Service Name

AWS Control Tower

Service Overview

AWS Control Tower offers a straightforward way to set up and govern an AWS multi-account environment following prescriptive best practices. It orchestrates capabilities of several AWS services including AWS Organizations, AWS Service Catalog, and AWS IAM Identity Center to build a secure, compliant landing zone in less than an hour. The service helps organizations maintain compliance and security standards across multiple accounts while providing account factory capabilities for rapid account provisioning. It implements preventive, detective, and proactive controls to ensure ongoing governance and prevent drift from best practices.

Key Use Cases

- Multi-account environment setup and governance for enterprises requiring standardized security and compliance controls
- Account Factory provisioning to enable distributed teams to quickly create new AWS accounts using configurable templates
- Regulatory compliance management through automated implementation of security guardrails and policy enforcement across organizational units

Features

- **Landing Zone**: Well-architected multi-account environment based on security and compliance best practices that scales to enterprise needs
- **Controls (Guardrails)**: High-level rules providing ongoing governance with preventive, detective, and proactive control types that can be mandatory, strongly recommended, or elective
- **Account Factory**: Configurable account template that standardizes provisioning of new accounts with pre-approved configurations and automated workflows
- **Dashboard**: Provides continuous oversight allowing administrators to see provisioned accounts, enabled controls, and noncompliant resources organized by accounts and OUs
- **Control Catalog**: Over 750 managed controls with support for various compliance frameworks and configurable exemptions for specific resources or IAM principals
- **Automated Account Enrollment**: Automatically enrolls accounts and applies appropriate baselines and controls when accounts are moved between organizational units

Value Proposition

AWS Control Tower provides the easiest way to set up and govern a secure, compliant multi-account AWS environment based on best practices established through thousands of enterprise engagements. It offers automated governance at scale, eliminating manual configuration overhead while ensuring consistent security posture:

- The service provides built-in Account Factory for rapid account provisioning, comprehensive control catalog with over 750 managed controls, and seamless integration with existing AWS Organizations structures
- It reduces operational complexity through centralized management while maintaining flexibility for customization and extensibility across different organizational requirements

Service Integration

AWS Control Tower deeply integrates with AWS Organizations for multi-account management and centralized billing, AWS Service Catalog for Account Factory provisioning workflows, and AWS IAM Identity Center for single sign-on capabilities. Core integrations include AWS Config for configuration governance and compliance monitoring, AWS CloudTrail for activity logging and audit trails, AWS CloudFormation StackSets for resource deployment across accounts, and AWS Security Hub for centralized security findings. Additional integrations encompass AWS Backup for data protection, AWS Lambda for automation functions, Amazon S3 for logging storage, Amazon SNS for notifications, and AWS Step Functions for orchestrating complex workflows.

Onboarding and Offboarding

Customers begin by selecting their home region and completing automated pre-launch checks for their management account. Setup involves choosing between full landing zone deployment or controls-dedicated experience for existing multi-account environments:

- The quick start process creates audit and log archive accounts, establishes organizational units, and deploys initial controls in approximately 30 minutes
- Prerequisites include sufficient AWS service limits, active AWS support plan, and proper IAM permissions
- For existing organizations, AWS Control Tower creates parallel structures without disrupting current OUs and accounts, allowing immediate use alongside existing AWS Organizations environments

Getting Started Guide:
https://docs.aws.amazon.com/controltower/latest/userguide/getting-started-with-control-tower.html

Data Removal

Offboarding requires careful decommissioning of AWS Control Tower resources while preserving account structures and data. Process involves disabling enabled controls, unregistering organizational units, and removing landing zone components. Data retention follows standard AWS service policies for integrated services like CloudTrail, Config, and S3. Organizations must manually delete specific resources like S3 buckets containing logs and CloudFormation stacks to ensure complete removal.

Backup/Restore and Disaster Recovery

AWS Control Tower integrates with AWS Backup to provide automated, centralized backup capabilities across the landing zone environment. The service offers prescriptive backup plans with predefined retention policies, backup frequencies, and time windows applied to organizational units. Backup functionality requires setup of dedicated backup administrator and central backup accounts with multi-region KMS keys for encryption. Integration ensures consistent data protection standards across all governed member accounts.

Backup Capabilities

AWS Control Tower supports comprehensive backup integration through AWS Backup service with prescriptive backup plans at the landing zone level. Backup capabilities include automated resource tagging for backup inclusion, centralized backup vault creation, and four types of backup plans with configurable retention periods. The service enables consistent backup policies across organizational units with automatic inclusion for new accounts provisioned under registered OUs.

Disaster Recovery

Disaster recovery is supported through underlying AWS service capabilities rather than native Control Tower features. Organizations can implement backup and restore, pilot light, warm standby, or multi-site active/active strategies using integrated services. AWS Control Tower's multi-region governance capabilities support disaster recovery architectures by enabling consistent security controls and account structures across regions for resilience planning.

Recovery Objectives

AWS Control Tower assists with RPO and RTO objectives through its integrated backup capabilities and multi-region governance structure. Automated backup plans help achieve specific recovery point objectives, while consistent account structures and security controls across regions support faster recovery time objectives. The service's centralized governance model enables standardized disaster recovery implementations across the multi-account environment.

Service Constraints

Service Quotas: https://docs.aws.amazon.com/controltower/latest/userguide/limits.html

FAQ: https://aws.amazon.com/controltower/faqs/

Technical Requirements

Service Documentation: https://docs.aws.amazon.com/controltower/latest/userguide/what-is-control-tower.html

User Guide: https://docs.aws.amazon.com/controltower/latest/userguide/getting-started-with-control-tower.html

API Reference: https://docs.aws.amazon.com/controltower/latest/APIReference/Welcome.html

Pricing Overview

Please see the AWS UK G Cloud 15 Pricing Document accompanying this service in the Digital Marketplace.

Public Pricing: https://aws.amazon.com/controltower/pricing/

Cost Optimization

AWS Control Tower itself incurs no additional charges as it's a free orchestration service. Cost optimization focuses on managing underlying AWS services usage including AWS Config configuration items, CloudTrail data events, and S3 storage for logs:

- Organizations can optimize costs by carefully selecting detective controls to avoid duplication, managing ephemeral workloads that generate excessive Config items, and leveraging organizational-level CloudTrail trails to prevent duplicate logging charges
- Proper tagging strategies enable accurate cost attribution across accounts and organizational units

Savings Considerations

Primary cost savings come from avoiding duplicate AWS service deployments through centralized governance and shared security infrastructure. Organizations benefit from consolidated billing across multiple accounts, optimized CloudTrail trail configurations at organization level, and standardized resource provisioning that prevents over-provisioning:

- The Account Factory reduces operational overhead costs by automating account creation and baseline application

- Centralized backup policies and security controls eliminate redundant implementations across accounts, while consistent governance reduces compliance audit costs and administrative overhead