METRODATA

AWS CONTROL TOWER HELP YOUR BUSINESS STAY AGILE & SECURE

Executive Summary

When moving to the cloud, cloud setup and governance can be complex and time consuming, slowing down the very innovation you're trying to speed up. AWS Control Tower provides the easiest way to **set up and govern a secure, multi-account AWS environment,** called a landing zone. It creates your landing zone using AWS Organizations, bringing ongoing account management and governance as well as implementation best practices based on AWS's experience working with thousands of customers as they move to the cloud.

Builders can provision new AWS accounts in a few clicks, while you have peace of mind knowing that **your accounts conform to company policies**. Extend governance into new or existing accounts, and gain visibility into their compliance status quickly. If you are building a new AWS environment, starting out on your journey to AWS, or starting a new cloud initiative, AWS Control Tower will help you get started quickly with built-in governance and best practices.

Top Value of Using AWS Control Tower

Quickly set up and configure a new AWS environment

Automate the setup of your multi-account AWS environment with just a few clicks. The setup employs blueprints that capture AWS best practices for configuring AWS security and management services to govern your environment. Blueprints are available to provide identity management, federate access to accounts, centralize logging, establish cross-account security audits, define workflows for provisioning accounts, and implement account baselines with network configurations.

Automate ongoing policy management

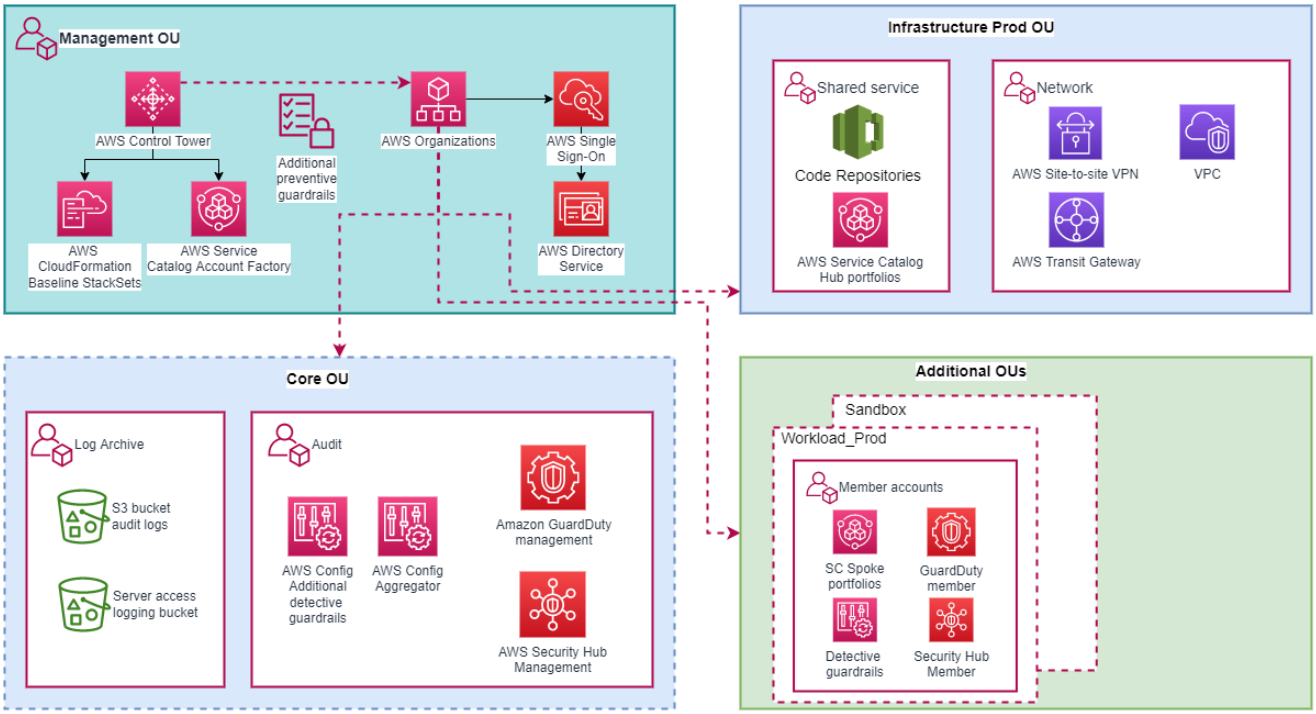
AWS Control Tower provides mandatory and strongly recommended high-level rules, called guardrails, that help enforce your policies using service control policies (SCPs), or detect policy violations using AWS Config rules. These rules remain in effect as you create new accounts or make changes to existing accounts, and AWS Control Tower provides a summary report of how each account conforms to your enabled policies. For example, you can enable data residency guardrails so that customer data, the personal data you upload to the AWS services under your AWS account, is not stored or processed outside a specific AWS Region or Regions.

View policy-level summaries of your AWS environment

AWS Control Tower provides an integrated dashboard so you can see a top-level summary of policies applied to your AWS environment. You can view details on the accounts provisioned, the guardrails enabled across your accounts, and account level status for compliance with your guardrails.

METRODATA

AWS Landing Zone High Level Design



Legend :

- **Management Account** : To apply guardrail to any OU level (best practices instead of on individual account)
- **Core and Custom OU** : by default consist of 2 Accounts Log Account and Audit Account (to centralize all account logs, and monitor config and detect guardrail/policy violation
- **Single Sign-On** : to get centralize account federation through single sign-on, optionally can be integrated with existing identity provider AD
- **AWS Service Catalog Account Factory** : to automate account provisioning and apply account baseline and guardrails
- **Log Archive** : to centralize log management for all created account
- **Guardrails** : AWS Config for detective control after account is up and running, preventive control is using service control policies while account creation
- **Production Infrastructure OU** : to host additional account for shared services account and netwok account
- **GuardDuty Management** : to configure member account for guardduty and security hub
- **Additional OU** : Created to host member account for Sandbox Testing App and for Production App

AWS Services/Building Stack	Technical Features
- AWS Organizations - Service Control Policies (SCPs) In AWS Organizations - AWS Organizational Units (Ous) - AWS Config Rules - AWS CloudTrail - Amazon S3 - Amazon SNS - AWS CloudFormation StackSets - AWS Service Catalog - AWS Single Sign-On (SSO)	- Account Provisioning via **AWS Service Catalog Account Factory** - Standardized Account Security Baseline via **Guardrails** - Centralized Log Storage for **AWS CloudTrail** or **AWS Config** services - Centralized multi-account account authentication via **AWS Single Sign-On (AWS SSO)** with an integrated directory - Auditor Support and Access Capabilities - Dashboard interface to view the status and notification events of AWS Control Tower-managed components and foundational services from the **AWS Management Console**

Monthly Billing Estimation for AWS Landing Zone: ***300 to 500 USD****

**Real billing may be higher based on the sizing and client's requirement*

***exclude tax & any Metrodata professional services, subject to be discussed*

****exclude workload compute power & software stack*

As you trusted partner, Metrodata are able to assist you in your cloud transformation, by providing correlate professional service as stated below to you organization:

- AWS Control Tower Design and Discovery Workshop with your organization
- Level Set on your Project Goals and Objectives as part of this project
- Review the AWS Control Tower Pre-Requisities required for deployment
- Define the AWS Control Tower Use Cases required
- Create an AWS Control Tower design based on requirements from the various design workshops which will become the playbook for the AWS platform implementation
- Establish a new AWS Control Tower account structure and configuration to establish security baselines across all AWS Clients Accounts
- Implement an AWS Landing Zone Model to standardize AWS accounts and create a Multi-Account Vending Model using Infrastructure as Code with AWS Cloudformation (If possible)
- Create and configure the base AWS Landing Zone Infrastructure
- Configure AWS Networking components including VPC definitions, subnets, security groups, transit gateways, and assist Client with establishing connectivity for AWS
- Configure the appropriate storage services based on requirements from the design workshops
- Configure Identity Management Integration with Client's SSO Platform
- Implement a tagging strategy, as designed for billing and administrative functionality
- Implement baseline security controls, such as logging and auditing configuration with AWS Config
- Configure up to (2) AWS SCP Policies for AWS Platform Governance
- Develop As Built Documentation for Amazon Control Tower Landing Zone Deployment

Partner Profile

PT Metrodata Electronics TBK, has been Amazon Web Services (AWS) Partner since 2016, currently on Advance Consulting Partner (highest for Indonesia local partner). Since 2021, we are the very first Strategic Collaboration Agreement (SCA) with AWS in Indonesia, commited to provide comprehensive and innovative cloud solution offering for all of the organizations in Indonesia Market. Equipped with a complete set of team, adopting CCOE (cloud center of excellence) team, consist of Product Specialist, Solution Architect, Technical Delivery, cloud managed service & a set of Subject Matter Expert (SME) in terms of application, database, networks, devops, big data and analytics.

For questions or enquiries please contact:

MIIProduct18@metrodata.co.id

aws partner network

Advanced Consulting Partner

Solution Provider

Public Sector Solution Provider

Amazon EC2 for Microsoft Windows Server

Immersion Day Partner

Written By :
RM Dana Suryo Saputro
AWS Certified Solution Architect
PT Metrodata Electronics Tbk.,