12-01-2021 09:00:53.806 INFO dispatchRunner - Search process mode: preforked (first search in process) (build 767223ac207f).
12-01-2021 09:00:53.806 INFO dispatchRunner - Initing LicenseMgr in search process: nonPro=0
12-01-2021 09:00:53.806 INFO LicenseMgr - Initing LicenseMgr
12-01-2021 09:00:53.806 INFO LMConfig - serverName=logsrv guid=B2F38184-60AE-43CF-92DB-3B904F81A8E7
12-01-2021 09:00:53.812 INFO LMConfig - connection_timeout=30
12-01-2021 09:00:53.812 INFO LMConfig - send_timeout=30
12-01-2021 09:00:53.812 INFO LMConfig - receive_timeout=30
12-01-2021 09:00:53.812 INFO LMConfig - key=license_warnings_update_interval not found in licenser stanza of server.conf, defaulting=0
12-01-2021 09:00:53.812 INFO LMConfig - squash_threshold=200
12-01-2021 09:00:53.812 INFO LMConfig - strict_pool_quota=1
12-01-2021 09:00:53.812 INFO LMConfig - key=pool_suggestion not found in licenser stanza of server.conf, defaulting=""
12-01-2021 09:00:53.812 INFO LMConfig - key=test_aws_metering not found in licenser stanza of server.conf, defaulting=0
12-01-2021 09:00:53.812 INFO LMConfig - key=test_aws_product_code not found in licenser stanza of server.conf, defaulting=0
12-01-2021 09:00:53.812 INFO LicenseMgr - Initing LicenseMgr
12-01-2021 09:00:53.812 INFO LMStackMgr - closing stack mgr
12-01-2021 09:00:53.812 INFO LMConfig - all slaves cleared
12-01-2021 09:00:53.812 INFO LMStackMgr - Initialized license_warnings_update_interval=auto
12-01-2021 09:00:53.812 INFO LMStackMgr - Skipping trial license as alternative license type in use
12-01-2021 09:00:53.816 INFO LMStack - Added type=enterprise license, from file=splunk-enterprise.lic, to stack=enterprise of group=Enterprise
12-01-2021 09:00:53.817 INFO LMStackMgr - created stack='enterprise'
12-01-2021 09:00:53.817 INFO LMStackMgr - Skipping trial pool stanza as alternative license in use
12-01-2021 09:00:53.817 INFO LMStackMgr - added pool auto_generated_pool_enterprise to stack enterprise
12-01-2021 09:00:53.817 INFO LMStackMgr - added pool auto_generated_pool_forwarder to stack forwarder
12-01-2021 09:00:53.817 INFO LMStackMgr - added pool auto_generated_pool_free to stack free
12-01-2021 09:00:53.817 INFO LMStackMgr - Initialized hideQuotaWarning = "0"
12-01-2021 09:00:53.817 INFO LMStackMgr - init completed [B2F38184-60AE-43CF-92DB-3B904F81A8E7,Enterprise,runContext_splunkd=false]
12-01-2021 09:00:53.817 INFO LicenseMgr - StackMgr init complete...
12-01-2021 09:00:53.817 INFO LMTracker - Setting default product type='enterprise'
12-01-2021 09:00:53.817 INFO LMTracker - this is not splunkd, will perform partial init
12-01-2021 09:00:53.817 INFO LMTracker - Setting feature=Acceleration state=ENABLED (featureStatus=1)
12-01-2021 09:00:53.817 INFO LMTracker - Setting feature=AdvancedSearchCommands state=ENABLED (featureStatus=1)
12-01-2021 09:00:53.817 INFO LMTracker - Setting feature=AdvancedXML state=ENABLED (featureStatus=1)
12-01-2021 09:00:53.817 INFO LMTracker - Setting feature=Alerting state=ENABLED (featureStatus=1)
12-01-2021 09:00:53.817 INFO  LMTracker - Setting feature=ArchiveToHdfs
state=ENABLED (featureStatus=1)
12-01-2021 09:00:53.817 INFO  LMTracker - Setting feature=Auth
state=ENABLED (featureStatus=1)
12-01-2021 09:00:53.817 INFO  LMTracker - Setting feature=CustomRoles
state=ENABLED (featureStatus=1)
12-01-2021 09:00:53.817 INFO  LMTracker - Setting feature=DeployClient
state=ENABLED (featureStatus=1)
12-01-2021 09:00:53.817 INFO  LMTracker - Setting feature=DeployServer
state=ENABLED (featureStatus=1)
12-01-2021 09:00:53.817 INFO  LMTracker - Setting feature=DistSearch
state=ENABLED (featureStatus=1)
12-01-2021 09:00:53.817 INFO  LMTracker - Setting feature=FwdData
state=ENABLED (featureStatus=1)
12-01-2021 09:00:53.817 INFO  LMTracker - Setting feature=GuestPass
state=ENABLED (featureStatus=1)
12-01-2021 09:00:53.817 INFO  LMTracker - Setting feature=KVStore
state=ENABLED (featureStatus=1)
12-01-2021 09:00:53.817 INFO  LMTracker - Setting feature=LDAPAuth
state=ENABLED (featureStatus=1)
12-01-2021 09:00:53.817 INFO  LMTracker - Setting feature=LocalSearch
state=ENABLED (featureStatus=1)
12-01-2021 09:00:53.817 INFO  LMTracker - Setting feature=MultifactorAuth
state=ENABLED (featureStatus=1)
12-01-2021 09:00:53.817 INFO  LMTracker - Setting feature=MultisiteClustering
state=ENABLED (featureStatus=1)
12-01-2021 09:00:53.817 INFO  LMTracker - Setting feature=NontableLookups
state=ENABLED (featureStatus=1)
12-01-2021 09:00:53.817 INFO  LMTracker - Setting feature=RcvData
state=ENABLED (featureStatus=1)
12-01-2021 09:00:53.817 INFO  LMTracker - Setting feature=RcvSearch
state=ENABLED (featureStatus=1)
12-01-2021 09:00:53.817 INFO  LMTracker - Setting feature=RollingWindowAlerts
state=ENABLED (featureStatus=1)
12-01-2021 09:00:53.817 INFO  LMTracker - Setting feature=SAMLAuth
state=ENABLED (featureStatus=1)
12-01-2021 09:00:53.817 INFO  LMTracker - Setting feature=ScheduledAlerts
state=ENABLED (featureStatus=1)
12-01-2021 09:00:53.817 INFO  LMTracker - Setting feature=ScheduledReports
state=ENABLED (featureStatus=1)
12-01-2021 09:00:53.817 INFO  LMTracker - Setting feature=ScheduledSearch
state=ENABLED (featureStatus=1)
12-01-2021 09:00:53.817 INFO  LMTracker - Setting feature=ScriptedAuth
state=ENABLED (featureStatus=1)
12-01-2021 09:00:53.817 INFO  LMTracker - Setting feature=SearchheadPooling
state=ENABLED (featureStatus=1)
12-01-2021 09:00:53.817 INFO  LMTracker - Setting feature=SigningProcessor
state=ENABLED (featureStatus=1)
12-01-2021 09:00:53.817 INFO  LMTracker - Setting feature=SplitWeb
state=ENABLED (featureStatus=1)
12-01-2021 09:00:53.817 INFO  LMTracker - Setting feature=SubgroupId
state=ENABLED (featureStatus=1)
12-01-2021 09:00:53.817 INFO  LMTracker - Setting feature=UnisiteClustering
state=ENABLED (featureStatus=1)
12-01-2021 09:00:53.817 INFO  LicenseMgr - Tracker init complete...
12-01-2021 09:00:53.829 INFO AdminManagerDispatch - added factory for admin handler: 'licenses'
12-01-2021 09:00:53.829 INFO AdminManagerDispatch - added factory for admin handler: 'pools'
12-01-2021 09:00:53.829 INFO AdminManagerDispatch - added factory for admin handler: 'stacks'
12-01-2021 09:00:53.829 INFO AdminManagerDispatch - added factory for admin handler: 'groups'
12-01-2021 09:00:53.829 INFO AdminManagerDispatch - added factory for admin handler: 'slaves'
12-01-2021 09:00:53.829 INFO AdminManagerDispatch - added factory for admin handler: 'localslave'
12-01-2021 09:00:53.829 INFO AdminManagerDispatch - added factory for admin handler: 'licensermessages'
12-01-2021 09:00:53.829 INFO AdminManagerDispatch - added factory for admin handler: 'scriptedwarning'
12-01-2021 09:00:53.829 INFO AdminManagerDispatch - added factory for admin handler: 'licenseusage'
12-01-2021 09:00:53.830 INFO dispatchRunner - registering build time modules, count=1
12-01-2021 09:00:53.830 INFO dispatchRunner - registering search time components of build time module name=vix
12-01-2021 09:00:53.830 INFO dispatchRunner - Getting search configuration data from: /opt/splunk/etc/modules/parsing/config.xml
12-01-2021 09:00:53.835 INFO BundlesSetup - Setup stats for /opt/splunk/etc: wallclock_elapsed_msec=66, cpu_time_used=0.06589, shared_services_generation=2, shared_services_population=1
12-01-2021 09:00:53.858 INFO UserManagerPro - Load authentication: forcing roles="admin, power, user"
12-01-2021 09:00:53.859 INFO PipelineComponent - Ingestion pipeline sets have been configured to use pipeline set policy=round_robin for multiple pipeline sets.
12-01-2021 09:00:53.861 INFO UserManager - Setting user context: splunk-system-user
12-01-2021 09:00:53.861 INFO UserManager - Done setting user context: NULL -> splunk-system-user
12-01-2021 09:00:53.863 INFO UserManager - Unwound user context: splunk-system-user -> NULL
12-01-2021 09:00:53.863 INFO UserManager - Setting user context: admin
12-01-2021 09:00:53.863 INFO UserManager - Done setting user context: NULL -> admin
12-01-2021 09:00:53.865 INFO dispatchRunner - search context: user="admin", app="search", bs-pathname="/opt/splunk/etc"
12-01-2021 09:00:53.881 INFO SearchParser - PARSING: search index="app" source="/data/app/*/*" (date_hour>1 AND (date_hour<23 OR (date_hour=23 date_minute<30))) "Packet Processed" OR "Normal Packet Received" \n| rex field=source "\[/<product\>/\w+/\]/\([^<date\[d]\]+\)/\([^<servername\>/\w+]\)" \n| rex RN\[\([^<RN>\[d]\]+\)\] \n| rex "^\([^<timestamp\.\[23]\)]) INFO \([^<customer>.\]*)\) \[TransactionProcessorService\] \([^<status>.\]*)\: M\([^<Acode>.\]*)\] T\[\([^<Bcode>\[d]\]+\)\]"\n| rex field=customer "\([^<customer2>.\]*)\)"\n| eval customer2=coalesce(customer2,customer), customer=if(customer=customer2,null(),customer)\n| eval sendTime=if(status="Packet Processed",strptime(timestamp,"%Y-%m-%d %H:%M:%S,%3Q"),null()), receiveTime=if(status="Normal Packet Received",strptime(timestamp,"%Y-%m-%d %H:%M:%S,%3Q"),null())\n| eval AcodeSend=if(status="Packet Processed",Acode,null()),BcodeSend=if(status="Packet Processed",Bcode,null())


Given the current status and the availability of resources, the system processes the received packets efficiently. The flowchart illustrates the process as follows:

1. **Packet Received**: The system identifies the incoming packets and their statuses.
2. **Packet LookUp**: It checks if the packet belongs to a specific look-up list.
3. **AcodeSend and BcodeSend**: It determines the codes associated with the packet.
4. **AcodeReceive and BcodeReceive**: It checks if the packet is normal or received.
5. **AcodeReceiveLookFor**: It calculates the expected Acode based on the received packets.
6. **Fields Management**: It enforces strict field management policies.
7. **Statistical Analysis**: It performs statistical analysis on the received packets.
8. **Search Criteria**: It applies search criteria based on the status and duration.
9. **Time Conversion**: It converts timestamps to human-readable formats.

The system ensures that all packets are processed correctly and efficiently, adhering to the established protocols and procedures.
index="summary_app" file="RMD54ddb7b013368c231_1295571394.stash_new" name="app-env-duration" marker=""
12-01-2021 09:00:53.882 INFO StatsContext - Setting Page Size at 65536
12-01-2021 09:00:53.882 INFO StatsContext - Setting max memory usage at 209715200
12-01-2021 09:00:53.882 INFO StatsContext - Setting Page Size at 65536
12-01-2021 09:00:53.882 INFO StatsContext - Setting max memory usage at 209715200
12-01-2021 09:00:53.882 INFO StatsProcessorV2 - Setting fallback to old stats because of reason="unsupported usage: Not stats, prestats or mstats"
12-01-2021 09:00:53.882 INFO SearchParser - PARSING: search index="app" source="/data/app/*/*" (date_hour>=1 AND (date_hour<23 OR (date_hour=23 date_minute<30))) "Packet Processed" OR "Normal Packet Received" ...

12-01-2021 09:00:53.885 INFO ISplunkDispatch - Not running in splunkd. Bundle replication not triggered.
12-01-2021 09:00:53.958 INFO SearchOrchestrator - Initializing the run time settings for the orchestrator.
12-01-2021 09:00:53.958 INFO UserManager - Setting user context: admin
12-01-2021 09:00:53.958 INFO UserManager - Done setting user context: NULL
12-01-2021 09:00:53.958 INFO SearchOrchestrator - Creating the search DAG.
12-01-2021 09:00:53.958 INFO SearchParser - PARSING: search index="app" source="/data/app/*/*" (date_hour=1 AND (date_hour<23 OR (date_hour=23 date_minute<30))) "Packet Processed" OR "Normal Packet Received" 
| rex field=source "\[/?(<product>\w+)\/(<servername>\w+)\]" \n| rex RN\[(<RN>\d+) \n \n| rex "^\<(<timestamp>.{23}) INFO \<(?<customer>.*)(?TransactionProcessorService\]) (?<status>.*)\}: M\[\((?<Acode>.*)\]\]
T\[(?<Bcode>\d+)\]\n| rex field=customer "+\((<customer2>.*)\)"
| eval customer2=coalesce(customer2,customer),
customer=if(customer=customer2,null(),customer)\n| eval sendTime=if(status="Packet Processed",strptime(timestamp,"%Y-%m-%d %H:%M:%S"),null()),
receiveTime=if(status="Normal Packet Received",strptime(timestamp,"%Y-%m-%d %H:%M:%S,%3Q"),null())\n| eval AcodeSend=if(status="Packet Processed",Acode,null()),
BcodeSend=if(status="Packet Processed",Bcode,null()),
AcodeReceive=if(status="Normal Packet Received",Acode,null()),
BcodeReceive=if(status="Normal Packet Received",Bcode,null())
| eval AcodeReceiveLookFor=AcodeSend+10,acr=coalesce(AcodeReceive,AcodeReceiveLookFor)\n| fields _time timestamp status AcodeReceiveLookFor\n| stats values(*) as *,count by customer2,acr,Bcode\n| eval duration=receiveTime-sendTime ,
customer=coalesce(customer,customer2)\n| eval status=case(isnull(AcodeSend),"No Send",isnull(AcodeReceive),"No receive")\n| eventstats max(duration) as duration by customer2\n| where count=2 OR (status="No receive" AND isnull(duration))\n| eval status=coalesce(customer2,duration)\n| search NOT status="No receive"\n| search NOT status="No Send"\n| search status>2\n| eval send=strftime(sendTime, ",%Y-%d-%m %H:%M:%S") | eval receive=strftime(receiveTime, ",%Y-%d-%m %H:%M:%S")\n| table servername send receive customer RN status | summaryindex spool=t uselb=t addtime=t index="summary_app" file="RMD544dbdb7b013368c231_1295571394.stash_new" name="app-env-duration" marker=""
12-01-2021 09:00:54.179 INFO CsvDataProvider - Reading schema for lookup
table='cardiran-reaprocde.csv', file size=5767, modtime=1634567353
12-01-2021 09:00:54.179 INFO CsvDataProvider - Reading schema for lookup
table='nix_endpoint_change_vendor_action_lookup', file size=186,
modtime=1623833632
12-01-2021 09:00:54.179 INFO CsvDataProvider - Reading schema for lookup
table='nix_fs_notification_change_type_lookup', file size=49,
modtime=1623833632
12-01-2021 09:00:54.179 INFO CsvDataProvider - Reading schema for lookup
table='nix_endpoint_change_object_category_lookup', file size=89,
modtime=1623833632
12-01-2021 09:00:54.180 INFO CsvDataProvider - Reading schema for lookup
table='nix_endpoint_change_status_lookup', file size=54,
modtime=1623833632
12-01-2021 09:00:54.180 INFO CsvDataProvider - Reading schema for lookup
table='informix-error-codes.csv', file size=101673, modtime=1634324307
12-01-2021 09:00:54.180 INFO CsvDataProvider - Reading schema for lookup
table='jboss_severity_type_lookup', file size=300, modtime=1624544699
12-01-2021 09:00:54.180 INFO CsvDataProvider - Reading schema for lookup
table='nix_linux_audit_action_lookup', file size=340, modtime=1623833632
12-01-2021 09:00:54.182 INFO CsvDataProvider - Reading schema for lookup
table='nmon_data_asset_description', file size=2563, modtime=1623833414
12-01-2021 09:00:54.183 INFO CsvDataProvider - Reading schema for lookup
table='pan-code.csv', file size=551, modtime=1634985619
12-01-2021 09:00:54.183 INFO CsvDataProvider - Reading schema for lookup
table='nix_linux_service_startmode_lookup', file size=3859,
modtime=1623833632
12-01-2021 09:00:54.183 INFO CsvDataProvider - Reading schema for lookup
table='nix_da_update_status_lookup', file size=176, modtime=1623833632
12-01-2021 09:00:54.183 INFO CsvDataProvider - Reading schema for lookup
table='nix_da_version_range_lookup', file size=152, modtime=1623833632
12-01-2021 09:00:54.183 INFO CsvDataProvider - Reading schema for lookup
table='use-error-code.csv', file size=31972, modtime=1634257933
12-01-2021 09:00:54.334 INFO SearchEvaluatorBasedExpander - Performing
lookup expansions
12-01-2021 09:00:54.334 INFO SearchEvaluatorBasedExpander - Lookup
calculation field expansions
12-01-2021 09:00:54.334 INFO SearchEvaluatorBasedExpander - Calculated
field expansion took 0 ms
12-01-2021 09:00:54.334 INFO SearchEvaluatorBasedExpander - Performing
field alias expansions
12-01-2021 09:00:54.334 INFO SearchEvaluatorBasedExpander - field alias
expansions took 0 ms
12-01-2021 09:00:54.334 INFO SearchEvaluatorBasedExpander - Performing
kvfield expansions
12-01-2021 09:00:54.334 INFO SearchEvaluatorBasedExpander - kvfield
expansions took 0 ms
12-01-2021 09:00:54.334 INFO SearchEvaluatorBasedExpander - Performing
reverse sourcetype expansions
12-01-2021 09:00:54.334 INFO SearchEvaluatorBasedExpander - sourcetype
expansions took 0 ms
12-01-2021 09:00:54.334 INFO UnifiedSearch - Expanded index search =

(index="app" source="/data/app/*/*" date_hour>=1 (date_hour<23 OR
(date_hour=23 date_minute<30)) ("Packet Processed" OR "Normal Packet
Received"))
12-01-2021 09:00:56.372 INFO UnifiedSearch - Processed search targeting arguments
12-01-2021 09:00:56.373 INFO AstOptimizer - SrcOptMetrics optimize_toJson=0.002797400
12-01-2021 09:00:56.374 INFO AstVisitorFactory - Not building visitor : replace_datamodel_stats_cmds_with_tstats
12-01-2021 09:00:56.374 INFO PredicatePushOptimizer - search cannot be pushed through eval. Reason='status' is modified (Ref:'status')
12-01-2021 09:00:56.374 INFO PredicatePushOptimizer - search cannot be pushed through eval. Reason='status' is modified (Ref:'status')
12-01-2021 09:00:56.374 INFO PredicatePushOptimizer - search cannot be pushed through eval. Reason='status' is modified (Ref:'status')
12-01-2021 09:00:56.375 INFO SearchParser - PARSING: | summaryindex spool=t uselb=t addtime=t index="summary_app" file="RMD54ddb7b013368c231_1295571394.stash_new" name="app-env-duration"
12-01-2021 09:00:56.375 INFO SearchParser - PARSING: | table servername, send, receive, customer, RN, status
12-01-2021 09:00:56.375 INFO SearchParser - PARSING: | eval receive=strftime(receiveTime,"%Y-%d-%m %H:%M:%S")
12-01-2021 09:00:56.375 INFO SearchParser - PARSING: | eval send=strftime(sendTime,"%Y-%d-%m %H:%M:%S")
12-01-2021 09:00:56.375 INFO SearchParser - PARSING: | search status>2
12-01-2021 09:00:56.375 INFO SearchParser - PARSING: | search NOT status="No Send"
12-01-2021 09:00:56.375 INFO SearchParser - PARSING: | search NOT status="No receive"
12-01-2021 09:00:56.375 INFO SearchParser - PARSING: | eval status=coalesce(status,duration)
12-01-2021 09:00:56.375 INFO SearchParser - PARSING: | where ((count == 2) OR ((status == "No receive") AND isnull(duration)))
12-01-2021 09:00:56.375 INFO SearchParser - PARSING: | eval status=case(isnull(AcodeSend),"No Send",isnull(AcodeReceive),"No receive")
12-01-2021 09:00:56.375 INFO SearchParser - PARSING: | eval duration=(receiveTime - sendTime), customer=coalesce(customer,customer2)
12-01-2021 09:00:56.375 INFO StatsContext - Setting Page Size at 65536
12-01-2021 09:00:56.375 INFO StatsContext - Setting Page Size at 65536
12-01-2021 09:00:56.375 INFO StatsContext - Setting max memory usage at 209715200
12-01-2021 09:00:56.375 INFO StatsProcessorV2 - Setting fallback to old stats because of reason="unsupported usage: Not stats, prestats or mstats"
12-01-2021 09:00:56.375 INFO StatsContext - Setting Page Size at 65536
12-01-2021 09:00:56.375 INFO StatsProcessorV2 - Setting fallback to old stats because of reason="unsupported usage: Not stats, prestats or mstats"
12-01-2021 09:00:56.375 INFO SearchParser - PARSING: | eventstats max(duration) as duration by customer2
12-01-2021 09:00:56.375 INFO StatsContext - Setting Page Size at 65536
12-01-2021 09:00:56.375 INFO StatsContext - Setting max memory usage at 209715200
12-01-2021 09:00:56.375 INFO StatsProcessorV2 - Setting fallback to old stats because of reason="unsupported usage: Not stats, prestats or mstats"
12-01-2021 09:00:56.375 INFO SearchParser - PARSING: | eval status=case(isnull(AcodeSend),"No Send",isnull(AcodeReceive),"No receive")
12-01-2021 09:00:56.375 INFO SearchParser - PARSING: | eval duration=(receiveTime - sendTime), customer=coalesce(customer,customer2)
12-01-2021 09:00:56.375 INFO StatsContext - Setting Page Size at 65536
12-01-2021 09:00:56.375 INFO StatsContext - Setting max memory usage at 209715200
12-01-2021 09:00:56.375 INFO SearchParser - PARSING: | stats values(*)
as *,count by customer2,acr,Bcode
12-01-2021 09:00:56.375 INFO StatsContext - Setting Page Size at 65536
12-01-2021 09:00:56.375 INFO StatsContext - Setting max memory usage at 209715200
SEARCHPARSER - PARSING: | fields - Acode, _time, timestamp, status, AcodeReceiveLookFor

SEARCHPARSER - PARSING: | eval AcodeReceiveLookFor=(AcodeSend + 10), acr=coalesce(AcodeReceive,AcodeReceiveLookFor)

SEARCHPARSER - PARSING: | eval AcodeSend=if((status == "Packet Processed"),Acode,null()), BcodeSend=if((status == "Packet Processed"),Bcode,null()), AcodeReceive=if((status == "Normal Packet Received"),Acode,null()), BcodeReceive=if((status == "Normal Packet Received"),Bcode,null())

SEARCHPARSER - PARSING: | eval sendTime=if((status == "Packet Processed"),strptime(timestamp,"%Y-%m-%d %H:%M:%S,%3Q"),null()), receiveTime=if((status == "Normal Packet Received"),strptime(timestamp,"%Y-%m-%d %H:%M:%S,%3Q"),null())

SEARCHPARSER - PARSING: | eval customer2=coalesce(customer2,customer), customer=if((customer == customer2),null(),customer)

SEARCHPARSER - PARSING: | rex field=customer "_(?<customer2>.*)"

SEARCHPARSER - PARSING: | rex field=_raw "^(?<timestamp>.{23}) INFO  (?<customer>.*)\[/TransactionProcessorService\] (?<status>.*): \[(?<Acode>.*)(?<Bcode>d+)\]"

SEARCHPARSER - PARSING: | search (index="app" source="/data/app/*/*" date_hour>=1 (date_hour<23 OR (date_minute<30 date_hour=23)) ("Packet Processed" OR "Normal Packet Received"))
"\"data\"/\(?<product>\\w+\)\/(<date>\\d+)\/(<servername>\\w+)\" | rex field=\_raw "RN\/(<RN>\\d+)\" | rex field=\_raw "\^(?<timestamp>.*):(23)\}\) INFO (?<customer>.*) \[(TransactionProcessorService\] (?<status>.*): M\[(?<Ac ode>.*)\]\] \[(?<Bcode>\\d+)\]\" | rex field=customer ",_\((?<customer>.*)\)" | eval customer2=coalesce(customer2,customer), customer-if((customer == customer2),null(),customer), sendTime-if((status == "Packet Processed"),strptime(timestamp,"%Y-%m-%d %H:%M:%S,%3Q"),null()), receiveTime-if((status == "Normal Packet Received"),strptime(timestamp,"%Y-%m-%d %H:%M:%S,%3Q"),null()), Ac odeSend-if((status == "Packet Processed"),Ac ode,null()), BcodeSend-if((status == "Packet Processed"),Bcode,null()), BcodeReceive-if((status == "Normal Packet Received"),Bcode,null()), BcodeReceiveLookFor=(Ac odeSend + 10),acr=coalesce(AcodeReceive,Ac odeReceiveLookFor) | fields - Acode, _time, timestamp, status, AcodeReceiveLookFor
12-01-2021 09:00:56.489 INFO SearchProcessor - Building search filter
12-01-2021 09:00:56.531 INFO CsvDataProvider - Reading schema for lookup table='drop downsLookup', file size=77, modtime=1638304201
12-01-2021 09:00:56.531 INFO CsvDataProvider - Reading schema for lookup table='nix_action_lookup', file size=413, modtime=1623833857
12-01-2021 09:00:56.531 INFO CsvDataProvider - Reading schema for lookup table='cardiran-bin.csv', file size=1194, modtime=1634653347
12-01-2021 09:00:56.531 INFO CsvDataProvider - Reading schema for lookup table='cardiran-respc ode.csv', file size=5767, modtime=1634567353
12-01-2021 09:00:56.531 INFO CsvDataProvider - Reading schema for lookup table='nix_endpoint_change_vendor_action_lookup', file size=186, modtime=1623833632
12-01-2021 09:00:56.532 INFO CsvDataProvider - Reading schema for lookup table='nix_fs_notification_change_type_lookup', file size=49, modtime=1623833632
12-01-2021 09:00:56.532 INFO CsvDataProvider - Reading schema for lookup table='nix_endpoint_change_object_category_lookup', file size=89, modtime=1623833632
12-01-2021 09:00:56.532 INFO CsvDataProvider - Reading schema for lookup table='nix_endpoint_change_status_lookup', file size=54, modtime=1623833632
12-01-2021 09:00:56.532 INFO CsvDataProvider - Reading schema for lookup table='informix-error-codes.csv', file size=101673, modtime=1634324307
12-01-2021 09:00:56.532 INFO CsvDataProvider - Reading schema for lookup table='jboss_severity_type_lookup', file size=300, modtime=1624544699
12-01-2021 09:00:56.532 INFO CsvDataProvider - Reading schema for lookup table='nix_linux_audit_action_lookup', file size=340, modtime=1623833632
12-01-2021 09:00:56.533 INFO CsvDataProvider - Reading schema for lookup table='nmon_data asset description', file size=2563, modtime=1623833414
12-01-2021 09:00:56.534 INFO CsvDataProvider - Reading schema for lookup table='pan-code.csv', file size=551, modtime=1634985619
12-01-2021 09:00:56.534 INFO CsvDataProvider - Reading schema for lookup table='nix_linux_service_startmode lookup', file size=3859, modtime=1623833632
12-01-2021 09:00:56.534 INFO CsvDataProvider - Reading schema for lookup table='nix_da_update_status_lookup', file size=176, modtime=1623833632
12-01-2021 09:00:56.534 INFO CsvDataProvider - Reading schema for lookup table='nix_da_version_range_lookup', file size=152, modtime=1623833632
12-01-2021 09:00:56.534 INFO CsvDataProvider - Reading schema for lookup table='use-error-code.csv', file size=31972, modtime=1634257933
12-01-2021 09:00:56.564 INFO SearchEvaluatorBasedExpander - Performing lookup expansions
UnifiedSearch - Expanded index search =
(index="app" source="/data/app/*/*" date_hour>=1 (date_hour<23 OR (date_minute<30 date_hour=23)) ("Packet Processed" OR "Normal Packet Received"))
UnifiedSearch - base lisp:
AND index::use message source::/data/app/*/*
GTE date_hour 1 ] [ OR [ LT date_hour 23 ] [ AND [ LT date_minute 30 ] [ EQ date_hour 23 ] ] ] [ OR processed [ AND normal received ] ]
UnifiedSearch - Processed search targeting arguments
UnifiedSearch - Setting Page Size at 65536
UnifiedSearch - Setting max memory usage at 209715200
UnifiedSearch - Setting Page Size at 65536
UnifiedSearch - Setting max memory usage at 209715200
UnifiedSearch - Setting Page Size at 65536
UnifiedSearch - Setting max memory usage at 209715200
UnifiedSearch - stats values(*) as *,count by customer2,acr,Bcode | eval duration=(receiveTime - sendTime), customer=coalesce(customer,customer2), status=case(isnull(AcodeSend),"No Send",isnull(AcodeReceive),"No receive") | eventstats max(duration) as duration by customer2 | where ((count == 2) OR (status == "No receive") AND isnull(duration)) | eval status=coalesce(status,duration)| search (NOT status="No receive" status>2) | eval send=strftime(sendTime,"%Y-%d-%m %H:%M:%S"), receive=strftime(receiveTime,"%Y-%d-%m %H:%M:%S") | table servername, send, receive, customer, RN, status | summaryindex spool=t uselb=t addtime=t index="summary_app" file="RMD54ddb7b013368c231.1295571394.stash_new" name="app-env-duration" marker=""
INFO StatsContext - Setting Page Size at 65536
INFO StatsContext - Setting max memory usage at 209715200
INFO StatsProcessorV2 - Setting fallback to old stats because of reason="unsupported usage: Not stats, prestats or mstats"
INFO StatsProcessorV2 - StatsV2 (stats) args: values(*), as, *, count, by, customer2, acr, Bcode
INFO StatsProcessorV2 - StatsProcessorV2::processArguments: Unaligned accesses are free
INFO SortOperator - maxmem = 209715200
INFO StatsProcessorV2 - Setting fallback to old stats because of reason="unsupported function=values"
INFO StatsProcessorV2 - Setting fallback to old stats because of reason="unsupported feature=wildcards"
INFO StatsProcessorV2 - Instantiating Stats function values for key=*, alias=*
INFO StatsProcessorV2 - StatsV2 (eventstats) args: max(duration), as, duration, by, customer2
INFO SearchPhaseParserControl - Disabling remote timeline computation due to processor name=fields, not allowing it
INFO SearchParser - PARSING: addinfo type=count label=prereport_events track_fieldmeta_events=true
INFO SearchParser - PARSING: prestats count values("*" by Bcode acr customer2
INFO StatsContext - Setting Page Size at 65536
INFO StatsContext - Setting max memory usage at 209715200
INFO StatsProcessorV2 - StatsV2 (stats) args: count, values(*), by, Bcode, acr, customer2
INFO StatsProcessorV2 - StatsProcessorV2::processArguments: Unaligned accesses are free
INFO StatsProcessorV2 - Instantiating Stats function count for key=, alias=count
INFO StatsProcessorV2 - Setting fallback to old stats because of reason="unsupported function=values"
INFO StatsProcessorV2 - Setting fallback to old stats because of reason="unsupported feature=wildcards"
INFO StatsProcessorV2 - Instantiating Stats function values for key=*, alias=values(*)
INFO SearchPhaseGenerator - No need for RTWindowProcessor
INFO SearchPhaseGenerator - Timeliner will not be executed
INFO  SearchPhaseGenerator - required fields list to add to different pipelines = *
INFO  SearchPhaseGenerator - Remote Timeliner= Remote Timeliner=
INFO  SearchPhaseGenerator - Adding noop to provide result collation at search head
INFO  SearchPhaseGenerator - Search Phases created.
INFO  UserManager - Setting user context: admin
INFO  UserManager - Done setting user context: admin -> admin
INFO  DistributedSearchResultCollectionManager - Stream search: litsearch (index=app source=/data/app/* date_hour>=1 (date_hour<23 OR (date_minute<30 date_hour=23)) ("Packet Processed" OR "Normal Packet Received") | rex field=source "\\\data\\\((?<product>\w+)\\(?<servername>\w+)\\(?<date>d+)\\(?<timestamp>.{23})" | rex field=_raw "RN\\([\<\R\\\d+])" | rex field=customer "_(?<customer2>.*): M\\(\<\Acodoe:.*\\) T\\(\<\Bcode:.*\\)" | eval customer2=coalesce(customer2,customer), customer=if((customer == customer2),null(),customer), sendTime=if((status == "Packet Processed"),strptime(timestamp,"%Y-%m-%d %H:%M:%S,%3Q"),null()), receiveTime=if((status == "Normal Packet Received"),strptime(timestamp,"%Y-%m-%d %H:%M:%S,%3Q"),null()), AcodeSend=if((status == "Packet Processed"),Acode,null()), BcodeSend=if((status == "Packet Processed"),Bcode,null()), AcodeReceive=if((status == "Normal Packet Received"),Acode,null()), BcodeReceive=if((status == "Normal Packet Received"),Bcode,null()), AcodeReceiveLookFor=if(AcodeSend + 10), acr=coalesce(AcodeReceive,AcodeReceiveLookFor) | fields - Acode, _time, status, AcodeReceiveLookFor | addinfo type=count label=prequest_events track_fieldmeta_events=true | fields keepcolorder=t "*" | prestats count values("*"), Bcode acr customer2
INFO  DistributedSearchResultCollectionManager - ERP_FACTORY initialized, but zero external result provider, hence disabling_isERPCollectionEnabled
INFO  DistributedSearchResultCollectionManager - Default search group:
INFO  SearchTargeter - Index list is not available for logsvr targeting based on splunk_server and splunk_server_group only
INFO  DistributedSearchResultCollectionManager - Connecting to peer logsvr connectAll 0 connectToSpecificPeer 1
INFO  SearchPhaseGenerator - Time spends on creating distributed search results infrastructure; dispatchcreatedSearchResultInfrastructure=0.000718248 seconds.
INFO  UserManager - Setting user context: admin
null
12-01-2021 09:00:56.822 INFO UnifiedSearch - Search summary_id=B2F38184-60AE-43CF-92DB-3B904F81ABE7_search_admin_Ns220a57ebd140e62, maxtimespan=12-01-2021 09:00:56.823 INFO UnifiedSearch - Initialization of search data structures took 122 ms
12-01-2021 09:00:56.823 INFO UnifiedSearch - Processed search targeting arguments
12-01-2021 09:00:56.823 INFO StatsProcessorV2 - StatsV2 (stats) args: count, values(*), by, Bcode, acr, customer2
12-01-2021 09:00:56.823 INFO StatsProcessorV2 - StatsProcessorV2:processArguments: Unaligned accesses are free
12-01-2021 09:00:56.823 INFO StatsProcessorV2 - Instantiating Stats function count for key=, alias=count
12-01-2021 09:00:56.823 INFO StatsProcessorV2 - Setting fallback to old stats because of reason="unsupported function=values"
12-01-2021 09:00:56.823 INFO StatsProcessorV2 - Setting fallback to old stats because of reason="unsupported feature=wildcards"
12-01-2021 09:00:56.823 INFO StatsProcessorV2 - Instantiating Stats function values for key=*, alias=values(*)
12-01-2021 09:00:56.866 INFO LocalCollector - Final required fields list = *,AAA_OS,AAA_serial,ACTIVE,AIX_LEVEL,AIX_processor,AIX_processor_clockspeed,AIX_processor_type,AIX_realmemory_lsvconf_MB,AIX_realmemory_online_MB,AIX_VIRTUALCPU,ARGS,Ac ode,Arch,Aval,AvailableProcessors,Bcode,COMMAND,CPUCPU_TIME,Command,CommittedVirtualMemorySize,CurrentThreadCpuTime,CurrentThreadUserTime,DaemonThreadCount,Device,ErrorCode,FileSystem,ForeignAddress,FreePhysicalMemorySize,FreeSwapSpaceSize,HeapMemoryUsage.committed,HeapMemoryUsage.max,HeapMemoryUsage.used,IFree,IUse_pct,IUsed,Idle,Idle_PCT,Inodes,LEVEL/Linux_arch,LEVEL/Linux_lsb_distribution,LEVEL/Linux_processor_clockspeed_1,LEVEL/Linux_processor_clockspeed_2,LEVEL/Linux_processor_clockspeed_3,LEVEL/Linux_processor_cpuinfo,LEVEL/Linux_processor lsconf,LEVEL/Linux_processor_mcpuinfo,LEVEL/Linux_processor_mcpuinfo,LEVEL/Linux_processor_mcpuinfo,LEVEL/Linux_processor_mcpuinfo,LEVEL/Linux_processor_mcpuinfo,LEVEL/Linux_processor_mcpuinfo,LEVEL/Linux_processor_mcpuinfo,LEVEL/Linux_processor_mcpuinfo,LEVEL/Linux_processor_mcpuinfo,LEVEL/Linux_processor_mcpuinfo,LEVEL/Linux_processor_mcpuinfo,LEVEL/Linux_realmemory_MB,LEVEL/Linux_release_distribution,LoadedClassCount,LocalAddress,MAC,MaxFileDescriptorCount,Packet,Mount,MountedOn,Name,NonHeapMemoryUsage.committed,NonHeapMemoryUsage.init,NonHeapMemoryUsage.max,NonHeapMemoryUsage.used,OSType,ObjectMonitorUsageSupported,ObjectPendingFinalizationCount,OpenFileDescriptorCount,PID,PeakThreadCount,PercentFreeSpace,PercentMemory,PercentSystemTime,PhysicalCPU,PoolIdle,Port,ProcessCpuTime,Proto,RSZ_KB,REAL Memory,REAL_Free_PCT,REAL_free_MB,REAL_total_MB,RESData,Reset,ResSize,ResText,Runnable,S,Size,LEVEL/SolarisLEVEL,LEVEL/Solaris_processor_type,LEVEL/Solaris_realmemory_MB,LEVEL/Solaris_version,StartMode,StartTime,STATE SwapMemory,SyncrhonizerUsageSupported,Sys_PCT,SystemLoadAverage,SystemUpTime,TTY,ThreadContentionMonitoringEnabled,ThreadContentionMonitoringSupported,ThreadCount,ThreadCpuTimeEnabled,ThreadCpuTimeSupported,TotalCompilationTime,TotalLoadedClassCount,TotalPhysicalMemorySize,TotalStartedThreadCount,TotalSwapSpaceSize,TYPE/UNIT,USER,Unit,UnloadedClassCount,UpTime,USER CPU,Use_pct,Used,USER_PCT,VP_Idle_PCT,VP_Sys_PCT,VP_User_PCT,VP_Wait_PCT,VSZ_KB,Virtual_FREE_MB,Virtual_FREE_PCT,Virtual_TOTAL_MB,VmName,VMVendor,VMVersion,Wait_PCT,raw,subsecond,TIME,acct,action,active,anonymous_enable,app,avgWaitMillis,binc ode,block_action,blocks,buffers,bytesReceived,bytesSent,bytes_in,bytes_out,cached,chg,cmd,collectd_host,command,cpu_cores_position1,cpu_cores_position2,cpu_freq,cpu_freq_unit,cpuinterrupt_value,cpu_system_value,cpu_user_value,customer,customer2,date_hour,dqc,datum,dest,dest_host,dest_ip,device,df_complex_free_value,df_complex_used_value,df_free_value,df_unused_value,dhcp_type,direction_pattern,disk_ops_read,disk_ops_write,dsnames,/,dvc_name,entitled,eventtype,exe,fillnull,fillnull,fillnull,frameID,grps,hash,host,hostname,id,ipv4octets_rx,ipv4octets_tx,ipv4packets_rx,ipv4packets_tx,ipv6octets_rx,ipv6octets_tx,ipv6packets_rx,ipv6packets_tx,inactive,incoming_connections,index,inet6Addr,inetAddr,interrupts_PS,jvmDescription,linux_con cectd_plugin,log_level,logical_cpus,logname,machine_arc
12-01-2021 09:07:30.001 INFO SortOperator - maxmem = 209715200
12-01-2021 09:07:30.151 INFO SortOperator - maxmem = 209715200
12-01-2021 09:07:30.303 INFO SortOperator - maxmem = 209715200
12-01-2021 09:07:30.457 INFO SortOperator - maxmem = 209715200
12-01-2021 09:07:30.607 INFO SortOperator - maxmem = 209715200
12-01-2021 09:07:30.753 INFO SortOperator - maxmem = 209715200
12-01-2021 09:07:30.896 INFO SortOperator - maxmem = 209715200
12-01-2021 09:07:31.043 INFO SortOperator - maxmem = 209715200
12-01-2021 09:07:31.188 INFO SortOperator - maxmem = 209715200
12-01-2021 09:07:31.326 INFO SortOperator - maxmem = 209715200
12-01-2021 09:07:31.465 INFO SortOperator - maxmem = 209715200
12-01-2021 09:07:31.607 INFO SortOperator - maxmem = 209715200
12-01-2021 09:07:31.744 INFO SortOperator - maxmem = 209715200
12-01-2021 09:07:31.879 INFO SortOperator - maxmem = 209715200
12-01-2021 09:07:32.021 INFO SortOperator - maxmem = 209715200
12-01-2021 09:07:32.158 INFO SortOperator - maxmem = 209715200
12-01-2021 09:07:32.296 INFO SortOperator - maxmem = 209715200
12-01-2021 09:07:32.436 INFO SortOperator - maxmem = 209715200
12-01-2021 09:07:32.576 INFO SortOperator - maxmem = 209715200
12-01-2021 09:07:32.716 INFO SortOperator - maxmem = 209715200
12-01-2021 09:07:32.847 INFO SortOperator - maxmem = 209715200
12-01-2021 09:07:32.984 INFO SortOperator - maxmem = 209715200
12-01-2021 09:07:33.122 INFO SortOperator - maxmem = 209715200
12-01-2021 09:07:33.263 INFO SortOperator - maxmem = 209715200
12-01-2021 09:07:33.400 INFO SortOperator - maxmem = 209715200
12-01-2021 09:07:33.529 INFO SortOperator - maxmem = 209715200
12-01-2021 09:07:33.664 INFO SortOperator - maxmem = 209715200
12-01-2021 09:07:33.849 INFO BatchSearch - Searching index:app with LISPY: '| [ AND message source:/data/app/*/ [ GTE date_hour 1 ] [ OR [ LT date_hour 23 ] [ AND [ LT date_minute 30 ] [ EQ date_hour 23 ] ] ] [ OR processed [ AND normal_received ] ] ]'
12-01-2021 09:07:35.855 INFO CsvDataProvider - Loading lookup table=dropdownsLookup
12-01-2021 09:14:02.090 INFO BatchSearch - Setting up cache file for bkt=use-4792-B2F38184-60AE-43CF-92DB-3B904F81A8E7
12-01-2021 09:14:02.204 INFO BatchSearch - Setting up cache file for bkt=use-4761-B2F38184-60AE-43CF-92DB-3B904F81A8E7
12-01-2021 09:27:34.932 INFO BatchSearch - Setting up cache file for bkt=use-4806-B2F38184-60AE-43CF-92DB-3B904F81A8E7