Splunk Real time SQL queries

1) Error in the last 24 hours

   error OR failed OR severe OR (sourcetype=access_* (404 OR 500 OR 503))

2) Kv store is not ready

   index=_internal log_level=ERROR sourcetype=splunkd ("KVStore is not ready") earliest=-30m

3) Lookups failed

   index=* sourcetype=* "query failed" | stats count by host | search count > 40

4) Pending jobs> 24 hours

   Jobs pending for more than 24 hours

   index=_internal sourcetype=name Status=PEND Pending_Time>86400 Pending_Reason!="Resource (slot) limit defined on queue has been reached;"

   | table Cluster User Jobid Jobname Status Submit_host Submit_Resreq

   Pending_Reason

5) Splunk errors in last 24 hours

   index=_internal " error " NOT debug source=*splunkd.log*

6) Duplicate IPS

   sourcetype=* "duplicate IP"

7) Search Peer Not Responding

   One or more of your search peers is currently down.

   | rest splunk_server=local /services/search/distributed/peers/

   | where status!="Up" AND disabled=0

   | fields peerName, status

   | rename peerName as Instance, status as Status

8) To find out all successful splunk configuration changes by user:

```
index=_audit action=edit* info=granted operation!=list host= object=*
| transaction action user operation host maxspan=30s
| stats values(action) as action values(object) as modified_object by
_time,operation,user,host
| rename user as modified_by
| table _time action modified_object modified_by
```

9) To find out all fields for an index :

```
index=yourindex| fieldsummary | table field
or,
index=yourindex | stats values(*) AS * | transpose | table column | rename column
AS Fieldnames
or,


index=yourindex | table *
```

10) To find out Failed Versus Successful Logon Attempts

```
source="WinEventLog:security" (Logon_Type=2 OR Logon_Type=7 OR Logon_Type=10)
(EventCode=528 OR EventCode=540 OR EventCode=4624 OR EventCode=4625 OR
EventCode=529 OR EventCode=530 OR EventCode=531 OR EventCode=532 OR
EventCode=533 OR EventCode=534 OR EventCode=535 OR EventCode=536 OR
EventCode=537 OR EventCode=539) | eval status=case(EventCode=528, "Successful
Logon", EventCode=540, "Successful Logon", EventCode=4624, "Successful Logon",
EventCode=4625, "Failed Logon", EventCode=529, "Failed Logon", EventCode=530,
"Failed Logon", EventCode=531, "Failed Logon", EventCode=532, "Failed Logon",
EventCode=533, "Failed Logon", EventCode=534, "Failed Logon", EventCode=535, "Failed
Logon", EventCode=536, "Failed Logon", EventCode=537, "Failed Logon",
EventCode=539, "Failed Logon") | stats count by status | sort - count
```

few windows event codes in splunk (with spl queries), used to appear while splunking :

11) Windows Event Code -4688

Windows defines Event Code 4688 as “A new process has been created," but it’s so much more—any process (or program)
that is started by a user (or even spawned from another process) is logged with this event ID. For instance, if a Windows PC
is infected with malware or a virus, searching code 4688 will show any processes that

were created by that malware.

Query -

```
sourcetype="wineventlog:security"EventCode=4688
| stats count, values(Creator_Process_Name) as Creator_Process_Name by
New_Process_Name
| table New_Process_Name, count, Creator_Process_Name
| sort count
```

Explaination - The search above returns newly created processes as well as their Parent Process ID (if created by a parent process).

12) Windows Event Code -4738

Now onto 4738; it's one of my personal favorites—"A user account was changed." This event is logged whenever a user account is altered, which is especially important when an account is granted Administrator
privileges in a domain or on a standalone Windows machine. I love hunting for this event and looking at anything that occurs
within 2 minutes on either side of it.

Query -

```
index=main
 [search index=main sourcetype=WinEventLog:Security EventCode=4738
 | eval earliest=_time-120
 | eval latest=_time+120
 | fields host,earlist, latest]
| table host, sourcetype, EventCode, Message
```

13) Windows Event Code -4624

Event Code 4624 is created when an account successfully logs into a Windows environment. This information can be used to
create a user baseline of login times and location. This allows Splunk users to determine outliers of normal login, which may
lead to malicious intrusion or a compromised account. Event Code 4624 also records the different types of logons—for instance,
network or local. Using this information, you can find outliers within your network filtering by time or even logon type.

Query -

```
index=main sourcetype="wineventlog:security" EventCode=4624
 | eventstats avg("_time") as avg stdev("_time") as stdev
 | eval lowerBound=(avg-stdev*exact(2)), upperBound=(avg+stdev*exact(2))
 | eval isOutlier=if('_time' < lowerBound OR '_time' > upperBound, 1, 0)
```

```
| table _time, body, isOutlier
```

Explaination - It should produce a list of events and tell you whether they are statistical outliers or not.

14) To find out Splunk users search activity ?

```
index=_audit splunk_server=local action=search (id=* OR search_id=*)
| eval search_id = if(isnull(search_id), id, search_id)
| replace '*' with * in search_id
| rex "search='search\s(?<search>.*?)',\sautojoin"
| search search_id!=scheduler_*
| convert num(total_run_time)
| eval user = if(user="n/a", null(), user)
| stats min(_time) as _time first(user) as user max(total_run_time) as total_run_time
first(search) as search by search_id
| search search!=*_internal* search!=*_audit*
| chart sum(total_run_time) as "Total search time" count as "Search count" max(_time) as
"Last use" by user
| fieldformat "Last use" = strftime('Last use', "%F %T.%Q")
```

15) To find out all props and transforms information in detail?

```
| rest /servicesNS/-/-/admin/directory count=0 splunk_server=local | fields eai:acl.app,
eai:acl.owner, eai:acl.perms.*, eai:acl.sharing, title, eai:type, disabled
| foreach eai:*.*
[ rename "<<FIELD>>" TO <<MATCHSEG2>> ]
| foreach eai:*
[ rename "<<FIELD>>" TO <<MATCHSTR>> ]
| eval attribute=replace(title,"(.*:\s+)(.*)","\2")
| eval st=replace(title,"(.*)(\s+:.*)","\1")
| eval props_sourcetype=if(st==attribute,"",st)
| join type=outer attribute
[| rest /servicesNS/-/-/admin/props-extract count=0 splunk_server=local | fields attribute
value stanza type | rename value TO props_value, stanza to props_stanza, type to
props_type ]
| join type=outer attribute
[| rest /servicesNS/-/-/admin/transforms-extract count=0 splunk_server=local
| fields REGEX FORMAT disabled eai:acl.app title FIELDS
| makemv delim="," FIELDS
| rename FIELDS to tf_fields, disabled to tf_disabled, REGEX to tf_regex, FORMAT to
tf_format, title to attribute, eai:acl.app to tf_app]
| fillnull disabled tf_disabled
| table disabled app type attribute props_type props_stanza props_value
props_sourcetype tf_disabled tf_format tf_fields tf_regex sharing perms.* location owner |
```

```
search (app="*" AND (sharing="*")) AND disabled=*
| rename attribute TO "Object Name"
```

16) To find out Bucket count by index?

```
|dbinspect index=* | chart dc(bucketId) over splunk_server by index
```

17) Query to calculate (currentDBSizeMB) per index:

```
| rest /services/data/indexes | stats sum(currentDBSizeMB) by title splunk_server
```

18) Query to calculate to display disk space utilized by each app in splunk:

```
index=_internal metrics kb group=per_sourcetype_thruput | eval sizeMB =
round(kb/1024,2)| stats sum(sizeMB) by series | sort -sum(sizeMB) | rename sum(sizeMB)
AS "Size on Disk (MB)"
```

19) Query to check version of all apps and add-ons installed on Splunk:

```
| rest /services/apps/local | search disabled=0 core=0|dedup label | table label version
```