

Monitoring

AWS Resources

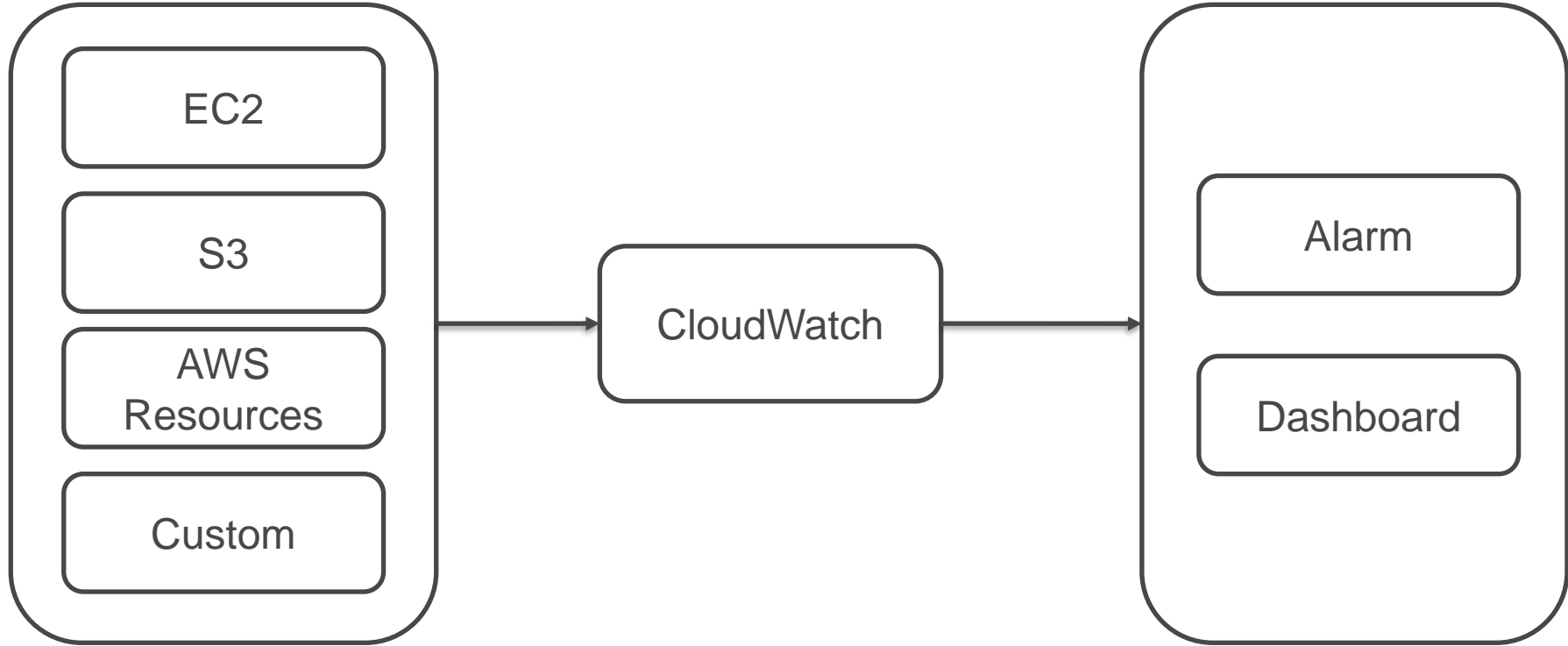
Chandra Lingam

Cloud Wave LLC

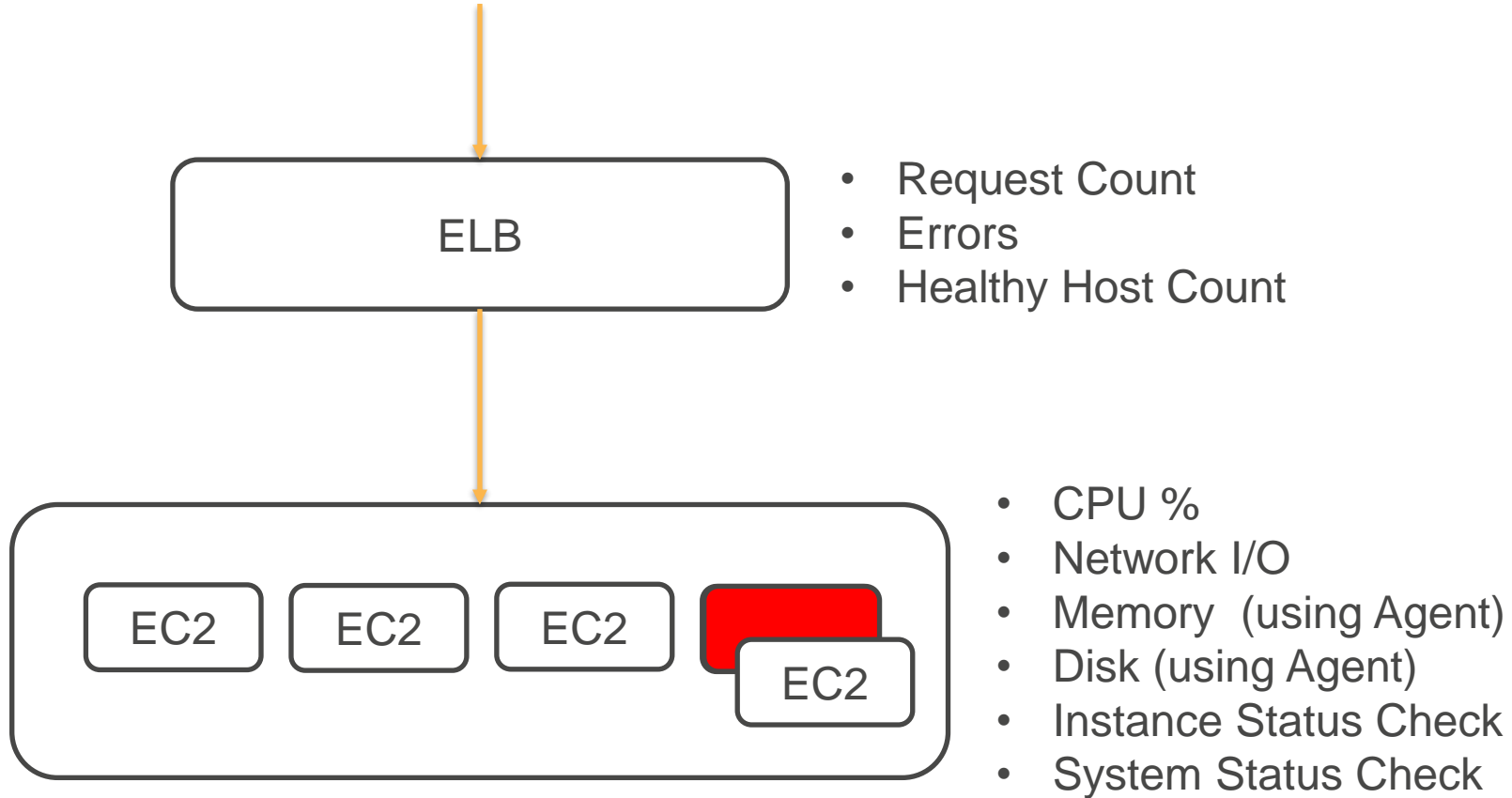
Monitoring

| Service | Purpose | Use |
|-------------------|-------------------|--|
| CloudWatch | Monitoring | Monitor your resources Configure Alarms to alert Take automated action |
| CloudWatch Log | Monitor Logs | Monitor log files Publish Custom metrics from log file |
| CloudWatch Events | Real-time Changes | Detect and act Automated Code Build, Scheduled EBS Snapshots |
| CloudTrail | Audit Trail | Logs all activities and who performed those actions Useful for investigation, compliance monitoring |

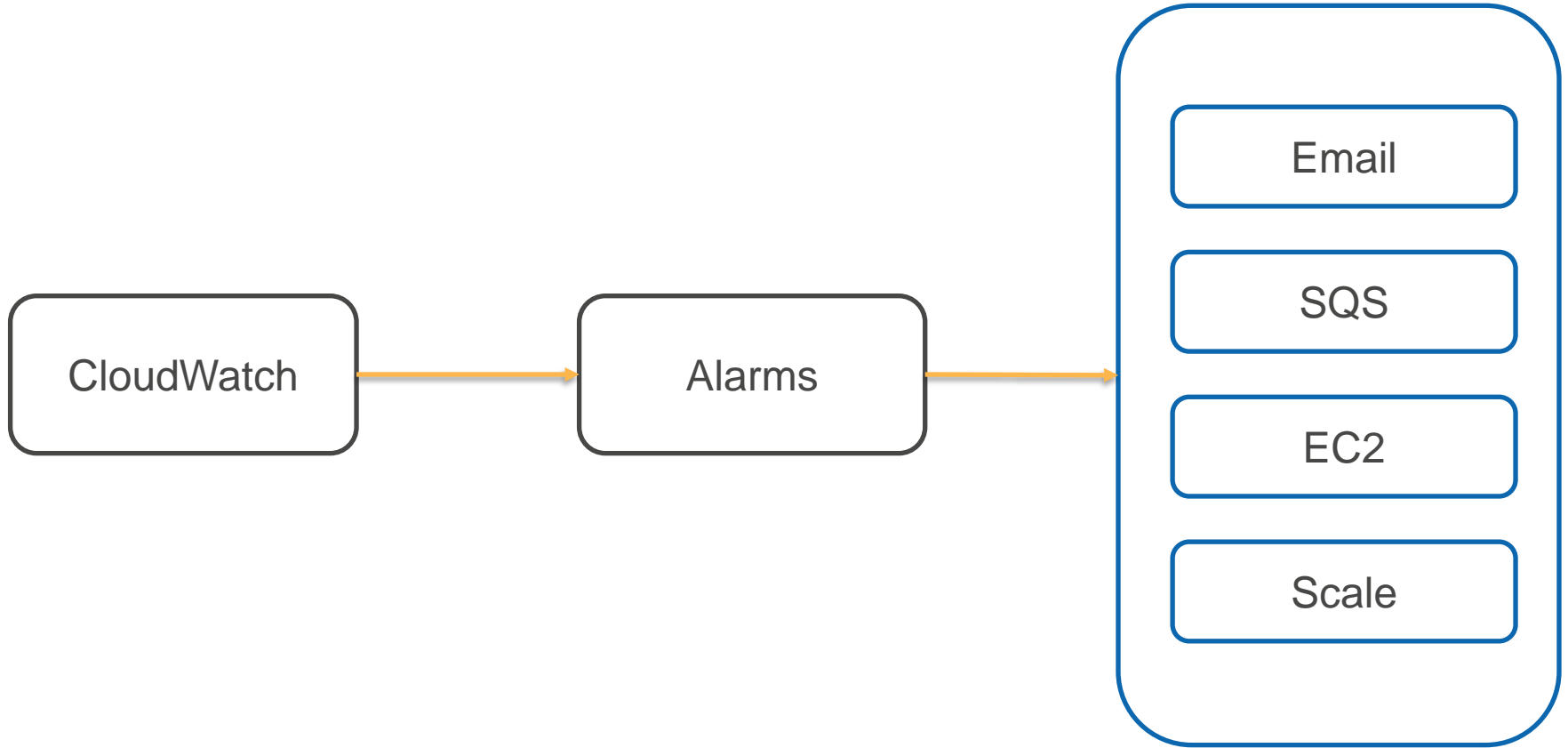
CloudWatch



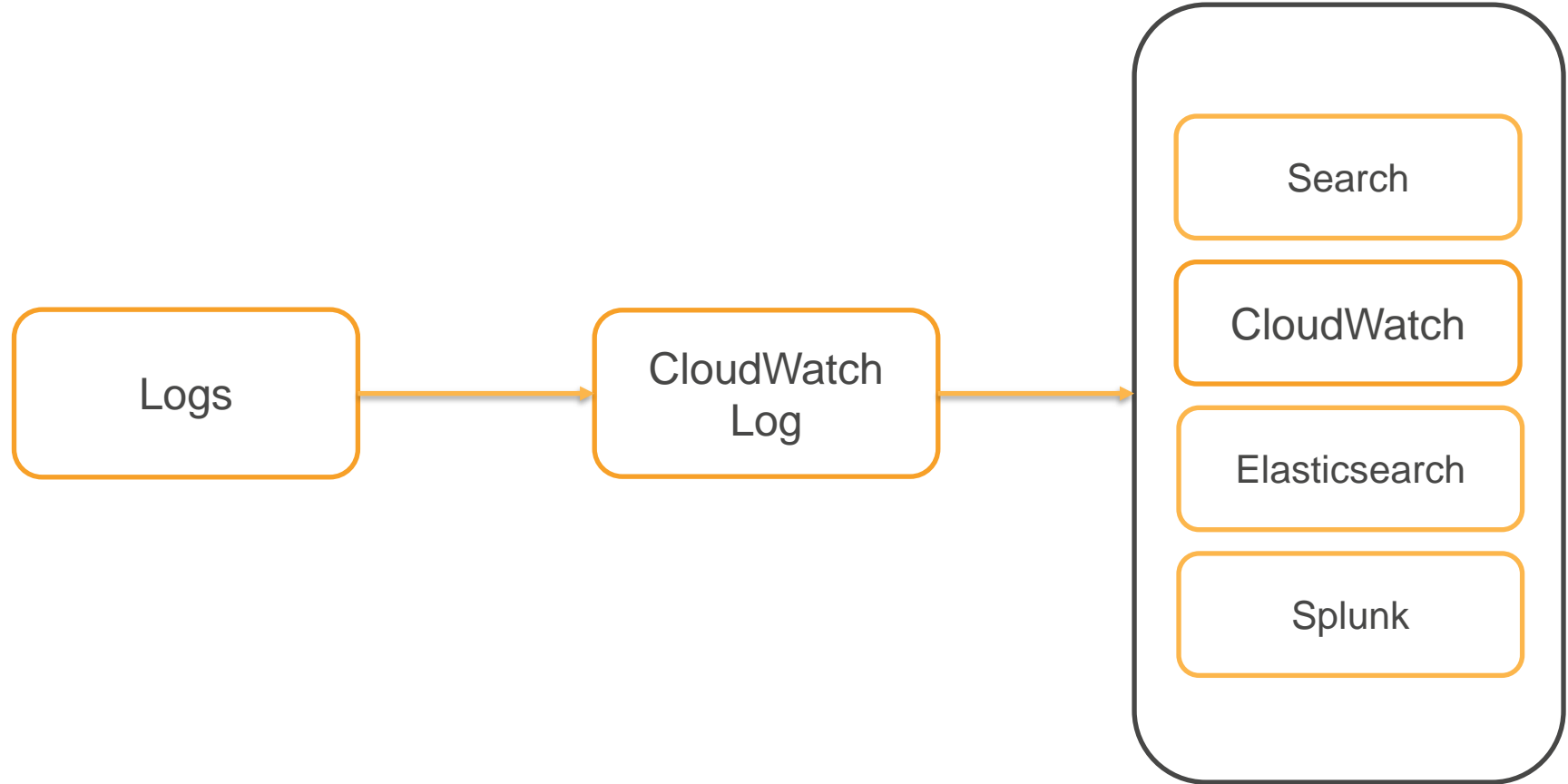
Elastic Load Balancer and EC2



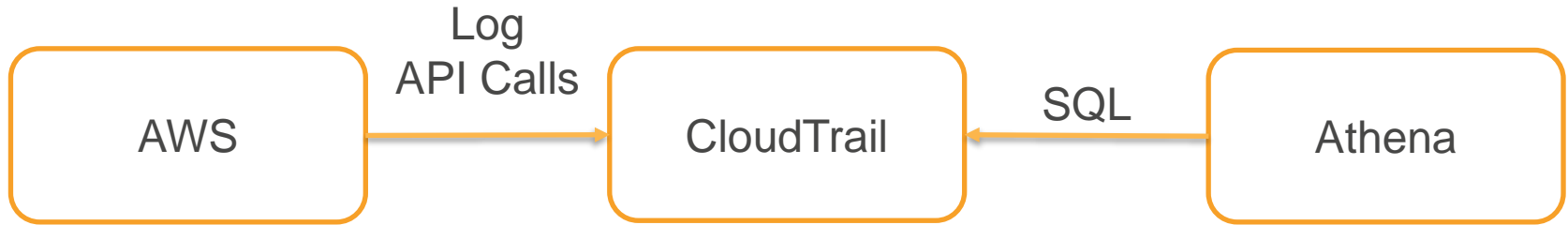
CloudWatch Alarms



CloudWatch Log – Consolidate Logs and Monitor



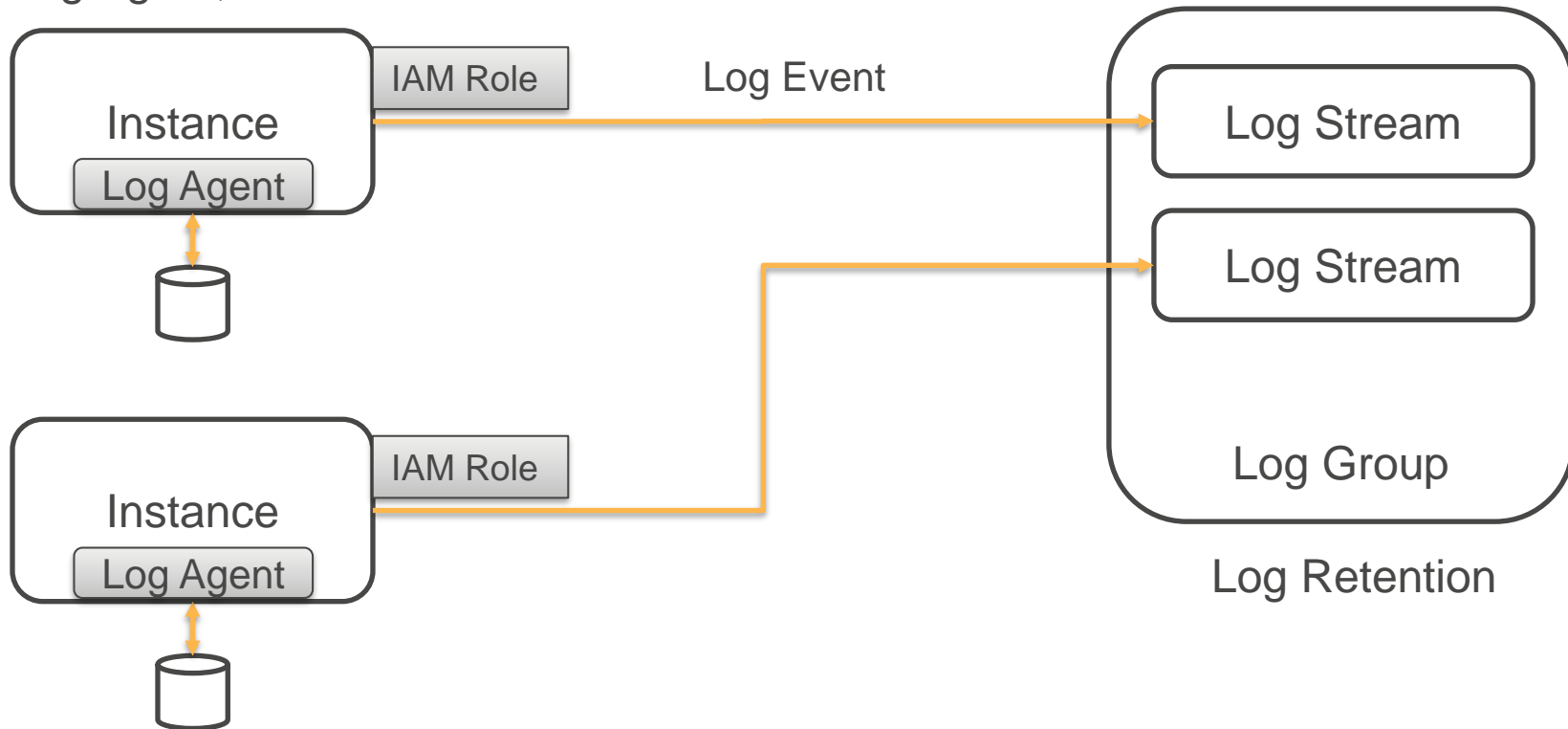
CloudTrail – Audit Trail of all API Activities



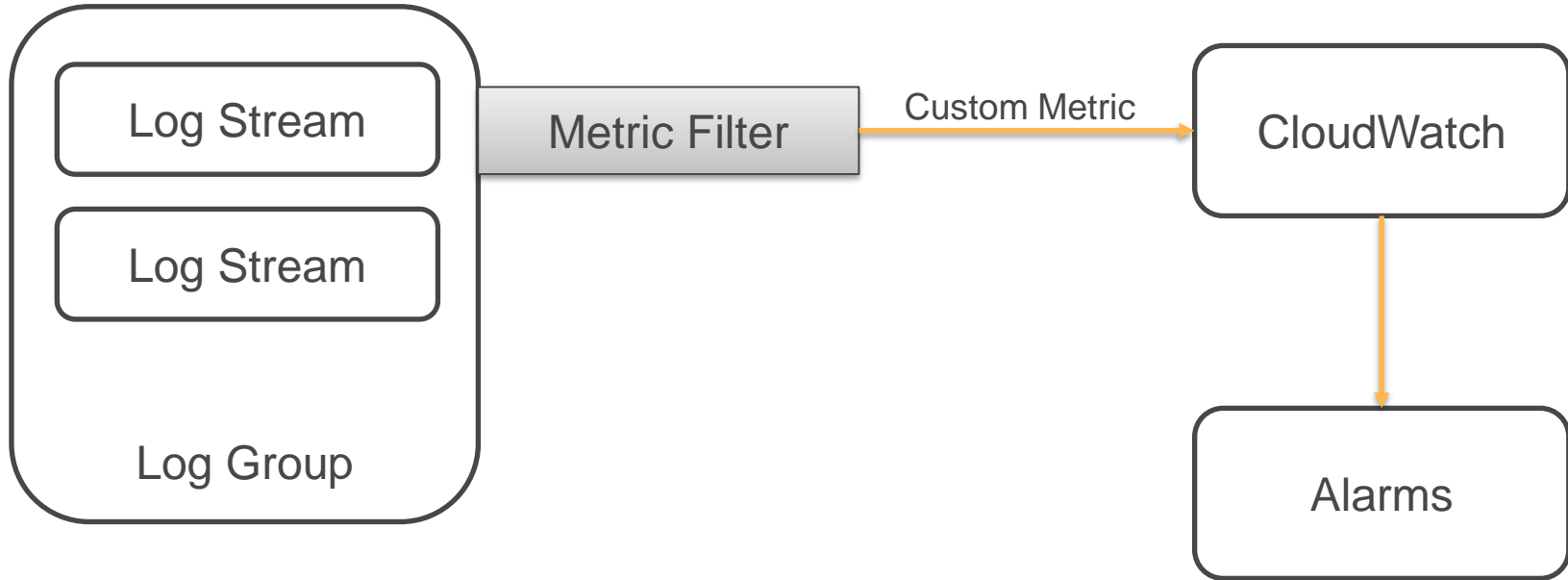
CloudWatch Logs

CloudWatch Log Architecture

Log Agent, SDK



CloudWatch Log Metric Filter



CloudWatch Logs

- Custom application and System log file monitoring capability
 - Monitor for specific terms, count of occurrence
 - Monitor logs from EC2 instance in Real-time
 - Monitor CloudTrail logs for specific events
 - Send to CloudWatch metric when match found
- CloudWatch Log Agent collects log from host and sends to log service – supports rotated and non-rotated files
- Archive Log data to highly durable storage with log retention setting and access when you need it

CloudWatch Terminologies

- Log Events
- Log Streams
- Log Groups
- Metric Filter
- Retention Settings

Log Events

- Activity recorded by an application or system
 - TimeStamp when event occurred
 - Event Message (UTF8 encoded)
- Logical record
- Example: Web server events, CloudTrail events

Log Stream

- Log Streams – Sequence of log events from the same source (application instance, resource)
- Example: Webserver log files on a specific host

Log Groups

- Group of Log Streams
- Shares the same retention, monitoring, and access control settings
- Each log stream belongs to one Log Group
- Fleet of servers generating same type of log

Metric Filters

- [Metric Filters](#) convert log file events to CloudWatch data points
- Specify patterns to look for
- Match Terms in: Text, JSON, Space-delimited Log Events
- Assigned to a Log Group
- Log Group can contain one or more metric filters

Retention Settings

- Specify retention period for events kept in CloudWatch logs
- Expired log events are deleted automatically
- Retention is applied to a Log Group which is in-turn applied to their log streams

Lab – Stop Idle Instance

Monitor CPU Utilization

Create Alarm

Stop the instance

90th percentile - CPU Utilization is less than 10% for 15 minutes

Lab – CloudWatch Logs

Log Group

Log Stream

Custom Metrics



Chandra Lingam

57,000+ Students



For AWS self-paced video courses, visit:

<https://www.cloudwavetraining.com/>

