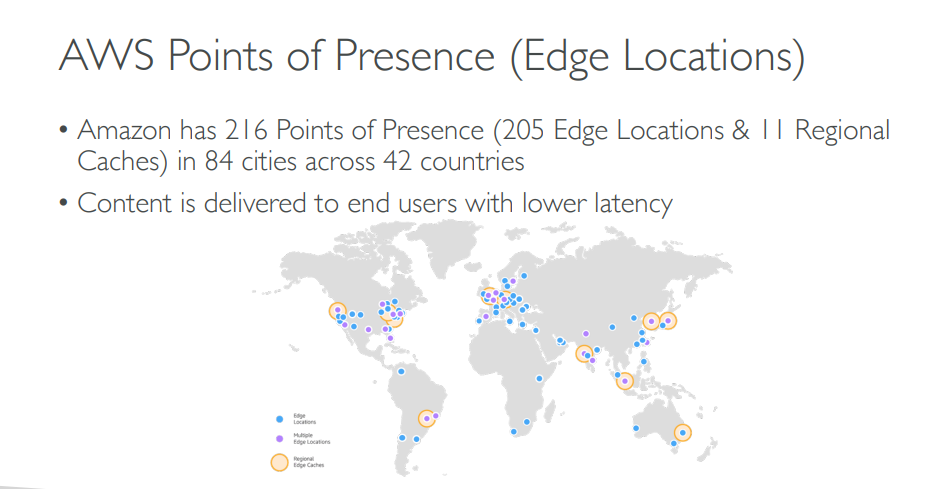
A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated



* Global service vs local service
* IAM -> Identity and access management service
* IAM user and Groups
* when we create account by default root user is created
* Multiple users can be grouped together.
* user can be part of multiple groups.
* user can exist without a group.
* policies can be assigned to users or groups.
* inside policy permissions are defined

zonal services

EC2,EBS

 zonal services, like Amazon EC2 and Amazon EBS. A zonal service is one that provides the ability to specify which Availability Zone the resources are deployed into. These services operate independently in each Availability Zone within a Region, and more importantly, fail independently in each Availability Zone as well.

Regional Services

Amazon SQS, Dynamo DB, Amazon S3

Regional services are services that AWS has built on top of multiple Availability Zones so that customers don’t have to figure out how to make the best use of zonal services. We logically group together the service deployed across multiple Availability Zones to present a single Regional endpoint to customers. Amazon SQS and [Amazon DynamoDB](http://aws.amazon.com/dynamodb/) are examples of Regional services. They use the independence and redundancy of Availability Zones to minimize infrastructure failure as a category of availability and durability risk. Amazon S3, for example, spreads requests and data across multiple Availability Zones and is designed to automatically recover from the failure of an Availability Zone. However, you only interact with the Regional endpoint of the service.

Global Services

IAM

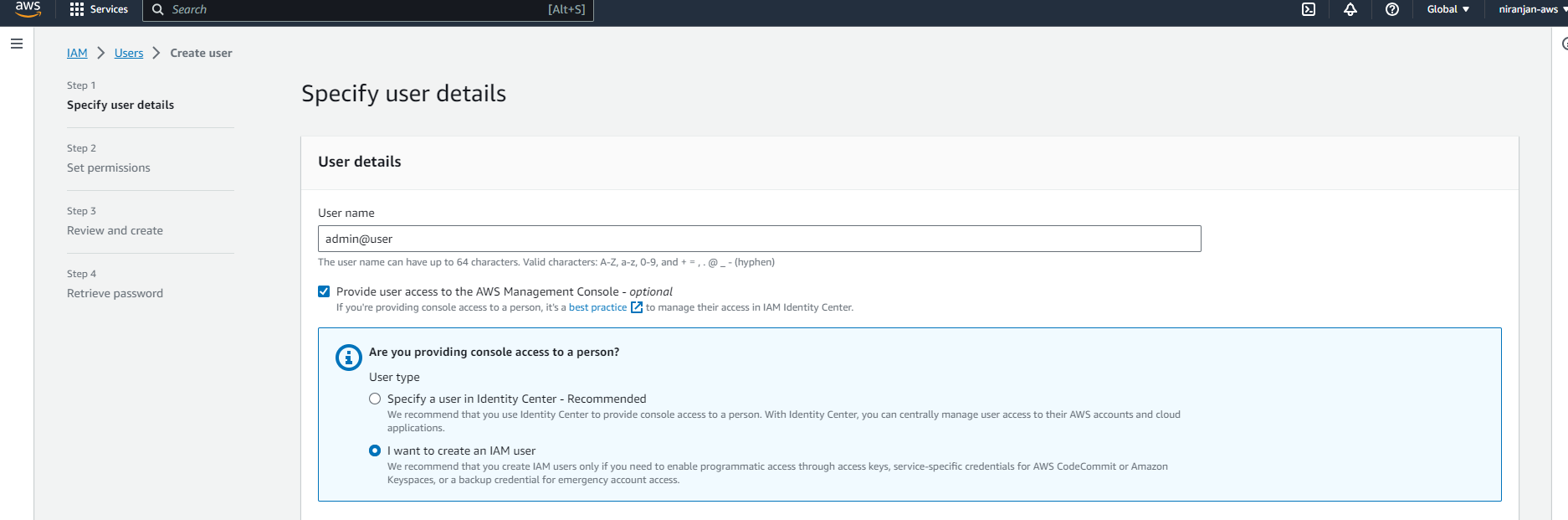
Route 53 (DNS)

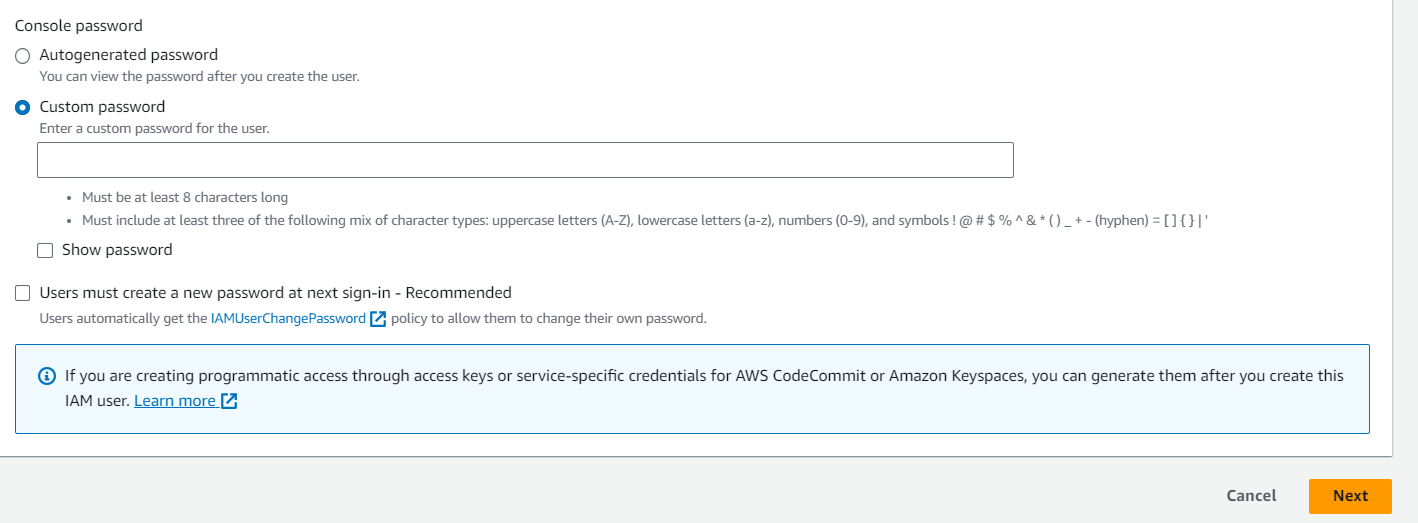
Cloud front (CDN )

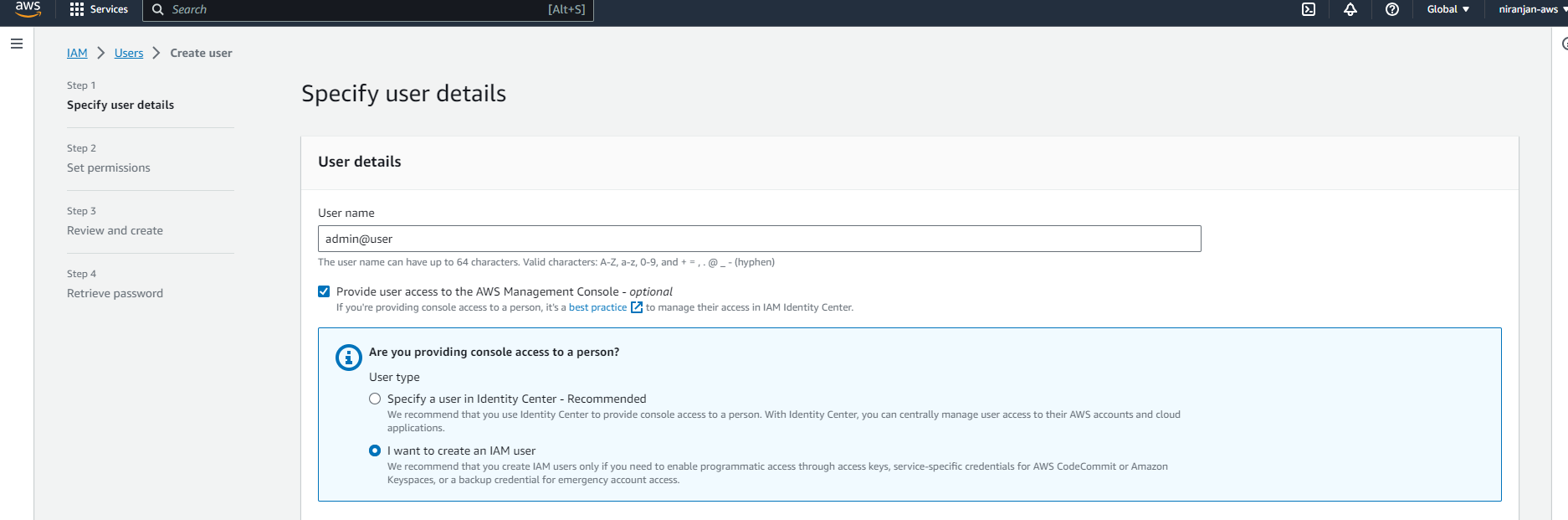
**Identity Centre:**

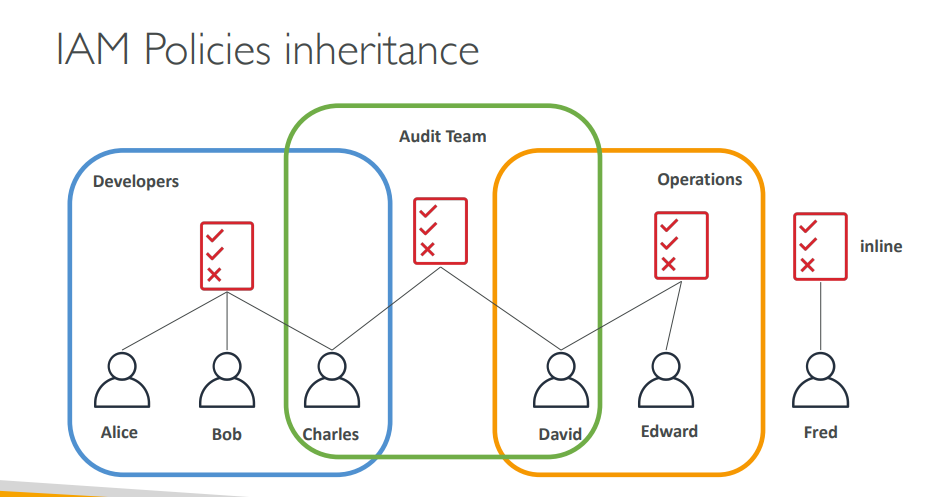
* IAM Identity Centre provides one place where you can create or connect workforce users and centrally manage their access across all their AWS accounts and applications.
* You can use multi-account permissions to assign your workforce users access to AWS accounts.
* You can use application assignments to assign your users access to IAM Identity Centre enabled applications, cloud applications.
* workforce users and groups in IAM Identity Center, or connect and synchronize to an existing set of users and groups in your own identity source for use across all your AWS accounts and applications.
* Ex : Microsoft Active Directory Domain Services, and external identity providers such as Okta Universal Directory or Microsoft Azure AD.
* You can grant your workforce users in IAM Identity Center single sign-on access to SAML 2.0 applications, such as Salesforce and Microsoft 365

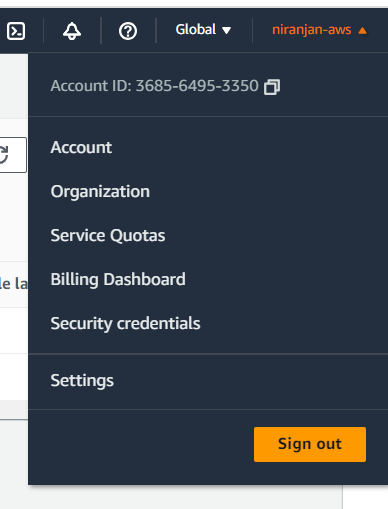
The difference between LDAP and Active Directory is that LDAP is a standard application protocol, while AD is a proprietary product. LDAP is an interface for communicating with directory services, such as AD. In contrast, AD provides a database and services for identity and access management (IAM)











A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A computer service with a chip and a helmet

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated

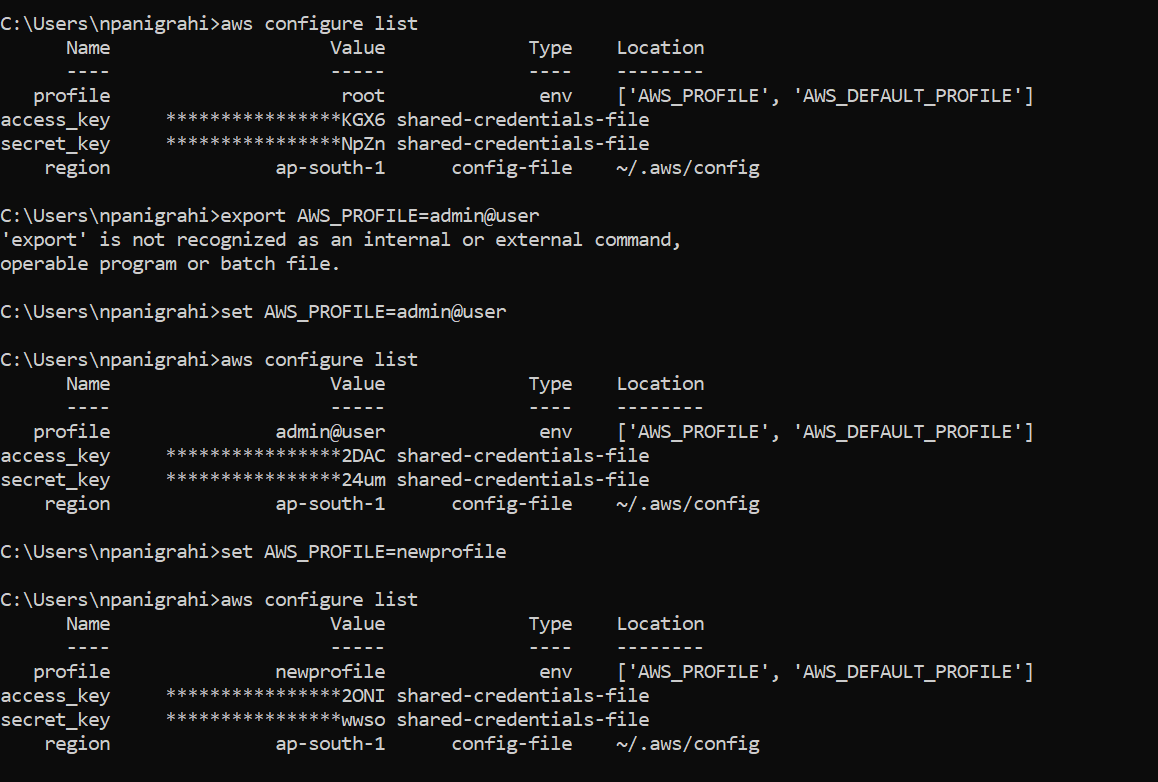
A screen shot of a computer code

Description automatically generated

Aws configure --profile profile\_name

A screen shot of a computer screen

Description automatically generated



A computer screen shot of a computer program

Description automatically generated

Aws cloud shell

<https://www.linkedin.com/pulse/aws-cli-multiple-profiles-bachar-hakam/>

<https://dev.to/hmintoh/how-to-use-multiple-aws-accounts-with-the-aws-cli-3lge#:~:text=To%20switch%20between%20different%20AWS,variable%20to%20a%20different%20value>.