**Aws developer the big piture**

* Developing in the clouds
* Develop on AWS
* Tools of the trade

**Local dev and AWS dev**

Similar

* -App runs on os/Platform
* -requires platform to be installed eg .net
* -https servers listens on ports
* -connects to outside database

different

* everything runds locally on same machine /
* one service = one responsibilit
* files stores in server/files server from S3
* Database on same server as app/database as service
* Connectios done manually/connections done with AWS SDK

**The Web of Web services**

Most service in AWS are accessed using TCP connections simply be http

each instance of a service oftentimes called as a resource is assigned IP where each services communicate, this ip are not connected to the outside N/W

the core of AWS is Elastic cloud compute(EC2) is a service which provide servers. EC2 forms basis of many otehr services as well like Relational database service, elastice bean stalk.

Aws Tooling : Web console

174 services available in AWS

**AWS Tooling: Command line interface**

Aws CLI features

* -Shell scripting
* -feture complete with console and SDks
* -interact with any service

AWS Tooling:Software development kits

Java, .net, js etc

Services to use

eg migrating a app to AWS

\*App hosting - EC2

\*images and assets - store and serve from S3, amazon's object storage service.

\*User data needs to stores use - dynamoDB

\*once a user has loggedin, session needs to be store in a cache for sessions - elastic cache to avoid wasting app memory

**Installing NodeJs**

is a java script platform that runs localy instead of a browser

https://www.nodejs.org/

command line

Node -v to display version

npm -v

=========

**Install AWS CLI**

Create and cconfigure resources in AWS in comfortable command line

https://aws.amazon.com/cli/

aws --version : for version check

============

Summary

-The AWS dev exp

-untanging the AWS web

-AWS toolbox

**IAM and cloud watch**

* -configuring and managing users
* -setting alarms and logging

**cloudwatch -** set alarms notification in response to events

**IAM** - Simple user and access management

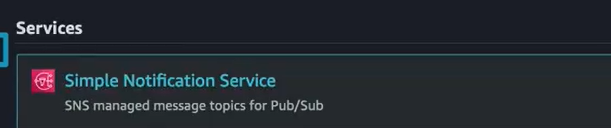
cloudwatch is a service

alerts via cloud watch to SNS simple notification service notification as email, sms and https req

also trigger auto scaling action, trigger EC2 action

============================

**SNS simple notification service notification**

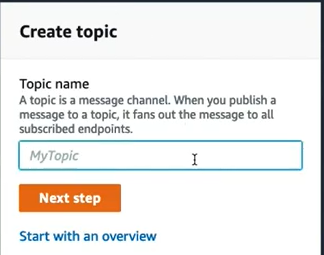


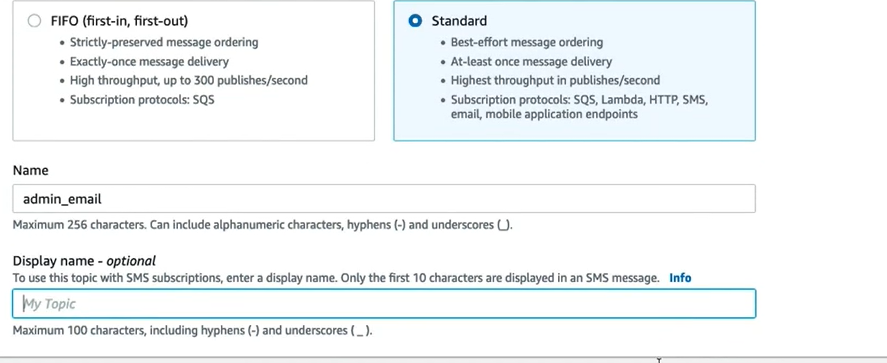
push alerts to a group of notification endpoints

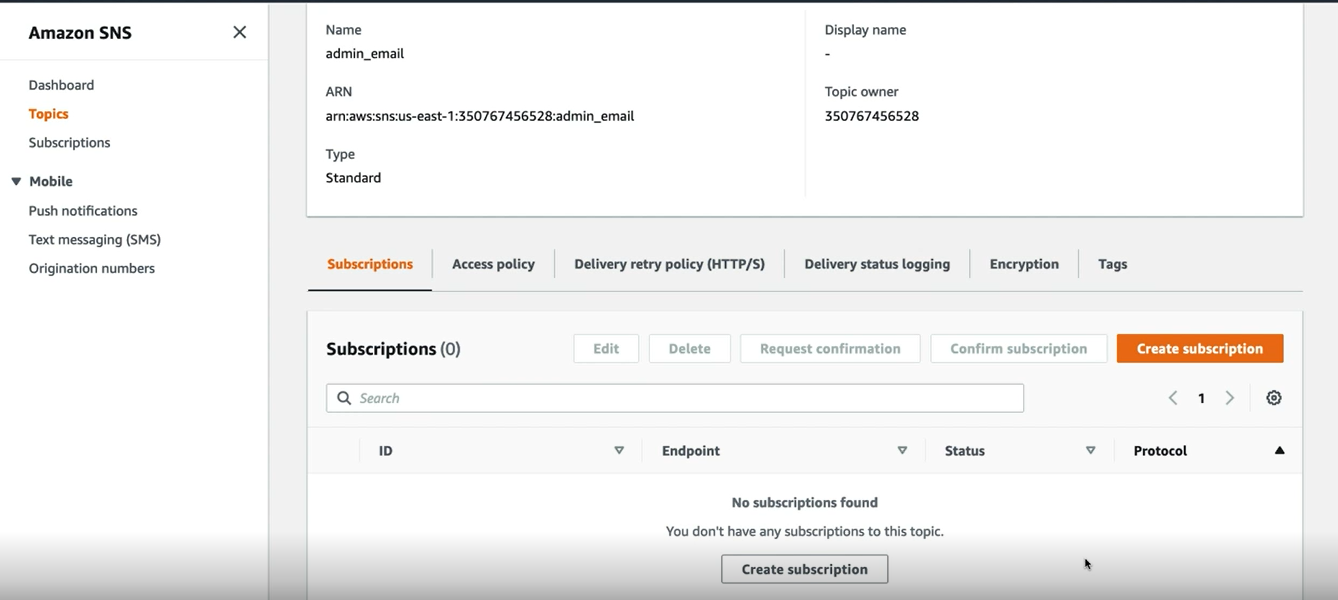
topic - subscribe email and SMS number any notification sent to that SNS topic will then be sent to subscribed email or number.

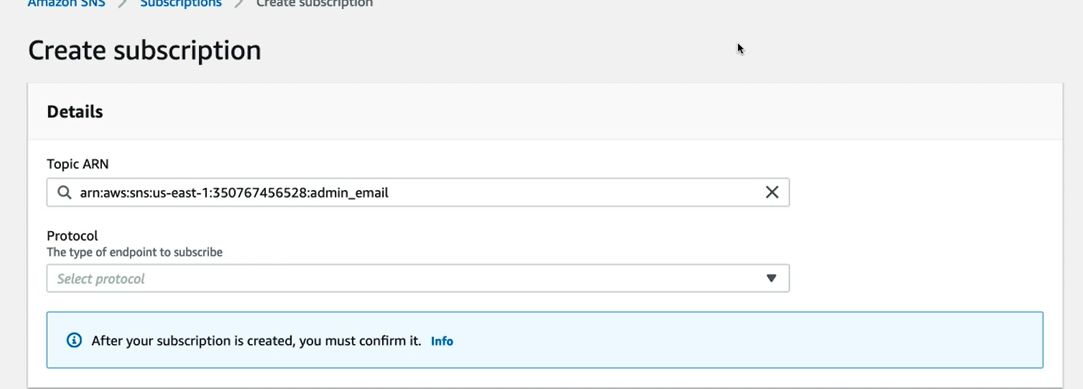
Topics are region specific

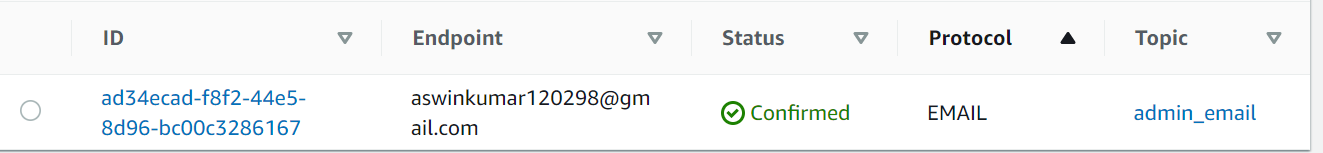
Select region - in global search search SNS - Create Topic and subscription







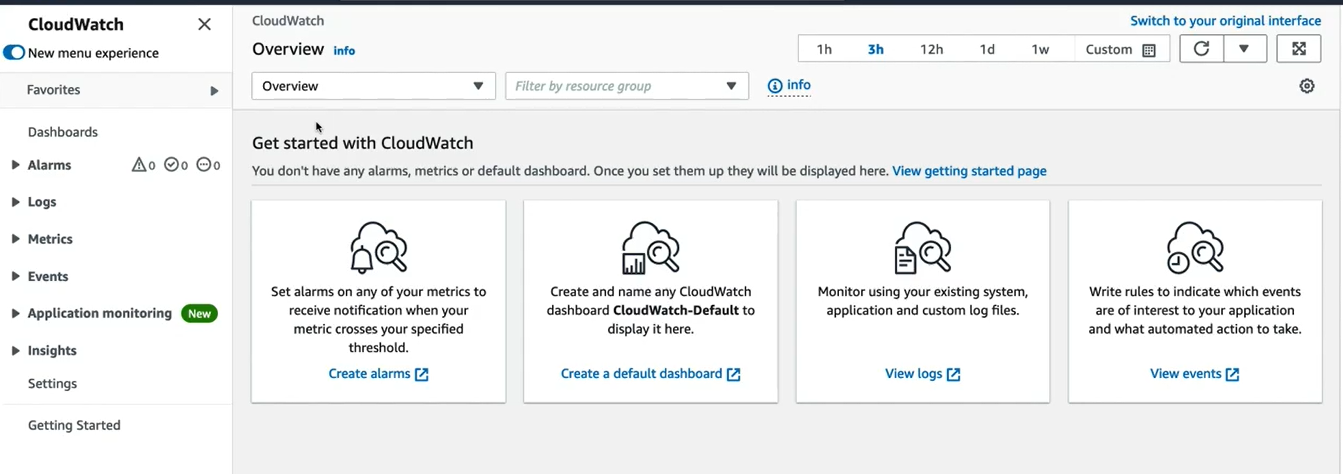


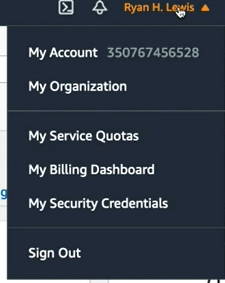
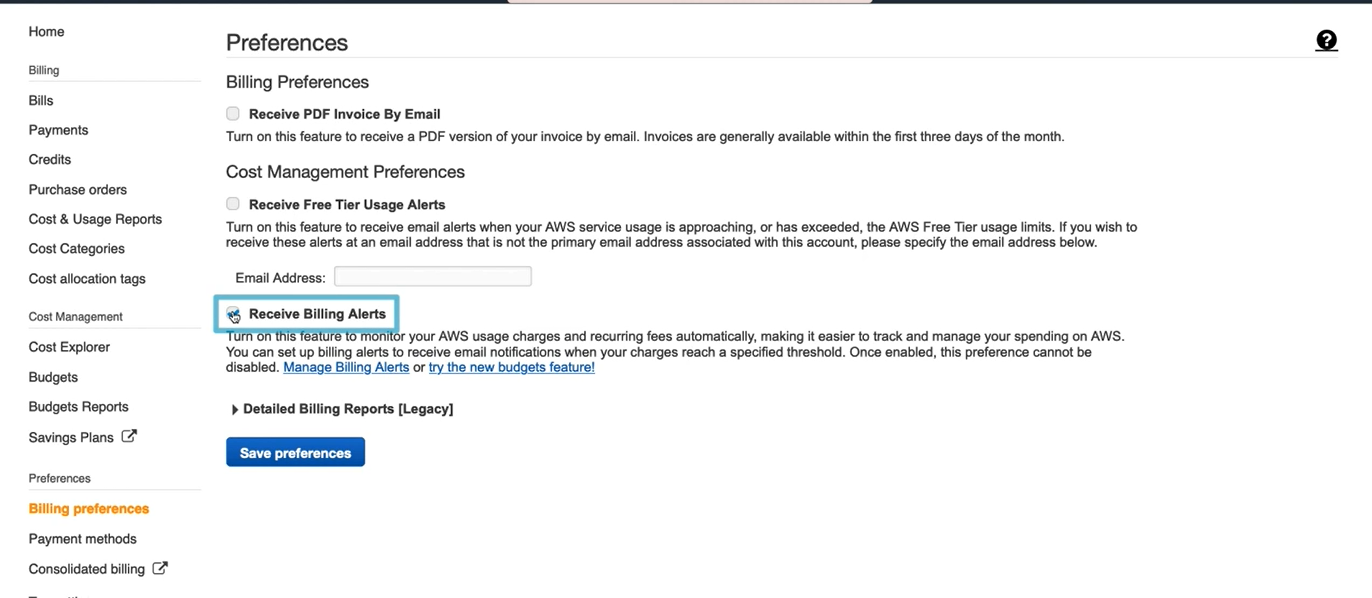


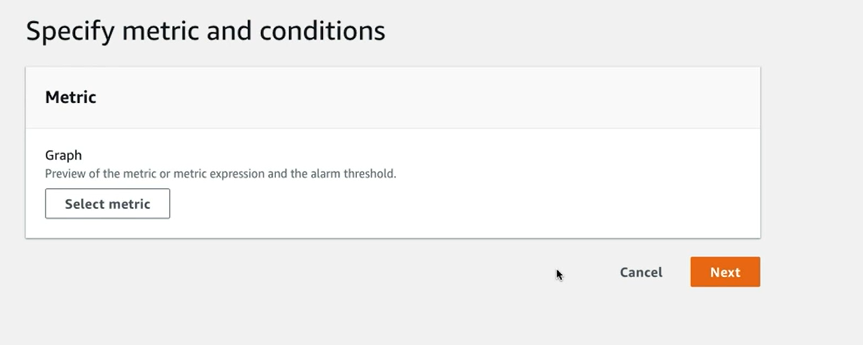
================================

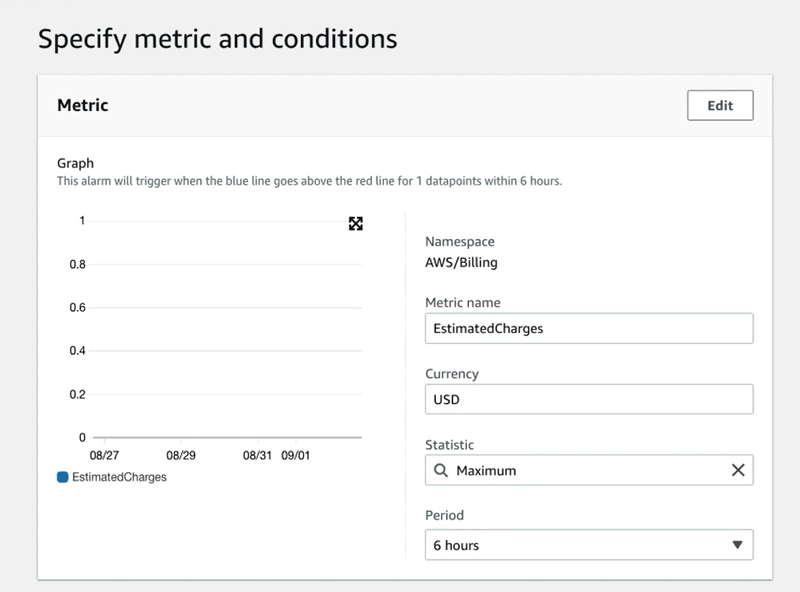
Creating a cloudwatch alarm

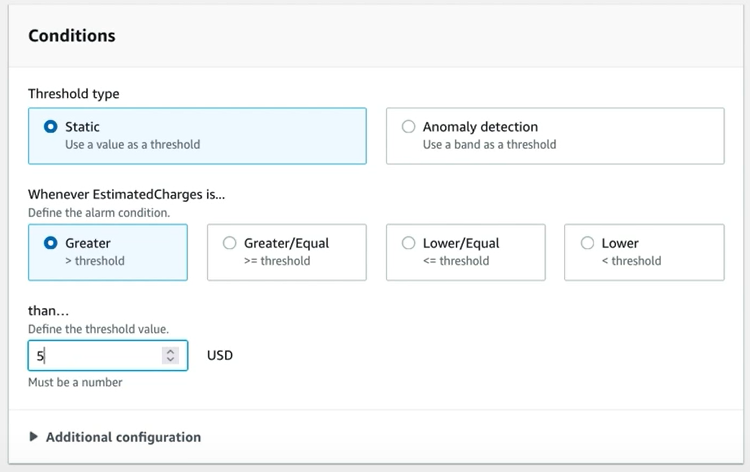
global search - cloudwatch - alarms - for eg billing - select metrics and threshold - topic and create.

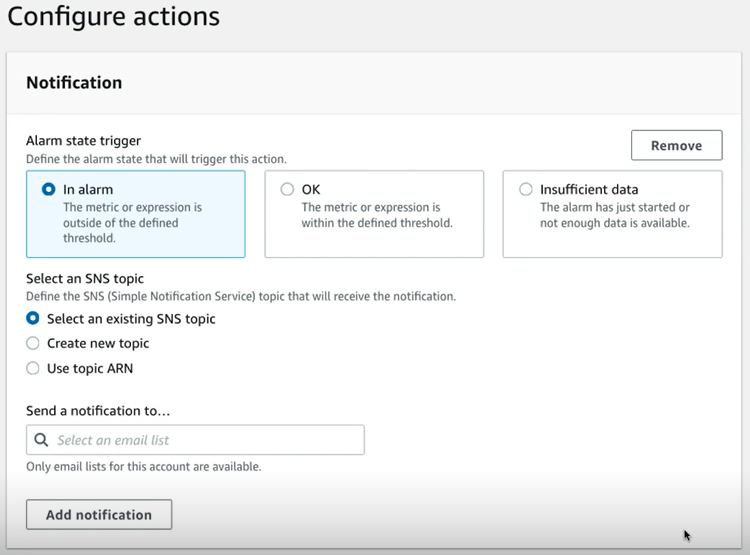


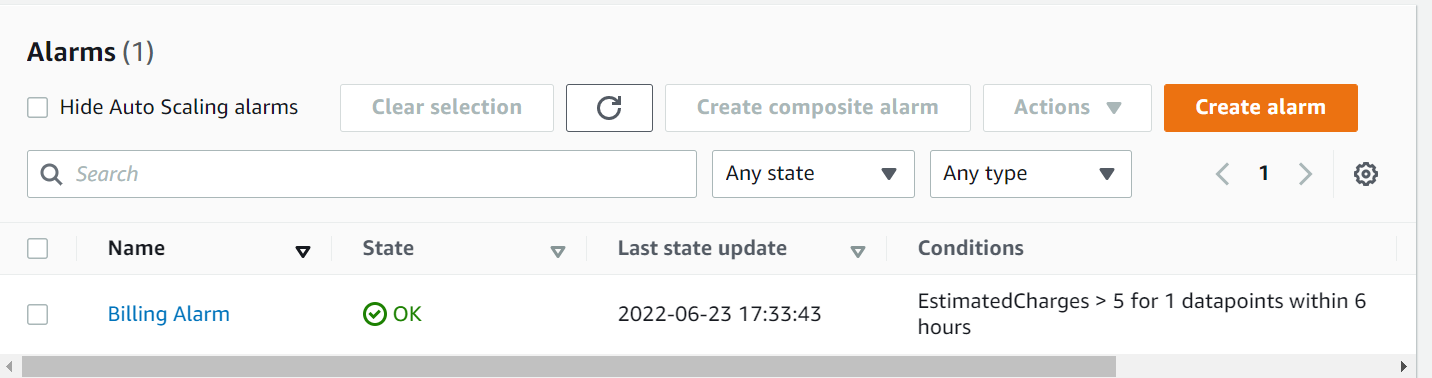
Billing alert  
  
  












========================

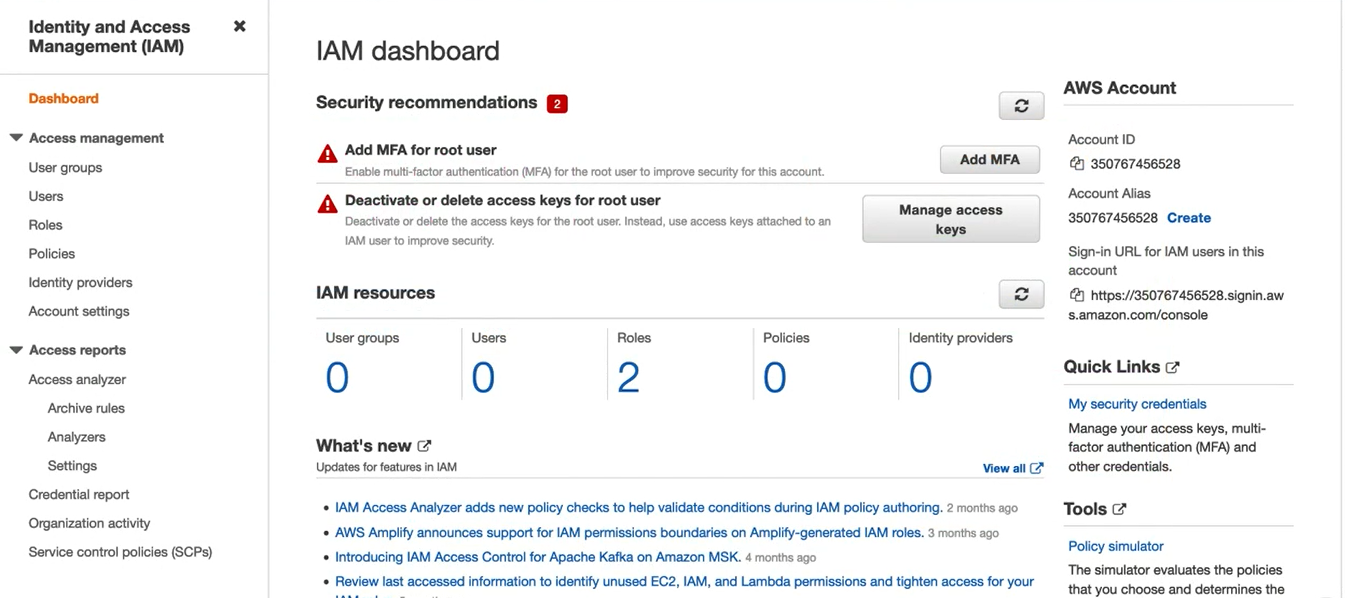
IAM - Identity and access management(IAM)

gate keeper to all of the serives

* -Passwords
* -multi factor authen
* -Access keys
* -SSh Keys

Policy - a policy is a colection of permissions to access different service in a particular way.

Policy - permission, resource permission, service permission



=================================

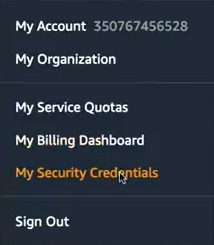
Securing your AWS account

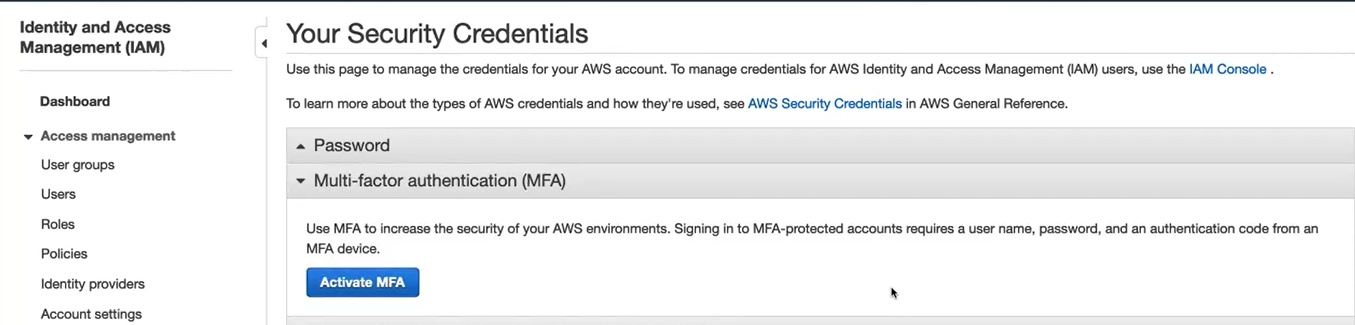
Root account permissons - Admin all service, modigy billing info, manage users

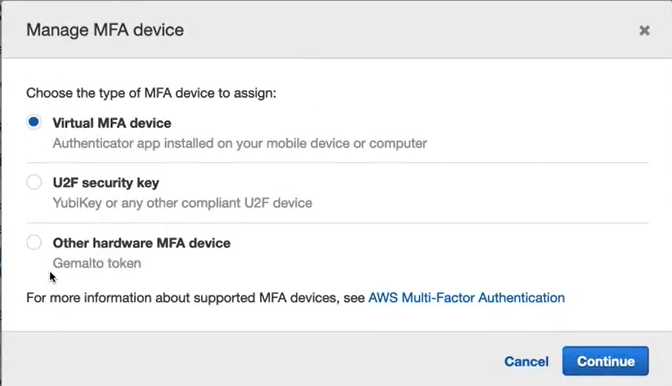
MFA- more than one way authen

Mfa either hardware or smartphone

enable mfa for root acc - select name -your security cred - Activate MFA









=================================

**Understand policy**

users have no perm by default

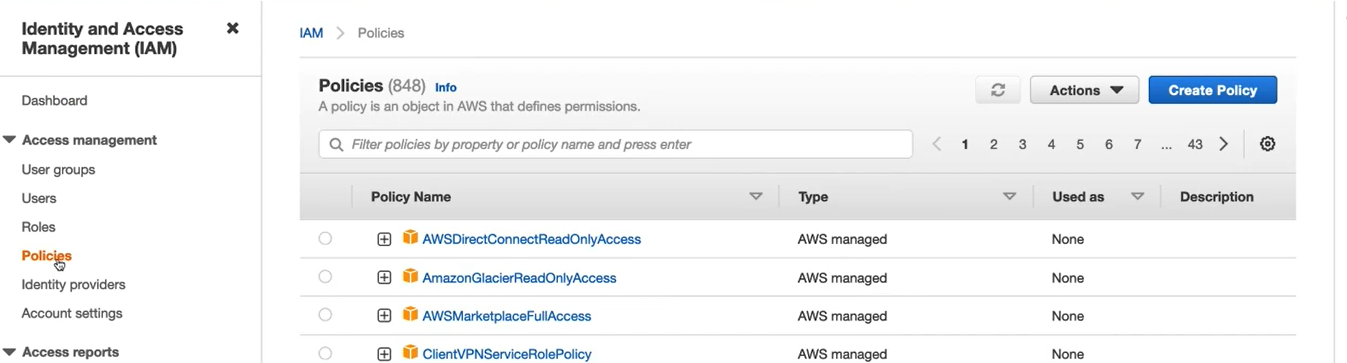
effect - allow or deny

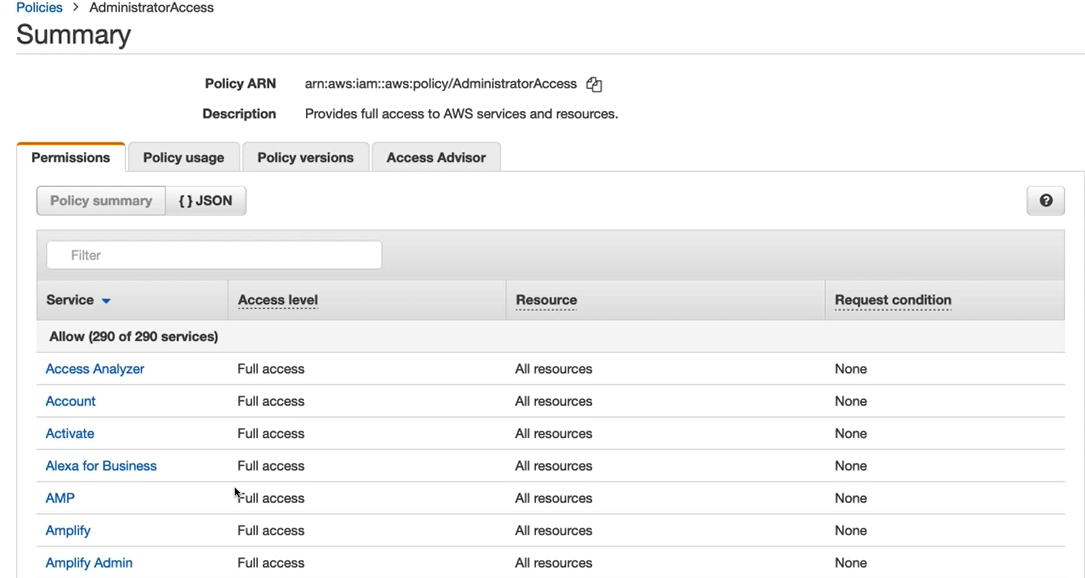
Action - Operations user can perform on service

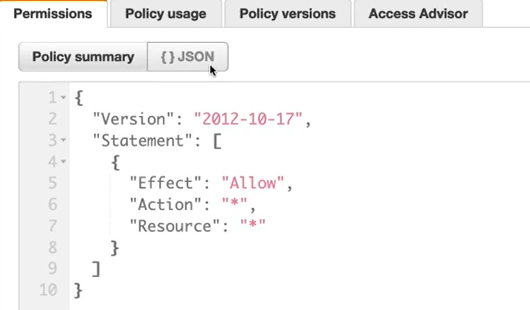
resource - sepcific resources can perform acton on

AWS Managed policy - general purpose service-wide permissions

Custom managed policy- custom specific resource permissions



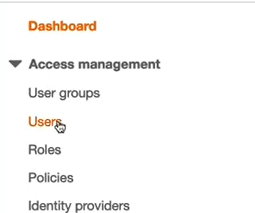


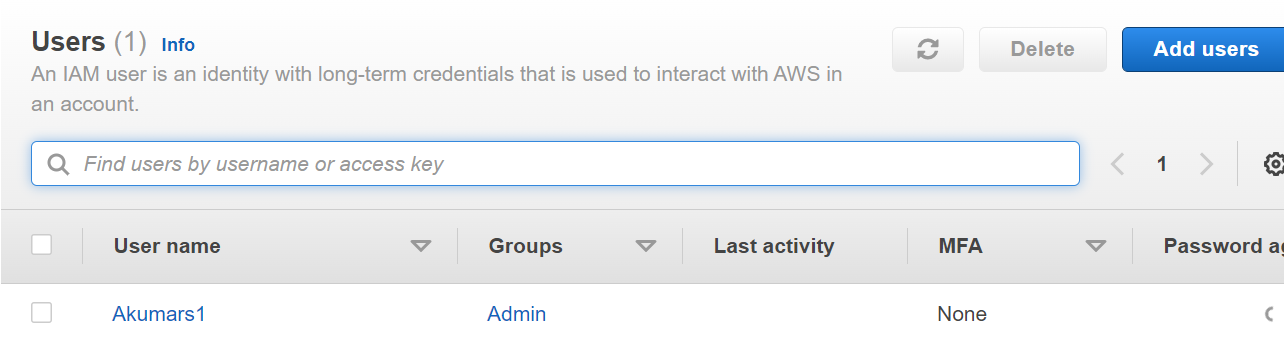


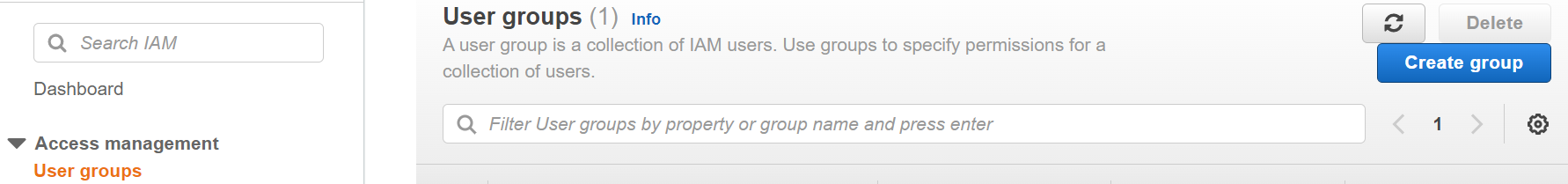
================================

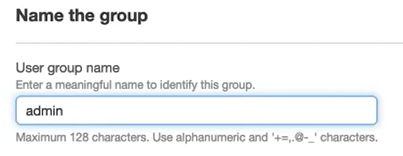
**config users and groups**

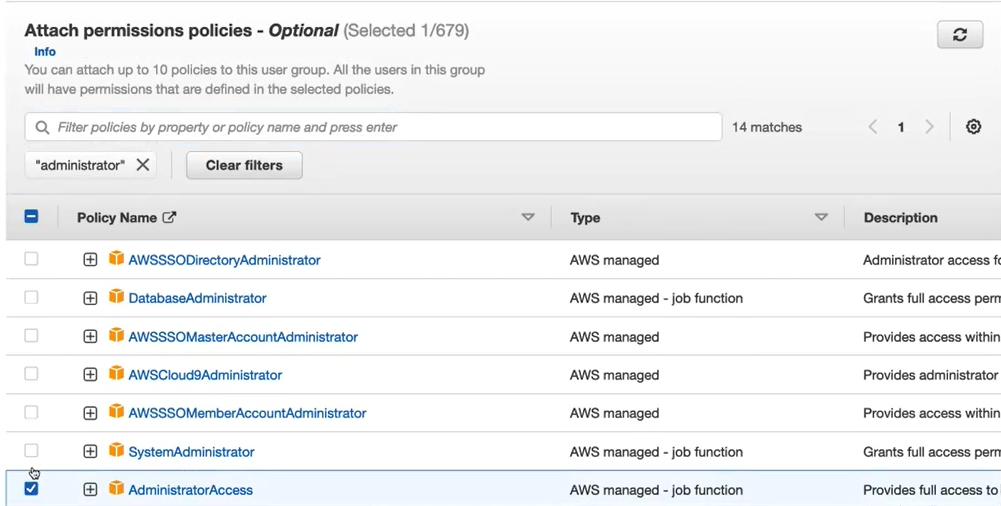
IAM groups - permissions via policies

Create a new user  




create a group  




  
=====================

**Getting Inside the virtual machine with EC2 and VPC(Virtual private cloud)**

VPC create a virtual network have private ip , free service can have max of 5 vpc in a acc.

**Key structures**

**Security group -** defines allowed incoming and outgoing Ip add and ports. mini firewall

**VPC uses routing table -** each vpc have 1 routing table

each vpc has 1 Network access control list - acts a ip filtering table and superpowered security groups that apply rules to the entire vpc

============================

**Create a VPC**

launch VPC wwizard

edit routing tables.

=========================

**Create a public subnet for scaling**

ssubnet can only exist in a single availability zone need to create more subnets to deploy into different availability zones.

Give subnet a name