Splunk Genesys Cloud Training Lab Guide – Day 2

Downloadble PPT Content :

https://github.com/SplunkBAUG/CCA/blob/main/SPLK_CCA_Genesys_Cloud_App_Training_Day2_2022_0315.pdf

Lab Exercise Guides :

Analysis Exercise #1 :

Search 1 :

```
`genesys_cloud_index` sourcetype="genesys:cloud:api:conversation_aggregate" group.ani="***"
group.conversationId="***"
| spath path="data{}.metrics{}" output=rec_metric
| spath path="group" output=rec_group
| spath input=rec_group
| mvexpand rec_metric
| spath input=rec_metric
| eval queueFlow.id=mvdedup(queueFlow.id)
| eval queueFlow.name=mvdedup(queueFlow.name)
| eval queueFlow.selfUri=mvdedup(queueFlow.selfUri)
| eval queueId=mvdedup(queueId)
| fields + *
| table _time ani conversationId direction mediaType metric originatingDirection purpose stats.count
queueId name
| rename stats.count as stats_count
| stats sum(eval(if(metric == "tAnswered", stats_count,0))) as cnt_answer, sum(eval(if(metric ==
"nOverSla", stats_count,0))) as cnt_over_sla, sum(eval(if(metric == "tAbandon", stats_count,0))) as
cnt_abandon by queueId name
| eval SLA=((cnt_answer-cnt_over_sla)/(cnt_answer+cnt_abandon))*100
```

Search 2:

```
`genesys_cloud_index` sourcetype="genesys:cloud:api:conversation_aggregate" group.ani="***"
group.conversationId="***"
| spath path="data{}.metrics{}" output=rec_metric
| spath path="group" output=rec_group
| spath input=rec_group
| mvexpand rec_metric
| spath input=rec_metric
| eval queueFlow.id=mvdedup(queueFlow.id)
| eval queueFlow.name=mvdedup(queueFlow.name)
| eval queueFlow.selfUri=mvdedup(queueFlow.selfUri)
| eval queueId=mvdedup(queueId)
| fields + *
| table _time ani conversationId direction mediaType metric originatingDirection purpose
stats.count queueId name
| rename stats.count as stats_count
| stats sum(eval(if(metric == "tAnswered", stats_count,0))) as cnt_answer,
sum(eval(if(metric == "nOverSla", stats_count,0))) as cnt_over_sla, sum(eval(if(metric ==
"tAbandon", stats_count,0))) as cnt_abandon by queueId name
| eval SLA=((cnt_answer-cnt_over_sla)/(cnt_answer+cnt_abandon))*100
| table name SLA
```

Search 3 :

```
`genesys_cloud_index` sourcetype="genesys:cloud:api:conversation_aggregate" group.ani="***"
group.conversationId="***"
| spath path="data{}.metrics{}" output=rec_metric
| spath path="group" output=rec_group
| spath input=rec_group
| mvexpand rec_metric
| spath input=rec_metric
| fields + *
| table _time ani conversationId direction mediaType metric originatingDirection purpose
stats.count stats.sum queueId name ```queueFlow.id queueFlow.name queueFlow.selfUri
queueId```
| rename stats.count as stats_count, stats.sum as stats_sum
| stats
    sum(eval(if(metric == "nBlindTransferred", stats_count,0))) as nBlindTransferred,
sum(eval(if(metric == "nConnected", stats_count,0))) as nConnected, sum(eval(if(metric ==
"nConsult", stats_count,0))) as nConsult, sum(eval(if(metric == "nConsultTransferred",
stats_count,0))) as nConsultTransferred, sum(eval(if(metric == "nError", stats_count,0)))
as nError, sum(eval(if(metric == "nOffered", stats_count,0))) as nOffered,
sum(eval(if(metric == "nOutbound", stats_count,0))) as nOutbound, sum(eval(if(metric ==
"nOutboundAttempted", stats_count,0))) as nOutboundAttempted, sum(eval(if(metric ==
"nOverSla", stats_count,0))) as nOverSla, sum(eval(if(metric == "nTransferred",
stats_count,0))) as nTransferred, sum(eval(if(metric == "tAbandon", stats_count,0))) as
nAbandon, sum(eval(if(metric == "tAlert", stats_count,0))) as nAlert, sum(eval(if(metric ==
"tAnswered", stats_count,0))) as nAnswered, sum(eval(if(metric == "tContacting",
stats_count,0))) as nContacting, sum(eval(if(metric == "tDialing", stats_count,0))) as
nDialing, sum(eval(if(metric == "tHandle", stats_count,0))) as nHandle, sum(eval(if(metric
== "tHeld", stats_count,0))) as nHeld, sum(eval(if(metric == "tHeldComplete",
stats_count,0))) as nHeldComplete, sum(eval(if(metric == "tIvr", stats_count,0))) as nIvr,
sum(eval(if(metric == "tNotResponding", stats_count,0))) as nNotResponding,
sum(eval(if(metric == "tShortAbandon", stats_count,0))) as nShortAbandon,
sum(eval(if(metric == "tTalk", stats_count,0))) as nTalk, sum(eval(if(metric ==
"tTalkComplete", stats_count,0))) as nTalkComplete, sum(eval(if(metric == "tVoicemail",
stats_count,0))) as nVoicemail, sum(eval(if(metric == "tWait", stats_count,0))) as nWait,
    sum(eval(if(metric == "tAbandon", stats_sum,0))) as tAbandon,  sum(eval(if(metric ==
"tAcd", stats_sum,0))) as tAcd, sum(eval(if(metric == "tAcw", stats_sum,0))) as tAcw,
sum(eval(if(metric == "tAlert", stats_sum,0))) as tAlert, sum(eval(if(metric ==
"tAnswered", stats_sum,0))) as tAnswered, sum(eval(if(metric == "tContacting",
stats_sum,0))) as tContacting, sum(eval(if(metric == "tDialing", stats_sum,0))) as
tDialing, sum(eval(if(metric == "tHandle", stats_sum,0))) as tHandle, sum(eval(if(metric ==
"tHeld", stats_sum,0))) as tHeld, sum(eval(if(metric == "tHeldComplete", stats_sum,0))) as
tHeldComplete, sum(eval(if(metric == "tIvr", stats_sum,0))) as tIvr, sum(eval(if(metric ==
"tNotResponding", stats_sum,0))) as tNotResponding, sum(eval(if(metric == "tShortAbandon",
stats_sum,0))) as tShortAbandon, sum(eval(if(metric == "tTalk", stats_sum,0))) as tTalk,
sum(eval(if(metric == "tTalkComplete", stats_sum,0))) as tTalkComplete, sum(eval(if(metric
== "tVoicemail", stats_sum,0))) as tVoicemail, sum(eval(if(metric == "tWait",
stats_sum,0))) as tWait
    by queueId name
```

Analysis Exercise #2 :

Search 4 :

```
`genesys_cloud_index` sourcetype="genesys:cloud:api:conversation_details" startTime
| dedup id
| rename id as conversation_id, address as caller_address
| spath path="participants{}" output=rec_participant
| spath path="divisions{}" output=rec_division
| spath input="rec_participant"
| rename id as participant_id,
| spath input="rec_division"
| table _time conversation_id participant_id id caller_address adress startTime endTime selfUri
recordingState entities{}.id rec_*
| mvexpand rec_participant
| spath input="rec_participant"
| lookup genesys_cloud_queue_info id AS participants{}.queueId
```

```
| fields - rec_* calls{}* startTime
| fields + *
| chart count by queueName attributes.Opt_Out_Reason_Code
```

Analysis Exercise #3 :

Search 5 :

```
`genesys_cloud_index` sourcetype="genesys:cloud:api:conversation_aggregate" group.ani="***"
group.conversationId="***"
| spath path="data{}.metrics{}" output=rec_metric
| spath path="group" output=rec_group
| spath input=rec_group
| mvexpand rec_metric
| spath input=rec_metric
| fields + *
| table _time ani conversationId direction mediaType metric originatingDirection purpose stats.count
queueId ```queueFlow.id queueFlow.name queueFlow.selfUri ```
| rename stats.count as stats_count
| timechart sum(stats_count) as count by metric
```

Search 6 :

```
`genesys_cloud_index` sourcetype="genesys:cloud:api:conversation_aggregate" group.ani="***"
group.conversationId="***"
| spath path="data{}.metrics{}" output=rec_metric
| spath path="group" output=rec_group
| spath input=rec_group
| mvexpand rec_metric
| spath input=rec_metric
| fields + *
| search metric=tAbandon
| table _time ani conversationId direction mediaType metric originatingDirection purpose stats.count
queueId ```queueFlow.id queueFlow.name queueFlow.selfUri ```
| rename stats.count as stats_count
| timechart sum(stats_count) as count by queueId
```

Alert Setting Exercise :

Search 7 :

```
`genesys_cloud_index` sourcetype="genesys:cloud:api:conversation_aggregate" group.ani="***"
group.conversationId="***"
| spath path="data{}.metrics{}" output=rec_metric
| spath path="group" output=rec_group
| spath input=rec_group
| mvexpand rec_metric
| spath input=rec_metric
| search metric="tAbandon"
| fields + *
| stats sum(stats.count) AS value by queueId
| sort - value
```

Alert Settings :

- Excessive Number of Abandon Calls Detected
- Alert type : Run on Cron Schedule
- Time Range : Last 7 Days
- Cron Expression : */2 * * * *
- Trigger alert when : Custom, search value>2
- Trigger : For Each Results
- Throttle : Checked
- Suppress results containing field value : queueId

- Suppress triggering for : 60
- Trigger Actions : Alert Manager
- Title : Excessive Abandon Calls Detected : $result.queueId$: $result.value$
- Impact : Medium
- Urgency : Medium
- Owner : Unassigned