Service Name

AWS CloudTrail

Service Overview

AWS CloudTrail is a service that enables operational and risk auditing, governance, and compliance of AWS accounts. It records actions taken by users, roles, or AWS services as events, providing a comprehensive audit trail of account activity. CloudTrail captures API calls made through the AWS Management Console, AWS CLI, and AWS SDKs, delivering these events to Amazon S3 buckets, CloudWatch Logs, or EventBridge. The service offers three ways to record events: Event History (90 days of management events at no cost), CloudTrail Lake (managed data lake for long-term storage and analysis), and Trails (configurable event delivery to S3).

Key Use Cases

- Security analysis and incident response: Monitor and investigate suspicious activities, unauthorized access, and security breaches across AWS resources
- Compliance auditing: Meet regulatory requirements by maintaining detailed logs of all AWS account activities for audit trails
- Operational troubleshooting: Debug issues by analyzing API call patterns, error rates, and resource interactions to identify root causes

Features

- **Event History**: Always-on recording of the past 90 days of management events with search, view, and download capabilities at no additional cost
- **CloudTrail Lake**: Managed data lake for capturing, storing, and analyzing events with retention up to 10 years, SQL-based querying, and support for multiple data sources
- **Trails**: Configurable event delivery to S3 buckets with support for management events, data events, network activity events, and multi-region logging
- **CloudTrail Insights**: Machine learning-powered anomaly detection to identify unusual API call patterns and error rates
- **Multi-region and Multi-account Support**: Centralized logging across all AWS regions and organization accounts with consolidated event delivery

Value Proposition

CloudTrail provides comprehensive, native AWS audit logging without requiring additional infrastructure setup or management. It offers automatic encryption, immutable event records, and seamless integration with other AWS security services like GuardDuty and Security Hub:

- The service scales automatically with AWS usage, provides real-time monitoring capabilities, and offers flexible retention options from 90 days to 10 years
- Unlike third-party logging solutions, CloudTrail captures all AWS service interactions natively, requires no agent installation, and provides cost-effective storage with multiple delivery options including S3, CloudWatch Logs, and EventBridge

Service Integration

CloudTrail integrates deeply with Amazon S3 for log file storage, Amazon CloudWatch for real-time monitoring and alerting, and Amazon EventBridge for event-driven architectures. It works with AWS KMS for encryption of log files and event data stores, AWS Organizations for centralized multi-account logging, and AWS IAM for access control:

- Additional integrations include Amazon SNS for delivery notifications, Amazon Athena for log analysis, AWS Config for configuration tracking, Amazon GuardDuty for threat detection, and AWS Security Hub for centralized security findings
- CloudTrail also supports integration with third-party SIEM solutions and custom applications through its APIs

Onboarding and Offboarding

CloudTrail is automatically enabled for all AWS accounts with Event History providing 90 days of management event logs at no cost. To get started with advanced features, customers can create trails through the AWS Management Console, AWS CLI, or APIs to deliver events to S3 buckets:

- CloudTrail Lake setup involves creating event data stores with chosen retention periods and pricing options
- The service provides managed policies (AWSCloudTrail_FullAccess and AWSCloudTrail_ReadOnlyAccess) for permissions management
- Getting started requires minimal configuration - simply specify an S3 bucket for trail delivery or create an event data store for Lake functionality

Getting Started Guide:
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html

Data Removal

Offboarding involves deleting trails, event data stores, and channels through the console or APIs. Deleting trails stops logging but doesn't remove existing log files in S3 buckets. Event data stores enter a PENDING_DELETION state for 7 days before permanent deletion, during which no queries or operations are possible. Customers must manually delete log files from S3 buckets and CloudWatch Logs if complete data removal is required.

Backup/Restore and Disaster Recovery

CloudTrail provides immutable audit logs stored in S3 with optional cross-region replication for disaster recovery. Event data stores offer durable storage with automatic backup across multiple Availability Zones. The service supports log file integrity validation using digest files to ensure data hasn't been tampered with. CloudTrail integrates with AWS Backup for centralized backup management of related resources.

Backup Capabilities

CloudTrail logs are automatically stored with high durability in S3 and replicated across multiple Availability Zones. Event data stores provide immutable storage with configurable retention periods:

- The service doesn't integrate directly with AWS Backup but supports S3 cross-region replication for additional protection
- Log file integrity validation ensures audit trail authenticity

Disaster Recovery

CloudTrail supports disaster recovery through multi-region trail configuration and S3 cross-region replication. Event data stores can be configured for multi-region logging with automatic failover capabilities. The service doesn't directly integrate with AWS Elastic Disaster Recovery but provides the audit trail necessary for compliance during disaster recovery scenarios.

Recovery Objectives

CloudTrail helps meet RPO objectives through real-time event logging with minimal delay (typically within 15 minutes). For RTO objectives, multi-region trails and event data stores provide rapid access to audit logs even during regional outages. Cross-region replication and immutable storage ensure audit continuity during disaster recovery scenarios.

Service Constraints

Service Quotas: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/WhatIsCloudTrail-Limits.html

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

Technical Requirements

Service Documentation: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html

User Guide: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html

API Reference: https://docs.aws.amazon.com/awscloudtrail/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/cloudtrail/pricing/

Cost Optimization

CloudTrail offers several cost optimization options including advanced event selectors to filter unnecessary events, choosing appropriate retention periods (1-year extendable vs 7-year for CloudTrail Lake), and using the free 90-day Event History for basic needs. Customers can optimize costs by creating single multi-region trails instead of multiple regional trails, using data event aggregation to reduce volume, and selecting the most cost-effective pricing tier based on ingestion patterns. S3 lifecycle policies can reduce storage costs for long-term log retention, and careful selection of event types prevents unnecessary logging charges.

Savings Considerations

Major cost savings come from avoiding duplicate trail creation (first copy of management events per region is free), using advanced event selectors to log only necessary resources, and choosing CloudTrail Lake one-year extendable retention for variable workloads. Organizations can save by using organization trails instead of individual account trails:

- For high-volume environments, aggregating data events and using appropriate retention periods based on compliance requirements provides significant savings
- Leveraging the free Event History tier for basic monitoring needs and upgrading to paid features only when advanced capabilities are required optimizes costs effectively