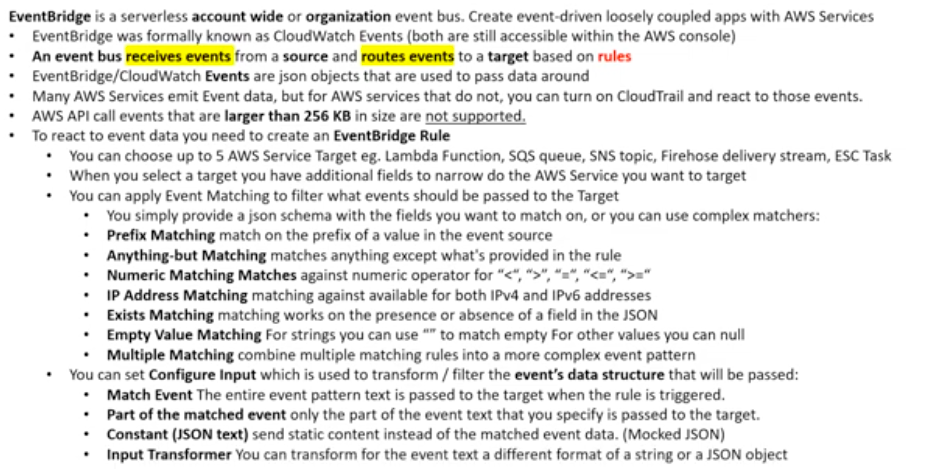
## **CloudWatch Alarms CheatSheet**

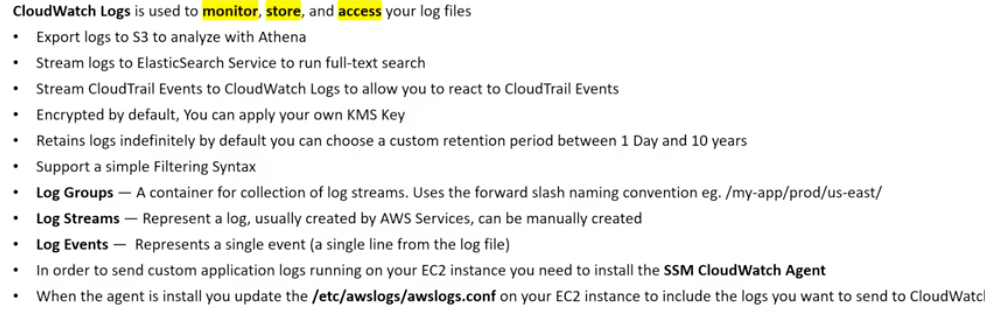
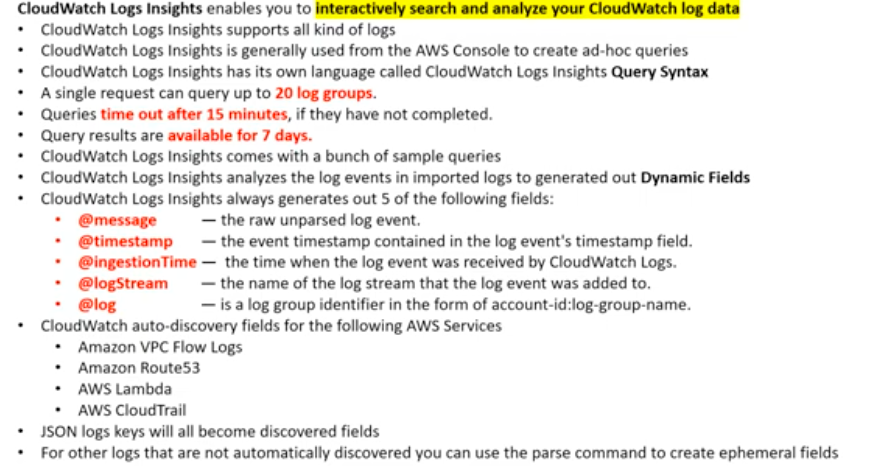
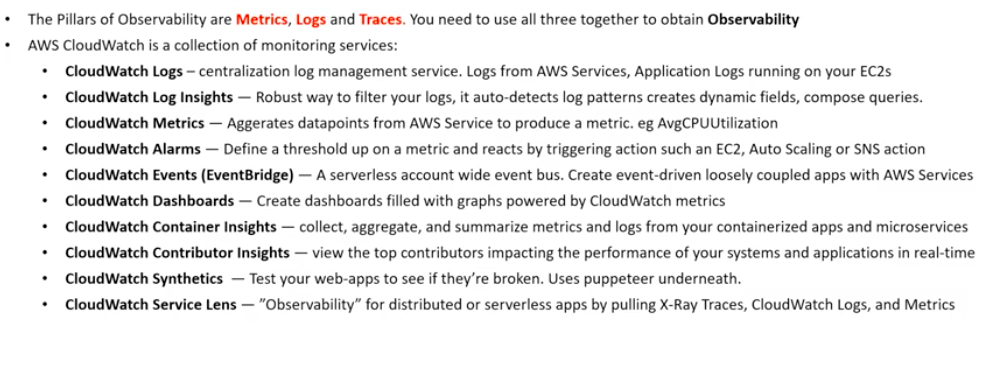
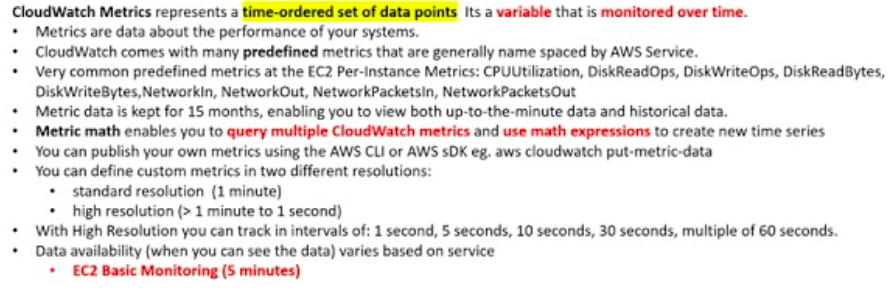
**A CloudWatch Alarm** monitors a CloudWatch Metric based on a defined threshold

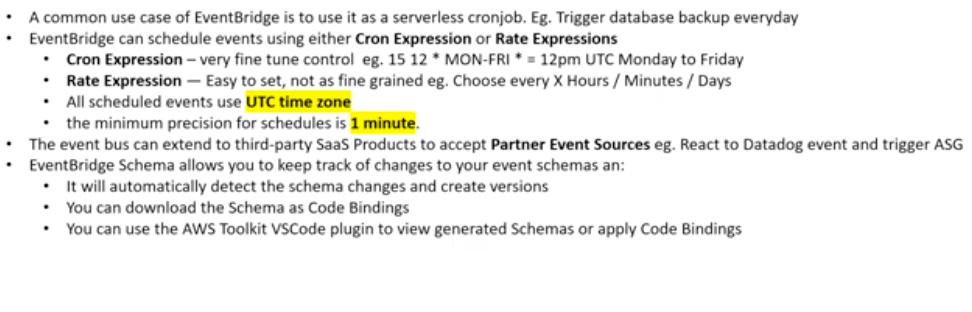
When an alarm **breaches** (goes outside the defined threshold) then it changes state

**Metric Alarm States**

* **OK** The metric or expression is **within** the defined threshold
* **ALARM** The metric or expression is **outside** of the defined threshold
* **INSUFFICIENT\_DATA**
* The alarm has **just started /** The metric is **not available / Not enough data** is available
  + When it changes state, we can define what action it should trigger:
  + Notification / Auto Scaling Group / EC2 Action
* You can define Conditions of either a **Static** or **Anomaly Detection**
  + **Static** set a static value as the threshold eg. 100 USD
  + **Anomaly Detection** sets a band around the data points, helps prevent false positives, more flexible if you have seasonal data
* **Composite Alarms** - This allows you to watch multiple alarms and require both to trigger before resulting in an alarm action
  + ~~The alarms being watch must have no actions sets~~
  + It is recommended to set "no action" to reduce alarm noise
  + You can only trigger an SNS as the action (so no EC2 or ASG actions)

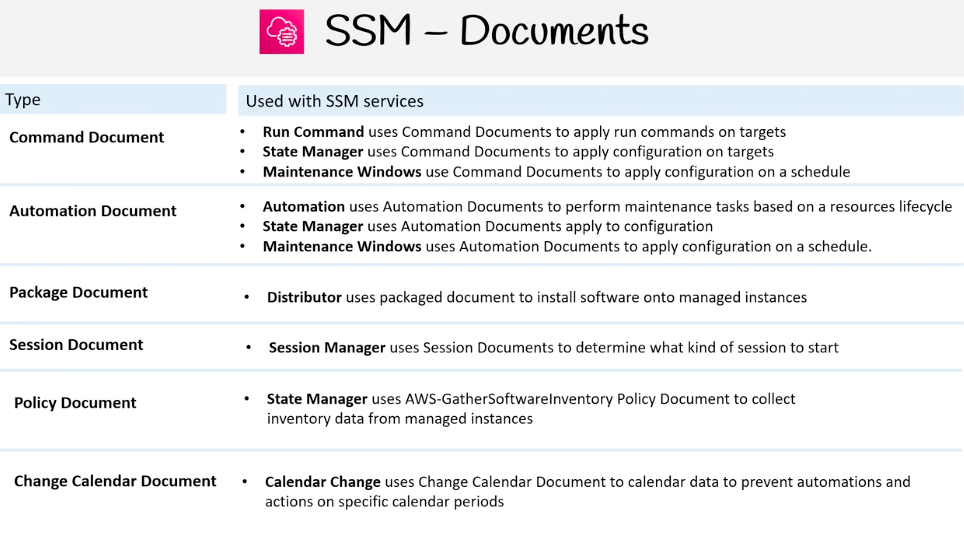




CloudTrail CheatSheet

* CloudTrail logs calls between AWS services **Governance, compliance, operational auditing,** and **risk auditing** are keywords relating to CloudTrail
* When you need to know **who to blame** think CloudTrail
* CloudTrail by default logs event data for the past 90s days via **Event History.**
* To track beyond 90 days, you need to create **Trail.**
* To ensure logs have not been tampered with, you need to turn on **Log File Validation** option
* CloudTrail logs can be encrypted using **KMS (Key Management Service)**
* CloudTrail can be set to log across all AWS accounts in an Organization and all regions in an account.
* CloudTrail logs can be streamed to CloudWatch logs
* Trails are outputted to an S3 bucket that you specify
* ~~CloudTrail logs two kinds of events:~~**~~Management Events~~**~~and~~**~~Data Events~~**
* CloudTrail logs three kinds of events: **Management events**, **Data events**, and **Insights events**
* **Management events** log management operations eg. AttachRolePolicy
* **Data Events** log data operations for resources (S3, Lambda) eg. GetObject, DeleteObject, and PutObject
* **CloudTrail Insights Events** capture unusual activity in your AWS account.
* Data events and Insights events are **disabled** by default when creating a Trail.
* Trail logs that are logged within S3 can be analyzed using Athena

AWS Simple System Manager