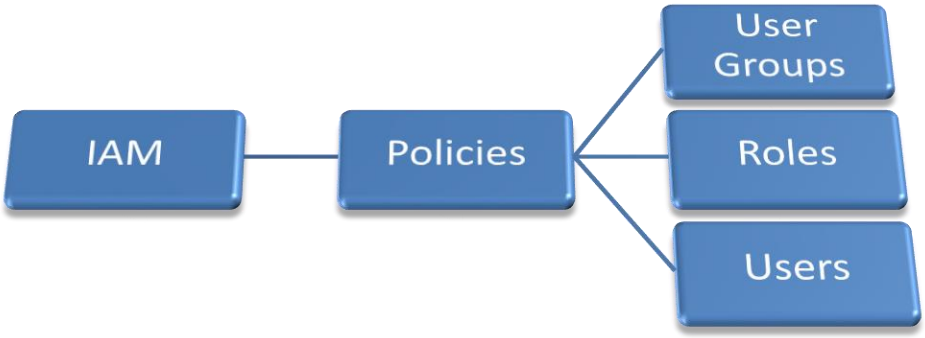
Day-4

.....

The topics that are covered are the base of an AWS which is IAM service i.e Identity & Access Management. Some other topics were also covered like CloudWatch Metrics and CIDR. All of their information are as follows:

IAM: It manages access to AWS resources securely. We can create and manage AWS users, groups, and roles, as well as define policies that allow or deny specific permissions to resources. The main topic it covers in Access Management are:



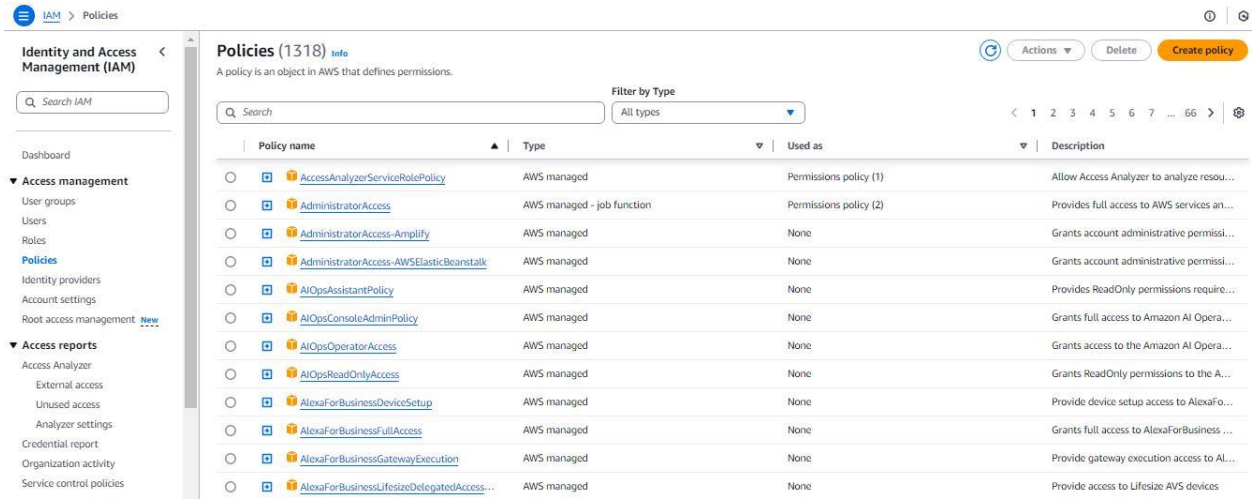
User Groups: Groups let you organize users according to criteria such as department or function, making it easier to administer access permissions. We can attach multiple users to a single group which share same type of policies and rules / rights in the AWS platform.

Roles: Roles are entities you create and assign specific permissions to that allow trusted identities perform actions in AWS. Like I have an Guest Access to the Wi-Fi, So my role can be considered as a Guest and permissions are given accordingly.

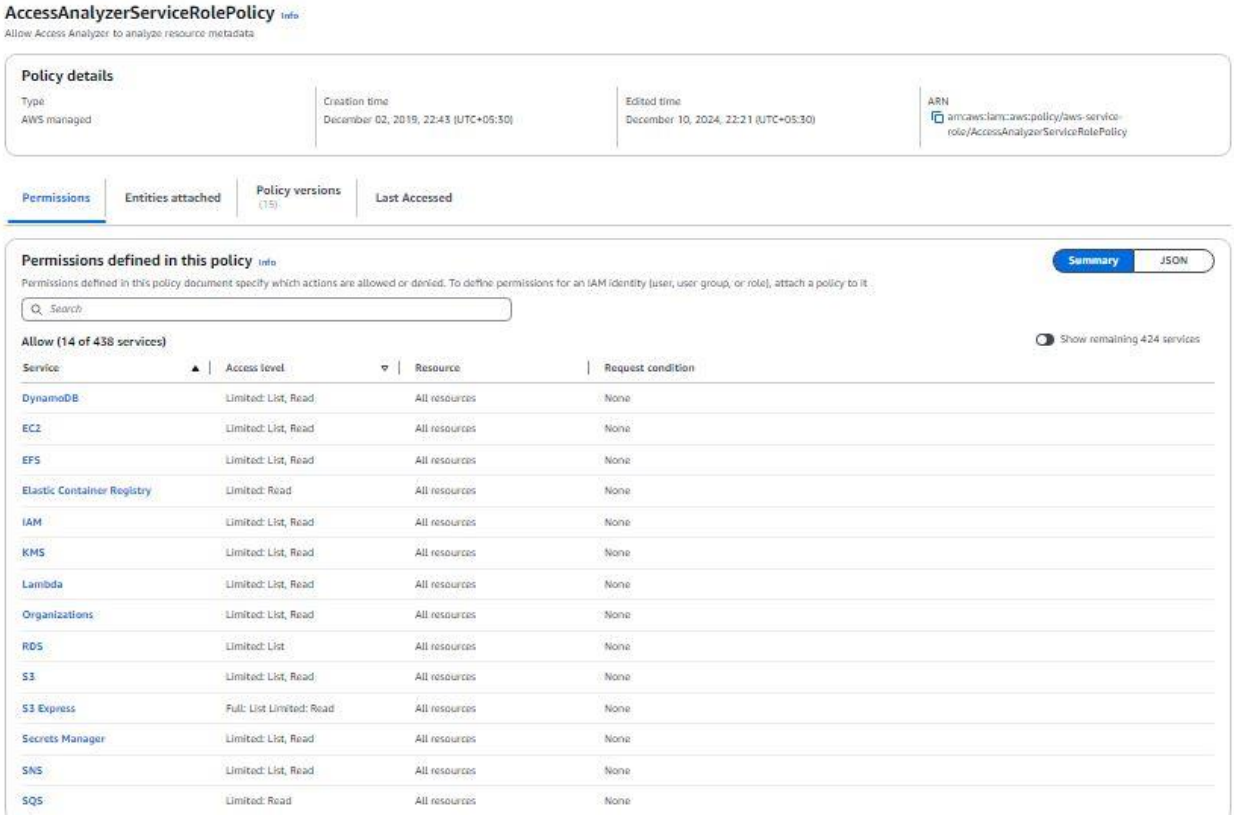
User: Users are identified by a unique login ID, password which is provided by the root IAM account. The user can be given a role, group or a specific policy according the requierment

Policies: A policy consists of rules that either allow or deny access to an action or service. Policies can be attached to users, groups, or roles. It is the most important and crucial part of IAM as it is the base security of your AWS Space.

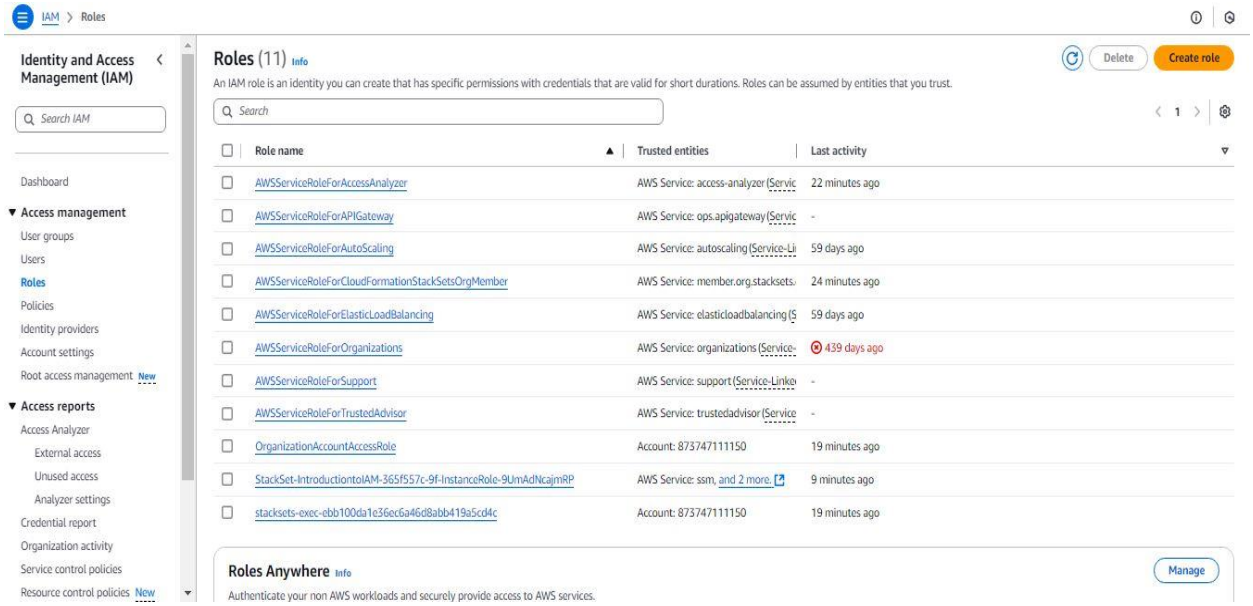
Policies Dashboard:



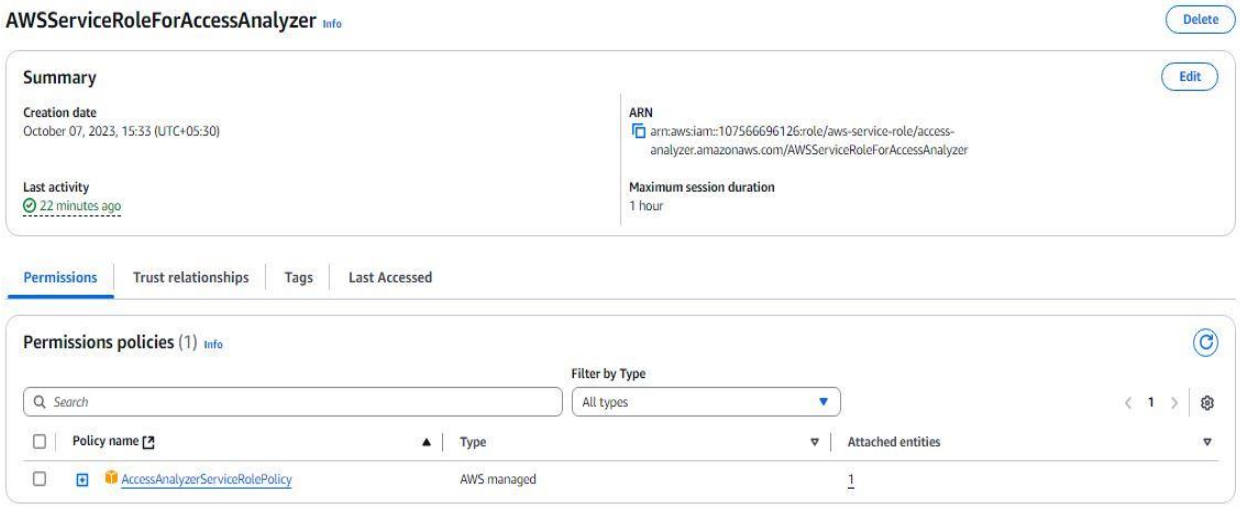
Criterias defined in a Policy:



Roles Dashboard:

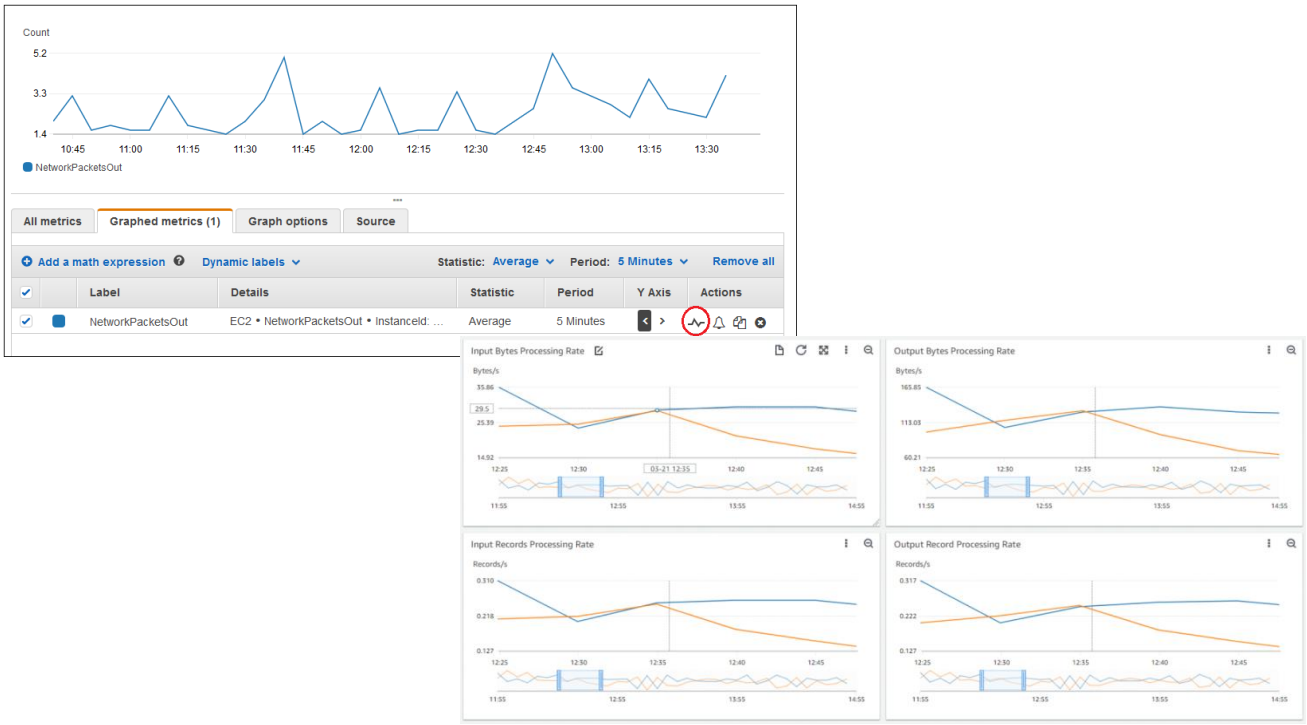


Policies assigned to a Role:



CloudWatch: It tracks their health, performance, and usage in real-time. You can set alarms to get notified if something goes wrong, and even automate responses to keep your systems running smoothly.

CloudWatch Metric & Analysis Page:



CIDR: CIDR (Classless Inter-Domain Routing) is a method of allocating subnet ranges to an IP. There is a way by which you can use to calculate that how many subnets that you can provide to a CIDR. I have attached some examples of CIDR and a self made calculation table of CIDR.

CIDR Subnet Range

Port	Formula	Range
/8	2*24	16777216
/9	2*23	8388608
/10	2*22	4194304
/11	2*21	2097152
/12	2*20	1048576
/13	2*19	524288
/14	2*18	262144
/15	2*17	131072
/16	2*16	65536
/17	2*15	32768
/18	2*14	16384
/19	2*13	8192
/20	2*12	4096
/21	2*11	2048
/22	2*10	1024
/23	2*9	512
/24	2*8	256
/25	2*7	128
/26	2*6	64
/27	2*5	32
/28	2*4	16
/29	2*3	8
/30	2*2	4

For example:

- 192.168.1.0/24
- 10.0.0.0/8
- 172.16.0.0/12

Facts:

1) You should rarely use your IAM Root account for security of your cloud space.

2) You should know the bits of CIDR, so you can assign the IP subnets accordingly.

3) Groups should be created in terms of Working and Confidentiality.

4) In cloud Metrics Disk space= Secondary Memory, Memory= Primary Memory.

5) Status check monitoring of an instance in a CloudWatch is most important and free of cost.