Prerequisite setup of multi-environment Aws accounts using control tower for stating a SAAS company.

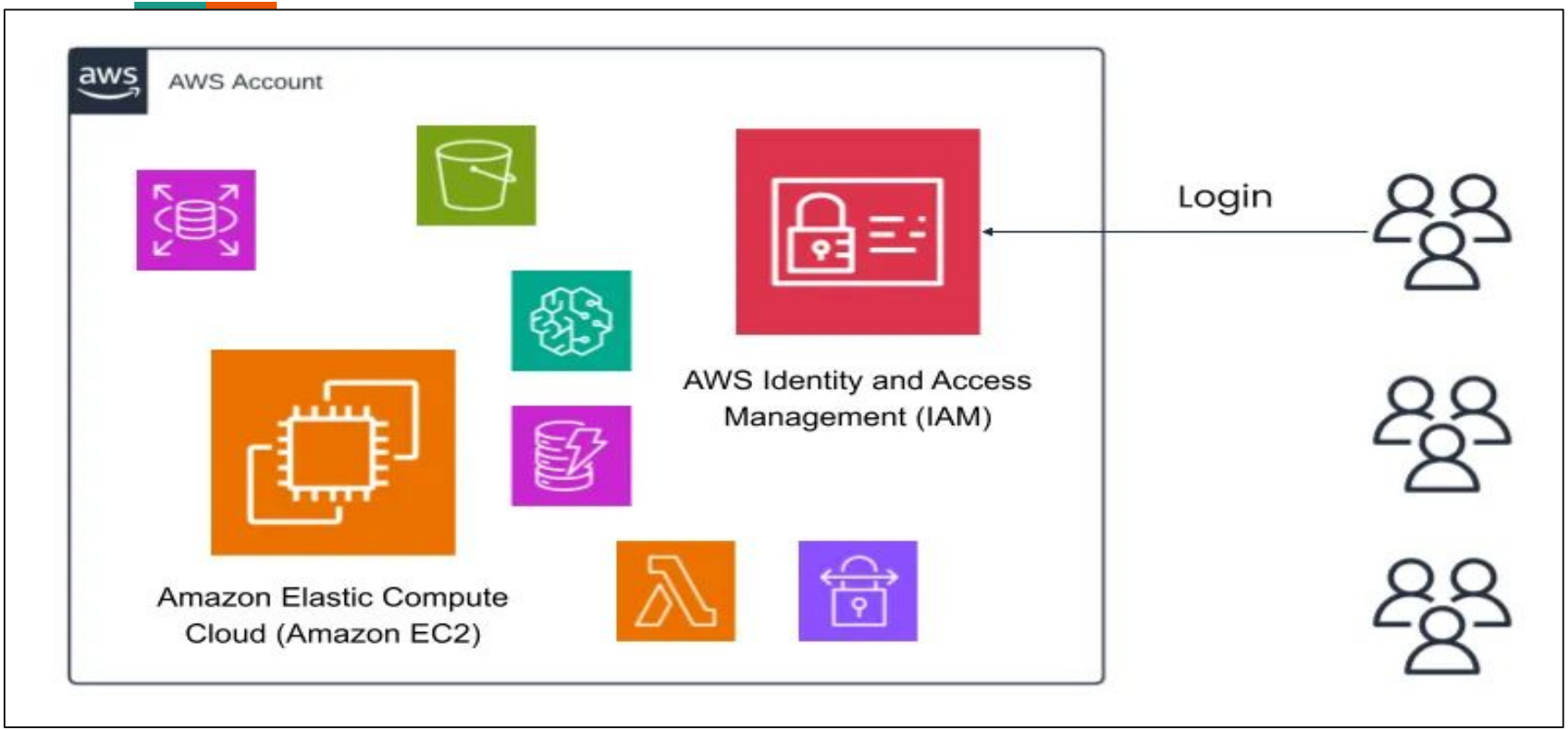
Prerequisite Setup of a Multi-Account for starting SaaS Company in AWS Cloud

The objective of this project is to build a scalable and secure infrastructure on AWS using Infrastructure as Code practices and to establish a Setup for a Multi account and multi region SaaS company setup in Cloud.

Setup of a Multi-Account for starting SaaS Company

- Setup of AWS Control tower/Landing Zone and creation of 3 dev, staging, prod accounts using AWS organizations.
- Configure SSO(Single Sign On) for the created AWS accounts.
- SCP implementation
- Applying Proactive and reactive controls from the AWS control tower console.
- Cross-account access and Role Based Access Control(RBAC) implementation .

How it was Before



Single AWS Account:

- An AWS account was created, and the team logged in directly.

Resource Deployment:

- Initial team deployed resources like EC2, databases, and storage.

Growth and New Teams:

- New teams also logged in directly and deployed their own resources.

Unstructured Management:

- Resources became mixed, making tracking and cost management difficult.

No Governance:

- No central policies, limited permissions, and no environment separation.

Security Risks:

- Direct logins and lack of control increased security vulnerabilities.

Key Questions for AWS Management:

Distinguishing Workloads:

How can we clearly separate each team's resources and ensure accountability?

+

Managing Permissions:

What is the best way to implement least-privilege access for different teams?

→

Handling Service Limits:

How do we monitor and manage service quotas to prevent disruptions?

Aws organisations

How do AWS organizations solve this problem?

AWS Organizations Overview:

- AWS Organizations is a service that helps you consolidate multiple AWS accounts into a single, centrally managed organization.

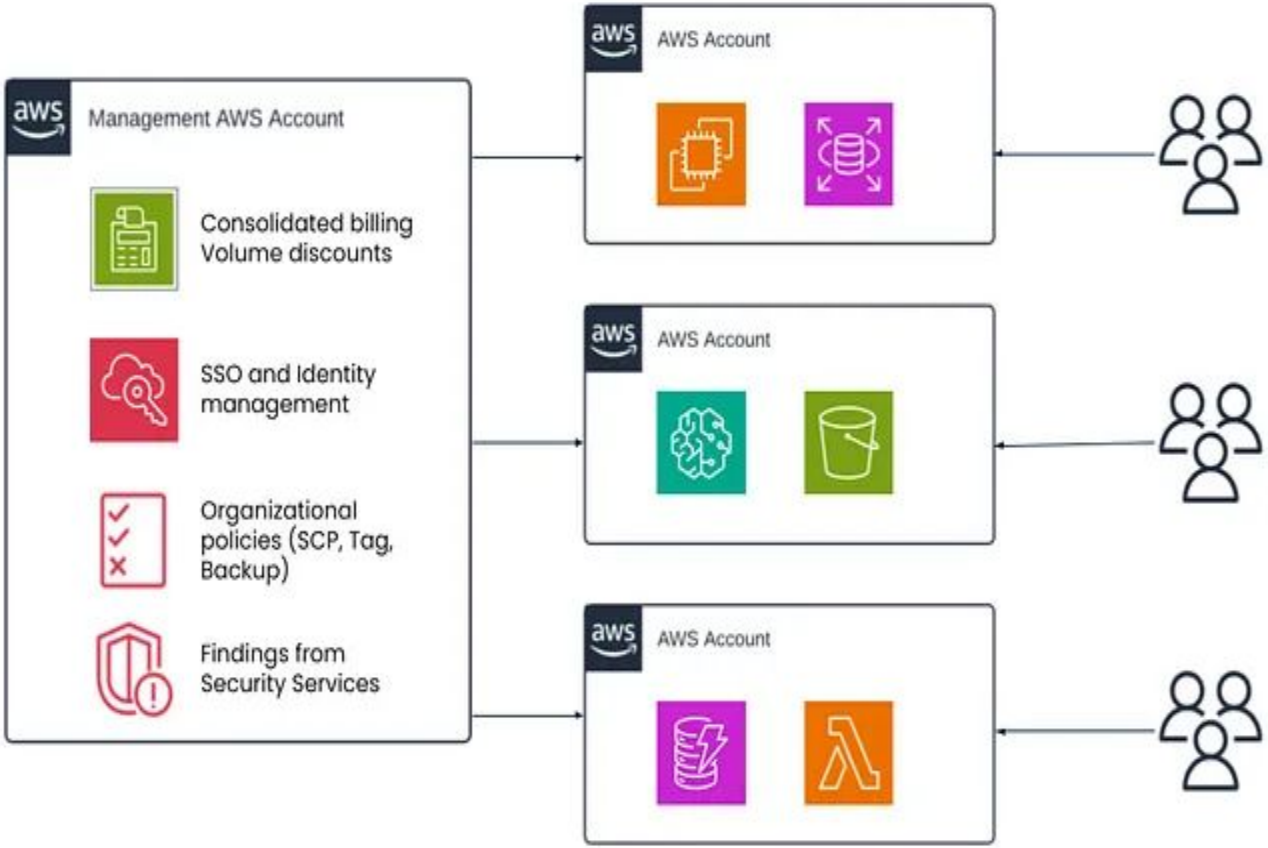
Account Management & Billing:

- It provides centralized account management and consolidated billing to meet budgetary, security, and compliance needs.

Administrator Capabilities:

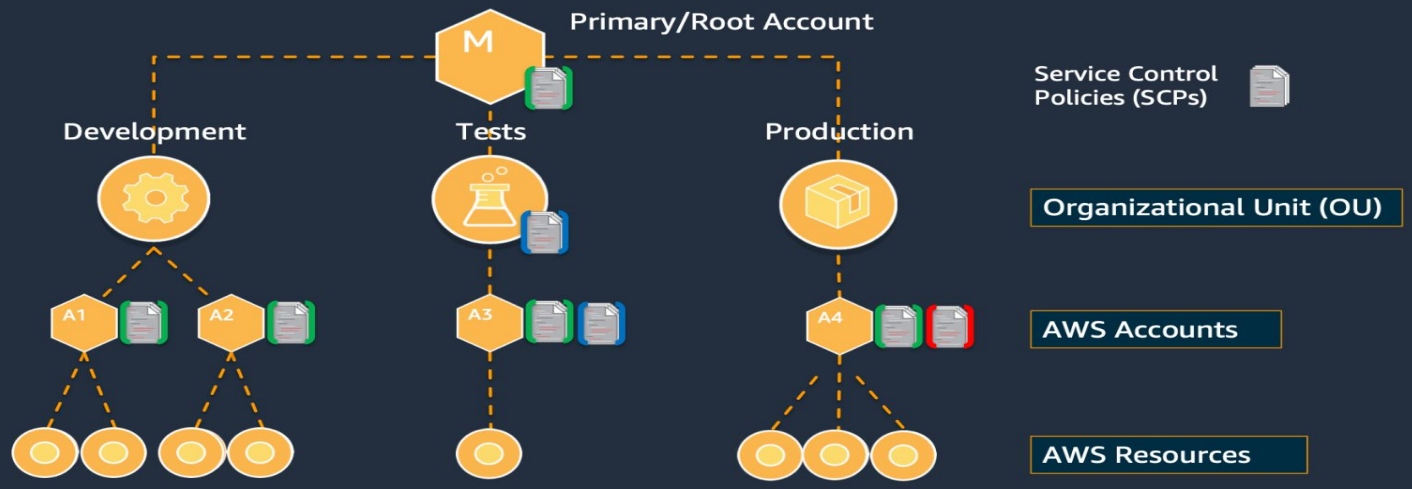
- As an administrator, you can:
  - Create new accounts within the organization.
  - Invite existing AWS accounts to join your organization.

AWS Organization



SCP Policies

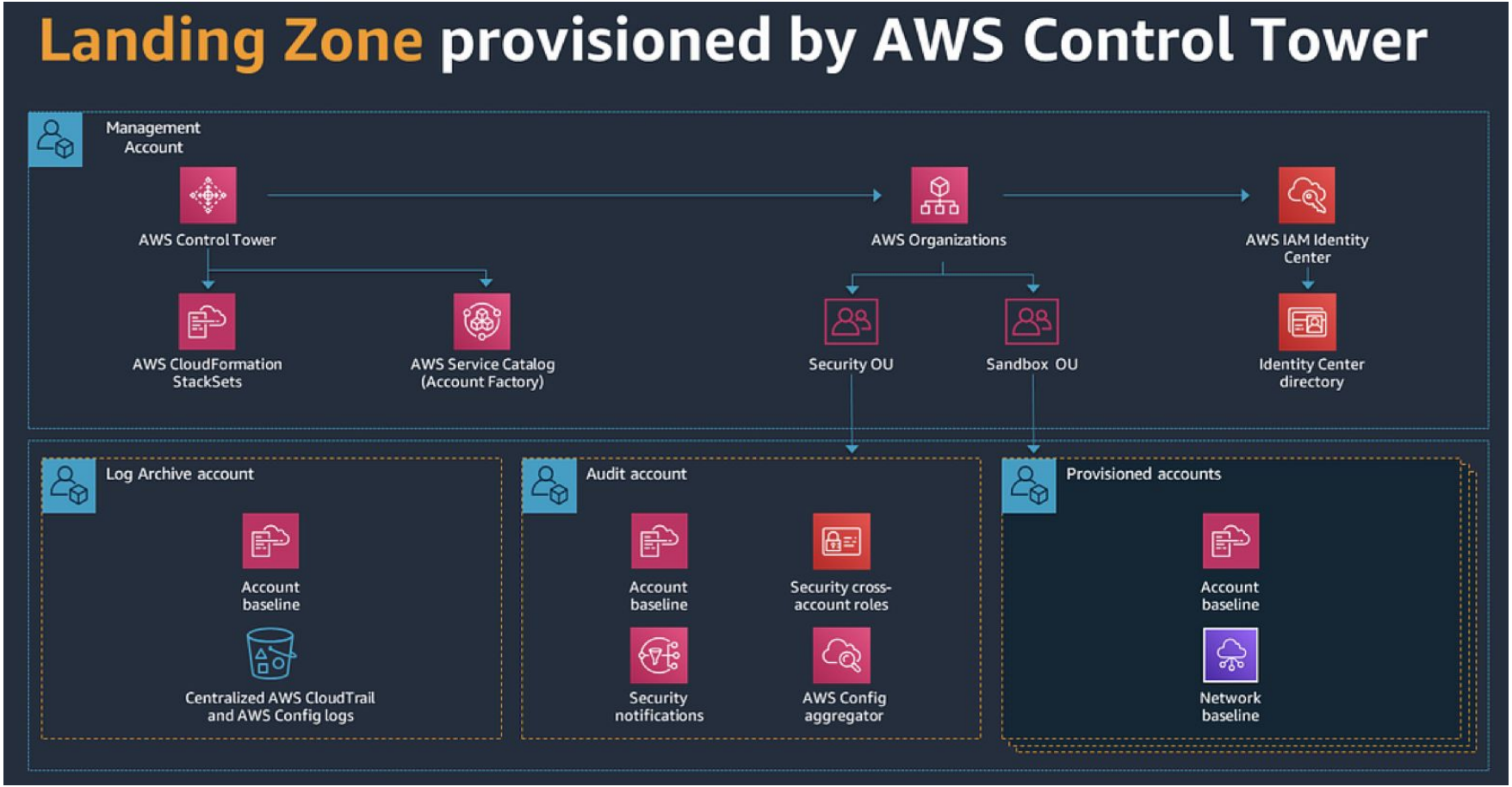
AWS Organizations – Service Control Policies (SCP)



What is AWS Control Tower?

- Automates the setup of a Landing Zone in AWS.
- Provides guardrails for governance and compliance.
- Integrates AWS Organizations to streamline multi-account setup.
- Simplifies account provisioning and management.

AWS Control Tower



Landing zone may help you with the following:

- **Security controls** — Different security policies for different workloads
- **Isolation —** The AWS account is a unit of security protection
- **Data isolation** — Limit access to highly private data
- **Different teams** with different responsibilities and resource needs
- **Different business units** with different purposes and processes
- **Billing** — separate charges (especially for traffic, as it can not be tagged)
- **Limit allocation** — Prevents one workload from affecting others (when service limit was reached)

Compliant and Non-compliant accounts

Enrolled accounts

Find accounts

1

Account name	Account email	Organizational unit	Owner	Compliance status	State
Devops Cloud Labs	devopscloudlabs@gmail.com	Root	AWS Control Tower	Compliant	Enrolled
Audit	devopscloudlabs+Audit@gmail.com	Security	AWS Control Tower	Compliant	Enrolled
Log Archive	devopscloudlabs+Logs@gmail.com	Security	AWS Control Tower	Compliant	Enrolled

AWS Organization

aws | Services | Search [Alt+S] | Sydney | sanjeev @ devopscloudlabs

AWS Control Tower

- Dashboard
- Getting started
- **Organization**
- Account factory
- **Controls library**
  - Categories
  - All controls
- Users and access
- Shared accounts
- Landing zone settings
- Activities
- AWS Marketplace for Control Tower
- See What's New in AWS Control Tower
- View our AWS Control Tower

AWS Control Tower > Organization

Organizational units (OUs) are entities created within your organization to group accounts for governance. You can add new OUs to your organization at any time.

Organization Info

Expand all | Group resources | Actions | Create resources

Find resources using properties

Resource type: View all resources — 6 matches — 1

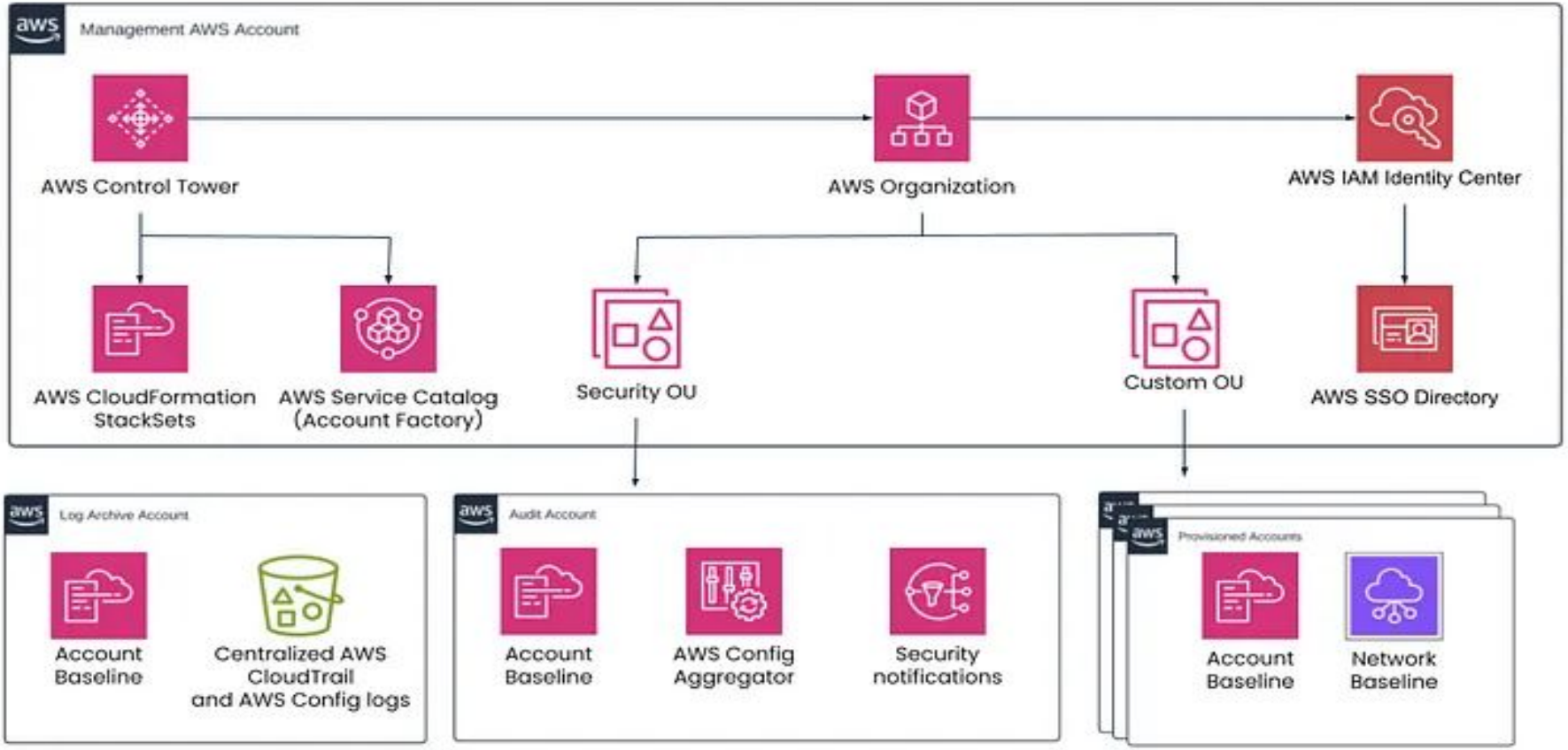
Name	State	ID	Email	Organizational units registered	Accounts enrolled	Blueprint product ID	Blueprint product version
Root	Registered	r-39qz	–	2 of 2	3 of 3	-	-
Sandbox	Registered	ou-39qz-ho7at5nz	–	0 of 0	0 of 0	-	-
Security	Registered	ou-39qz-5mr5sizv	–	0 of 0	2 of 2	-	-
Audit	Enrolled	476303940127	devopscloudlabs+Audit@gmail.com	–	–	-	-
Log Archive	Enrolled	580798369745	devopscloudlabs+Logs@gmail.com	–	–	-	-

Aws Control tower demo

https://youtu.be/e_AIUg2B-ac?si=Y6JqMs-lAlpdCksn

Why we use AWS Control Tower??

- Setup best practices AWS environment in few clicks
- Standardize AWS Accounts
- Centralize Management Policy
- Enforce governance and compliance proactively
- Enable end-user self-service
- Get continuous visibility into the AWS account
- Gain peace of mind


Management AWS Account
AWS Control Tower
AWS Organization
AWS IAM Identity Center
AWS CloudFormation StackSets
AWS Service Catalog (Account Factory)
Security OU
Custom OU
AWS SSO Directory
Log Archive Account
Account Baseline
Centralized AWS CloudTrail and AWS Config logs
Audit Account
Account Baseline
AWS Config Aggregator
Security notifications
Provisioned Accounts
Account Baseline
Network Baseline


Management account
Consolidated billing
SSO
Controls
Account factory
Log Archive account
Centralized AWS CloudTrail and AWS Config logs
Other logs
Audit account
AWS Config Aggregator
Security Hub
GuardDuty
Inspector
Macie
Firewall Manager
Patch Manager
Chatbot
Notifications
Infrastructure OU
Network Hub
Shared Services
CI/CD
Backup
Workloads OUs
Prod
Stage
Dev
Appl
App2
Sandbox OU
Dev 1
Dev 2
Dev 3
Fixed spending limit
Disconnected from network
Suspended OU
CLOSE
Account closure
Block account

Account Structure in Landing Zone

Management Account:

- Consolidated billing and AWS SSO.
- Manages Control Tower Guardrails (security rules).
- Used to enroll new accounts via Account Factory.

Log Archive Account:

- Stores logs in S3 buckets.
- Used for centralized logging (security, access, application logs).

Audit Account:

- Central point for security services like Security Hub, GuardDuty, and Inspector.
- Receives delegated administrator access from Management account.

Infrastructure OU:

- Contains accounts for core services like networking, shared services, DevOps tools, and backups.

Workloads OU:

- Segregates accounts for different environments (Prod, Stage, Dev) or applications.

Sandbox OU:

- Provides personal AWS accounts for employees' testing and experiments.
- Can have budget limits and restrictions, disconnected from main network for security.

Suspended OU:

- Fully restricted (SCP: deny all).
- Used temporarily for accounts pending closure or budget breaches (e.g., move Sandbox accounts here).

Organizational structure

- Root
  - Development
    ou-wj
  - Infrastructure
    ou-wj
    - Backup
      541 .com
    - Network
      68 .com
    - devops
      91 .com
  - Production
    ou-wj
  - Quarantine
    ou-wj
  - Security
    ou-wj
    - Audit
      24 .com
    - Log Archive
      36 .com
  - Staging
    ou-wj

Create a control tower by referring the below video

https://youtu.be/e_AIUg2B-ac?si=Y6JqMs-lAlpdCksn

Step2 – create extra dev ,stage, prod accounts from the control tower console

aws | Services | Search [Alt+S] | Mumbai | Deepak Reddy

AWS Control Tower

- Dashboard
- Getting started
- Organization
- Account factory
- Controls library
  - Categories
  - All controls
- Users and access
- Shared accounts
- Landing zone settings
- Recent operations
- Activities
- AWS Marketplace for Control Tower

Organizational units (OUs) are entities created within your organization to group accounts for governance. You can add new OUs to your organization at any time.

Organization Info

Expand all | Group resources | Actions | Create resources

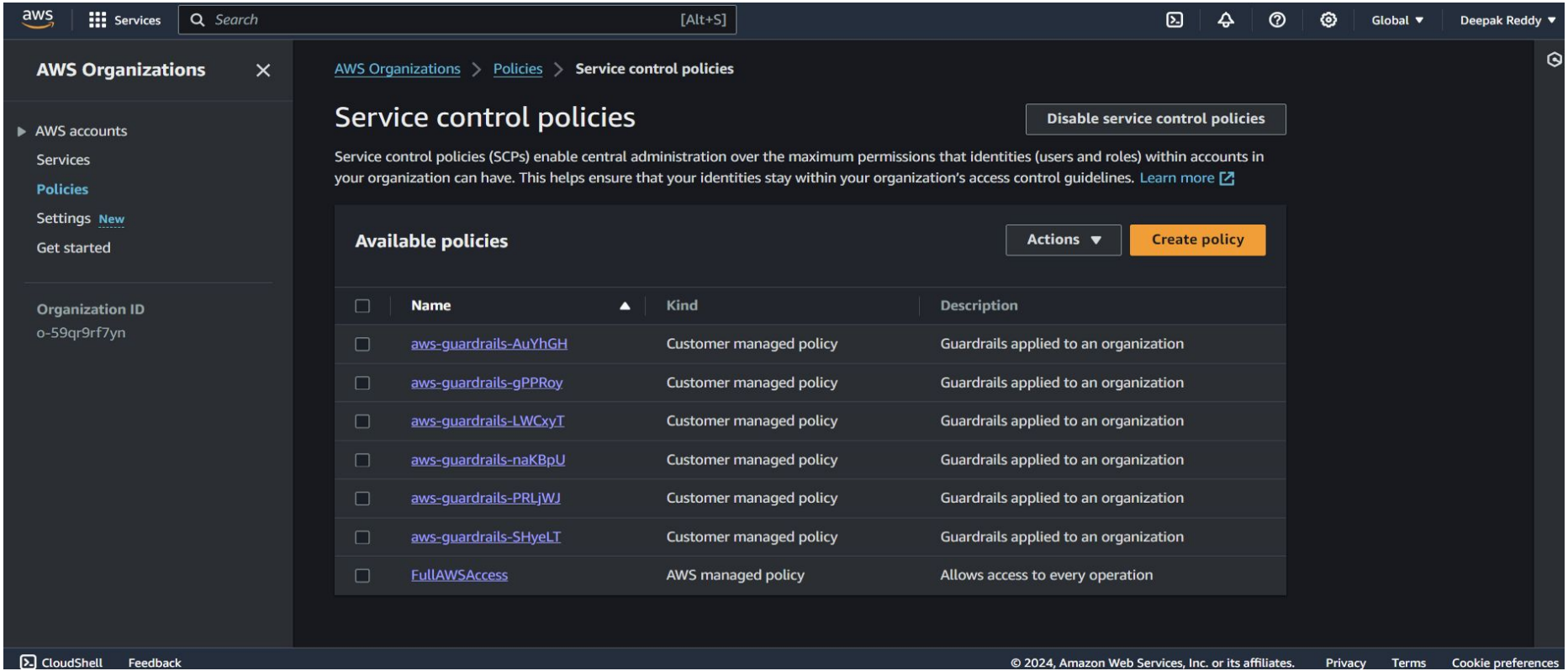
- Create organizational unit
- Create account

Find resources using properties

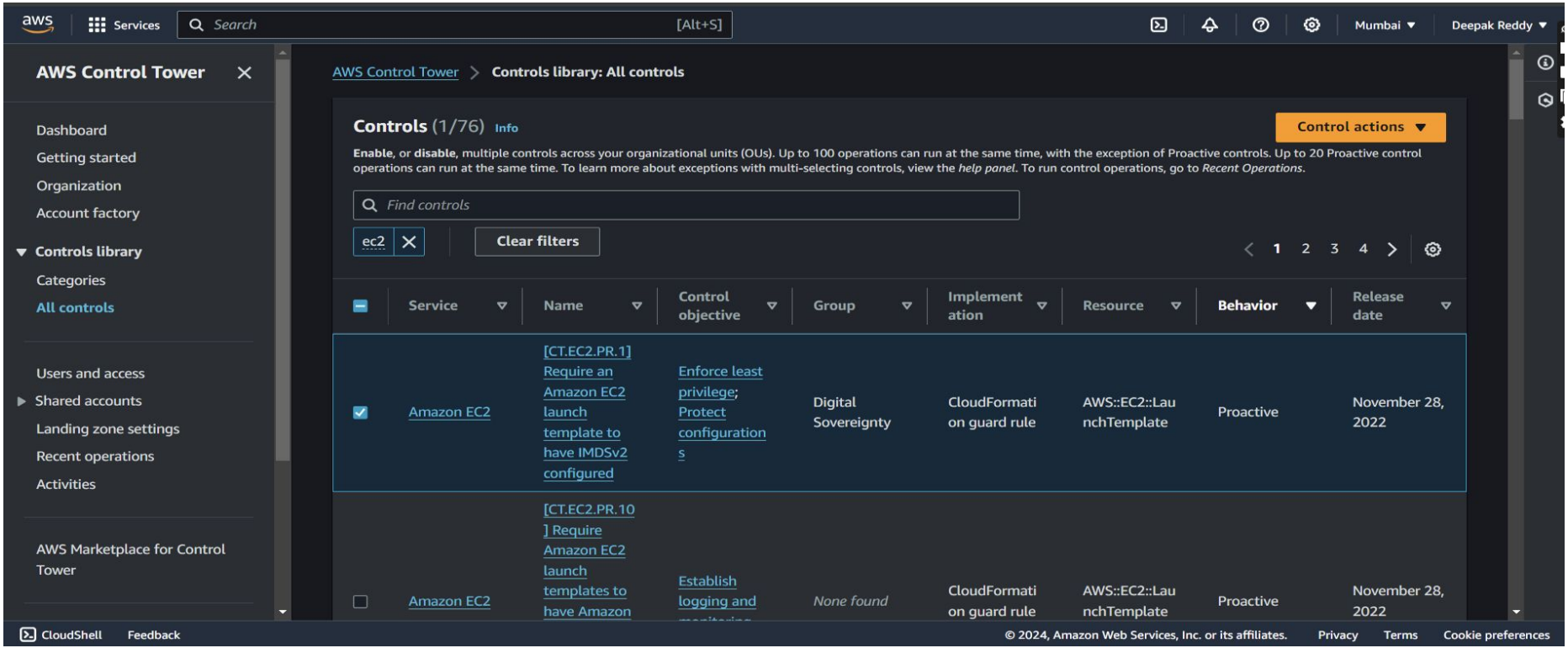
Resource type: View all resources

Name	Baseline state	ID	Email	Organizational units registered	Accounts enrolled	Blueprint product ID	Blueprint product version
Root	Succeeded	r-yv90	–	3 of 3	3 of 3	-	-
Sandbox	Succeeded	ou-yv90-p9390n4z	–	0 of 0	0 of 0	-	-
Security	Succeeded	ou-yv90-h0qlgajb	–	0 of 0	2 of 2	-	-
environments	Succeeded	ou-yv90-obz3hqha	–	0 of 0	0 of 0	-	-

Step 3 – go to aws organisations console and apply some SCP'S , play with scp's to get better understanding



Step4 – after applying policies , for additional compliance go back to again control tower console to apply proactive ,detective controlls



Step5 – Try to apply these most used SCP’S across multiple accounts

Most used SCP’S are –

https://aws.amazon.com/blogs/industries/best-practices-for-aws-organizations-service-control-policies-in-a-multi-account-environment/

Step6 –setup a single sign-on (SSO) using aws identity centre.

Search for identity centre in aws and setup the SSO

aws | Services | Search [Alt+S] | Mumbai | Deepak Reddy

IAM Identity Center

Managing instance
ssoins-6595f7cfc1754296

- Dashboard
- Users
- Groups
- Settings

Multi-account permissions
- AWS accounts
- Permission sets

Application assignments
- Applications

Related consoles
- CloudTrail Recommended
- AWS Organizations
- IAM

Attributes for access control
Configure this option to grant access to users based on specific characteristics. Learn more

Enable

Identity source | Authentication | Management | Tags

Identity source

Actions

Choose the directory where you want to manage your users and groups. Learn More

Identity source
Identity Center directory

Authentication method
Password

Provisioning method
Direct

AWS access portal URL
https://d-9f6707f33a.awsapps.com/start

Identity store ID
d-9f6707f33a

Issuer URL
https://identitycenter.amazonaws.com/ssoins-6595f7cfc1754296

Multiple account access at one page – SSO

aws

AWS Control Tower | MFA devices | Sign out

Introducing the Create shortcut button

We've added a Create shortcut button so you can generate secure shortcut links to AWS Management Console pages that you can bookmark or share with others that have AWS account access. Learn more

AWS access portal

Accounts | Applications

AWS accounts (3)

Create shortcut

Filter accounts by name, ID, or email address

- **Audit**
  905418118214 | [redacted]
- **Deepak Reddy**
  684371204192 | [redacted]
- **Log Archive**
  975049927996 | [redacted]

Using SCP and Permission Set Together

Scenario:

You have 3 developers, and you want them to:

- Access **only RDS and DynamoDB** in 5 AWS accounts.
- Prevent all users (even admins) from using EC2 across the organization.

Step 1: Create a Service Control Policy (SCP)

1. Go to the **AWS Organizations** console.

2. Click **Policies** → **Create policy**.

3. Create an SCP that denies EC2 access but allows everything else:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "*"
    }
  ]
}
```

   1. Name it: `DenyEC2`.

   2. Attach this SCP to the **OU** or **accounts** where you want to restrict EC2.

Step 2: Create a Permission Set in IAM Identity Center

1. Go to **IAM Identity Center → Permission sets**.
2. Click **Create permission set**.
3. Choose **Custom permission set**.
4. Attach:
   - `AmazonRDSFullAccess`
   - `AmazonDynamoDBFullAccess`
5. Name it: `DatabaseAdminAccess`.

✅ This gives access to **RDS and DynamoDB only**.

Step 3: Assign Users to AWS Accounts

Go to **IAM Identity Center → AWS accounts**.

Select the **5 AWS accounts**.

Click **Assign users or groups**.

Select the 3 developers.

Choose the `DatabaseAdminAccess` permission set.

✅ This grants RDS + DynamoDB access to those users in those accounts.

Step 4: Users Access AWS

Developers log in via the **IAM Identity Center portal**.

They choose an account and role (`DatabaseAdminAccess`).

They will see **only RDS and DynamoDB** available.

EC2 will be **completely blocked**, even if they try