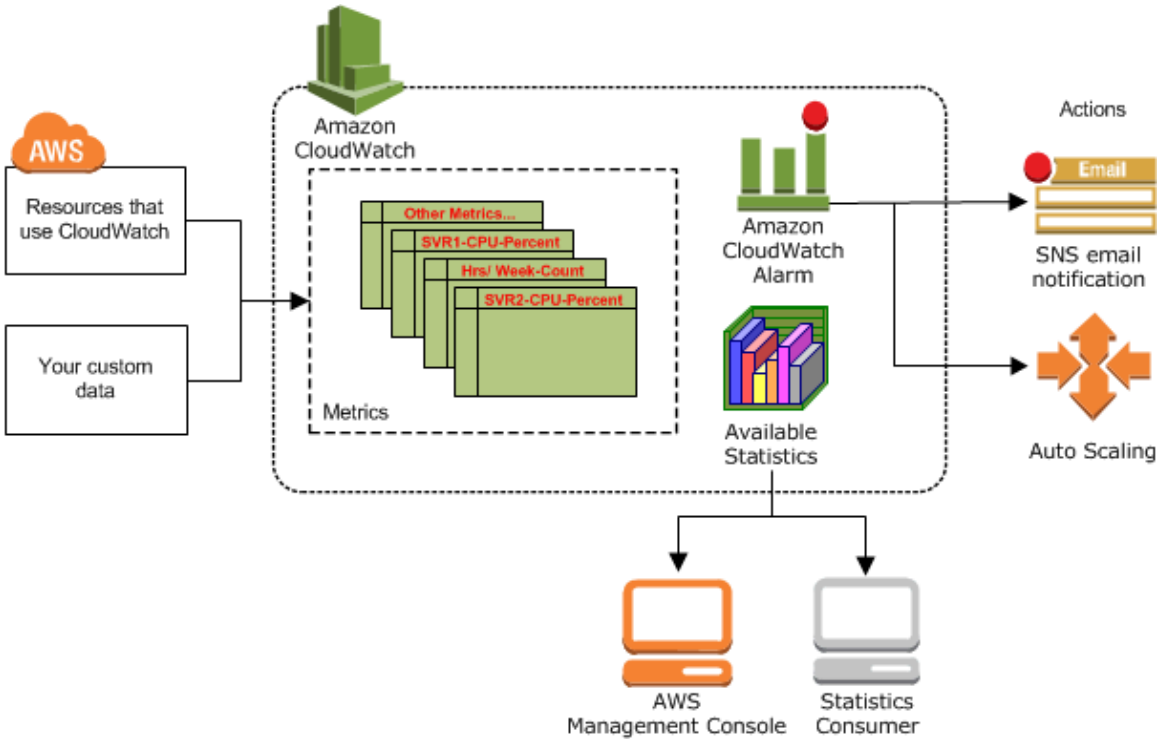
# AWS
# Monitoring
## Concepts

# Concept Overview:

# Amazon CloudWatch:

Amazon CloudWatch monitors your Amazon Web Services (AWS) resources and the applications you run on AWS in real time, and offers many tools to give you system-wide observability of your application performance, operational health, and resource utilization.

## Simple Monitoring Architechture



# Amazon CloudWatch:

## Metrics:

Metrics are data about the performance of your systems. By default, many services provide free metrics for resources (such as Amazon EC2 instances, Amazon EBS volumes, and Amazon RDS DB instances). You can also enable detailed monitoring for some resources, such as your Amazon EC2 instances, or publish your own application metrics. Amazon CloudWatch can load all the metrics in your account (both AWS resource metrics and application metrics that you provide) for search, graphing, and alarms.

Metric data is kept for 15 months, enabling you to view both up-to-the-minute data and historical data.

To graph metrics in the console, you can use CloudWatch Metrics Insights, a high-performance SQL query engine that you can use to identify trends and patterns within all your metrics in real time.

# Amazon CloudWatch:

## Features of Metrics:

### Automatic and Custom Metric Collection:

- Automatic metrics: AWS services (EC2, Lambda, S3, etc.) publish standard metrics by default.
- Custom metrics: You can publish application-specific metrics (such as transaction volumes, error rates, memory usage).

### High-Resolution Data:

- Standard resolution: 1-minute frequency.
- High resolution: Custom metrics with 1-second granularity for real-time insights.

### Data Organization & Analysis:

- Namespaces: Containers for metrics (AWS/EC2).
- Dimensions: Key-value pairs for filtering & grouping (InstanceId).
- Metric math: Perform calculations across multiple metrics.
- Metrics Insights: SQL-based query engine for large-scale analysis.

# Amazon CloudWatch:

## Features of Metrics:

### Visualization & Alerting

- Dashboards: Unified, real-time view of metrics & logs.
- Alarms: Trigger notifications/actions on threshold breaches.
- Anomaly detection: Machine learning–based alarms.
- Composite alarms: Combine multiple alarms, fewer noisy alerts.

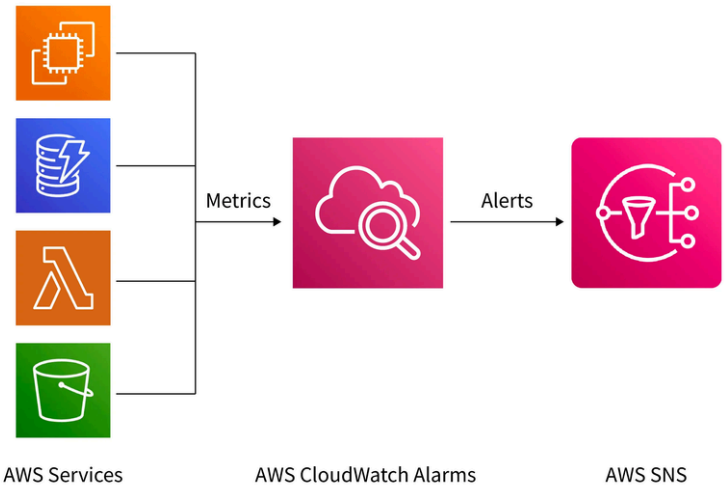
### Integration & Ecosystem:

- AWS service integration: Works natively with 70+ AWS services.
- Metric streams: Continuous, near-real-time export to S3 or third-party tools.
- Cross-account observability: Centralized monitoring across multiple AWS accounts.

# Amazon CloudWatch:

## Alarms:

AWS CloudWatch alarm is a tool that monitors a specific metric over a set period and triggers an action if the metric crosses a user-defined threshold. These alarms can send notifications via Amazon SNS, automatically scale an application's resources, or even terminate a resource when certain conditions are met, providing automated responses to changes in your AWS environment.



# Amazon CloudWatch:

## Features of Alarms:

### Alarm States:

- OK: Metric is within threshold.
- ALARM: Metric breached threshold.
- INSUFFICIENT_DATA: Not enough data to evaluate.

### Actionable Insights (Alarm Actions):

- Notifications: Send alerts via Amazon SNS (email, SMS, etc.).
- Auto Scaling: Scale EC2 instances up/down automatically.
- EC2 actions: Stop, terminate, or recover instances.
- Systems Manager integration: Create an OpsItem in OpsCenter for incident tracking.

### Types of Alarms:

- Metric alarms: Monitor one metric or a metric math expression.
- Composite alarms: Combine multiple alarms, reduce noise.
- Anomaly detection alarms: ML-based dynamic thresholds:adapt to patterns & reduce false alarms.

# Amazon CloudWatch:

## Features of Alarms:

### Flexible Configuration:

- Static thresholds: Fixed numeric value for alarm trigger.
- Missing data treatment: Define alarm behavior when data points are missing.
- High-resolution alarms: Work with 1-second metrics; periods as short as 10s or 30s.
- Metrics Insights alarms: Use SQL-based queries to create alarms for entire fleets of dynamic resources.

## Use Case of Alarms:

- Optimize EC2 resources: Shut down or terminate underutilized EC2 instances to reduce costs.
- Monitor application health: Use a composite alarm (such as API Gateway 5xx errors AND high latency) to avoid false positives from isolated spikes.
- Ensure queue processing: Alarm on Amazon SQS queue length to trigger Auto Scaling when backlog grows.
- Validate new deployments: Anomaly detection alarms adapt to new baselines, highlighting only real performance issues.
- Handle missing data: Alarm when a critical app stops sending metrics, indicating a potential outage or failure.

# Amazon CloudWatch:

## Logs:

You can use Amazon CloudWatch Logs to monitor, store, and access your log files from Amazon Elastic Compute Cloud (Amazon EC2) instances, AWS CloudTrail, Route 53, and other sources.

CloudWatch Logs enables you to centralize the logs from all of your systems, applications, and AWS services that you use, in a single, highly scalable service. You can then easily view them, search them for specific error codes or patterns, filter them based on specific fields, or archive them securely for future analysis. CloudWatch Logs enables you to see all of your logs, regardless of their source, as a single and consistent flow of events ordered by time.

CloudWatch Logs also supports querying your logs with a powerful query language, auditing and masking sensitive data in logs, and generating metrics from logs using filters or an embedded log format.

CloudWatch Logs supports two log classes. Log groups in the CloudWatch Logs Standard log class support all CloudWatch Logs features. Log groups in the CloudWatch Logs Infrequent Access log class incur lower ingestion charges and support a subset of the Standard class capabilities.

# Amazon CloudWatch:

## Features of Logs:

### Log Storage & Classes:

- Two log classes:
  1. Cost-effective class for infrequent access.
  2. Full-featured class for real-time monitoring & advanced features.
- Log retention: Default is indefinite; customizable from 1 day to 10 years.
- Archive log data: Store logs in durable storage for long-term access.

### Querying & Analysis:

- CloudWatch Logs Insights: Purpose-built query language with sample queries, auto-completion, and field discovery.
- Field indexes: Speed up queries by skipping irrelevant log events.
- Metrics from logs: Convert log patterns (such as error counts, 404s) into CloudWatch metrics for monitoring.

# Amazon CloudWatch:

## Features of Logs:

### Real-time Monitoring & Debugging:

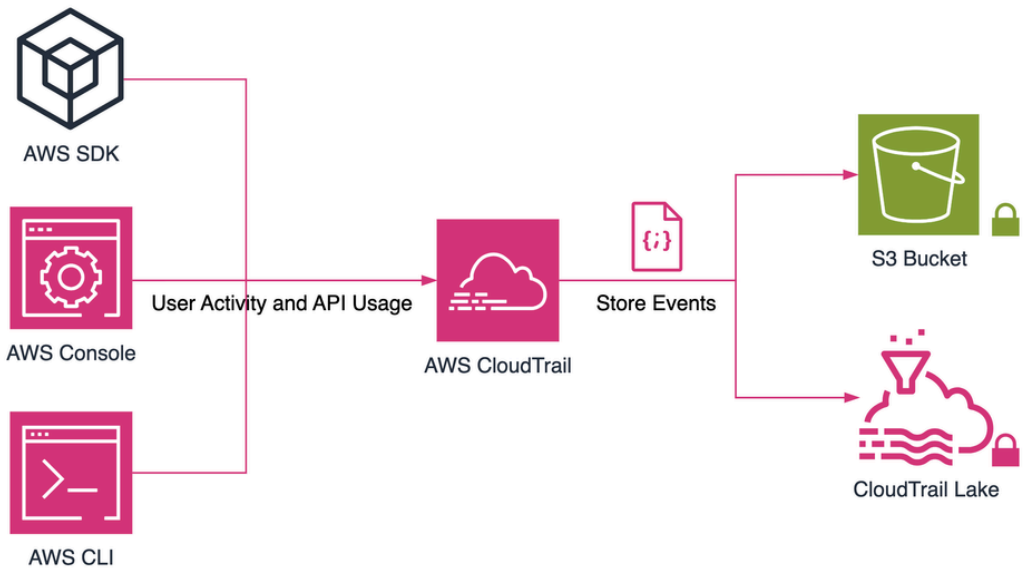
- Live Tail: Stream logs in near real time to detect and troubleshoot issues faster (filter & highlight supported).
- EC2 log monitoring: Collect & analyze application/system logs without code changes.
- CloudTrail integration: Monitor API activity via CloudTrail logs + CloudWatch alarms.
- Route 53 DNS logs: Capture DNS query information.

### Data Protection & Security

- Encryption: Logs are encrypted in transit and at rest.
- Data protection policies: Audit & mask sensitive data automatically using identifiers.

# Amazon CloudTrail:

AWS CloudTrail is an AWS service that helps you enable operational and risk auditing, governance, and compliance of your AWS account. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail. Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs.



# Amazon CloudTrail:

## Features of CloudTrail:

### Event Logging Methods:

- Event History:
  - Default (enabled on all accounts).
  - Last 90 days of management events.
  - Free, immutable, searchable record.
- Trails:
  - Continuous logging to Amazon S3.
  - Optional delivery to CloudWatch Logs (monitoring/alerting) or EventBridge (automation).
  - Long-term, durable storage.
- CloudTrail Lake:
  - Managed data lake for log storage & SQL-based queries.
  - Stores events for up to 10 years.
  - Supports ingestion from non-AWS sources (other clouds / on-prem apps).

# Amazon CloudTrail:

## Features of CloudTrail:

### Event Types:

- Management events: Control-plane actions (e.g., IAM changes, EC2 termination).
- Data events: High-volume, resource-level actions (such as S3 object access, Lambda invokes). Not logged by default.
- Insights events: Detect unusual patterns (spikes in API calls, error rates) via ML analysis.
- Network activity events: Capture API calls via VPC endpoints for enhanced network security.

### Security & Compliance:

- Log file integrity validation: Detects tampering using SHA-256.
- Encryption: Logs encrypted by default (S3 SSE); supports KMS keys for stronger security.
- Consolidated logging: Organization trail aggregates logs from all AWS accounts in AWS Organizations.

# Amazon CloudTrail:

## Features of CloudTrail:

### Analytics & Troubleshooting:

- Event filtering: Filter history by user, resource, event source, and time range.
- Service integrations:
  - Athena: Ad-hoc SQL queries on S3 logs.
  - CloudWatch Logs: Alarms & dashboards.
  - EventBridge: Automated workflows on captured API activity.
- CloudTrail Lake dashboards: Built-in visualization of event trends.

### Management & Administration:

- Multi-account support: Aggregate logs into one S3 bucket.
- Multi-region support: Single trail captures events across all AWS regions.
- Resource-level permissions: IAM policies allow fine-grained access to CloudTrail resources.

# Amazon CloudTrail:

## Use cases of CloudTrail:

**Security Analysis & Incident Response:**

- Detect unauthorized activity: Identify suspicious API calls, user sessions, and IP addresses.
- Investigate compromised accounts: Review detailed action history to see what was done and when.
- Data exfiltration detection: Monitor S3 object-level API events for unauthorized data access or transfers.

**Compliance & Auditing:**

- Meet regulatory standards: Provides an immutable audit trail for compliance (PCI DSS, HIPAA, SOC 2).
- Internal policy enforcement: Track activity to ensure adherence to security policies & best practices.

**Operational Troubleshooting:**

- Identify resource changes: See who changed what, when, and how.
- Debugging & root cause analysis: Use CloudTrail + Athena queries to analyze failures.

# Amazon CloudTrail:

## Use cases of CloudTrail:

### Analytics & Usage Insights:

- Understand usage patterns: Analyze trends in resource usage and user activity.
- Anomaly detection (CloudTrail Insights): ML-based detection of unusual activity (such as IAM spikes, resource provisioning anomalies).

### Automated Responses & Notifications:

- Real-time alerts: Integrate with EventBridge + Lambda for automated remediation workflows.
- Custom alerts: Use CloudWatch alarms on CloudTrail logs for sensitive/critical actions.

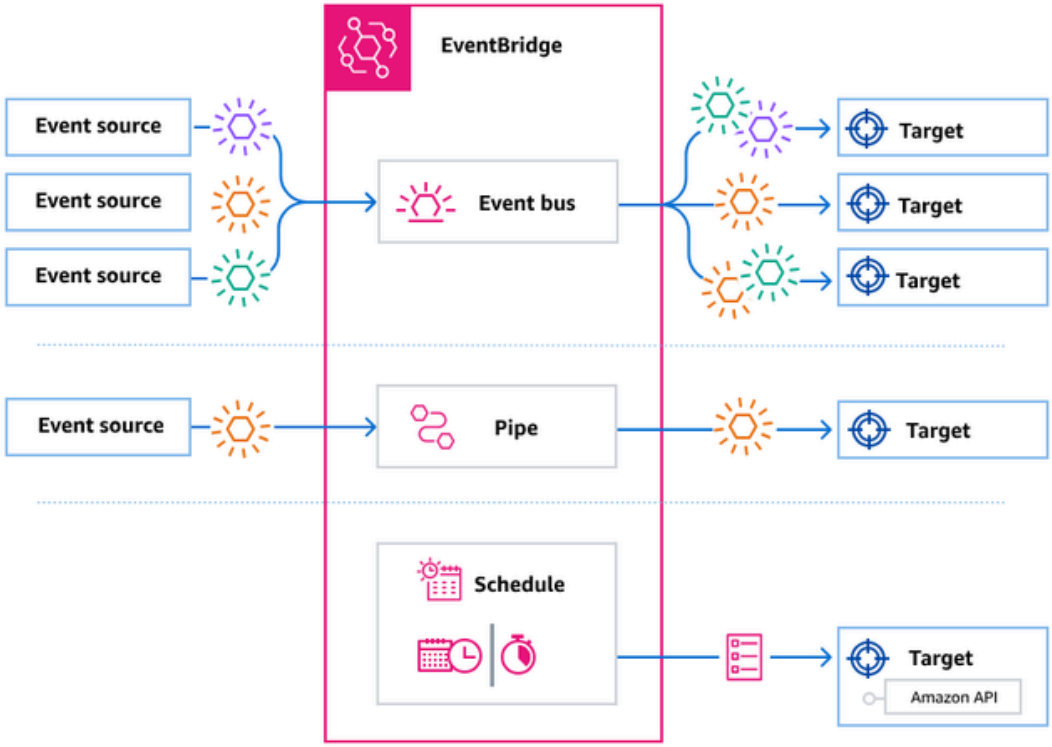
# Amazon EventBridge:

EventBridge is a serverless service that uses events to connect application components together, making it easier for you to build scalable event-driven applications. Event-driven architecture is a style of building loosely-coupled software systems that work together by emitting and responding to events. Event-driven architecture can help you boost agility and build reliable, scalable applications.

EventBridge provides simple and consistent ways to ingest, filter, transform, and deliver events so you can build applications quickly.

You can create it using current distribution or previous distribution too.

## EventBridge Architecture



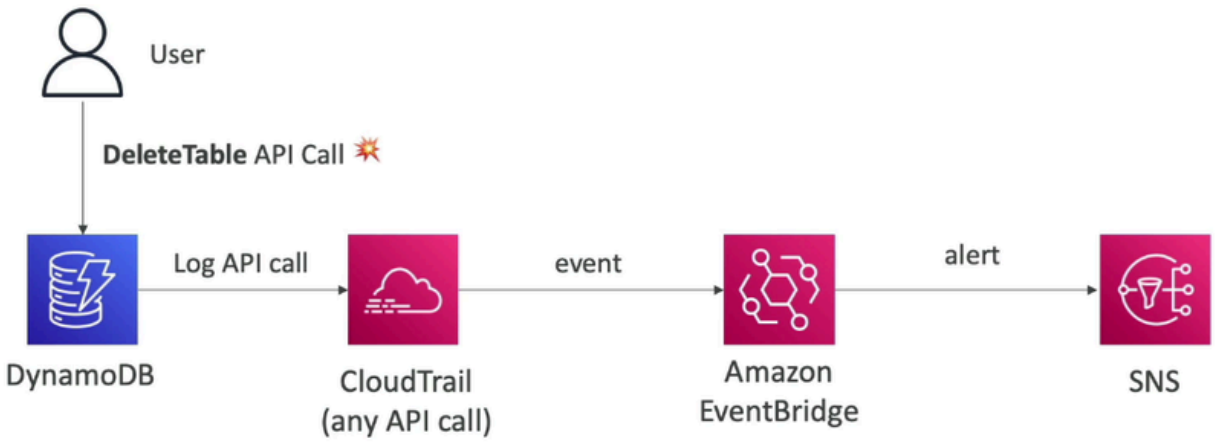
# Amazon EventBridge with CloudTrail:

**API activity monitoring:**
CloudTrail events (such as IAM changes, EC2 termination, S3 object access) can be sent to EventBridge in near real time.

**Automated security responses:**

- Detect unauthorized API calls → EventBridge → Lambda → revoke credentials / notify security team
- Trigger Systems Manager Automation to quarantine a resource when suspicious activity is logged.

**Compliance enforcement:**
Automatically enforce tagging or security policies when CloudTrail detects non-compliance actions.



# Amazon EventBridge with CloudWatch:

**Forward metrics & alarms:**
CloudWatch alarms can publish events to EventBridge for automated responses (such as auto-remediation workflows).

**Event-driven dashboards:**
Use EventBridge to trigger updates to CloudWatch dashboards when specific events occur.

**Log monitoring:**
Forward CloudWatch Logs events (via subscription filters) into EventBridge → trigger workflows (such as notify on critical log patterns).