§ Monitoring & Troubleshooting

Collect
Monitor
Analyze
} applications health.

Cloudwatch
- Metrics
- Logs
- Agent
- Alarm

① Cloudwatch Metrics

→ metric is a variable to monitor (CPU util, ...)

→ metrics belong to namespaces. { 1 namespace per service }

"dimension" is an attribute of a metric
{ instance id, env., etc. }

30 dim per metric

→ metrics have timestamp

→ dashboards from many metrics

* Can create custom metrics!

In EC2 if u enable detailed monitoring it has updates in 1 min (default every 5)

Metric Streams!

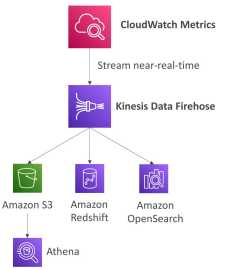
cstream cloudwatch metrics to a destination in near-real-time & low latency

using ① Kinesis data firehose KDF

or

3rd party Datadog, Dynatrace

Can filter metrics to only stream a subset of them



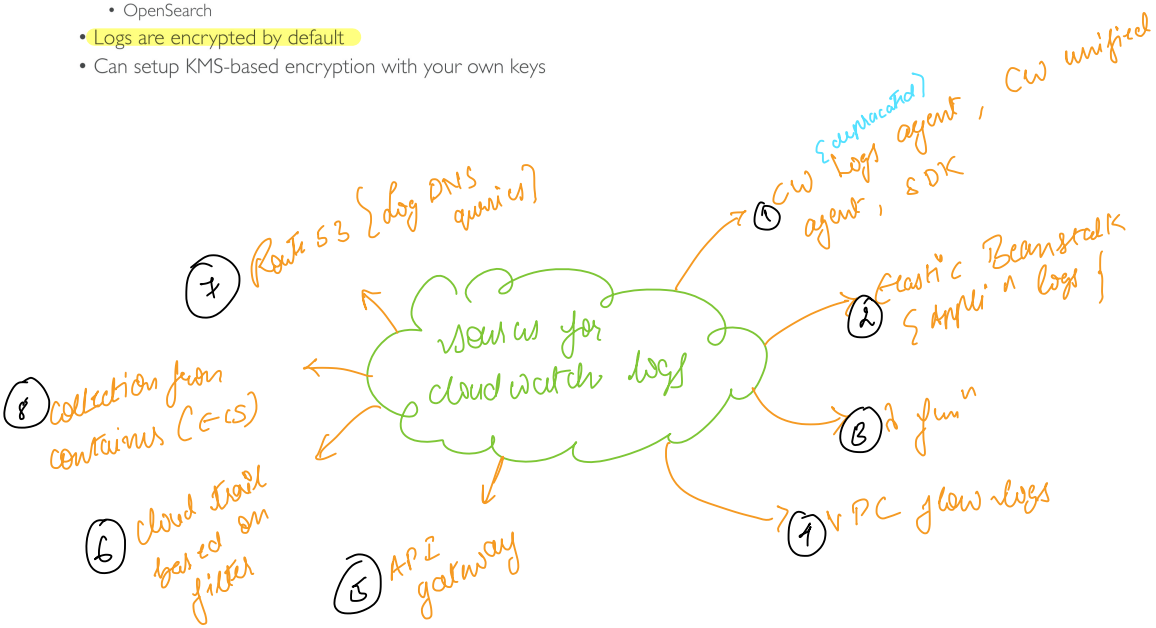
(2) Cloud Watch logs

CloudWatch Logs

→ to store application logs!

need to define

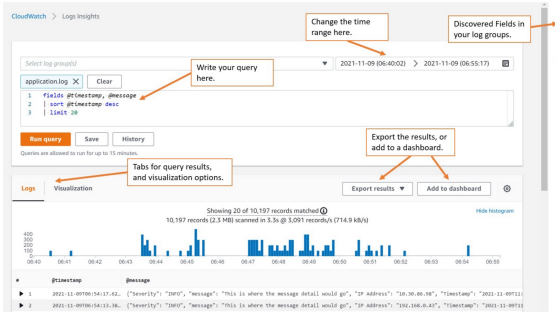
- **Log groups:** arbitrary name, usually representing an application
- **Log stream:** instances within application / log files / containers
- Can define log expiration policies (never expire, 1 day to 10 years…)
- CloudWatch Logs can send logs to:
  - Amazon S3 (exports)
  - Kinesis Data Streams
  - Kinesis Data Firehose
  - AWS Lambda
  - OpenSearch
- Logs are encrypted by default
- Can setup KMS-based encryption with your own keys



CloudWatch Logs Insights

query engine to query on historical data.

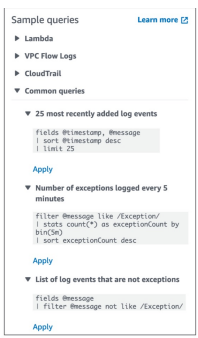
query on CW logs.



save queries.

https://mng.workshop.aws/operations-2022/detect/cwlogs.html

- Search and analyze log data stored in CloudWatch Logs
- Example: find a specific IP inside a log, count occurrences of "ERROR" in your logs…
- Provides a purpose-built query language
  - Automatically discovers fields from AWS services and JSON log events
  - Fetch desired event fields, filter based on conditions, calculate aggregate statistics, sort events, limit number of events…
  - Can save queries and add them to CloudWatch Dashboards
- Can query multiple Log Groups in different AWS accounts
- It's a query engine, not a real-time engine



Cloudwatch → export → S3 bucket

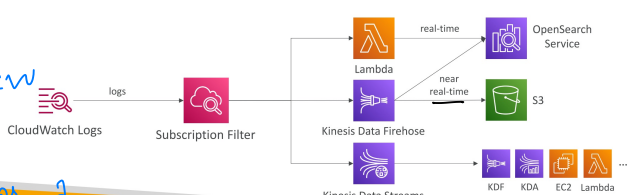
1. log data needs 12 hrs to be able to be uploaded
2. API call is called Create Export Task
3. Not real time or near-real-time bc its a batch export task instead → use "subscription!"

cloudwatch logs subscriptions

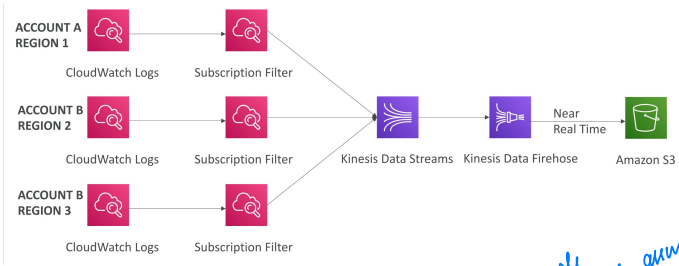
→ get real time log events from CW logs for processing & analysis.

→ send data to KDS, KDF or Amazon Managed Service for Apache Flink

→ filter based on which logs to be considered events } subscription filters



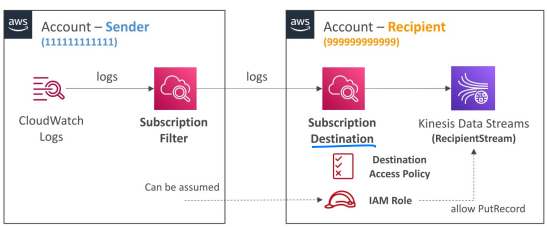
subscription filters allows cloudwatch logs in other regions or AWS account to log into a single account for analysis



the role can be assumed by the first account.

create IAM role in recipient acc. which has perm to send data into KDS

- Cross-Account Subscription – send log events to resources in a different AWS account (KDS, KDF)



IAM Role (Cross-Account)

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "kinesis:PutRecord",
      "Resource": "arn:aws:kinesis:us-east-1:
999999999999:stream/RecipientStream"
    }
  ]
}
```

to allow first acc to send data into dest

Destination Access Policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "111111111111"
      },
      "Action": "logs:PutSubscriptionFilter",
      "Resource": "arn:aws:logs:us-east-1:999999999999:
destination:testDestination"
    }
  ]
}
```

* log groups are populated with logs.

log groups: metric $set }

* create 2 subscription filters per group.

* log also has expiration.

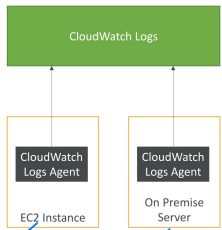
* create log stream & Live Tail to debug your application on a go.

Cloudwatch Agents

→ take logs from your EC2 instance to CW

CloudWatch Logs for EC2

- By default, no logs from your EC2 machine will go to CloudWatch
- You need to run a CloudWatch agent on EC2 to push the log files you want
- Make sure IAM permissions are correct
- The CloudWatch log agent can be setup on-premises too



CloudWatch Logs Agent & Unified Agent

- For virtual servers (EC2 instances, on-premises servers…)
- CloudWatch Logs Agent
  - Old version of the agent
  - Can only send to CloudWatch Logs
- CloudWatch Unified Agent → at more granular level
  - Collect additional system-level metrics such as RAM, processes, etc…
  - Collect logs to send to CloudWatch Logs
  - Centralized configuration using SSM Parameter Store for all agents.

CloudWatch Unified Agent – Metrics

- Collected directly on your Linux server / EC2 instance
- **CPU** (active, guest, idle, system, user, steal)
- **Disk metrics** (free, used, total), Disk IO (writes, reads, bytes, iops)
- **RAM** (free, inactive, used, total, cached)
- **Netstat** (number of TCP and UDP connections, net packets, bytes)
- **Processes** (total, dead, bloqued, idle, running, sleep)
- **Swap Space** (free, used, used %)

- Reminder: out-of-the box metrics for EC2 – disk, CPU, network (high level)

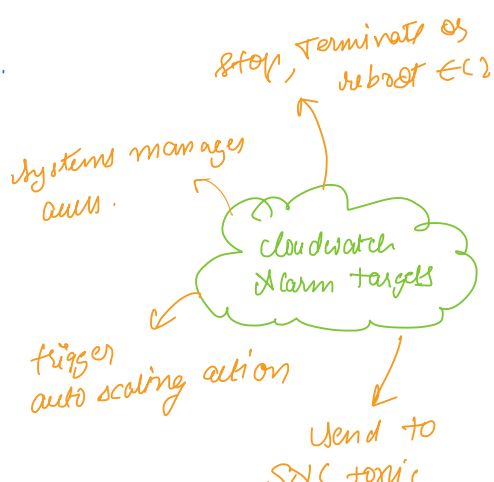
③ Cloudwatch Alarms → to trigger Notif. on metrics.

CloudWatch Alarms

- Alarms are used to trigger notifications for any metric
- Various options (sampling, %, max, min, etc…)
- Alarm States:
  - OK
  - INSUFFICIENT_DATA
  - ALARM

} states

- Period:
  - Length of time in seconds to evaluate the metric
  - High resolution custom metrics: 10 sec, 30 sec or multiples of 60 sec



Composite Alarms

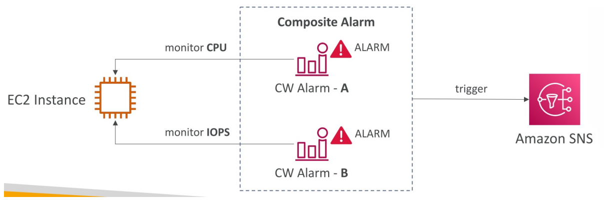
→ diff alarms for a single metric

→ put an alarm monitoring other alarms. {using AND OR}

→ reduce "alarm noise"

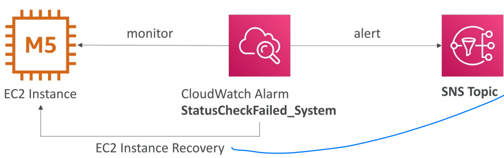
CPU(↑) OR Network(↑) → isme दोनो ज्यादा but

instead CPU(↑) AND Network(↓)



EC2 instance recovery

- Status Check:
  - Instance status = check the EC2 VM
  - System status = check the underlying hardware

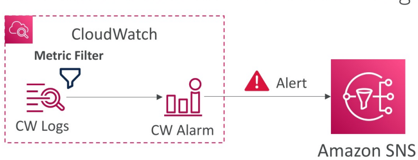


this will move EC2 inst. from one host to another.

- Recovery: Same Private, Public, Elastic IP, metadata, placement group

CloudWatch Alarm: good to know

- Alarms can be created based on CloudWatch Logs Metrics Filters



google karo

to test alarm set alarm state!

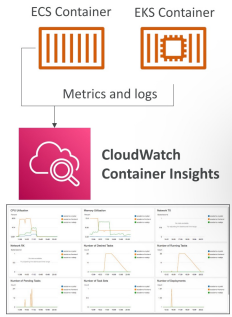
- To test alarms and notifications, set the alarm state to Alarm using CLI

```
aws cloudwatch set-alarm-state --alarm-name "myalarm" --state-value
ALARM --state-reason "testing purposes"
```

CloudWatch operational insights { Analysis }

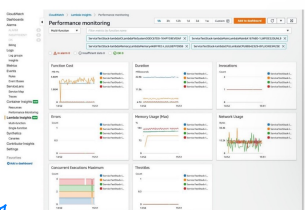
1 CloudWatch Container Insights

- Collect, aggregate, summarize metrics and logs from containers
- Available for containers on…
  - Amazon Elastic Container Service (Amazon ECS)
  - Amazon Elastic Kubernetes Services (Amazon EKS)
  - Kubernetes platforms on EC2
  - Fargate (both for ECS and EKS)
- In Amazon EKS and Kubernetes, CloudWatch Insights is using a containerized version of the CloudWatch Agent to discover containers



2 CloudWatch Lambda Insights

- Monitoring and troubleshooting solution for serverless applications running on AWS Lambda
- Collects, aggregates, and summarizes system-level metrics including CPU time, memory, disk, and network
- Collects, aggregates, and summarizes diagnostic information such as cold starts and Lambda worker shutdowns
- Lambda Insights is provided as a Lambda Layer

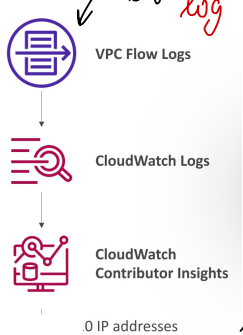


know more about lambda

create a dashboard to monitor ?

3 CloudWatch Contributor Insights

- Analyze log data and create time series that display contributor data.
  - See metrics about the top-N contributors
  - The total number of unique contributors, and their usage.
- This helps you find top talkers and understand who or what is impacting system performance.
- Works for any AWS-generated logs (VPC, DNS, etc..)
- For example, you can find bad hosts, identify the heaviest network users, or find the URLs that generate the most errors.
- You can build your rules from scratch, or you can also use sample rules that AWS has created – leverages your CloudWatch Logs
- CloudWatch also provides built-in rules that you can use to analyze metrics from other AWS services.



network logs

log contributors on insight lens

top contributor
top websites.

4 CloudWatch Application Insights

- Provides automated dashboards that show potential problems with monitored applications, to help isolate ongoing issues
- Your applications run on Amazon EC2 Instances with select technologies only (Java, .NET, Microsoft IIS Web Server, databases…)
- And you can use other AWS resources such as Amazon EBS, RDS, ELB, ASG, Lambda, SQS, DynamoDB, S3 bucket, ECS, EKS, SNS, API Gateway…
- Powered by SageMaker
- Enhanced visibility into your application health to reduce the time it will take you to troubleshoot and repair your applications
- Findings and alerts are sent to Amazon EventBridge and SSM OpsCenter

operating issue / resource

if there is some issue with our application CW will automatically put in automated dashboard.

Amazon EventBridge

Amazon EventBridge (formerly CloudWatch Events)

Event every 1 hour (scheduled pattern)

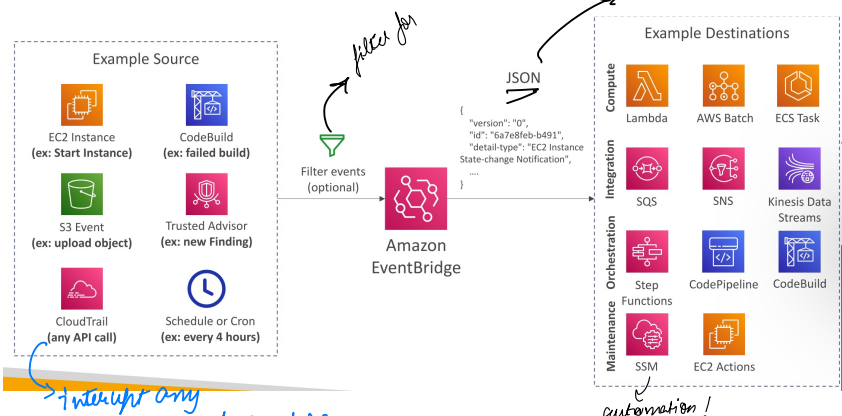
CRON → Command Run On Notice

- **Schedule**: Cron jobs (scheduled scripts)

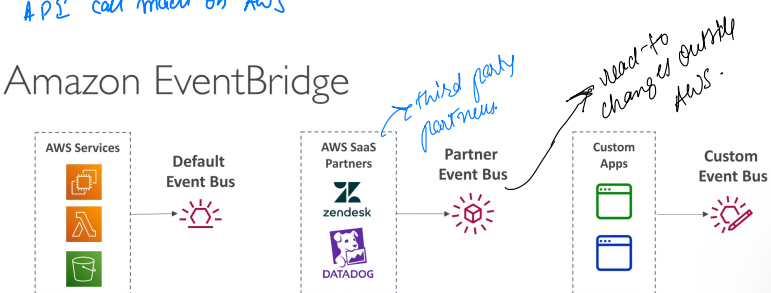
- **Event Pattern**: Event rules to react to a service doing something

- Trigger Lambda functions, send SQS/SNS messages…

Events are in JSON format!



Amazon EventBridge



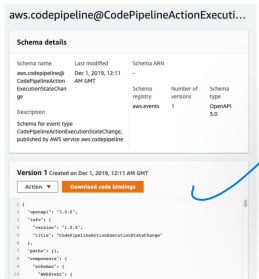
AWS service / Custom / Partner all events (Central bus)

- Event buses can be accessed by other AWS accounts using Resource-based Policies
- You can **archive events** (all/filter) sent to an event bus (indefinitely or set period) → retention
- Ability to replay archived events for trouble shooting & debugging.

suppose there is a bug in Lambda & we fix it replay events to check if the bug still there

Amazon EventBridge – Schema Registry

- EventBridge can analyze the events in your bus and infer the schema
- The Schema Registry allows you to generate code for your application, that will know in advance how data is structured in the event bus
- Schema can be versioned



this code will know how to infer the schema & structure the data out of the event bus.

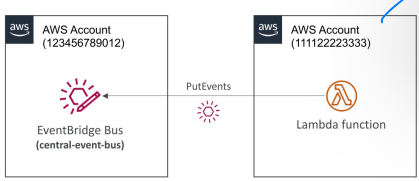
Amazon EventBridge – Resource-based Policy

own account capability for event buses.

- Manage permissions for a specific Event Bus
- Example: allow/deny events from another AWS account or AWS region
- Use case: aggregate all events from your AWS Organization in a single AWS account or AWS region

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "events:PutEvents",
            "Principal": { "AWS": "111122223333" },
            "Resource": "arn:aws:events:us-east-1:123456789012:
event-bus/central-event-bus"
        }
    ]
}
```

Allow **events** from another AWS account



other account to put events into event bus using this policy.

central event bus in a specific region & account.

* default event bus is created already in an AWS acc.

- CloudWatch Container Insights
  - ECS, EKS, Kubernetes on EC2, Fargate, needs agent for Kubernetes
  - Metrics and logs
- CloudWatch Lambda Insights
  - Detailed metrics to troubleshoot serverless applications
- CloudWatch Contributors Insights
  - Find "Top-N" Contributors through CloudWatch Logs
- CloudWatch Application Insights
  - Automatic dashboard to troubleshoot your application and related AWS services

AWS CloudTrail

Global Service

→ to gain governance, compliance & audit

→ default enabled

→ gives history of events & API calls within the AWS account by console, SDK, CLI, or other services

→ cloudtrail ⟹ CW logs
or
⟹ S3

→ trail can be applied to All regions (by default) or a single region

→ we can get to bottom of any event {who did what & when}

CloudTrail Events

(1) Management Events:
- Operations that are performed on resources in your AWS account
- Examples:
  - Configuring security (IAM `AttachRolePolicy`)
  - Configuring rules for routing data (Amazon EC2 `CreateSubnet`)
  - Setting up logging (AWS CloudTrail `CreateTrail`)
- By default, trails are configured to log management events.
- Can separate Read Events (that don't modify resources) from Write Events (that may modify resources)

* Read events → listing users, listing policies
* write events → delete table

↳ destructive

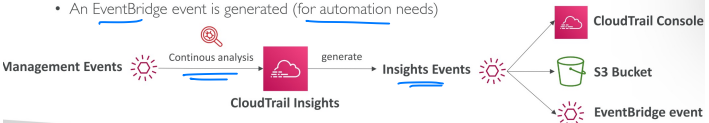
(2) Data Events:
- By default, data events are not logged (because high volume operations)
- Amazon S3 object-level activity (ex: `GetObject`, `DeleteObject`, `PutObject`): can separate Read and Write Event
- AWS Lambda function execution activity (the `Invoke` API)

(3) CloudTrail Insights Events:
- See next slide ☺

when we have so many management events & API calls then keeping track will be cumbersome.
so use CT insights!
{ . need to enable
. pay

CloudTrail Insights

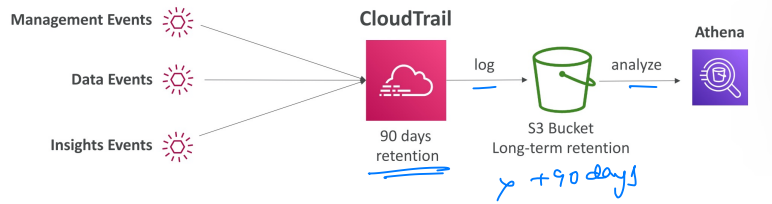
- Enable CloudTrail Insights to detect unusual activity in your account:
  - inaccurate resource provisioning
  - hitting service limits
  - Bursts of AWS IAM actions
  - Gaps in periodic maintenance activity
- CloudTrail Insights analyzes normal management events to create a baseline
- And then continuously analyzes write events to detect unusual patterns
  - Anomalies appear in the CloudTrail console
  - Event is sent to Amazon S3
  - An EventBridge event is generated (for automation needs)



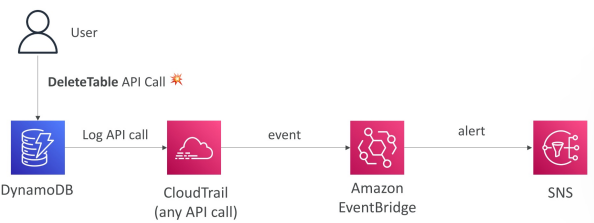
CloudTrail Events Retention

Let say we need to audit some events that happened an year ago.

- Events are stored for 90 days in CloudTrail (default)
- To keep events beyond this period, log them to S3 and use Athena

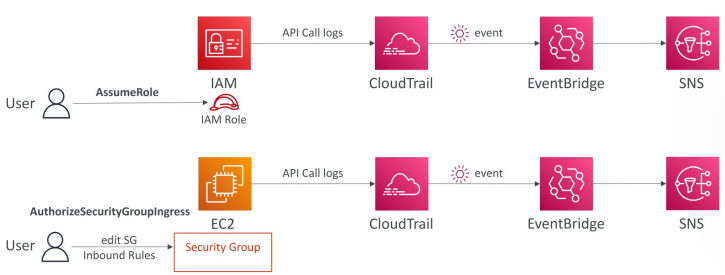


Cloud trail integration with eventbridge



* Intercepting API calls!

Amazon EventBridge + CloudTrail



* cloudtrail → Auditing security to Analyze "who" performed "what" actions & "when" on your resource

AWS Config

→ helps with auditing & recording compliance of AWS resources on some rules which we set.

→ record configurations & their changes over time to quickly be able to rollback and figure out what went wrong in the infrastructure

AWS Config

- Helps with auditing and recording **compliance** of your AWS resources
- Helps record configurations and changes over time
- Questions that can be solved by AWS Config:
  - Is there unrestricted SSH access to my security groups?
  - Do my buckets have any public access?
  - How has my ALB configuration changed over time?
- You can receive alerts (SNS notifications) for any changes
- AWS Config is a per-region service
- Can be aggregated across regions and accounts
- Possibility of storing the configuration data into S3 (analyzed by Athena)

→ checks these rules are compliant or not we can receive alert for any change

→ need to config. for all regions if need to 3

Config Rules

- Can use AWS managed config rules (over 75)
- Can make custom config rules (must be defined in AWS Lambda)
  - Ex: evaluate if each EBS disk is of type gp2
  - Ex: evaluate if each EC2 instance is t2.micro
- Rules can be evaluated / triggered:
  - For each config change
  - And / or: at regular time intervals
- AWS Config Rules does not prevent actions from happening (no deny)

→ they are just for compliance, they cannot react to them & prevent them.
→ gives overview & compliance of our resources.

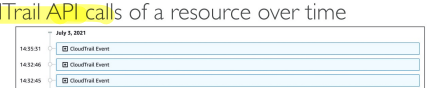
- Pricing: no free tier, $0.003 per configuration item recorded per region, $0.001 per config rule evaluation per region

AWS Config Resource

- View compliance of a resource over time

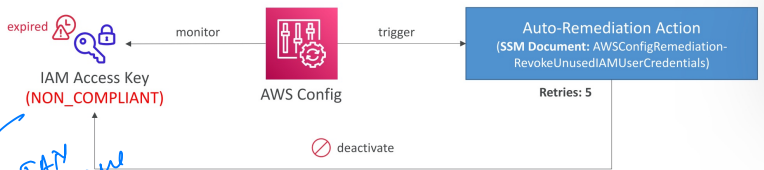
- View configuration of a resource over time

- View CloudTrail API calls of a resource over time



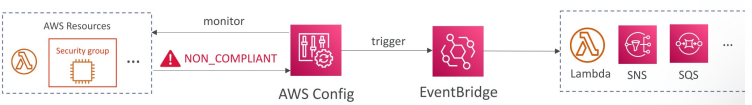
Config Rules – Remediations

- Automate remediation of non-compliant resources using SSM Automation Documents
- Use AWS-Managed Automation Documents or create custom Automation Documents
  - Tip: you can create custom Automation Documents that invokes Lambda function
- You can set **Remediation Retries** if the resource is still non-compliant after auto-remediation



Config Rules – Notifications

- Use EventBridge to trigger notifications when AWS resources are non-compliant



- Ability to send configuration changes and compliance state notifications to SNS (all events – use SNS Filtering or filter at client-side)

CloudWatch vs CloudTrail vs Config

- CloudWatch
  - Performance monitoring (metrics, CPU, network, etc…) & dashboards
  - Events & Alerting
  - Log Aggregation & Analysis
- CloudTrail
  - Record API calls made within your Account by everyone
  - Can define trails for specific resources
  - Global Service
- Config
  - Record configuration changes
  - Evaluate resources against compliance rules
  - Get timeline of changes and compliance

For an Elastic Load Balancer

- CloudWatch:
  - Monitoring Incoming connections metric
  - Visualize error codes as % over time
  - Make a dashboard to get an idea of your load balancer performance
- Config:
  - Track security group rules for the Load Balancer
  - Track configuration changes for the Load Balancer
  - Ensure an SSL certificate is always assigned to the Load Balancer (compliance)
- CloudTrail:
  - Track who made any changes to the Load Balancer with API calls