Account Management, Billing & Support Section

AWS Organization

- → Global service
- → Allows to manage multiple AWS accounts
- → Cost Benefits :

① Consolidated Billing accross all accounts - single payment method

② Pricing benefits from aggregated usage (volume discount for EC2, S3, ...)

③ Pooling of Reserved EC2 instances for optional savings.

- → API is available to automate AWS account creation
- → Restrict account privileges using Service Control Policies. (SCP)

Multi Account Strategies

① Create accounts per dept, per cost center, per dev/test/prod, based on regulatory restrictions (using SCP), for better & resource isolation(ex: VPC), to have seperate per-accout service limits, isolated account for logging.

- Multi Account Vs One Account MultiVPC.

- Use tagging stadards for billing purposes

- Enable CloudTrail on all accounts, send logs to central S3 account.

- Send CloudWatch logs to central logging account.

* Organization Unit [OU] :- simple words nothing but dept or categories or projects. of organization

Service Control Policies (SCP)

① Whitelist or blacklist IAM actions

② Applied at the OU or Account level

③ Does not apply to the Master Account

④ SCP is applied to all the users & Roles of the account, including Root

⑤ The SCP does not affect service-link roles

- Service-linked roles enable other AWS services to integrate with AWS organizations and can't be restrikted by SCPs.

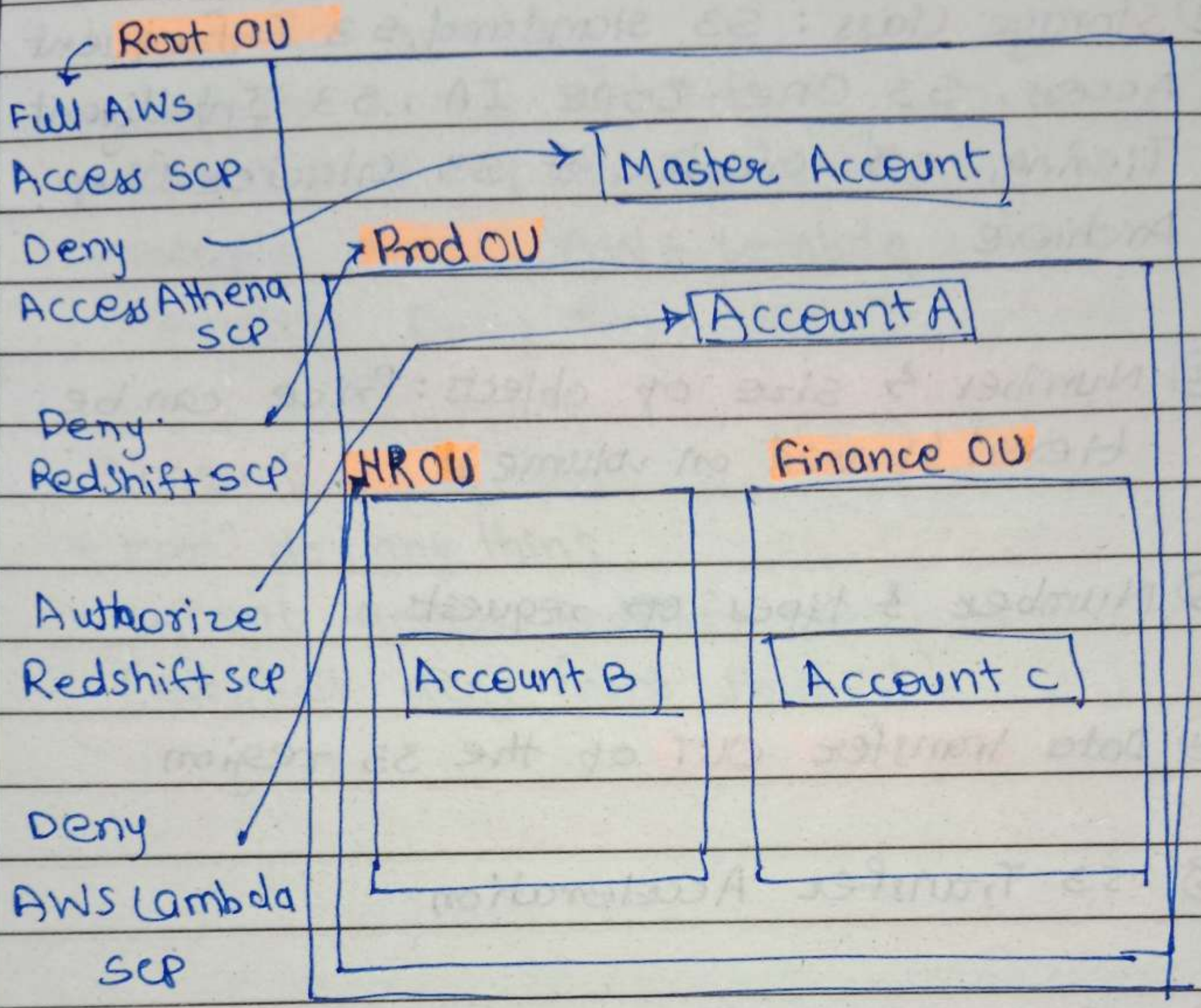
⑥ SCP must have an explicit Allow (does not allow anything by default)

⑦ Use Cases:

① Restrict access to certain services (for exe: can't use EMR)

② Enforce PCI compliance by explicitly disabling services.

SCP Hierarchy



- Master Account
  - Can do anything
  - No SCP apply

- Account A
- Can do anything
- except access deny redshift (explicit Deny from OU)

- Account B
  - can do anything
  - except access RedShift (explicit Deny for Prod OU)
  - except access AWS Lambda (explicit Deny from HROU)

- Account C
  - can do any thing
  - except access RedShift (explicit deny from Prod OU)

AWS organization- Consolidated Billing

- When enabled, provides you with:

- Combined Usage- combine the usage the all across AWS accounts in the AWS organization to share volume pricing, Reserved Instance & saving Plans discounts

- OneBill - get one bill for all AWS accounts in the AWS organization

- The management account can turn off Reserved Instances discount sharing for any account in the AWS Organizatio, including itself.

AWS Control Tower

① Easy way to setup & govern a secure and compliant Multi-account AWS environment based on best practices.

② Benefits:-

1] Automate the set up of your env in few clicks.

2] Automate ongoing policy management using guardrails.

3] Detect policy violations & remediate them

4] Monitor compliance through an interactive dashboard.

③ AWS Control Tower runs on top of AWS Organizations:

It automatically sets up AWS organizations to organize accounts and implement SCPs (Service Control Policies)

AWS Resource Access Manager (AWS RAM)

① Share AWS resources that you own with others AWS accounts

② Share with any account or within your Organization.

③ Avoid resource duplication!

④ Supported resources include Aurora, VPC Subnets, Transit Gateway, Route 53, EC2 Dedicated Hosts, License Manager Configurations.... so on

~~AWS Resource Catelog~~

AWS Service Catalog

① Users that are new to AWS have too many options, and may create stacks that are not compliant / in line with the rest of the organization.

② Some users just want a quick self-servi portal to launch a set of authorized products pre-defined by admins.

③ Includes: virtual machines, databases, storage options, etc....

④ Enter AWS Service Catalog!

For AWS Service Catalog :-

① Admin needs to do following tasks:

Product - Cloudformation Templates

Portfolia - Collection of Products

Control - IAM permissions to Access Portfolios

② User tasks:

Product list - Authorized by IAM

↓ Launch

Provisioned Products - Ready to use Properly Configured properly Tagged

Account Best Practises - Summary

① Operate multiple accounts using Oraganization

② Use SCP (service Control Policies) to restrict account ower ~~owner.~~ power

③ Easily setup multiple accounts with best practices with AWS control Tower

④ Use Tags & Cost Allocation Tags for easy management & billing.

⑤ IAM guidelines : MFA, least- privilege, password policy, password rotation

⑥ Config to record all resources configuratio s & compliance over time.

⑦ Cloud formation to deploy stacks across accounts & regions

⑧ Trusted Advisor & to get insights, Support Plan adapted to your needs.

⑨ send service Logs & Access Logs to S3 or CloudWatch Logs

⑩ CloudTrail to record API calls made within your account.

⑪ If your account is compramized: change the root password, delete and rotate all passwords | keys, contact the AWS support

⑫ Allow users to create pre-defined stacks defined by admins using AWS service Catalog.