# High-Level Design: AWS Control Tower, Landing Zone, Organizations, OU Structure, SSO (AWS IAM Identity Center) and Entra ID

## 1. Purpose

This document provides a high-level architecture and design for implementing an enterprise-grade AWS landing zone using **AWS Control Tower** and **AWS Organizations**, with a recommended Organizational Unit (OU) structure, account strategy, SSO integration via **AWS IAM Identity Center** (formerly AWS SSO) and **Microsoft Entra ID (Azure AD)**. It is intended to guide cloud architects, platform engineers, security teams and stakeholders through design decisions, components, governance controls and operational considerations.

## 2. Audience

* Cloud/Platform Architects
* Security & Compliance teams
* Infrastructure / DevOps Engineers
* IT Identity & Access Management teams
* Project/Product owners responsible for cloud adoption

## 3. Introduction

An enterprise landing zone provides the foundational multi-account AWS environment, implementing security, compliance, baseline networking, account vending and identity integration so teams can onboard workloads safely and consistently. AWS Control Tower accelerates landing zone deployment and brings guardrails, account factory and centralized logging. This design also integrates corporate identity (Entra ID) for centralized authentication and user lifecycle management.

## 4. Architecture & Design Overview

### 4.1. High-level components

* **AWS Organizations** — root for account management and policy enforcement.
* **AWS Control Tower** — automated landing zone deployment, Account Factory, baseline guardrails (mandatory and strongly recommended).
* **Organizational Units (OUs)** — logical grouping of accounts (Core, Security, Shared Services, Sandbox, Non-Prod, Prod, etc.).
* **AWS IAM Identity Center (Identity Center)** — central SSO for AWS console and roles.
* **Microsoft Entra ID (Azure AD)** — corporate IdP integrated with Identity Center using SAML and SCIM for provisioning.
* **Logging & Security** — centralized CloudTrail, AWS Config, Security Hub, GuardDuty, Amazon Detective.
* **Networking** — Shared Services VPCs, Transit Gateway or AWS Network Manager, account-level VPCs with Transit connectivity.
* **Account Vending** — Control Tower Account Factory / Account Factory for Organizations (or custom automation via Landing Zone pipeline).
* **Baseline Tooling** — AWS Config rules, Guardrails (SCPs), IAM baseline
* **Backup & Recovery** — AWS Backup, cross-region replication, AMI & snapshot lifecycle

### 4.2. Logical architecture

* **Management/Shared Services (Management)**: Root and management accounts hosted under a Management OU — runs Control Tower, centralized logs, security tooling and account factory.
* **Security OU**: Dedicated accounts for security services (Security, SIEM, Threat Detection).
* **Shared Services OU**: Networking, Directory, DevOps tooling, Bastion, NAT, DNS (Route53 private hosted zones) and CI/CD systems.
* **Workload OUs**: Prod, Non-Prod, Sandbox. Each OU contains multiple accounts (per team, environment, application lifecycle) to isolate blast radius, billings and permissions.

### 4.3. Identity integration (Entra ID → Identity Center)

* Configure **AWS IAM Identity Center** as the AWS-managed SSO solution.
* Connect Identity Center to **Entra ID (Azure AD)** using **SAML 2.0** for federation (single sign-on).
* Optional: Configure **SCIM** provisioning from Entra ID to Identity Center where supported, enabling automated user/group provisioning and de-provisioning.
* Map Entra ID groups to IAM Identity Center permission sets (which map to IAM roles in target AWS accounts).
* Use **Just-in-Time** role assignments for least privilege and role-based access.

### 4.4. Guardrails & Governance

* Use Control Tower mandatory guardrails for identity, logging and account baseline.
* Implement additional **Service Control Policies (SCPs)** at OU level to restrict risky services or enforce encryption.
* Apply AWS Config & Conformance Packs for continuous compliance.
* Use AWS CloudFormation / Terraform to codify guardrails, baseline resources and Account Factory templates.

## 5. List of Components & Services (by AWS region)

Note: The Control Tower management account and several security services are recommended to be hosted in a **primary region** (commonly us-east-1) to minimize service availability issues. Many services (CloudTrail, Config Aggregator) support multi-region aggregation.

Common services used across regions (select the regions you operate in): - **AWS Organizations** (global) - **AWS Control Tower** (regional endpoint per Control Tower management region) - **AWS IAM Identity Center** (global/region-scoped depending on setup) - **AWS CloudTrail** (multi-region trails) - **AWS Config** (multi-account, multi-region aggregator) - **Amazon S3** (central logging buckets; versioning + MFA delete recommended) - **Amazon CloudWatch** (metrics/logs) - **AWS Backup** (cross-region backup) - **AWS Transit Gateway** / **VPC Peering** (network transit) - **AWS Directory Service** (if required) or put a managed AD in Shared Services - **GuardDuty, Security Hub, Amazon Detective** (security monitoring) - **Route 53** (private hosted zones, resolver endpoints)

Example region-specific deployment suggestions: - Primary management region: us-east-1 (Control Tower, CloudTrail aggregator, Config aggregator) - Secondary region(s) for fault tolerance and data residency: eu-west-1, ap-south-1 (as applicable)

## 6. Organizational Unit (OU) & Account Structure (recommended)

Root  
├─ Audit-Ou / Management-Ou  
│ ├─ Management Account (Control Tower)  
│ ├─ Audit Account (centralized logging & CloudTrail)  
│ └─ Security Account (Security Hub, GuardDuty, SIEM forwarder)  
├─ Shared-Services-Ou  
│ └─ Networking Account (Transit GW, NAT, DNS)  
├─ Platform-Ou  
│ └─ DevOps/Tooling Account (CI/CD, Artifact repos)  
├─ Sandbox-Ou  
│ └─ Sandbox accounts (one per team)  
├─ NonProd-Ou  
│ └─ Non-prod workload accounts  
└─ Prod-Ou  
 └─ Prod workload accounts

### OU design considerations

* Keep at least one **audit** account (read-only) for forensic and logging analysis.
* Use separate **security** account(s) to host threat detection and incident response tools.
* Limit the number of accounts directly under Root; use OUs for scoping SCPs and guardrails.
* Enforce naming, tagging and billing tags via IAM policies and guardrails.

## 7. Account Baseline & Guardrails (examples)

* **Mandatory guardrails**: Enforce CloudTrail, prevent disabling of CloudTrail, require encryption at rest, enforce MFA for console users.
* **SCP examples**:
  + Deny actions that modify IAM permissions outside of the security account.
  + Deny creation of public S3 buckets unless explicitly allowed.
  + Restrict management of Key Management Service (KMS) keys to security principals.

## 8. Networking & Connectivity

* **Centralized Transit Architecture**: Deploy a Transit Gateway in the Networking account to centralize connectivity between account VPCs and on-prem/VPN/Direct Connect.
* **Shared Services VPC**: Hosts shared services such as DNS, AD, Bastion Hosts and connectivity appliances.
* **Security Controls**: Network ACLs, segmentation using VPC subnet design (public/private/management), AWS Network Firewall or third-party appliances in Shared Services.

## 9. Logging, Monitoring & Observability

* **CloudTrail**: Enable multi-region CloudTrail and deliver logs to central S3 in the Audit account. Enable CloudTrail insights for anomalous API activity.
* **AWS Config**: Enable aggregator to collect compliance across accounts and regions.
* **Security Hub**: Centralize findings from GuardDuty, Inspector, and external scanners.
* **CloudWatch**: Central metrics and cross-account dashboards (or metrics forwarding to a central account).
* **SIEM Integration**: Forward CloudTrail logs and GuardDuty findings to SIEM/tooling in Security/Ops account.

## 10. Backup & Restore / Disaster Recovery

* Use **AWS Backup** to configure backup plans for EBS, RDS, DynamoDB and S3 (where supported).
* Define **RPO/RTO** per workload and implement cross-region replication (CRR for S3, cross-region snapshots for RDS).
* Regularly test restores from backups in a sandbox account.
* Maintain AMI catalog and snapshot lifecycle policies tied to tagging and retention rules.

## 11. Security & Compliance

* **Identity & Access**: Enforce least privilege with Identity Center permission sets and attribute-based access where possible.
* **Secrets Management**: Centralize secrets in AWS Secrets Manager or AWS Systems Manager Parameter Store.
* **Encryption**: Default encrypt all persistent storage (S3, EBS, RDS) using KMS CMKs managed centrally. Control KMS via key policies and grants.
* **Vulnerability Management**: Integrate Amazon Inspector (or external scanners) with Security Hub.
* **Patch & Baseline Management**: Use Systems Manager Patch Manager and Automation documents.

## 12. Integration with Entra ID (detailed)

1. In **Entra ID** create an Enterprise Application for AWS IAM Identity Center using **SAML**.
2. Configure **Assertion Attributes** (NameID, SessionDuration) and map Entra AD groups to SAML attributes for role mapping.
3. In **AWS IAM Identity Center**, configure external identity provider and exchange metadata with Entra ID.
4. Optionally enable **SCIM** provisioning from Entra ID to Identity Center to sync users/groups automatically.
5. Test group-to-permission-set mappings and verify role assumption flows.

## 13. Operational Model & Runbook highlights

* **Account provisioning**: Use Control Tower Account Factory (or automated pipeline) to create accounts with tags, baseline IAM roles, network attachments and logging.
* **Onboarding process**: Document steps for team onboarding, SOC escalation, incident response and drift remediation.
* **Cost Management**: Use AWS Cost & Usage reports centrally; enforce tagging and budgets per account.

## 14. Automation & IaC

* Prefer Infrastructure-as-Code (CloudFormation/Terraform) for reproducibility: Account vending templates, SCPs, Config rules and baseline resources.
* Store IaC in a central Git repo with CI/CD pipeline in Platform/DevOps account.

## 15. Screenshots & Diagrams (placeholders)

Insert architecture diagram here: *High-level multi-account diagram showing Root → OUs → Accounts (Management, Audit, Security, Shared Services, Prod/NonProd/Sandbox) and connectivity via Transit Gateway; arrows for centralized logging & Identity Center integration with Entra ID.*

Insert sample Control Tower landing page and Account Factory screenshots here (mock or real).  
Insert Identity Center configuration screenshot (Permission sets mapping) and Entra ID Enterprise App mapping screenshot here.

(When producing the final Word/PDF deliverable, include realistic console mockups or sanitized screenshots for the above.)

## 16. Common Services (summary)

* Identity: Entra ID (IdP), AWS IAM Identity Center
* Logging & Audit: CloudTrail, Config, CloudWatch, S3 centralized logs
* Security: GuardDuty, Security Hub, Inspector, Detective
* Networking: Transit Gateway, VPC, Direct Connect / VPN
* Storage & Backup: S3, AWS Backup, EBS snapshots, RDS snapshots
* Automation: CloudFormation / Terraform, Systems Manager

## 17. Recommendations & Best Practices

* Host Control Tower and primary security tooling in a stable, low-latency primary region (e.g., us-east-1).
* Keep the number of root-level accounts minimal and use OUs for policy application.
* Automate user provisioning via Entra ID SCIM where feasible to improve security posture and reduce manual tasks.
* Test backup and restore quarterly and rehearse runbooks for account compromise and data loss.
* Use least privilege permission sets and periodic access reviews.

## 18. Appendix

* **Sample tags**: Project, Environment, Owner, CostCenter, Compliance.
* **Sample naming convention**: acct-<org>-<env>-<team>-<purpose>.
* **Onboarding checklist**: Account creation, IAM baseline, network peering, logging enabled, patch baseline, cost tags.

*Document prepared as a high-level design. For a deployment-ready implementation we can add: detailed architecture diagrams, Terraform/CloudFormation snippets for Account Factory, sample SCPs, sample IAM Identity Center permission sets and a Word/PDF output with embedded mock screenshots.*