Automat-IT AWS Landing Zone Solution

AWS best practice, tailored to your organization

AWS Landing Zone is a fully-automated enterprise-scale, governance and security solution for multi-account environments. Once implemented, its automated processes save you time, lower costs and reduce complexity. However, out of the box, the solution requires a lot of configuration to meet your specific requirements, which can be time consuming and require a deep understanding of AWS services.

Reduce implementation from weeks to days

Deployed by startups, mature SaaS companies and enterprise organizations alike, Automat-IT's AWS Landing Zone uses the following cloud-native services to provide you with a pre-configured solution.

Control Tower | AWS Config | CloudTrail | GuardDuty | Service Control Policies |

Security Hub | Inspector | Service Catalog

In order to reduce time to implementation from weeks to just days, we have built a baseline which can be easily modified to meet the requirements of your internal governance and other specific compliance issues.

Your 3 steps to Landing Zone success

1. Our delivery team will have a brief session with you to understand the specific parameters of your cloud environments, including user accounts and security requirements.
2. Within 3 days, we will have configured those parameters into your tailored AWS Landing Zone solution.
3. We will then deploy your tailored Landing Zone solution.

Benefits

- Have your Landing Zone solution up and running within days, not weeks.
- Easily modify the solution to meet your business needs.
- Save time, lower costs and reduce complexity.

Solution Scope

AWS Organization & Accounts Structure

The solution comes out of the box with three predefined custom organization unit profiles - Networking, Non-Production and Production - each using a custom set of guardrails and alerts.

Automated Delivery Pipeline

A serverless delivery pipeline sets templates and service control policies, providing change management procedures and continuous delivery.

Identity and Access Management (IAM)

Default configuration deploys federated Single Sign-On (SSO) with external 3rd party SAML IdP (GSuite, AzureAD, OneLogin, Okta, etc.). The solution implements your organization's IAM policies, while automation also deploys service control policies to govern access guardrails.

Logging and Monitoring

Using a dedicated account for centralized logging, all findings and alerts are consolidated to the AWS Security Hub, providing a single pane of glass for all events and notifications in each AWS region.

Infrastructure Security

A set of network blue-print topologies leverages AWS resource sharing capabilities, giving you full control over your organization's network, without limiting the end-users.

Data Protection

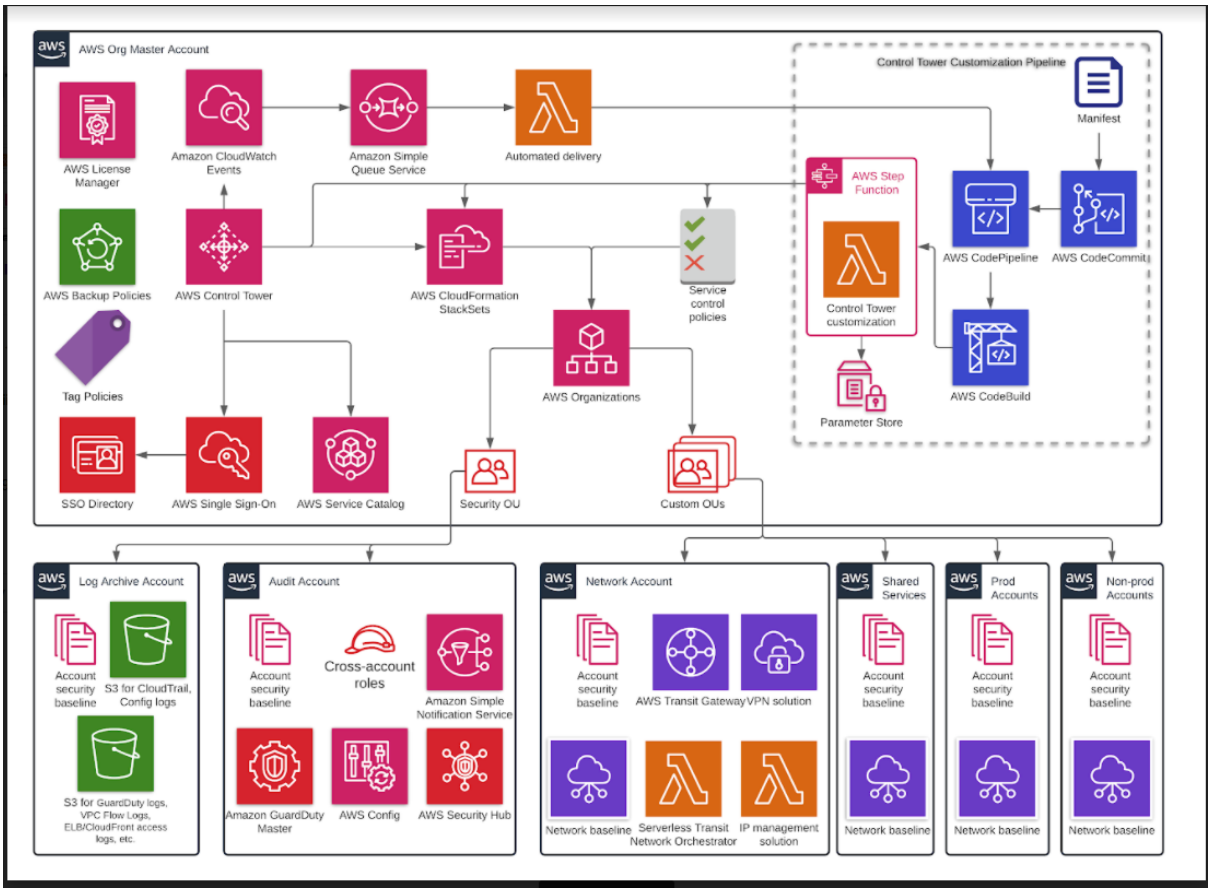
An organization unit-based data protection policy prevents creation of public S3 buckets, enforces EBS and RDS encryption, deploys detective guardrails for KMS key deletion, and instigates organization-wide deployment of backup strategy using AWS Backup.

Incident Response

Incident response integration is provided with an external workflow/ticketing system, cloud-native investigation tools and automated IOC (Indicators of Compromise) detection and response in code.

Cost Governance and Control

Detective guardrails are deployed for unused EIP and EBS volumes, enforcement of resources tags, custom settings of AWS account limits, setup of budget alerts, instance scheduling (stop/start) based on tags, and automatic moving of AWS accounts that exceed limits to a blocking OU.


AWS Org Master Account
AWS License Manager
Amazon CloudWatch Events
Amazon Simple Queue Service
Automated delivery
Control Tower Customization Pipeline
Manifest
AWS Step Function
AWS CodePipeline
AWS CodeCommit
AWS Backup Policies
AWS Control Tower
AWS CloudFormation StackSets
Service control policies
Control Tower customization
Tag Policies
AWS Organizations
AWS CodeBuild
Parameter Store
SSO Directory
AWS Single Sign-On
AWS Service Catalog
Security OU
Custom OUs
Log Archive Account
Account security baseline
S3 for CloudTrail, Config logs
S3 for GuardDuty logs, VPC Flow Logs, ELB/CloudFront access logs, etc.
Audit Account
Account security baseline
Cross-account roles
Amazon Simple Notification Service
Amazon GuardDuty Master
AWS Config
AWS Security Hub
Network Account
Account security baseline
AWS Transit Gateway
VPN solution
Network baseline
Serverless Transit Network Orchestrator
IP management solution
Shared Services
Account security baseline
Network baseline
Prod Accounts
Account security baseline
Network baseline
Non-prod Accounts
Account security baseline
Network baseline