**CLOUD TRAIL**

* In aws every activity will register in cloud trail from where you call like cli,console,programming., every call will record
* For account level activity logings
* In this two concepts will be there

1. event history
2. trails
3. **event history** : By default event history is enabel,for any account we are using this event.

* In the event history we can’t delete or update we will not have any permissions.
* no charges by aws.
* Only the last 90 days of data will availabe-->use it for beta accounts
* no integrations

1. **Trails** : by custom we need to create the trail.

* It is chargabel on basis of usage .
* If you want more than 90 days of your data than should use trail--> for production account.
* In this trail services integrations will suport by S3,cloudwatch,event bridge.
* Use event brige why because if you want to use third party tools then push this evet brige .
* 1) **Region base trial** : only in region
* 2) **Multi region trail** : if you want to multi region in all regions then when you are creating the trail choose option multi region and the aws will automatically it replicate to all regions.

In the events we have two types

1)Rights events

2)Read evet

* **Events:**

1. **Managements events** : any action as done in aws it will comes under management events.any resourse we create or delete that will come under management events.only resourse level activities will be recorded in managements events.all services will suport.
2. **Data events** : any datalike files., you update or manipulate that wil comes under data events.in this S3,Lamda,dynamoDB will suport.only use when have usecase because it is chargabel.
3. **Insight events** : any unusual activies are done in account then use the insight events.

\***Log file validation**: if any tamparing or delete or download or file modifie.

\***encryption**:by default if you push any log file that will use SSE-SE3.