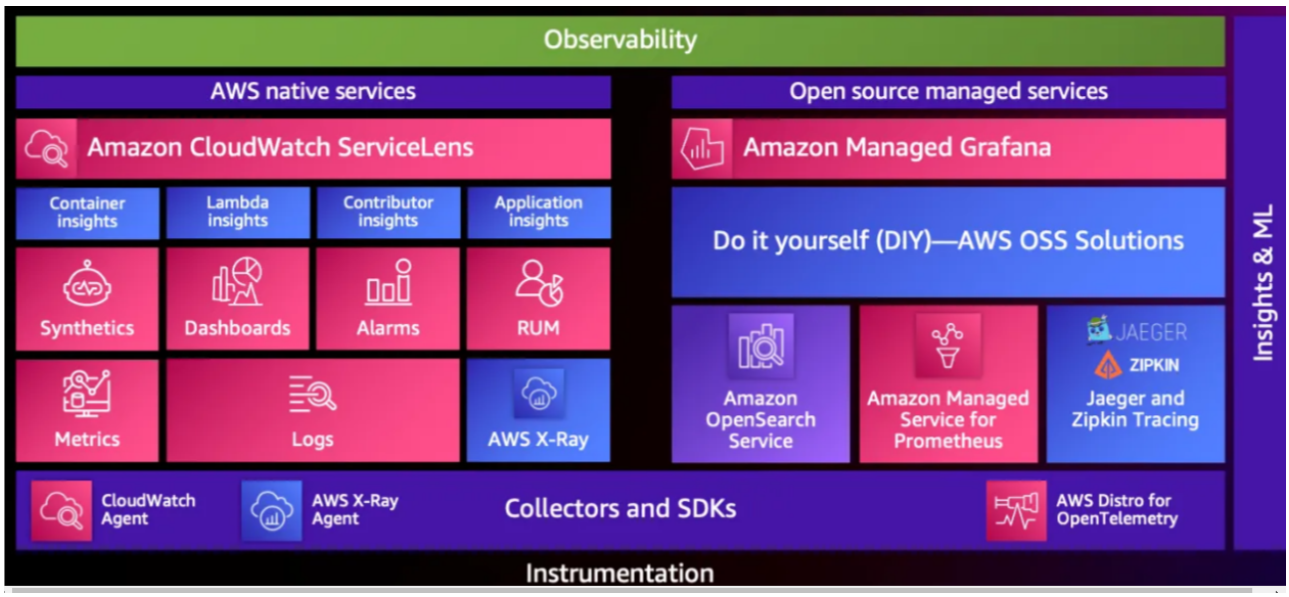
Azure Monitoring

- KQL is a query language for querying logs from analytics workspace Refer Here
- SQL to KQL cheatsheet Refer Here
- KQL reference Refer Here
- For collecting metrics on virtual machines/physical machines into Azure Monitoring, we use Agents Refer Here
- For collecting insights about code executed in non Azure environments, we use instrumentation libraries
    - Python Refer Here
    - .net Refer Here

AWS Monitoring Stack

- Overview



- AWS Native Stack
    - Metrics
    - Logs
    - Traces (XRay)
- To collect metrics from aws services, we generally need not do anything, if you want to collect more frequently then we need to go into paid models
- To Collect metrics from non AWS Services, we can use Agents and to collect traces from code, we can use xray sdks
- Once we have data stored, then we can do analytics
- Cloud Watch is a central native service, which we can use to view metrics and store logs

Lets send an email for low cpu consumption

- IN AWS we have a service called as SNS (Simple Notification Service) for sending notifications

- Lets create an sns topic
- Lets create an ec2 instance
- All metrics published Refer Here and Refer Here for Namespaces
- States in CloudWatch Metric
    - insufficent data
    - ok
    - alarm
- I want to findout which user has created ec2 instance use Cloud Trail -> Event History