Monitering

**Amazon CloudWatch**

* CloudWatch provides metrics for every services in AWS
* Metric is a variable to monitor (CPUUtilization, NetworkIn, etc..)
* Metrics have timestamps
* Can create CloudWatch dashboards of metrics

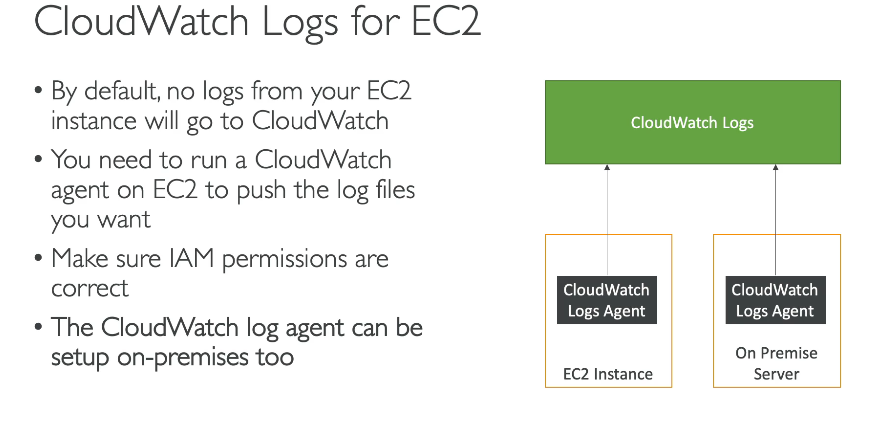
**Important Metrics**

* EC2 instances: CPU Utilization, Status Checks, Network (not RAM)
  + Default metrics every 5 minutes
  + Option for Detailed Monitoring ($$$): metrics every 1 minute
* EBS volumes: Disk Read/Writes
* S3 buckets: BucketSizeBytes, NumberOfObjects, AllRequests
* 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**

* Alarms are used to trigger notifications for any metric
* Alarms actions…
  + Auto Scaling: increase or decrease EC2 instances “desired” count
  + 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…)
* Can choose the period on which to evaluate an alarm
* Example: create a billing alarm on the CloudWatch Billing metric
* Alarm States: OK. INSUFFICIENT\_DATA, ALARM

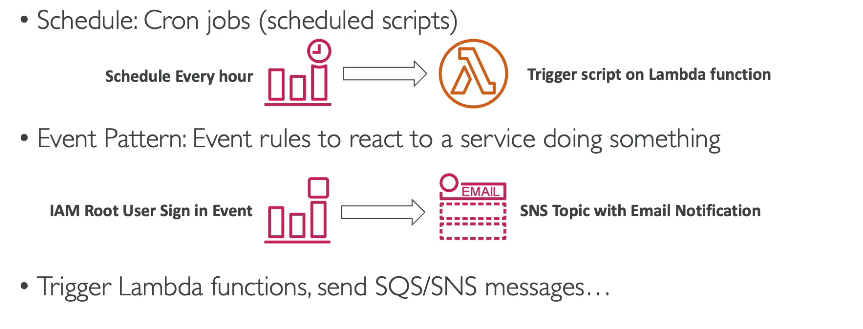
**Amazon CloudWatch Logs**

* 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
* 



**Amazon CloudWatch Events**

* 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



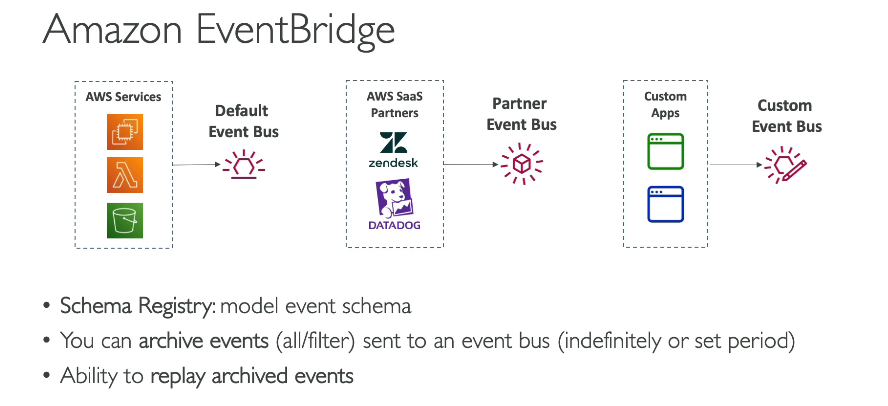
**AWS X-Ray{** n short, X-Ray is like a detective for your application. It helps you identify problems quickly and efficiently, keeping your application running smoothly and your users happy.}

* Debugging in Production, the good old way:
  + Test locally
  + Add log statements everywhere
  + Re-deploy in production
* Log formats differ across applications and log analysis is hard.
* Debugging: one big monolith “easy”, distributed services “hard”
* No common views of your entire architecture

**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 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 Event Bridge
* 

**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:((tracks your aws account))
  + 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!

**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**

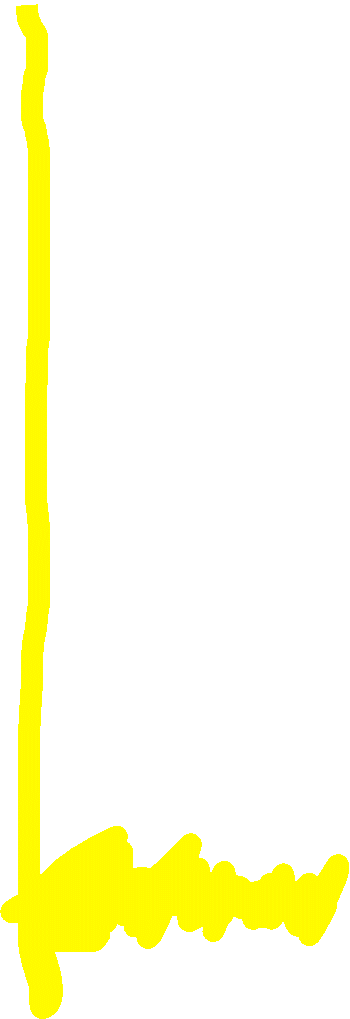
* Events are stored for 90 days in CloudTrail
* To keep events beyond this period, log them to S3 and use Athena

**CloudTrail Eventsoptianal**

* 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)

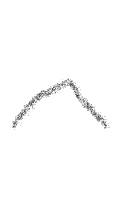
**CloudTrail Insights Events**

* Enable CloudTrail Insights to detect unusual activity in your account:
  + inaccurate resource provisioning

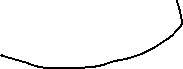


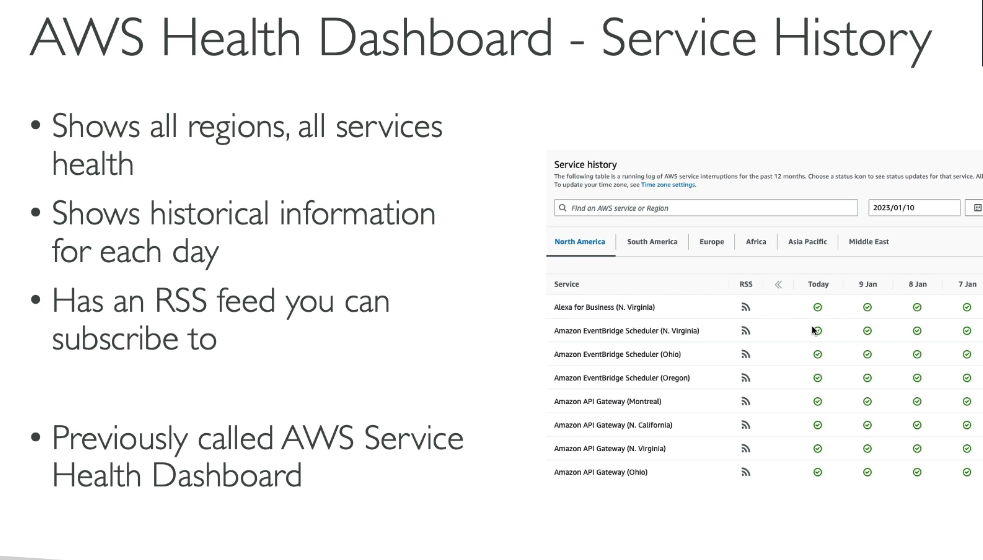
* + hitting service limits
  + Bursts of AWS IAM actions
  + Gaps in periodic maintenance activity
* CloudTrail Insights analyzes normal management events to create a baseline
* And then continuously analyzes write events to detect unusual patterns
  + Anomalies appear in the CloudTrail console
  + Event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

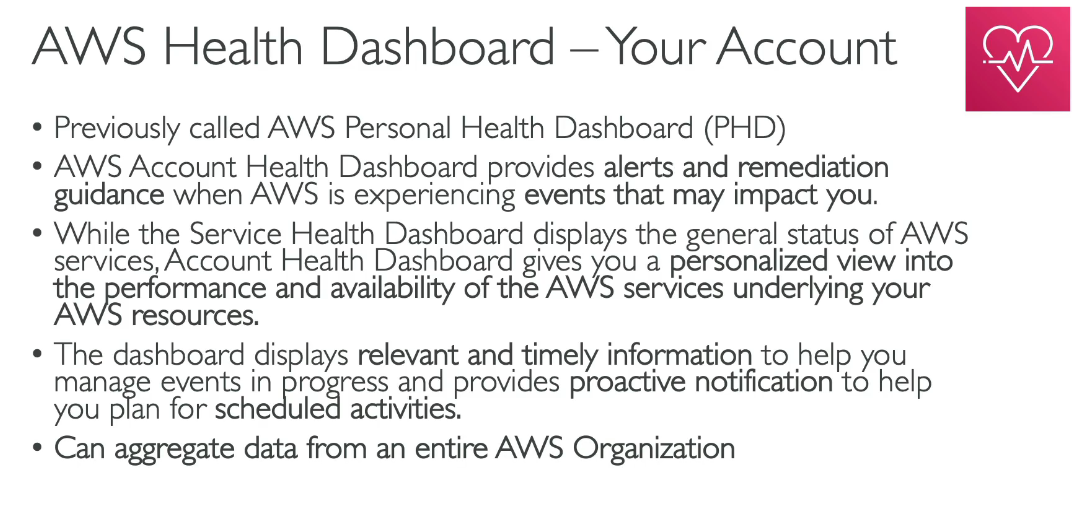
**CloudTrail Events Retention**

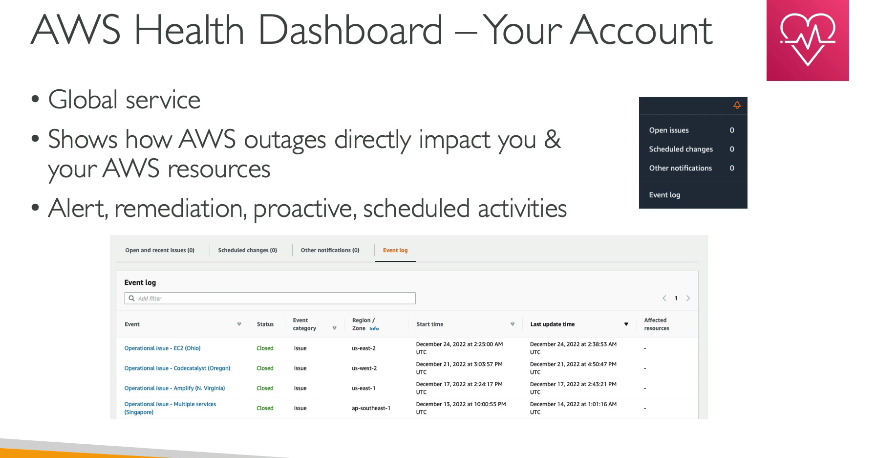
* Events are stored for 90 days in CloudTrail
* To keep events beyond this period, log them to S3 and use Athena

Just read









is a valuable tool for monitoring the health of your specific AWS account.