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 |