INDEPENDENT HANDS-ON PROJECT

IAM Governance and Cross-Account Access

Permission boundaries, explicit trust, MFA and access analysis

Portfolio track	Independent Hands-on Engineering
Evidence level	Terraform fmt, init and validate passed
Author	Saurabh Dindokar

Evidence boundary: This is a public-safe personal implementation lab. It is not client production work, and no live deployment is claimed.

Overview

A Terraform IAM governance lab demonstrating a permission boundary, cross-account read-only role with MFA and an external ID, one-hour sessions, IAM Access Analyzer, a strict password policy and CloudTrail log-role preparation.

Engineering Problem

Cross-account access is often implemented with overly broad trust or policies. The lab shows how trust conditions, maximum-permission boundaries, time-limited sessions and external-access analysis combine without creating long-lived access keys.

Architecture

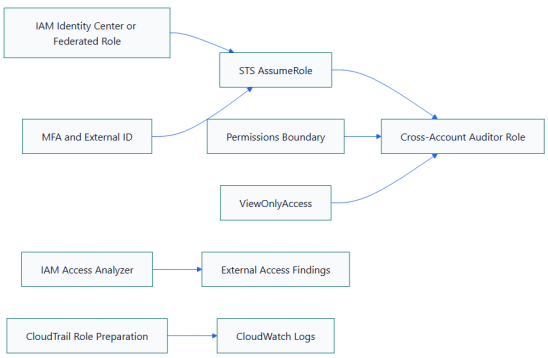

Figure 1. IAM Governance and Cross-Account Access architecture

What I Implemented

- Created a permission boundary that defines the maximum approved service and region scope.
- Defined explicit trusted principals plus MFA and external-ID conditions for STS role assumption.
- Limited role sessions to one hour and attached view-only permissions inside the boundary.
- Enabled account-level IAM Access Analyzer for external-access findings.
- Added strict account password settings and CloudTrail-to-CloudWatch role preparation.

Important Technical Decisions

- IAM Identity Center is preferred for workforce access; the lab creates no IAM users or access keys.
- A permission boundary limits maximum permissions but grants nothing by itself.
- The sample external ID is not treated as a secret and must be replaced at runtime.
- SCPs and identity policies solve different governance problems.

Security Controls

- MFA, external ID and named principals restrict role trust.
- One-hour sessions reduce credential lifetime.
- Access Analyzer surfaces resource access from outside the account.

Reliability and Operations

- Policy Simulator and CloudTrail review are part of the verification approach.
- Explicit boundaries reduce unintended permission expansion during delegated administration.
- Regional deny behavior includes exceptions for global services.

Cost and Cleanup Guardrails

- IAM controls have limited direct cost, while CloudWatch Logs storage depends on retention and ingestion.
- The design uses a 90-day log-group retention value instead of unlimited storage.
- Access Analyzer scope and CloudTrail destinations should be reviewed before broad rollout.

Validation Evidence

The following local checks passed on 2026-08-13:

```
terraform fmt -check -recursive
terraform init -backend=false
terraform validate
```

Scope boundary: Format, initialization and validation passed on 2026-08-13. No cross-account role assumption, Policy Simulator test, Access Analyzer finding review or complete CloudTrail trail deployment is claimed.

Delivery and Verification Runbook

- 1. Define approved principals and regions
- 2. Apply permission boundary
- 3. Require MFA and external ID

- 4. Assume one-hour role
- 5. Test allowed and denied actions
- 6. Review CloudTrail and Access Analyzer findings
- 7. Revoke or tighten unexpected access

Technology Stack

Terraform | AWS IAM | AWS STS | Permission Boundaries | MFA | IAM Access Analyzer | CloudTrail | CloudWatch Logs

Key Learnings

- Infrastructure evidence must distinguish code validation, plan review and live deployment.
- Security, reliability, cost and cleanup decisions should be documented before apply.
- A useful platform lab includes verification and rollback thinking, not only resource declarations.