AWS Multi-Account Secure Landing Zone Implementation Guide

1. Introduction

This document provides a step-by-step guide for implementing a secure AWS multi-account landing zone using AWS Organizations. It covers organizational unit (OU) design, Service Control Policy (SCP) deployment, IAM cross-account role configuration, and centralized logging and monitoring for compliance and incident response.

2. Architecture Design

The landing zone is designed to separate environments into organizational units for better governance. Accounts are created for Management, Security, Log Archiving, and Workloads (Development, Testing, Production). AWS Control Tower may be optionally used for automated setup.

Key Accounts:

- Management Account: Governance, SCP administration, consolidated billing.
- Security Account: Centralized security services (GuardDuty, Security Hub, IAM Access Analyzer).
- Log Archive Account: Aggregated CloudTrail, AWS Config, and access logs.
- Workload Accounts: Environment-specific accounts for workloads (Dev, Test, Prod).

3. Service Control Policies (SCPs)

Service Control Policies enforce organizational guardrails across all accounts. Examples include:

- Denying the ability to disable CloudTrail.
- Preventing creation of public S3 buckets.
- Restricting IAM privilege escalation (wildcard * permissions).

4. IAM Configuration

IAM Identity Center is integrated with a corporate IdP (e.g., Okta, Azure AD) for Single Sign-On. Cross-account IAM roles are configured with least-privilege access for Security and DevOps teams.

5. Centralized Logging & Monitoring

Organization-wide CloudTrail and AWS Config are enabled, with logs stored in the Log Archive Account. AWS GuardDuty and Security Hub are enabled across all accounts, with findings aggregated in the Security Account.

6. Compliance Alignment

The implementation aligns with the CIS AWS Foundations Benchmark and NIST 800-53 controls for cloud governance. Policies are mapped to specific control objectives in a separate compliance document.

7. Lessons Learned & Recommendations

Testing SCPs in sandbox accounts prevents disruptions in production environments. Automating new account provisioning with AWS Control Tower significantly reduces manual configuration effort.