Cloud Monitoring

- Cloud Monitoring
  - Amazon CloudWatch
    - Important Metrics
    - Amazon CloudWatch Alarms
    - Amazon CloudWatch Logs
      - CloudWatch Logs for EC2
    - Amazon CloudWatch Events
    - Amazon EventBridge
  - AWS CloudTrail
    - CloudTrail Events
    - CloudTrail Insights Events
    - CloudTrail Events Retention
  - AWS X-Ray
    - AWS X-Ray advantages
  - Amazon CodeGuru
    - Amazon CodeGuru Reviewer
    - Amazon CodeGuru Profiler
  - AWS Status - Service Health Dashboard
  - AWS Personal Health Dashboard
  - Cloud Monitoring Summary

Amazon CloudWatch

- A monitoring and observability service for AWS resources and applications.
- Enables real-time monitoring of AWS resources, applications, and custom metrics.
- Metric is a variable to monitor (CPUUtilization, NetworkIn, etc..)
- Can create CloudWatch dashboards of metrics

Key Features:

- Collect and track metrics.
- Set alarms and take automated actions.
- Store and access logs for troubleshooting.

Important Metrics

- **EC2 Instances:** CPU utilization, disk I/O, network I/O.
  - Default metrics every 5 minutes
  - Option for Detailed Monitoring ($$$): metrics every 1 minute
- **EBS volumes**: Disk Read/Writes
- **RDS Databases:** CPU utilization, free storage space, read/write IOPS.
- **S3 Buckets:** Number of requests, latency, and errors., AllRequests
- **Lambda Functions:** Invocation count, error count, duration.
- **Billing**:Total Estimated Charge (only in us-east-1)
- **Service Limits**: how much you've been using a service API
- **Custom metrics**: push your own metrics

Amazon CloudWatch Alarms

- Trigger notifications or automated actions when a metric exceeds a threshold.
- Examples:
  - Send an alert if EC2 CPU utilization exceeds 80%.
  - Scale out EC2 instances based on demand.
  - EC2 Actions: stop, terminate, reboot or recover an EC2 instance
  - SNS notifications: send a notification into an SNS topic
- Various options (sampling, %, max, min, etc…)
- Example: create a billing alarm on the CloudWatch Billing metric
- Alarm States: OK. INSUFFICIENT_DATA, ALARM

Amazon CloudWatch Logs

- Centralized logging for AWS services and applications.
- CloudWatch Logs can collect log from:
  - Elastic Beanstalk: collection of logs from application

  - ECS: collection from containers
  - AWS Lambda: collection from function logs
  - CloudTrail based on filter
  - CloudWatch log agents: on EC2 machines or on-premises servers
  - Route53: Log DNS queries
- Enables real-time monitoring of logs
- Adjustable CloudWatch Logs retention

CloudWatch Logs for EC2

- By default, no logs from your EC2 instance 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

Amazon CloudWatch Events

- Delivers a stream of system events describing changes in AWS resources.
- Example: Trigger a Lambda function when an EC2 instance state changes.
- Schedule: Cron jobs (scheduled scripts)
  - Schedule Every hour => Trigger script on Lambda function
- Event Pattern: Event rules to react to a service doing something
  - IAM Root User Sign in Event => SNS Topic with Email Notification
- Trigger Lambda functions, send SQS/SNS messages

Amazon EventBridge

- EventBridge is the next evolution of CloudWatch Events
- Default event bus: generated by AWS services (CloudWatch Events)
- Partner event bus: receive events from SaaS service or applications (Zendesk, DataDog, Segment, Auth0…)
- Custom Event buses: for your own applications
- Schema Registry: model event schema
- EventBridge has a different name to mark the new capabilities
- The CloudWatch Events name will be replaced with EventBridge

AWS CloudTrail

- Tracks and logs API calls made in your AWS account for auditing and governance.
- Useful for security analysis, compliance, and operational troubleshooting.
- 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 Regions (default) or a single Region.
- If a resource is deleted in AWS, investigate CloudTrail first!

Key Features:

- Logs API calls across AWS services, including CLI, SDK, and Management Console.
- Tracks who made the call, when, and from where.

CloudTrail Events

- 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)
- 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 (the Invoke API)

CloudTrail Insights Events

- 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

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

AWS X-Ray

- Helps analyze and debug distributed applications by providing request tracing.
  - Test locally
  - Add log statements everywhere
  - Re-deploy in production

Key Features:

- Trace requests across AWS services and custom applications.
- Identify performance bottlenecks and errors.
- Visualize service maps to understand dependencies.

AWS X-Ray advantages

- Troubleshooting performance (bottlenecks)
- Understand dependencies in a microservice architecture
- Pinpoint service issues
- Review request behavior
- Find errors and exceptions
- Are we meeting time SLA?
- Where I am throttled?
- Identify users that are impacted

Amazon CodeGuru

- Code review and performance profiling service.
- Provides suggestions to improve the performance of applications.
- Identifies the most costly lines of applications.
- It is based on machine learning models long used at Amazon.
- Identifies code errors and risks with automatic code reviews.
- CodeGuru Reviewer: automated code reviews for static code analysis (development)
- CodeGuru Profiler: visibility/recommendations about application performance during runtime (production)

Amazon CodeGuru Reviewer

- Uses machine learning to identify:
  - Security vulnerabilities.
  - Code inefficiencies.
  - Best practices violations.
- Provides recommendations to improve code quality.
- Supports Java and Python
- Integrates with GitHub, Bitbucket, and AWS CodeCommit

Amazon CodeGuru Profiler

- Helps understand the runtime behavior of your application
- Example: identify if your application is consuming excessive CPU capacity on a logging routine
- Features:
  - Identify and remove code inefficiencies
  - Improve application performance (e.g., reduce CPU utilization)
  - Decrease compute costs
  - Provides heap summary (identify which objects using up memory)
  - Anomaly Detection
- Support applications running on AWS or on- premise
- Minimal overhead on application

AWS Status - Service Health Dashboard

- Service Health Dashboard is the single place to learn about the availability and operations of AWS services.
- You can view the overall status of AWS services, and you can sign in to view personalized communications about your particular AWS account or organization.
- Shows all regions, all services health
- Shows historical information for each day
- Has an RSS feed you can subscribe to
- https://status.aws.amazon.com/

AWS Personal Health Dashboard

- AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact you.
- While the Service Health Dashboard displays the general status of AWS services, Personal Health Dashboard gives you a personalized view into the performance and availability of the AWS services underlying your AWS resources.
- The dashboard displays relevant and timely information to help you manage events in progress and provides proactive notification to help you plan for scheduled activities.
- Global service https://phd.aws.amazon.com/
- Shows how AWS outages directly impact you & your AWS resources
- Alert, remediation, proactive, scheduled activities

Cloud Monitoring Summary

Service	Key Features
Amazon CloudWatch	Metrics, Alarms, Logs, Events, EventBridge. - Metrics: monitor the performance of AWS services and billing metrics - Alarms: automate notification, perform EC2 action, notify to SNS based on metric - Logs: collect log files from EC2 instances, servers, Lambda functions… - Events (or EventBridge): react to events in AWS, or trigger a rule on a schedule
AWS CloudTrail	Tracks API calls, detects unusual activity.
CloudTrail Insights	automated analysis of your CloudTrail Events
AWS X-Ray	Trace requests made through your distributed applications
Amazon CodeGuru	automated code reviews and application performance recommendations
Service Health Dashboard	status of all AWS services across all regions
Personal Health Dashboard	AWS events that impact your infrastructure