Service Name

AWS Config

Service Overview

AWS Config is a fully managed service that provides a detailed view of AWS resource configurations in an account, including how resources are related to one another and their historical configurations. It enables organizations to assess, audit, and evaluate the configurations of AWS resources by continuously monitoring and recording configuration changes as configuration items. AWS Config helps maintain visibility into resource relationships, tracks configuration drift, ensures compliance through rules and conformance packs, and provides centralized governance across multiple accounts and regions through aggregators.

Key Use Cases

- Compliance monitoring: Continuously monitor resource configurations against industry standards, security best practices, and organizational policies using AWS Config rules and conformance packs
- Configuration management: Track and audit configuration changes across AWS resources to maintain visibility, troubleshoot issues, and understand resource relationships
- Security governance: Assess security postures by evaluating resource configurations against desired states, identifying vulnerabilities, and enabling automated remediation of non-compliant resources

Features

- **Configuration Recording**: Records configuration changes for supported AWS resources as configuration items with point-in-time snapshots
- **AWS Config Rules**: Evaluates resource compliance against desired configurations using managed or custom rules with automatic evaluation
- **Conformance Packs**: Bundles multiple rules and remediation actions for compliance against industry standards and best practices
- **Multi-Account Aggregation**: Aggregates configuration and compliance data across multiple AWS accounts, regions, and organizations
- **Advanced Query**: Provides SQL-like queries to search and analyze current configuration state across resources
- **Automated Remediation**: Automatically fixes non-compliant resources using AWS Systems Manager documents or Lambda functions
- **Resource Relationships**: Maps and tracks relationships between AWS resources to understand dependencies and impact

Value Proposition

AWS Config provides unique value through its comprehensive configuration management and compliance automation capabilities that are deeply integrated with the AWS ecosystem. Unlike third-party solutions, Config offers native integration with over 150 AWS services, enabling real-time configuration tracking without performance impact:

- Its managed rules library covers industry standards like PCI DSS, HIPAA, and CIS benchmarks, reducing compliance overhead
- The service scales automatically across multi-account environments with centralized aggregation, provides sub-second configuration change detection, and integrates seamlessly with AWS Security Hub, CloudTrail, and Systems Manager for holistic governance

Service Integration

AWS Config integrates deeply with core AWS services to provide comprehensive governance capabilities. It works with AWS Organizations for multi-account management, AWS Control Tower for automated compliance in landing zones, and AWS CloudTrail to correlate configuration changes with API events:

- Security integrations include AWS Security Hub for centralized security findings, AWS Audit Manager for evidence collection, and AWS Systems Manager for automated remediation
- Config also integrates with Amazon S3 for configuration storage, Amazon SNS for notifications, CloudWatch for monitoring, AWS Firewall Manager for security policy compliance, and AWS Trusted Advisor for operational recommendations

Onboarding and Offboarding

Customers can start with AWS Config using the 1-click setup in the AWS Management Console, which automatically configures best-practice settings for resource recording, delivery channels, and IAM roles. The setup process includes selecting recording strategies (continuous or daily), choosing resource types to monitor, configuring S3 buckets for configuration storage, and optionally setting up SNS topics for notifications:

- For multi-account environments, customers can deploy Config using AWS CloudFormation, Terraform, or AWS Systems Manager Quick Setup
- AWS Control Tower automatically enables Config in enrolled accounts across all regions

Getting Started Guide:
https://docs.aws.amazon.com/config/latest/developerguide/getting-started.html

Data Removal

AWS Config data can be removed by configuring retention periods between 30 days and 7 years for configuration items, with a default of 7 years. Configuration recorders can be stopped and deleted to cease new data collection. Historical configuration data stored in customer-owned S3 buckets must be manually deleted. When offboarding, customers should delete Config rules, conformance packs, aggregators, and delivery channels. The service automatically stops generating new configuration items when recorders are stopped.

Backup/Restore and Disaster Recovery

AWS Config stores configuration data in customer-owned Amazon S3 buckets, providing durability and availability through S3's built-in redundancy. Configuration items are automatically backed up with customizable retention periods up to 7 years. The service supports cross-region replication of configuration data through S3 bucket replication. However, AWS Config primarily focuses on configuration tracking rather than operational backup and disaster recovery capabilities for customer workloads.

Backup Capabilities

AWS Config does not provide traditional backup capabilities but maintains historical configuration data through configuration items stored in S3 buckets. The service retains configuration history for up to 7 years and does not integrate directly with AWS Backup service. Configuration snapshots can be generated on-demand and stored in S3 for point-in-time recovery of configuration states, but this is for configuration data only, not application or user data.

Disaster Recovery

AWS Config does not directly integrate with AWS Elastic Disaster Recovery as it focuses on configuration management rather than operational disaster recovery. The service achieves high availability through AWS's global infrastructure and stores configuration data in durable S3 buckets. For disaster recovery scenarios, customers can replicate Config aggregators and rules across regions, but the service is primarily designed for governance and compliance rather than operational recovery.

Recovery Objectives

AWS Config helps customers meet Recovery Point Objectives (RPO) by maintaining detailed configuration history up to 7 years, enabling point-in-time configuration recovery. For Recovery Time Objectives (RTO), Config provides rapid configuration state queries through Advanced Query API and aggregators for quick assessment during incidents. The service supports automated compliance evaluation and remediation, helping reduce recovery time by ensuring consistent configurations that meet operational requirements.

Service Constraints

Service Quotas: https://docs.aws.amazon.com/config/latest/developerguide/configlimits.html

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

Technical Requirements

Service Documentation: https://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html

User Guide: https://docs.aws.amazon.com/config/latest/developerguide/getting-started.html

API Reference: https://docs.aws.amazon.com/config/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/config/pricing/

Cost Optimization

AWS Config offers several cost optimization strategies including selective resource recording to monitor only critical resources, periodic recording (daily vs. continuous) for less critical resources, and configurable retention periods from 30 days to 7 years to balance compliance needs with storage costs:

- Customers can optimize costs by excluding non-essential resource types from recording, using frequency overrides for different resource categories, and leveraging managed rules instead of custom Lambda-based rules to reduce compute costs
- The service integrates with Cost Explorer for tracking Config-related expenses

Savings Considerations

Cost savings with AWS Config can be achieved through strategic configuration recording approaches. Customers should implement periodic recording for static resources and continuous recording only for critical, frequently-changing resources:

- Using managed rules reduces Lambda execution costs compared to custom rules
- Proper retention period configuration prevents unnecessary long-term storage costs
- Organizations can achieve economies of scale through multi-account aggregation, reducing redundant rule evaluations across accounts

- Proactive compliance monitoring prevents costly misconfigurations and security incidents that could result in significant operational expenses