

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:

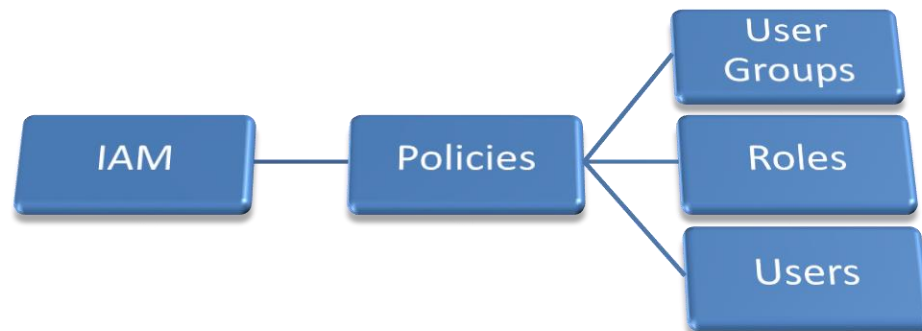
▼ Access management

User groups

Users

Roles

Policies



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 requirement

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:

IAM > Policies

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

Access reports

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management

Access Analyzer

External access

Unused access

Analyzer settings

Credential report

Organization activity

Service control policies

Policies (1318)

A policy is an object in AWS that defines permissions.

Filter by Type

All types

Search

1234567...66

Policy name	Type	Used as	Description
AccessAnalyzerServiceRolePolicy	AWS managed	Permissions policy (1)	Allow Access Analyzer to analyze resou...
AdministratorAccess	AWS managed - job function	Permissions policy (2)	Provides full access to AWS services an...
AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permissi...
AdministratorAccess-AWSElasticBeanstalk	AWS managed	None	Grants account administrative permissi...
AIOpsAssistantPolicy	AWS managed	None	Provides ReadOnly permissions require...
AIOpsConsoleAdminPolicy	AWS managed	None	Grants full access to Amazon AI Opera...
AIOpsOperatorAccess	AWS managed	None	Grants access to the Amazon AI Opera...
AIOpsReadOnlyAccess	AWS managed	None	Grants ReadOnly permissions to the A...
AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaFo...
AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness ...
AlexaForBusinessGatewayExecution	AWS managed	None	Provide gateway execution access to AL...
AlexaForBusinessLifesizeDelegatedAccess...	AWS managed	None	Provide access to Lifesize AVS devices

Criteria defined in a Policy:

AccessAnalyzerServiceRolePolicy

Allow Access Analyzer to analyze resource metadata

Policy details

Type

AWS managed

Creation time

December 02, 2019, 22:43 (UTC+05:30)

Edited time

December 10, 2024, 22:21 (UTC+05:30)

ARN

arn:aws:iam::aws:policy/aws-service-role/AccessAnalyzerServiceRolePolicy

Permissions

Entities attached

Policy versions

Last Accessed

Permissions defined in this policy

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

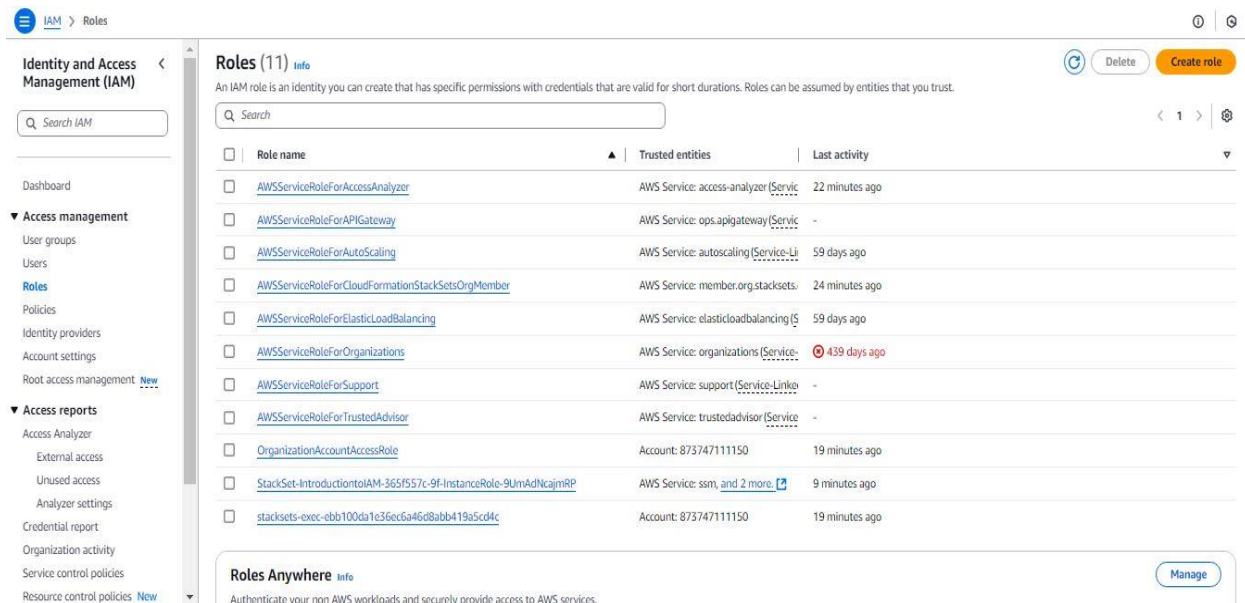
Search

Allow (14 of 438 services)

Show remaining 424 services

Service	Access level	Resource	Request condition
DynamoDB	Limited: List, Read	All resources	None
EC2	Limited: List, Read	All resources	None
EFS	Limited: List, Read	All resources	None
Elastic Container Registry	Limited: Read	All resources	None
IAM	Limited: List, Read	All resources	None
KMS	Limited: List, Read	All resources	None
Lambda	Limited: List, Read	All resources	None
Organizations	Limited: List, Read	All resources	None
RDS	Limited: List	All resources	None
S3	Limited: List, Read	All resources	None
S3 Express	Full: List Limited: Read	All resources	None
Secrets Manager	Limited: List, Read	All resources	None
SNS	Limited: List, Read	All resources	None
SQS	Limited: Read	All resources	None

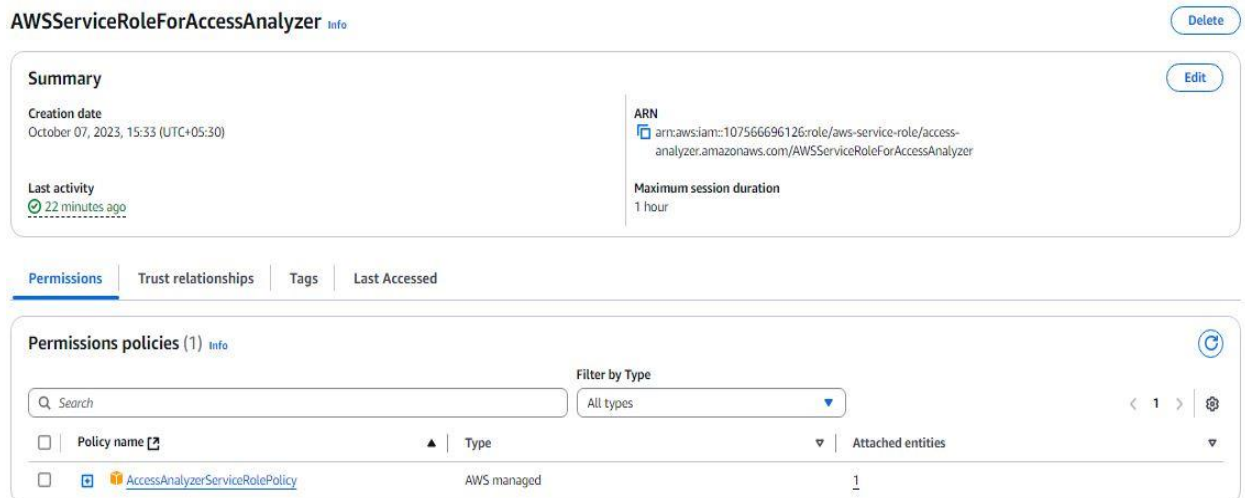
Roles Dashboard:



The screenshot shows the AWS IAM Roles Dashboard. On the left is a navigation sidebar with sections like 'Identity and Access Management (IAM)', 'Access management', 'Access reports', and 'Resource control policies'. The main content area is titled 'Roles (11)' and includes a search bar and a table of roles. The table has columns for 'Role name', 'Trusted entities', and 'Last activity'. Roles listed include 'AWSServiceRoleForAccessAnalyzer', 'AWSServiceRoleForAPIGateway', 'AWSServiceRoleForAutoScaling', 'AWSServiceRoleForCloudFormationStackSetsOrgMember', 'AWSServiceRoleForElasticLoadBalancing', 'AWSServiceRoleForOrganizations', 'AWSServiceRoleForSupport', 'AWSServiceRoleForTrustedAdvisor', 'OrganizationAccountAccessRole', 'StackSet-IntroductiontoIAM-365f557c-9f-InstanceRole-9UmAdNcajmRP', and 'stacksets-exec-ebb100da1e36ec6a46d8abb419a5cd4c'. Below the table is a section for 'Roles Anywhere' with a 'Manage' button.

Role name	Trusted entities	Last activity
AWSServiceRoleForAccessAnalyzer	AWS Service: access-analyzer (Service-Linked Role)	22 minutes ago
AWSServiceRoleForAPIGateway	AWS Service: ops.apigateway (Service-Linked Role)	-
AWSServiceRoleForAutoScaling	AWS Service: autoscaling (Service-Linked Role)	59 days ago
AWSServiceRoleForCloudFormationStackSetsOrgMember	AWS Service: member.org.stacksets (Service-Linked Role)	24 minutes ago
AWSServiceRoleForElasticLoadBalancing	AWS Service: elasticloadbalancing (Service-Linked Role)	59 days ago
AWSServiceRoleForOrganizations	AWS Service: organizations (Service-Linked Role)	439 days ago
AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-
OrganizationAccountAccessRole	Account: 873747111150	19 minutes ago
StackSet-IntroductiontoIAM-365f557c-9f-InstanceRole-9UmAdNcajmRP	AWS Service: ssm, and 2 more (Service-Linked Role)	9 minutes ago
stacksets-exec-ebb100da1e36ec6a46d8abb419a5cd4c	Account: 873747111150	19 minutes ago

Policies assigned to a Role:

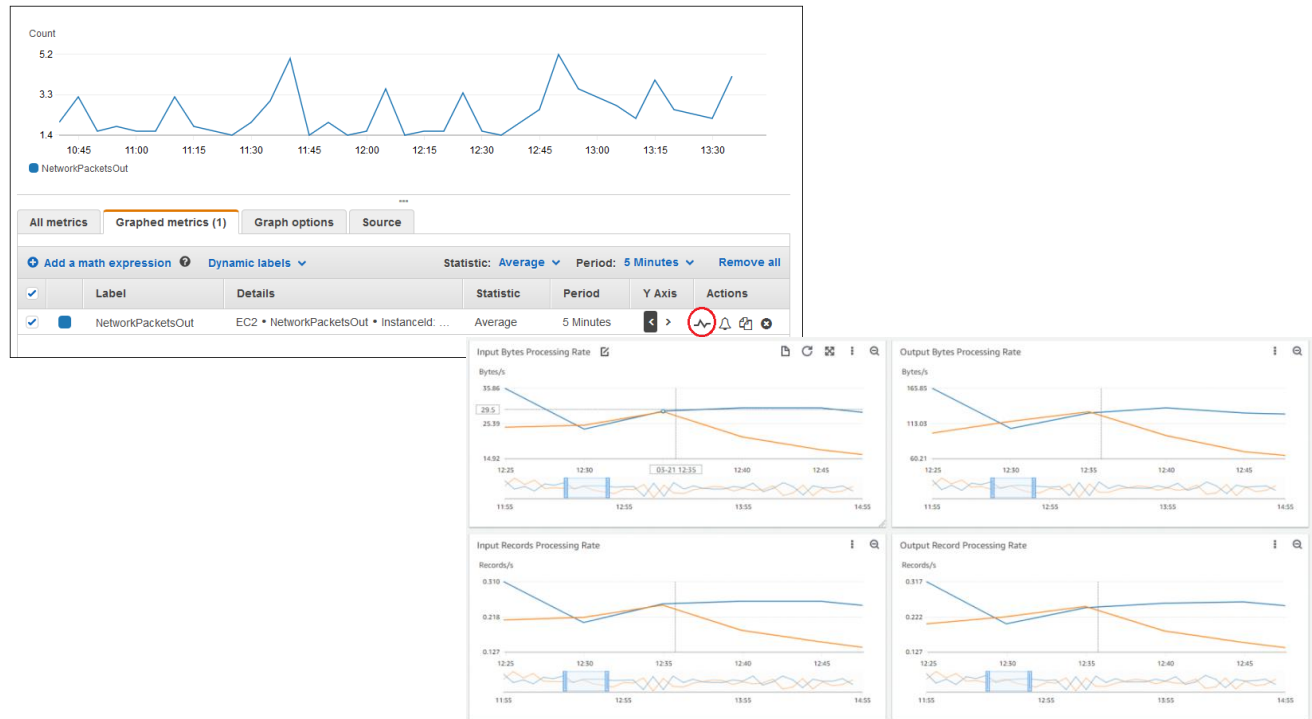


The screenshot shows the 'Policies assigned to a Role' page for the 'AWSServiceRoleForAccessAnalyzer' role. It includes a 'Summary' section with 'Creation date' (October 07, 2023, 15:33 (UTC+05:30)) and 'Last activity' (22 minutes ago). The 'ARN' is 'arn:aws:iam::107566696126:role/aws-service-role/access-analyzer.amazonaws.com/AWSServiceRoleForAccessAnalyzer' and the 'Maximum session duration' is '1 hour'. Below this are tabs for 'Permissions', 'Trust relationships', 'Tags', and 'Last Accessed'. The 'Permissions' tab is active, showing 'Permissions policies (1)' with a search bar and a table. The table has columns for 'Policy name', 'Type', and 'Attached entities'. One policy is listed: 'AccessAnalyzerServiceRolePolicy' of type 'AWS managed' with 1 attached entity.

Policy name	Type	Attached entities
AccessAnalyzerServiceRolePolicy	AWS managed	1

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.