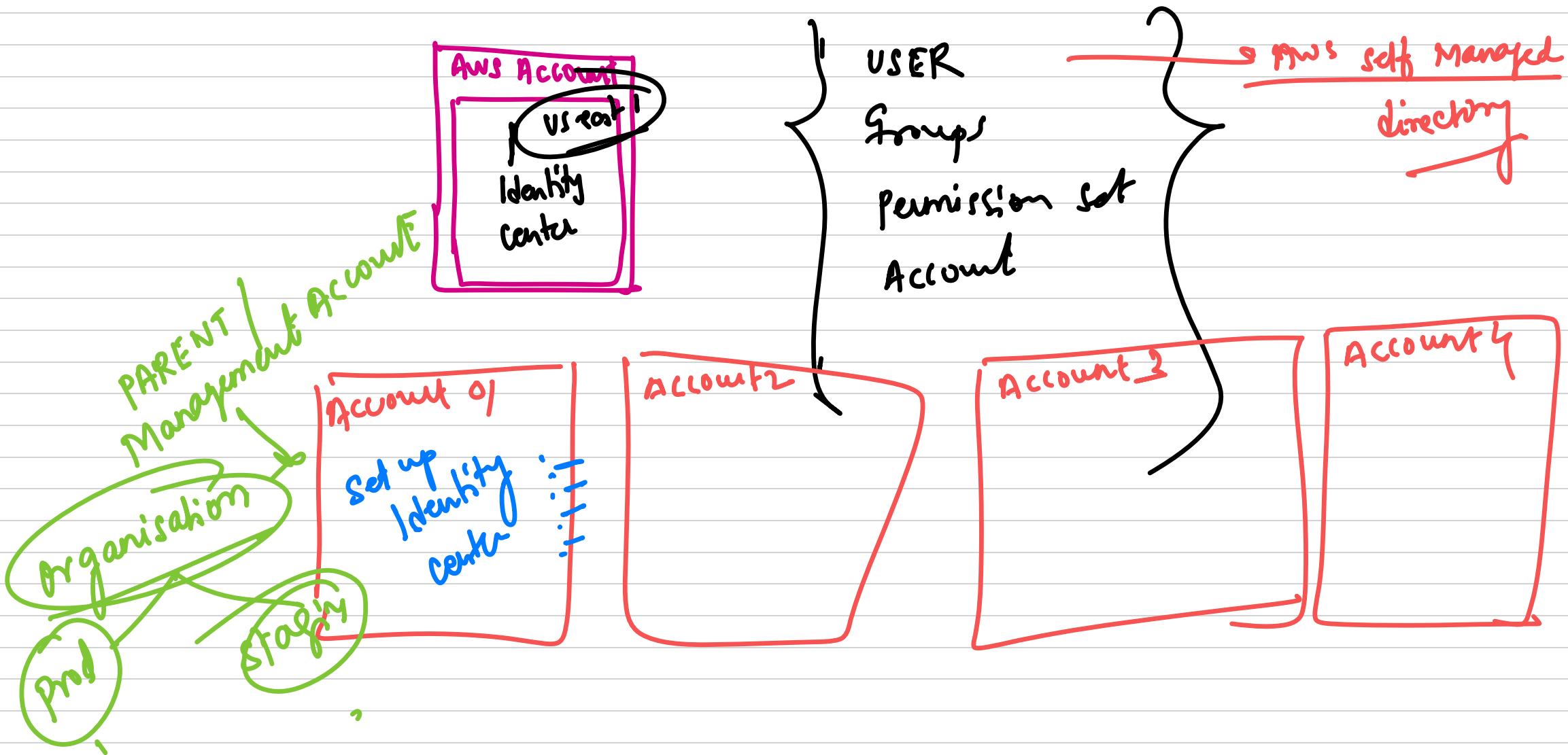
Specify and audit data access based on your user and group information

IAM Identity Centre: Additional Functionality

📢 **Use these features if you don't already have your own** 📢

Native identity store

Create users and groups in IAM Identity Center for use in AWS

Use this if you don't already have an existing corporate directory

AWS account access

Grant workforce users access to AWS accounts with permission sets

*Use this if you are looking for a new way to grant humans access with IAM roles*

Account instance of IAM Identity Center

Connect your directory or create users within a single account

Use this to get started with AWS applications

Connect Corporate Directory to AWS

Identity provider configuration

External IdP

Configure the relying party

Configure SCIM provisioning

User directory — Create groups

Builder — Add users to groups

Synced using SCIM

AWS configuration

AWS organization

Delegated admin

IAM Identity Center instance

Set identity source as an **external IdP**

Enable automatic provisioning

AWS Account

USER 1

Identity Center

USER
Groups
Permission Set
Account

AWS self Managed directory

PARENT / Management Account

Organisation

Prod

staging

Account 0

Set up
Identity
Center

Account 2

Account_3

Account 4

# Permissions to resources in one account

More Realistic Scenario
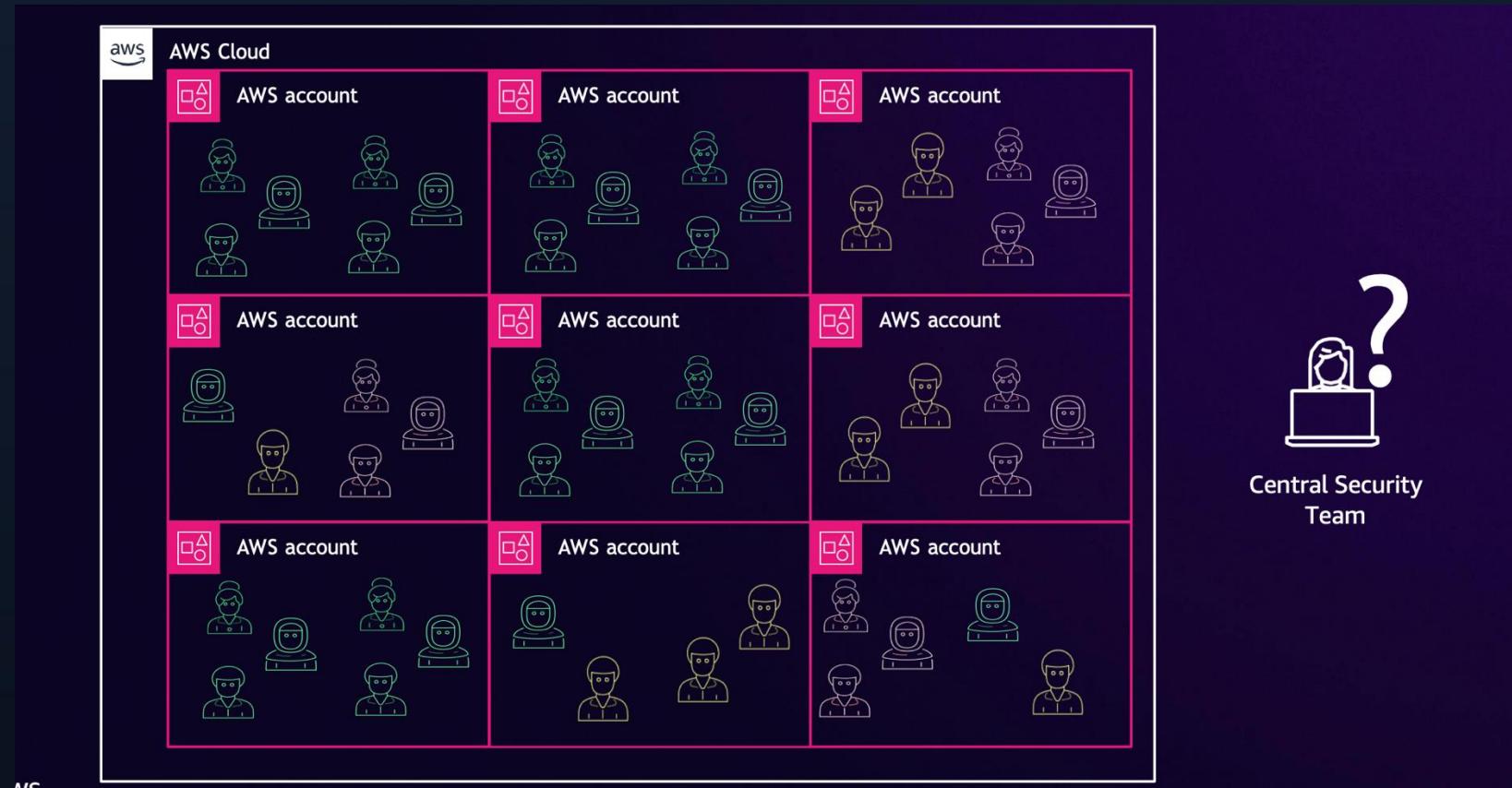
# Permissions to resources in one account
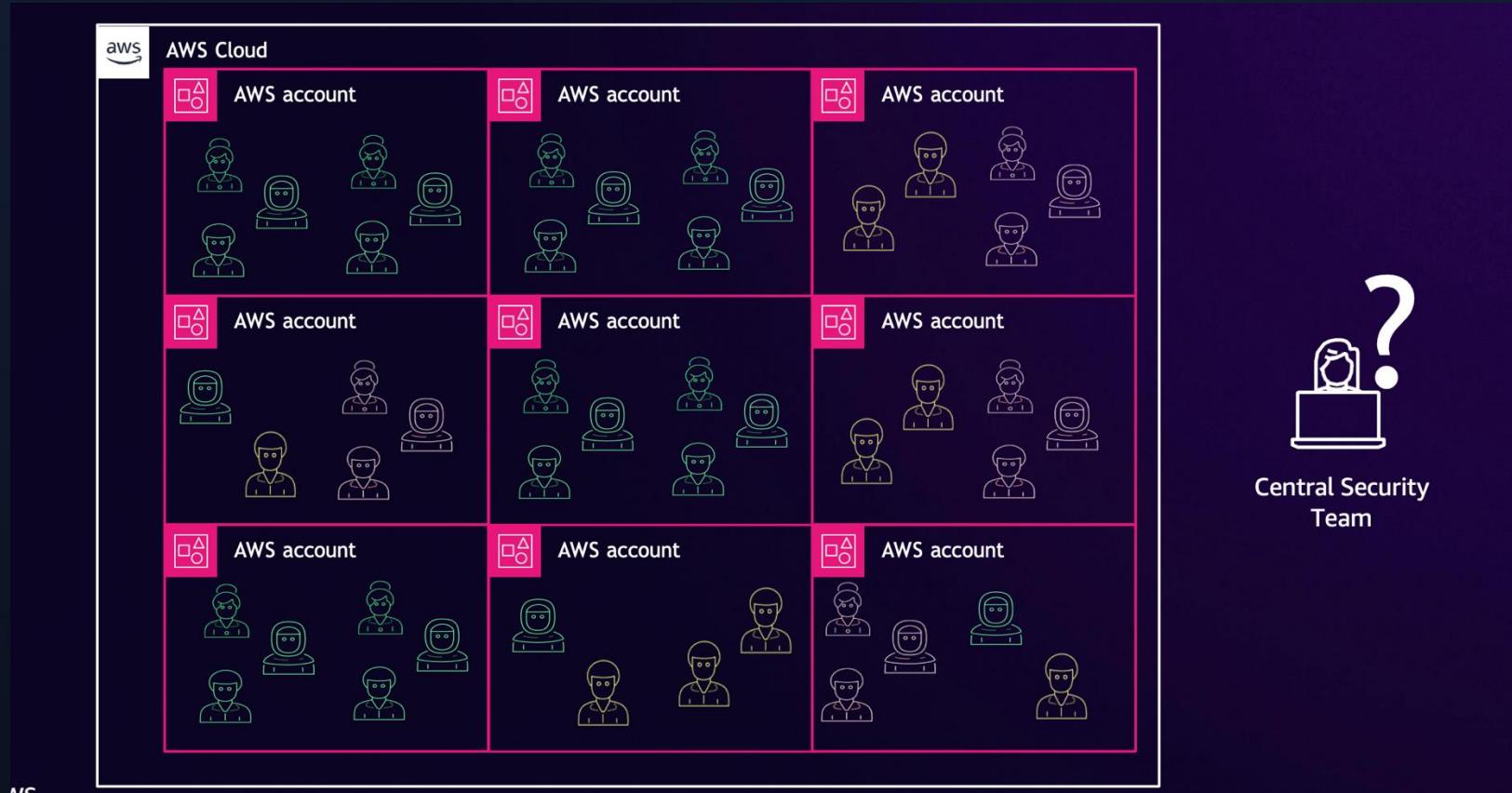
A Common Customer Scenario

Central Team Managing Access

Central Team Managing Access

Central Team Managing Access

AWS IAM vs AWS IAM Identity Center

Feature	AWS IAM	IAM Identity Center
Purpose	Manages access within a single AWS account.	Centralized access across multiple AWS accounts.
Access Type	IAM policies for users, roles, and permissions.	Permission sets and external identity provider integration.
Best For	Developers, admins, and apps needing programmatic access.	Organizations needing SSO and centralized control.
User Management	Manually create and manage users.	Syncs users and groups from external directories.
External Identity Provider Integrations	Limited. Requires custom federation.	Yes, integrates with Okta, Azure AD, etc.
Credential Type	Long-term IAM credentials.	Temporary credentials upon login.
SSO	No, each user logs in separately.	Yes, single login for multiple accounts.
Multi-Account Access	No, managed per AWS account.	Yes, central access for multiple accounts.