**IAM: - Its web services full of API – Identity Access management**

* IAM stands for 12 digit authentication number which fix –it provide by AWS randomly
* (Cloud base authentication)
* Login with 1 ID that protocol – Open ID connect service
* Its Free service from AWS – Global Service
* Tenancy Model
* Backward Compatible –AD /LDAP
* Web base service
* Collection of API’s
* Secure service
* Service – federation –language--- SMAL format
* **Protocol – OAuth2**

## Main Function of IAM?

1. **Who you are**—user name & password (credentials)-Authenticate
2. **What are you allow to do** –check your permission – Authorization

## Advantages of IAM:-

* High Availability--HA
* High Security ----HS

IAM stand for global service authentication in all regions

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

Where we can find the IAM in other cloud: -

**In Azure: -**

* + Inside the Azure AD we can see IAM

**In GCP:-**

* + Direct IAM

Data Centre’s: -

1. Local profile—In side computer
2. Remote Profile – Roaming

How to login Linux machine & windows machine with which process?

**Linux machine** login: - 1) etc / password –User name & password

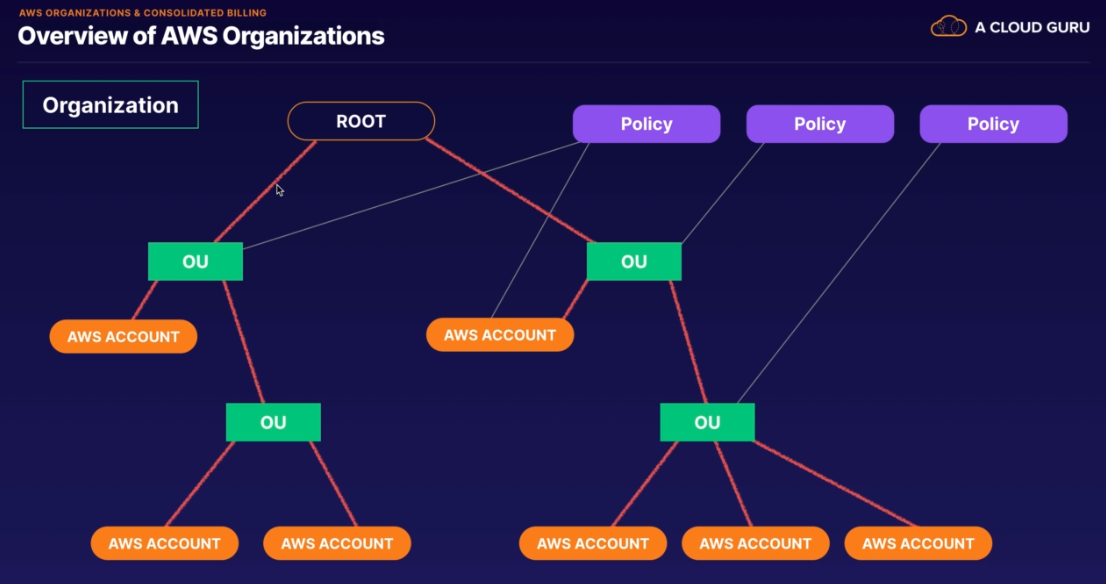
2) etc shadow

**Windows Machine** login: - SAM – User name & password

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

LDAP – Login in Linux –AD for windows---Centralised authentication

**AWS Organisations Structure**



**Below 4 are IAM Identity: -**

1. **Users (physical Identity) :-**

* AWS user have by default no permission (**Implicit denied)—just create User without any Access.**
* User give any other access or permissions/policy (Explicit denied) ---Provide the permission (Policy)

Every user or create object are **ARN –Unique Identity**

**Allow permission – called policy in format of Jason (JSON-Java Script Object Notification) ymal**

* ~~P- principle~~ – Identity /user / Role / group ------ARN --not necessary
* E- **Effect** – Either allow or denied
* A-**Action** – Create /Delete

Compulsory

* R-**Resource** – Specific instance name / resource
* ~~C-Condition~~- Date & time --------------------------------not necessary for now

**Statement ID for particular policy**

**\*(star indicate) Means “allow” for them in policy**

1. **Groups (Logical Identity) :-**

* To add the users in group for identifying the organisation

1. **Policy :-**

Policy are having 2 types:-

1. Managed Policy :-

----Manage are reusable

* AWS Policy
* Customer Policy

1. Inline Policy :-

---Intune are not reusable

**Why we called Policy- Asked who, what, which, when, why**

1. **Roles (Temp Access) :-**

* This is use for service to service access
* This role is linked service link Role
* 3rd party access provided from Roles (cross account access)
* Federation – integrate the users from 1 company to other company
* Security Token Service (STS)-----It required Token ----use Kerberos server

**Not Provide** – i) User name & password

ii) Access key & Sec. Key.

* + Its base for temp identity access
  + Access/Guest: - for temp access only

**MFA (Multi-Factor Authenticator):-**

* H/w Authenticator-- Gemalto token ,hard token ----Hardware Device token
* Virtual Authenticator – Google Authenticator ,Microsoft Authenticator -------pin/otp generate

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

Practical for 3rd party access provided from Roles

(cross account access):-

* **Trusting/Product: - Account Number: - 437523601341 (KD)----12-digit number**

1. Create a Role …..out 12 ac no of trusted 371533563389
2. Attached policy to the ……depending on access requirements
3. Share ARN and Name with trusted given below :-

ARN of my role: - arn:aws:iam::437523601341:role/hp\_poc

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Going to next Client \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

* **Trusted /Client :- Account Number :- 371533563389 (MG)-----12 digit number**

1. Create group POC
2. Add users to POC group
3. Create a policy for STS access
   * Service – STS
   * Action - AssumeRole
   * Resource – add trusting company ARN(arn:aws:iam::437523601341:role/hp\_poc)

Attached policy to POC\_group.

1. Login as hp user ……..switch role …..access to trusting account.

**Permission Boundary: - SCP** (Service Control Policy) ---------------------------------AWS Organization

* It acting as guard rails
* Never grant the permission

Advantages of SCP (Service Control Policy)---

* Unable to delete the root account
* SCP is not applied on master account (root mater account)
* SCP working as top to bottom & you have taken authority

**Blacklist – Permissions Denied ---**always follow this

**White list- Permissions Access**

**AWS Permission & What should be Affect...**

**Permission flow logic:-**

1. By default Implicit denied :-
2. Explicate allow :-

* IAM Policy- Users & group attach

--Within aws only –Internal policy for with aws

* Resource policy – S3 ,Dynamic , applications

-- External policy for all over internet

* When you’re not member of AWS account we can use Resource policy

1. Permission boundary :-

* Applied on Users & group
* Its block the policy

1. SCP (Service Control Policy)

* Applied in organization

1. Explicit Deny: -