Logging Services

Cloud Trail- Logs all API calls (SDK, CLI) between AWS service (who can we blame)

CloudWatch-Collection of multiple services

CW Logs-A centralized place to store your cloud services log data or application logs
CW Metrics- Represents a time-ordered set of data points.
CW Events (Even bridge)-Trigger an event based on a condition
CW Alarms- Tiggers notification based on metrics
CW Dashboard- Create visualization based on metrics

AWS X-RAY is a distributed tracing system. We can use it to pin point issues within our microservices. See how data moves for one app to another, how long it took to move and if it failed to move forward.

Cloud Trail- Is a service that enables governance,compliance, operational aduting and risk audting of AWS account.

AWS Cloud trail is used to moniter API calls and Acionns made on AW account.
Easily identify which users and accounts made the call to AWS
Where-Souce if IP address
When-EventTime
Who-User, UserAgent
What-Region, Resouce, Action

It already logging by default and will collets logs for last 90 days via even history.
IF need more than 90 days we need to create a trail
Trails are output to s3 bucted and do not have GUI like Event history. To analyze we would need Amazon Athena.

Cloud Watch Alarm

Mointers a cloud wacth metric based on defined threshold.

Three states-
OK
Alarm
Inssuficent Dtat-
The alrm has just started
The metric is not available
Not enough data

We can define what action needs to taken when the state changes

Notification
ASG (Auto scaling group)
EC2 Action

Cloud Watch log

Log Streams- A log streams represent a sequence of events form a application or instance being monitered

We can crate log steams manually but generally this is automatically done by the service.

Log Events- Represents a single event in a log file. Log vents can be seen within a log stream. We can filter them as well.

Log Insights- Enables use to interactively search and analyze our cloud watch log data.
It supports all types of logs.
It is commonly used via the console to do the ad-hoc queries against logs groups.

It has it own language called Query syntax.
A single request can query up to 20 logs groups.

Queries time out after 15 minutes, if they have not completed
Queries are available for 7 days

CloudWatch Metrics-Represent a time-ordered set of data points it is a variable that is monitored over time. It come with predefined metrics eg EC2- CPU Utilization, DiskWriteOps