Training Course

Amazon Web Service

Module 9:

CloudWatch

Module 9: CloudWatch

- **Goal**: Understanding Monitoring in AWS
  - ✓ CloudWatch
  - ✓ CloudTrail
  - ✓ AWS Config

  Lab: Create and configuring Monitoring

AWS CloudWatch Metrics

- CloudWatch provides metrics for every services in AWS
- Metric is a variable to monitor (CPUUtilization, NetworkIn…)
- Metrics belong to namespaces
- Dimension is an attribute of a metric (instance id, environment, etc…)
- Up to 10 dimensions per metric
- Metrics have timestamps
- Can create CloudWatch dashboards of metrics

AWS CloudWatch EC2 Detailed monitoring

- EC2 instance metrics have metrics “every 5 minutes”
- With detailed monitoring (for a cost), you get data “every 1 minute”
- Use detailed monitoring if you want to more promt scale your ASG!
- The AWS Free Tier allows us to have 10 detailed monitoring metric
- Note: EC2 Memory usage is by default not pushed (must be pushed from inside the instance as a custom metric)

AWS CloudWatch Custom Metrics

- Possibility to define and send your own custom metrics to CloudWatch
- Ability to use dimensions (attiributes) to segment metrics
  - Instance.id
  - Environment.name
- Metric resolution (StorageResolution API parameter – two possible value)
  - Standard: 1 minute (60 seconds)
  - High Resolution: 1 second – Higher cost
- Use API call **PutMetricData**
- Use exponential back off in case of throttle errors

CloudWatch Dashboards

- Great way to setup dashboards for quick access to keys metrics
- Dashboards are global
- Dashboards can include graphs from different regions
- You can change the time zone & time range of the dashboards
- You can setup automatic refresh (10s, 1m, 2m, 5m, 15m)
- Pricing
  - 3 dashboards (up to 50 metrics) for free
  - $3/dashboard/month afterwards

AWS CloudWatch Logs

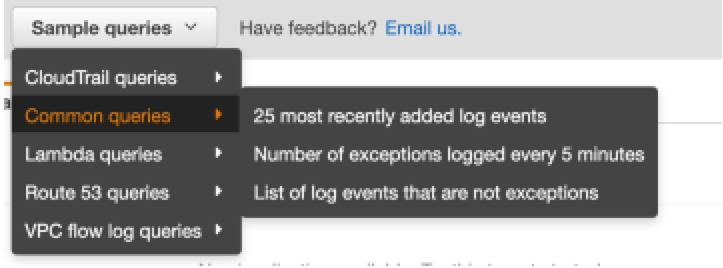
- Applications can send logs to CloudWatch using the SDK
- CloudWatch can collect log from
  - Elastic Beanstalk: collection of logs from application
  - EC2: collection from containers
  - AWS Lambda: collection from function logs
  - VPC Flow Logs: VPC specific logs
  - API Gateway
  - CloudTrail based on filter
  - CloudWatch Log agents: for example on EC2 machines
  - Route53: Log DNS queries
- CloudWatch logs can go to: Batch exporter to S3 or Stream to ElasticSearch

AWS CloudWatch Logs

- Logs storage architecture
  - Log groups: arbitrary name, usually representing an application
  - Log stream: instances within application / log files / container
- Can define log expiration policies (never expire, 30 days, etc…)
- Using the AWS CLI we can tail CloudWatch logs
- To send logs to CloudWatch, make sure IAM permissions are correct!
- Security: encryption of logs using KMS at the Group Level

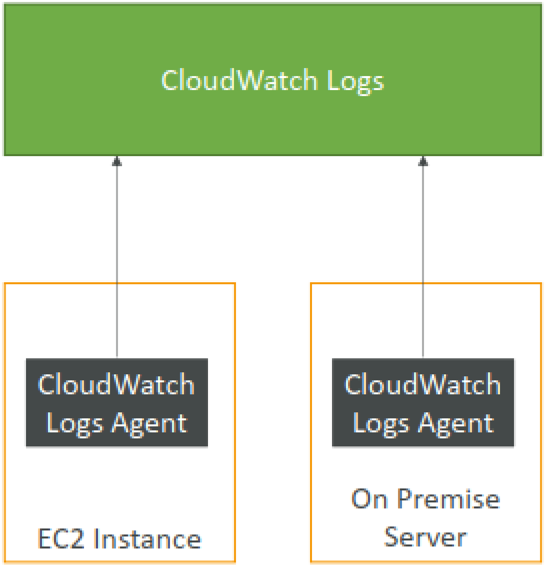
AWS CloudWatch Logs Metric Filter & Insights

- CloudWatch Logs can use filter expressions
  - For example, find a specific IP inside of a log
  - Metric filters can be used to trigger alarms
- CloudWatch Logs Insights (new – Nov 2018) can be used to query logs and add queries to CloudWatch Dashboards



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-premise servers…)
- CloudWatch Logs Agent
  - Old version of the agent
  - Can only send to CloudWatch Logs
- CloudWatch Unified Agent
  - Collect additional system-level metrics such as RAM, processes, etc…
  - Collect logs to send to CloudWatch Logs
  - Centralized configuration using SSM Parameter Store

CloudWatch Unified Agent - Metrics

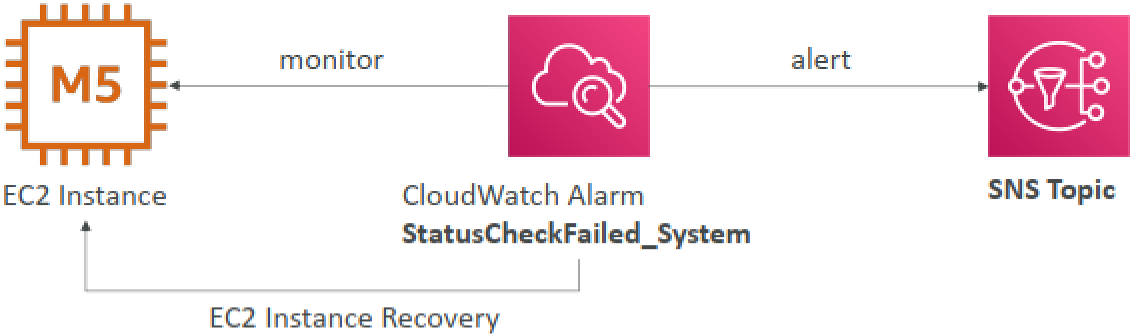
- Collected directly on your Linux server/ EC2 instance
- CPU (active, guest, idle, system, user, steal)
- Disk metrics (free, used, total), Disk IO (writes, reads, bytes, iops)
- RAM (free, inactive, used, total, cached)
- Netstat (number of TCP and UDP connections, net packets, bytes)
- Processes (total,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

AWS CloudWatch Alarm

- Alarms are used to trigger notifications for any metric
- Alarms can go to Auto Scaling, EC2 actions, SNS notifications
- Various options (sampling,%, max,min, etc…)
- Alarm States
  - OK
  - INSUFFICIENT_DATA
  - ALARM
- Period
  - Length of time in seconds to evaluate the metric
  - High resolution custom metrics: can only choose 10 sec or 30 sec

EC2 Instance Recovery

- Status Check
  - Instance status = check the EC2 VM
  - System status = check the underlying hardware
- Recovery: Same Private, Public, Elastic IP, metadata, placement group



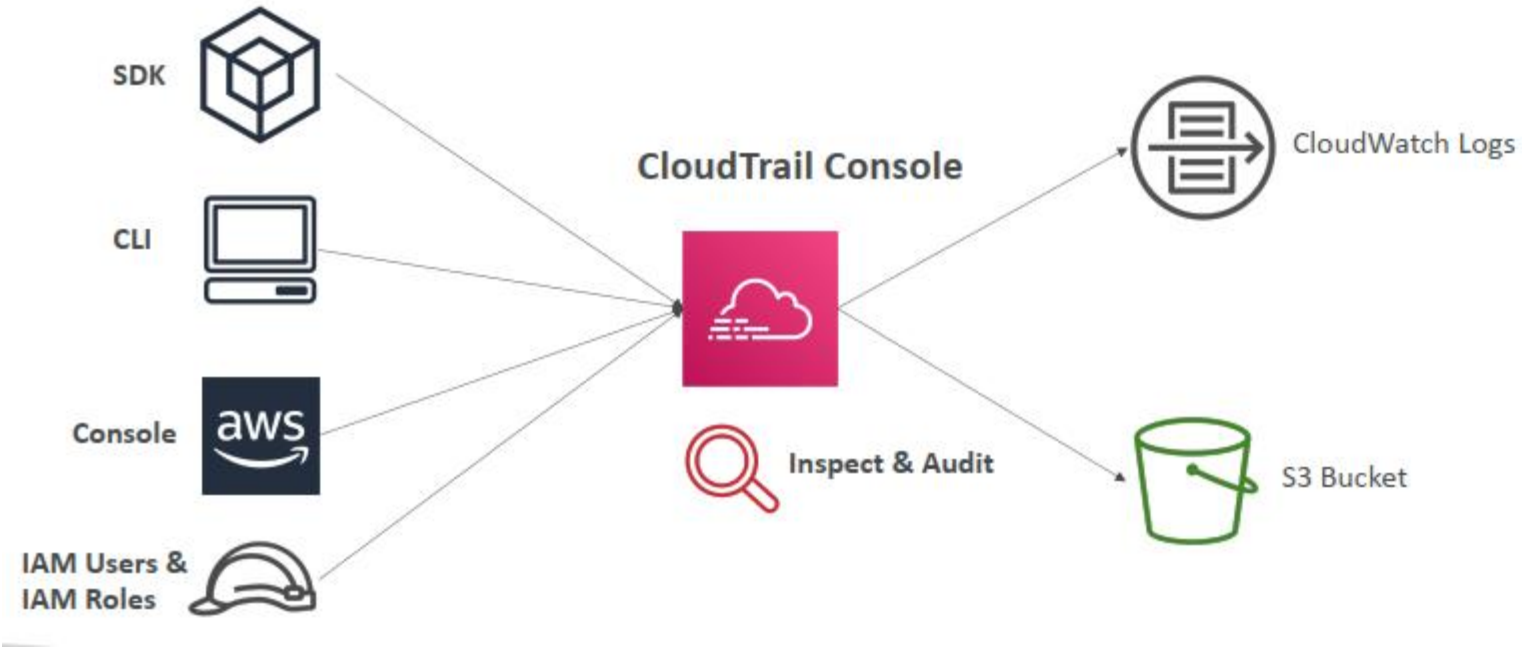
AWS CloudWatch Event

- Source + Rule => Target
- Schedule: Cron jobs
- Event Pattern: Event rules to react to a service doing something
  - Ex: CodePipeline state changes
- Triggers to Lambda functions, SQS/SNS/Kinesis Messages
- CloudWatch Event creates a small JSON document to give information about the change

AWS CloudTrail

- Provides governance, compliance and audit for your AWS Account
- CloudTrail is enabled by default
- Get an history of events/API calls made within your AWS Account by:
  - Console
  - SDK
  - CLI
  - AWS Services
- Can put logs from CloudTrail into CloudWatch Logs or S3
- A trail can be applied to All Region (default) or a single Region
- If a resource is deleted in AWS, investigate CloudTrail first

AWS CloudTrail Diagram

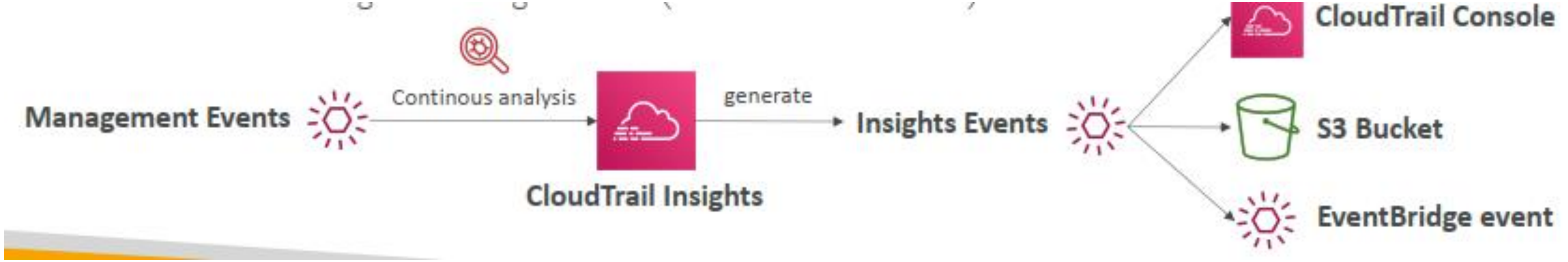


AWS CloudTrail Events

- Management Events
  - Operations that are performed on resources in your AWS account
  - Examples:
    - Configuring security (IAM Attach Role Policy)
    - Configuring rules for routing data (Amazon EC2 Create Subnet)
    - Setting up logging (AWS CloudTrail Create Trail)
  - 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)
- 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 Events
  - AWS Lambda function execution activity
- CloudTrail Insights Events
  - See next slide

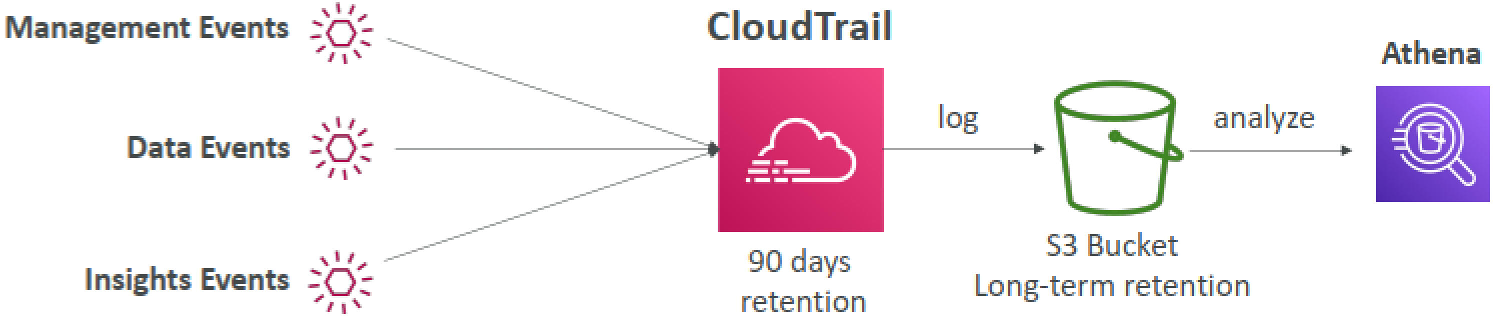
AWS CloudTrail Insights

- Enable CloudTrail Insights to detect unusual activity in your account
- CloudTrail Insight analyzes normal management events to create a baseline
- And then continuously analyzes write events to detect unusual patterns



AWS CloudTrail Events Retention

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

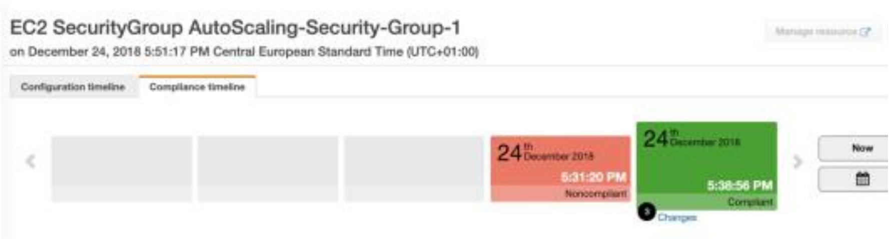


AWS Config

- Helps with auditing and recording compliance of your AWS resources
- Helps record configurations and changes over time
- Possibility of storing the configuration data into S3 (analyzed by Athena)
- 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 changesd over time?
- You can receive alerts (SNS notifications) for any changes
- AWS Config is a per- region service
- Can be aggreagated across regions and accounts

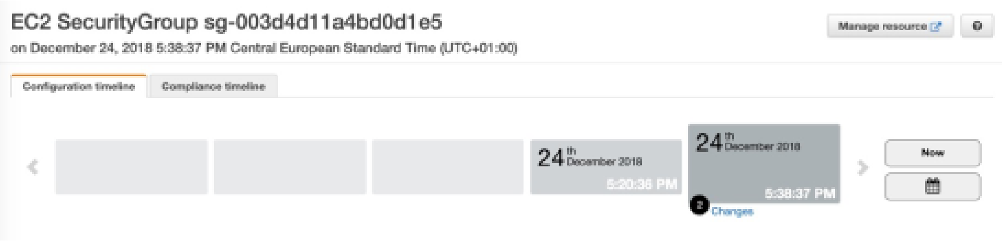
AWS Config Resource

- View compliance of a resource over time
- View configuration of a resource over time
- View CloudTrail API call if enabled



EC2 SecurityGroup AutoScaling-Security-Group-1

on December 24, 2018 5:51:17 PM Central European Standard Time (UTC+01:00)



EC2 SecurityGroup sg-003d4d11a4bd0d1e5

on December 24, 2018 5:38:37 PM Central European Standard Time (UTC+01:00)

AWS Config Rules

- Can use AWS managed config rules (over 75)
- Can make custom config rules (must be defined in AWS Lambda)
- Rules can be evaluated/ triggered
- Rules can hava auto remediations:
- AWS Config Rules does not prevent actions from happening (no deny
- Pricing: no free tier, $2 per active rule per region per month

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 resouces
  - 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

Thank you!!!