Advanced AWS CloudWatch Workshop

Instructor: Govind Kumar

Date: 23-May-2025 | Time: 9:00 PM - 11:30 PM IST

Service Integrations

CloudWatch integration with EC2, CloudFront, and S3 services.

EventBridge

Working with Events, Rules, and Event Buses for event-driven architectures.

CloudWatch AIOps

Exploring the new AI-powered operations capabilities in CloudWatch.

CloudWatch Integration with EC2

Monitoring EC2 Instances

Comprehensive monitoring and alerting for your compute resources.

Default EC2 Metrics in CloudWatch

Amazon EC2 automatically sends the following metrics to CloudWatch at 5-minute intervals (1-minute with detailed monitoring):

Metric	Description	Use Case
CPUUtilization	Percentage of allocated EC2 compute units being used	Identify overloaded or underutilized instances
NetworkIn/NetworkOut	Bytes received/sent on all network interfaces	Monitor network traffic patterns and costs
DiskReadOps/DiskWriteOps	Completed read/write operations to all instance store volumes	Identify I/O bottlenecks
StatusCheckFailed	Reports whether instance or system status checks have failed	Detect hardware and software issues

EC2 Monitoring Levels

- **Basic Monitoring:** Metrics sent at 5-minute intervals (free)
- **Detailed Monitoring:** Metrics sent at 1-minute intervals (additional cost)

Common EC2 Alarms

- **High CPU:** Alert when CPU > 80% for 5+ minutes
- **Low CPU:** Identify underutilized instances
- **Status Check:** Detect and recover failed instances
- **Burst Credit Balance:** For burstable instances

Cloudwatch Components

① Dashboard
- custom (3 custom dashboard referencing upto 50 metrics each/month
- Automatic

② Alerting

Components
- Metrics
  - Default
  - Custom
- logs

Types of logs

① VPC flow logs

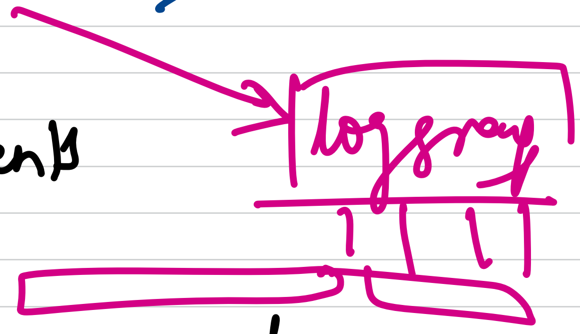
② OS logs

③ Appl^n logs

④ Cloudtrail logs

⑤ CDN logs

⑥ Cloudwatch events



log group
stream

CloudWatch Integration with CloudFront

Monitoring Content Delivery

Track performance and usage of your CloudFront distributions.

CloudFront Metrics in CloudWatch

CloudFront automatically publishes operational metrics to CloudWatch, helping you monitor your content delivery:

Metric	Description	Use Case
Requests	Total number of viewer requests received by CloudFront	Track usage patterns and traffic spikes
BytesDownloaded	Number of bytes downloaded by viewers	Monitor bandwidth usage and costs
BytesUploaded	Number of bytes uploaded to your origin	Track data transfer for PUT/POST requests
4xxErrorRate / 5xxErrorRate	Percentage of all requests for which HTTP status code is 4xx or 5xx	Identify client or server errors
TotalErrorRate	Percentage of all requests for which HTTP status code is 4xx or 5xx	Monitor overall error rates

Performance Monitoring

- **OriginLatency:** Time spent from request to first byte from origin
- **CacheHitRate:** Percentage of viewer requests served from cache
- **OriginThrottleRate:** Percentage of requests throttled by origin

These metrics help identify performance bottlenecks and optimize your CDN configuration.

Security Monitoring

- **Bot traffic:** Monitor and filter unwanted bot traffic
- **WAF blocks:** Track blocked requests by AWS WAF rules
- **Geographic restrictions:** Monitor blocked countries

Set up alarms to detect unusual patterns that might indicate security issues.

CloudWatch Integration with S3

Monitoring Storage Resources

Track usage, performance, and operations of your S3 buckets.

S3 Metrics in CloudWatch

Amazon S3 automatically sends metrics to CloudWatch at 1-minute intervals:

Metric	Description	Use Case
BucketSizeBytes	Amount of data stored in a bucket	Track storage growth and costs
NumberOfObjects	Total number of objects stored in a bucket	Monitor object count trends
AllRequests	Total number of HTTP requests made to an S3 bucket	Track API usage patterns
4xxErrors / 5xxErrors	Count of HTTP 4xx/5xx status code responses	Identify client or server errors
FirstByteLatency	Per-request time from request to first byte received	Monitor performance and identify bottlenecks

CloudWatch Integration with CloudTrail

Monitoring API Activity

Track and analyze AWS API calls across your account.

CloudTrail Events in CloudWatch

CloudTrail can send events to CloudWatch Logs for real-time monitoring and alerting:

Event Type	Description	Use Case
Management Events	API operations on AWS resources	Track resource changes and security events
Data Events	Object-level API activity	Monitor S3 object access, Lambda executions
Insights Events	Unusual API activity patterns	Detect potential security issues or misconfigurations

Setup and Configuration

Steps to integrate CloudTrail with CloudWatch:

```
# Create a CloudWatch Logs role for CloudTrail
aws iam create-role --role-name CloudTrail_CloudWatchLogs_Role
  --assume-role-policy-document file://trust-policy.json

# Create a trail that logs to CloudWatch Logs
aws cloudtrail create-trail \
  --name management-events-trail \
  --cloud-watch-logs-log-group-arn arn:aws:logs:region:account
  --cloud-watch-logs-role-arn arn:aws:iam::account-id:role/Cl
```

Security Monitoring

Common CloudWatch Alarms for CloudTrail events:

- Root account usage
- IAM policy changes
- Security group modifications
- Network ACL changes
- VPC configuration updates

CloudWatch Integration with VPC Flow Logs

Network Traffic Analysis

Monitor and analyze network traffic patterns in your VPC.

VPC Flow Logs in CloudWatch

VPC Flow Logs capture information about IP traffic going to and from network interfaces:

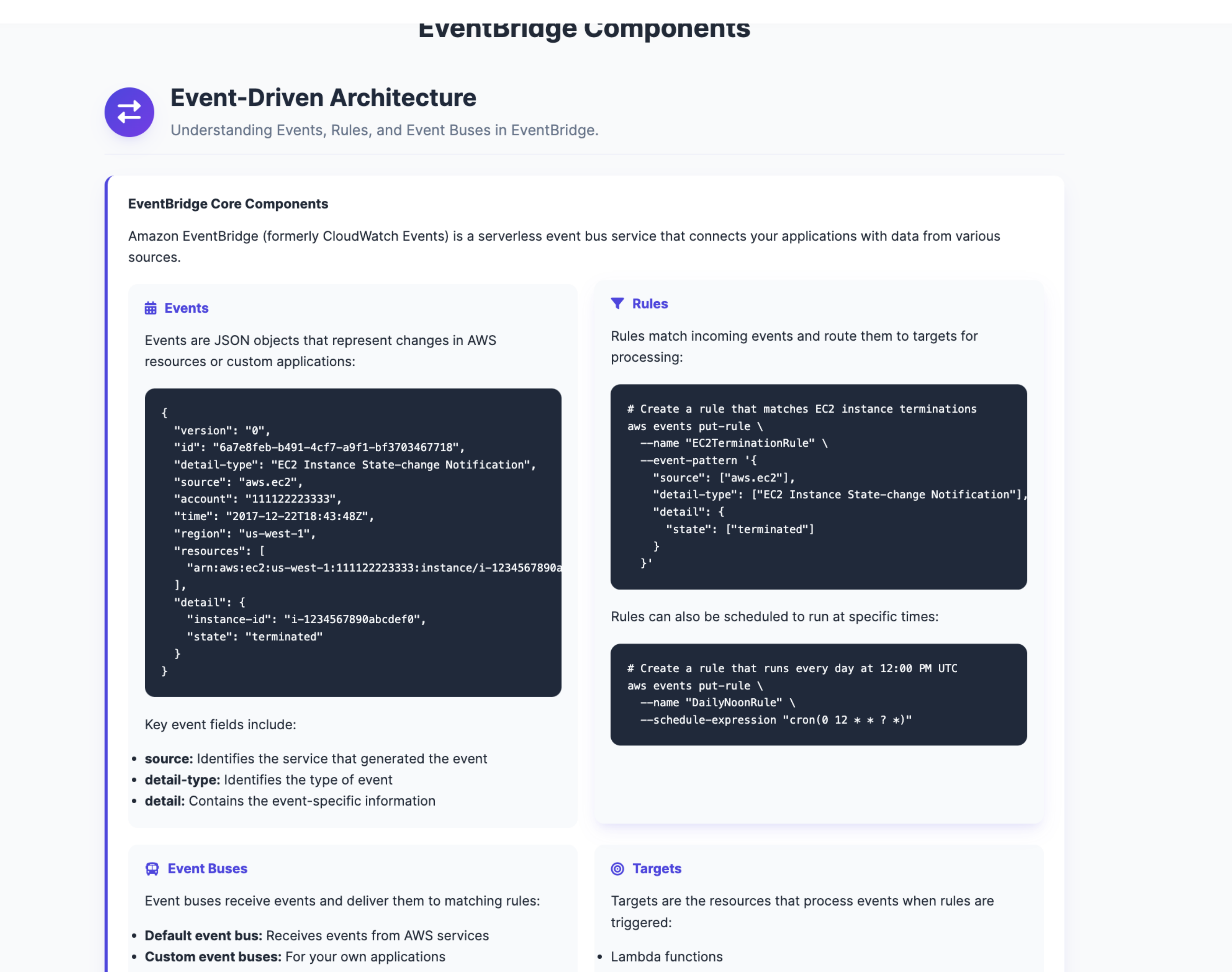
Log Field	Description	Use Case
srcaddr, dstaddr	Source and destination IP addresses	Track traffic patterns and identify communication paths
srcport, dstport	Source and destination ports	Identify application-level communications
protocol	Protocol number (TCP=6, UDP=17)	Analyze protocol usage patterns
action	Accept or reject status	Monitor security group and NACL effectiveness

Flow Logs Setup

Enable VPC Flow Logs with CloudWatch integration:

Analysis with CloudWatch Logs Insights

Sample queries for analyzing flow logs:



EventBridge Components

Event-Driven Architecture

Understanding Events, Rules, and Event Buses in EventBridge.

EventBridge Core Components

Amazon EventBridge (formerly CloudWatch Events) is a serverless event bus service that connects your applications with data from various sources.

Events

Events are JSON objects that represent changes in AWS resources or custom applications:

```
{
  "version": "0",
  "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
  "detail-type": "EC2 Instance State-change Notification",
  "source": "aws.ec2",
  "account": "111122223333",
  "time": "2017-12-22T18:43:48Z",
  "region": "us-west-1",
  "resources": [
    "arn:aws:ec2:us-west-1:111122223333:instance/i-1234567890a
  ],
  "detail": {
    "instance-id": "i-1234567890abcdef0",
    "state": "terminated"
  }
}
```

Key event fields include:

- **source:** Identifies the service that generated the event
- **detail-type:** Identifies the type of event
- **detail:** Contains the event-specific information

Rules

Rules match incoming events and route them to targets for processing:

```
# Create a rule that matches EC2 instance terminations
aws events put-rule \
  --name "EC2TerminationRule" \
  --event-pattern '{
    "source": ["aws.ec2"],
    "detail-type": ["EC2 Instance State-change Notification"],
    "detail": {
      "state": ["terminated"]
    }
  }'
```

Rules can also be scheduled to run at specific times:

```
# Create a rule that runs every day at 12:00 PM UTC
aws events put-rule \
  --name "DailyNoonRule" \
  --schedule-expression "cron(0 12 * * ? *)"
```

Event Buses

Event buses receive events and deliver them to matching rules:

- **Default event bus:** Receives events from AWS services
- **Custom event buses:** For your own applications

Targets

Targets are the resources that process events when rules are triggered:

- Lambda functions

AI-Powered Operations

Exploring the new AI capabilities in CloudWatch for intelligent monitoring.

CloudWatch AIOps Overview

CloudWatch AIOps (Preview) uses machine learning to help you detect, diagnose, and remediate operational issues faster.

Automated Investigations

CloudWatch AIOps automatically investigates anomalies and issues by:

- Analyzing patterns across metrics, logs, and traces
- Correlating related anomalies
- Identifying root causes
- Suggesting remediation actions

This reduces mean time to resolution (MTTR) and helps operators focus on solving problems rather than diagnosing them.

Intelligent Grouping

AIOps groups related alerts to reduce alert fatigue:

- Correlates alerts across services
- Identifies cascading failures
- Prioritizes issues based on impact
- Creates incident timelines

This helps teams focus on the most critical issues first and understand the relationships between different alerts.

Key Components of CloudWatch AIOps

Investigations

Automatically analyzes operational issues to determine root causes:

- Identifies contributing factors
- Analyzes historical patterns
- Provides context-aware insights
- Suggests next steps for remediation

Investigations are triggered automatically when anomalies are detected or can be started manually.

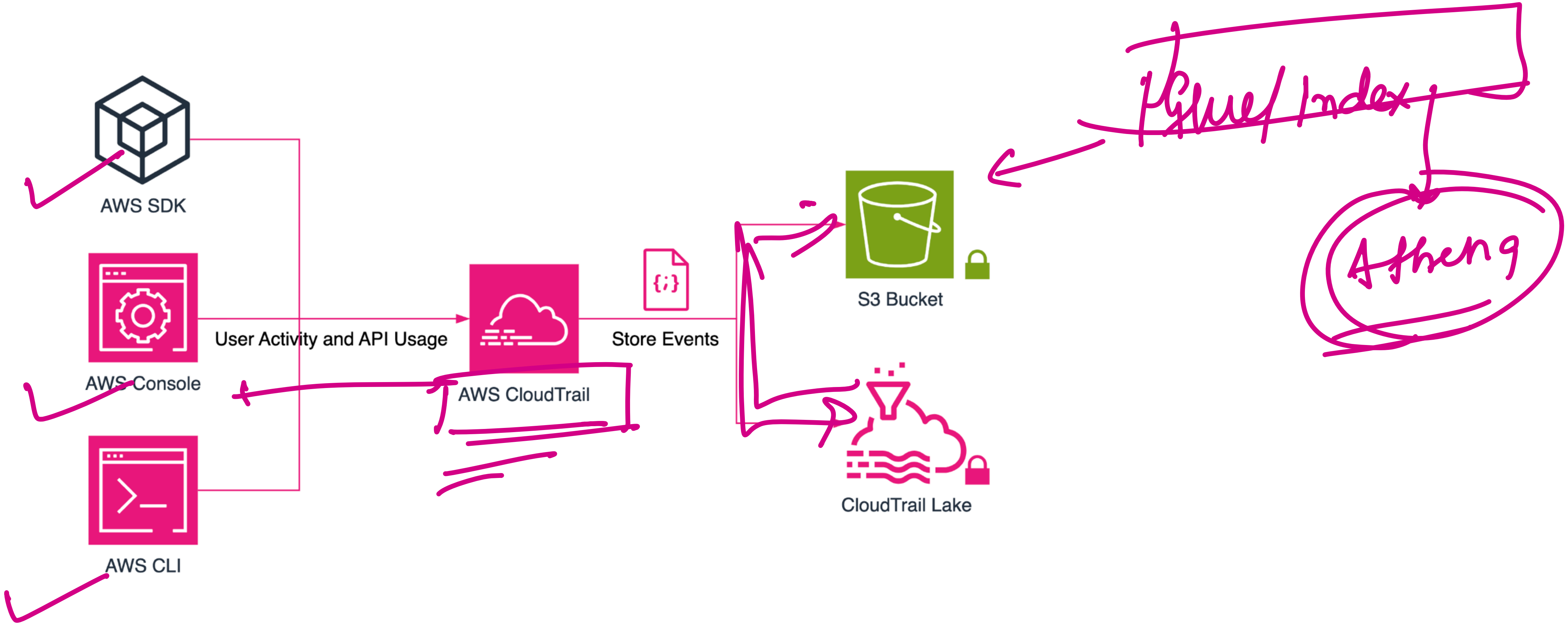
Configuration

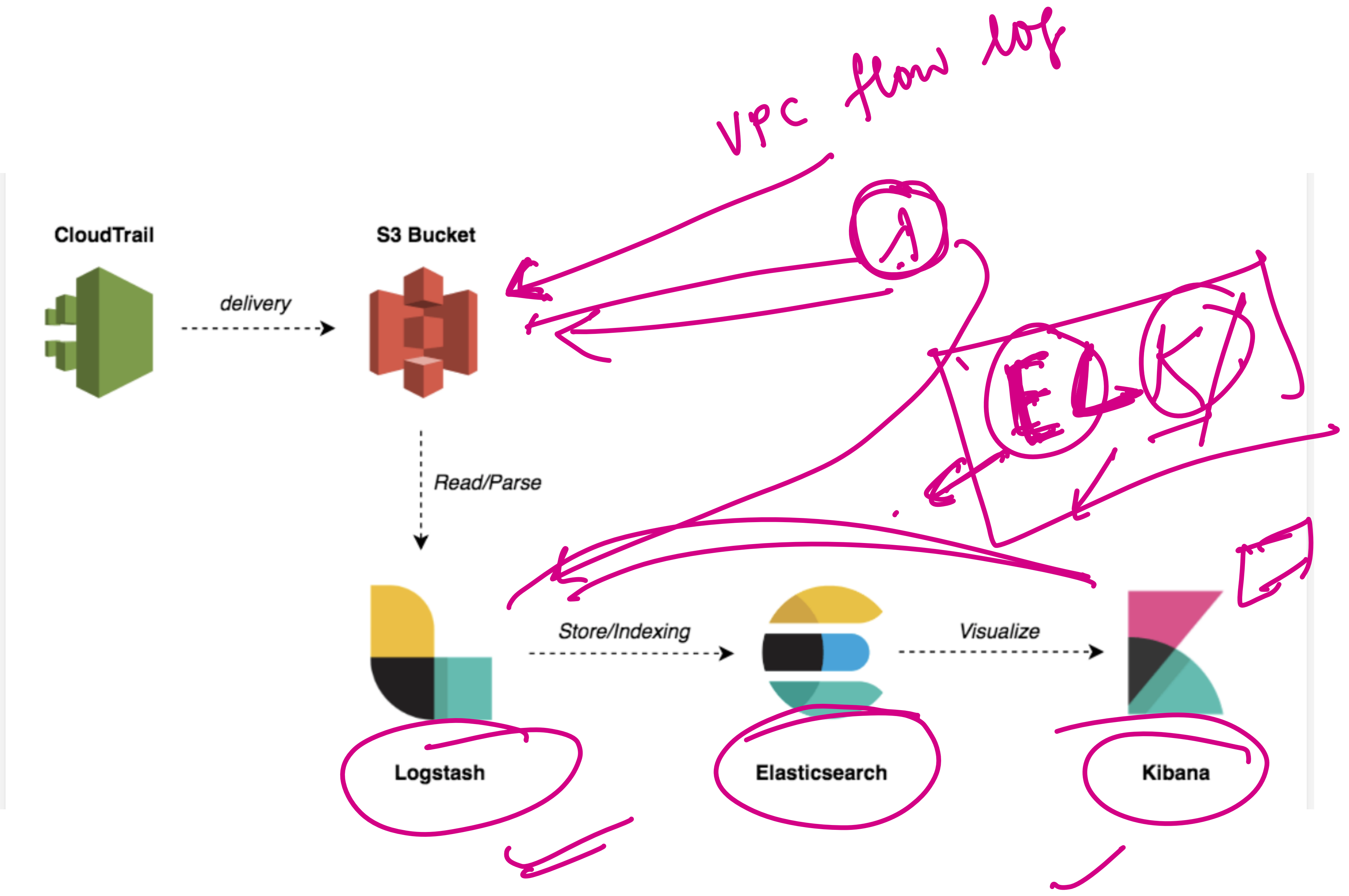
Set up AIOps to monitor your specific environment:

- Define service boundaries
- Set monitoring thresholds
- Configure notification preferences
- Integrate with existing workflows

Configuration is done through the CloudWatch console or API.

Amazon CloudTrail





CloudTrail

delivery

S3 Bucket

Read/Parse

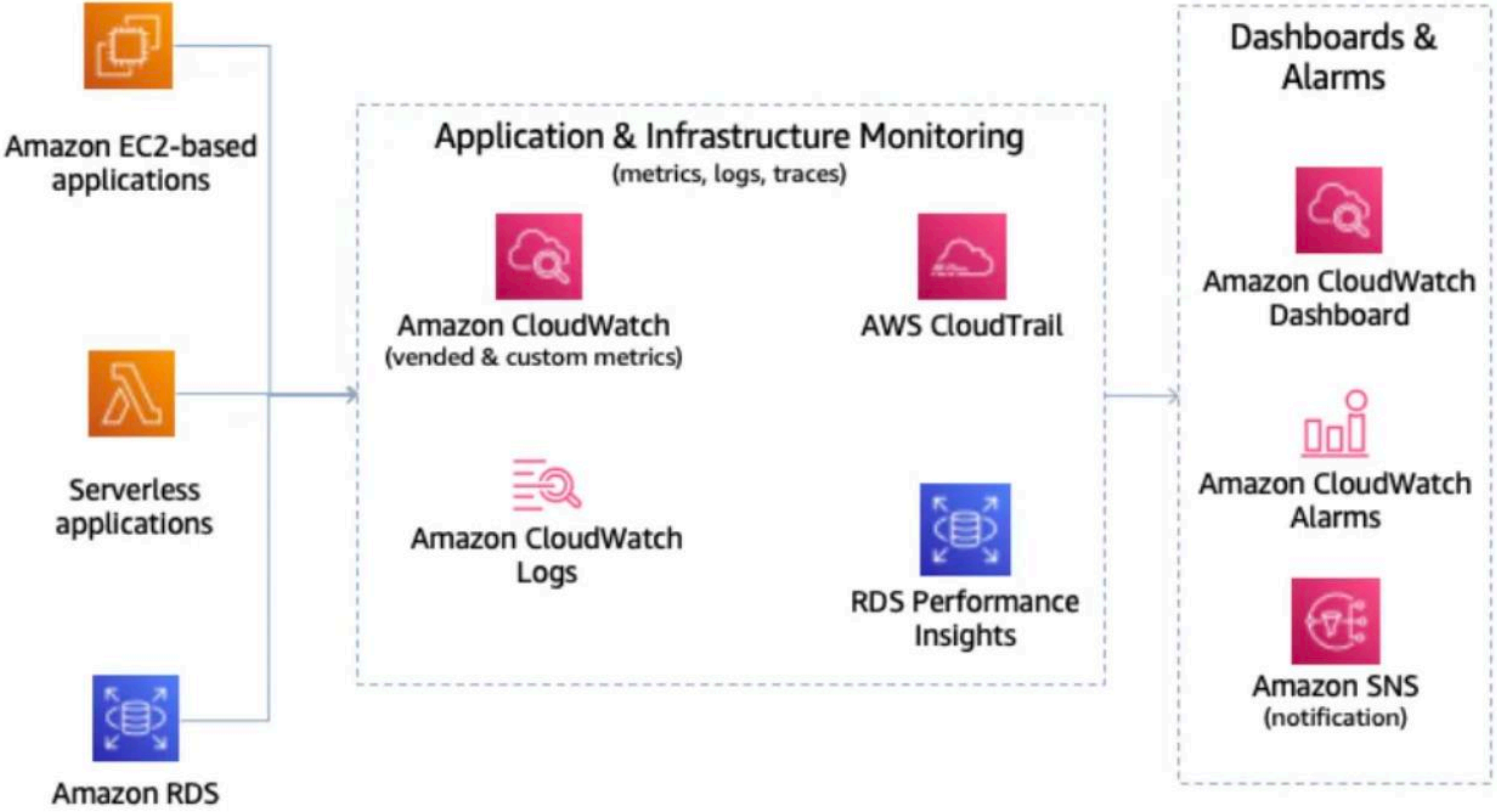
Logstash

Store/Indexing

Elasticsearch

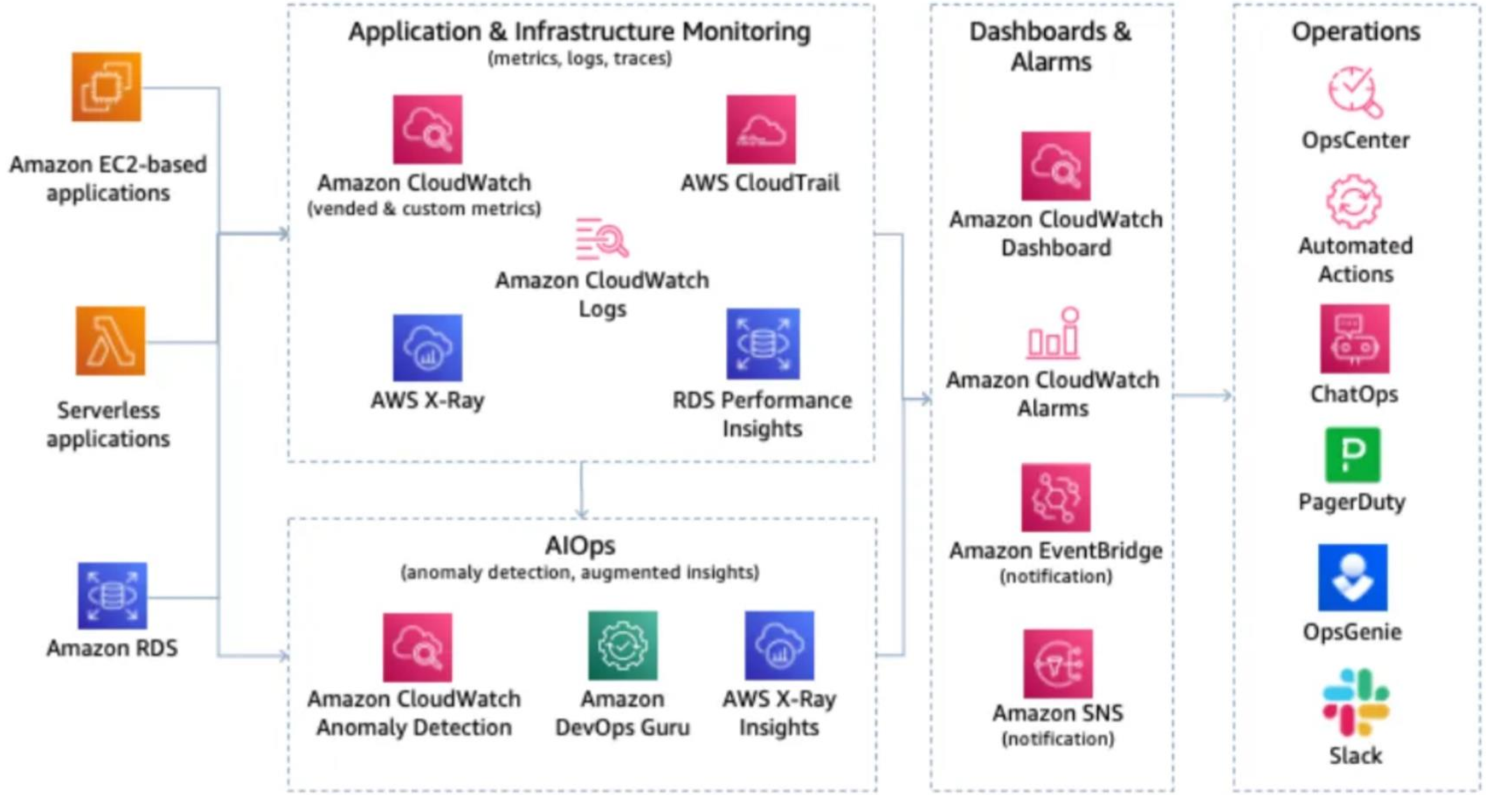
Visualize

Kibana



Traditional Architecture of Observability

1. The need for periodic review and potential modification of monitor


Amazon EC2-based applications
Serverless applications
Amazon RDS
Application & Infrastructure Monitoring
(metrics, logs, traces)
Amazon CloudWatch
(vended & custom metrics)
AWS CloudTrail
Amazon CloudWatch Logs
AWS X-Ray
RDS Performance Insights
AIOps
(anomaly detection, augmented insights)
Amazon CloudWatch Anomaly Detection
Amazon DevOps Guru
AWS X-Ray Insights
Dashboards & Alarms
Amazon CloudWatch Dashboard
Amazon CloudWatch Alarms
Amazon EventBridge
(notification)
Amazon SNS
(notification)
Operations
OpsCenter
Automated Actions
ChatOps
PagerDuty
OpsGenie
Slack