lec-18

IAM Groups

*

- IAM Group = Collection of IAM users.
- It is possible to attach multiple policies to the IAM user & IAM Group, Max = 10.
- You can add & remove policies to IAM user & groups anytime.
- If you attach ~~anytime~~ any IAM user to IAM Group, IAM user individual permissions will not be lost, Group level permissions will be inherited.
- An IAM user can be attached to multiple IAM Groups at the same time.
- For new IAM user by default there are not policies to attached.

* - IAM ~~user~~ groups are used to assign policies to bunch of IAM users at same time.

- Policies contains permissions.

** - Policies / permissions are written in JSON format.

- AWS has policies editor or policy genrator, these will help you to genrate JSON code Automatically.

* Managed Policies = created & managed by AWS (Predefined Policies)

- Inline policy = created & managed by customer (Customer managed policies)
- ARN = Amazon Resource Name
  - ARN's will be used in JSON Policies.

- IAM User is used to access AWS console & services but not login to EC2 instance.

* IAM ROLES

Roles = Temporary access without Credentials.

- If you use IAM Roles, you no need to configure keys on the machines.
- Based on the permissions that you have attached to the role, those permission are available from the instance
- 1 EC2 instance can have only 1 ROLE attached at at time.
- 1 Role can be attached to multiple EC2 instance

---

lect - 20

What is SAML?

- SAML = Security Assertion Markup Language is a open fedration standard that allow an identity provider (idP) to authonticate users and pass identity & securit info about them to a service provider (SP). This info is sent in XML Document.

- SAML Performs two functions.
  - Authentication - Who are you?
  - Authorization - what can you do?

- When you enable organizations in the AWS account, this account will become Management Account.

* IAM TAGS

* - Tags are key-value pair
- Tags are used for identification purpose.
- TAGS are not IAM specific, it is through out AWS
- TAGS are very important, but it is optional.
- TAGS are useful for Billing Purpose also.
- TAGS are useful for doing Automations in AWS.
- TAGS are helpful for doing cost optimization.

features

* **IAM Credential Report** :- A Report that list all your account users and status of their various credentials

* **IAM Access Advisor** :- It shows the service permissions granted to the user and when those were last used.

* **IAM Access Analyzer** := It is used to analyze access of IAM users (unused & external access).

IAM Policies Structure

Consist of
- Version - Policy language version.
- Id - An identifier for the policy (optional)
- Statement - one or more individual statements. (required)

* **Statement Consist of** :-
  - Sid = An identifier for the statement (optional)
  - Effect = Allow or Deny
  - Principle = Account / user / Role to which policy is applied to.
  - Action = List of actions this policy allows or denies.
  - Resourse = List of resources which the actions apply to.
  - Conditions = Conditions for when the policy is in effect (optional).

IAM Users
IAM Groups
IAM Roles
IAM Policies
IAM Tags
IAM Federations
organization

→ IAM service.

This also comes in IAM service. **