# License Master Monitoring (0 MB license Usage Overall & per Pool)

1. REST Based Approach:
   1. Overall license Usage on the license Master is 0 MB (with REST)
   2. License Usage per Pool is 0 MB (with REST)
   3. Issue with REST based search
2. REST and Internal Logs:
   1. Overall license Usage on the license Master is 0 MB (Internal logs)
   2. License Usage per Pool is 0 MB (with REST & Internal logs)

When there are any connectivity issues and License master does not receive any License information from the Slave Indexers, these two alerts can be used to trigger an alarm as an indicator.

REST Based Approach:

1. a. Overall license Usage on the license Master is 0 MB

| rest splunk\_server=local /services/licenser/pools | rename title AS Pool

| search [rest splunk\_server=local /services/licenser/groups | search is\_active=1

| eval stack\_id=stack\_ids | fields stack\_id] | stats sum(used\_bytes) as used

| eval usedMB=round(used/1024/1024,3)

| table usedMB

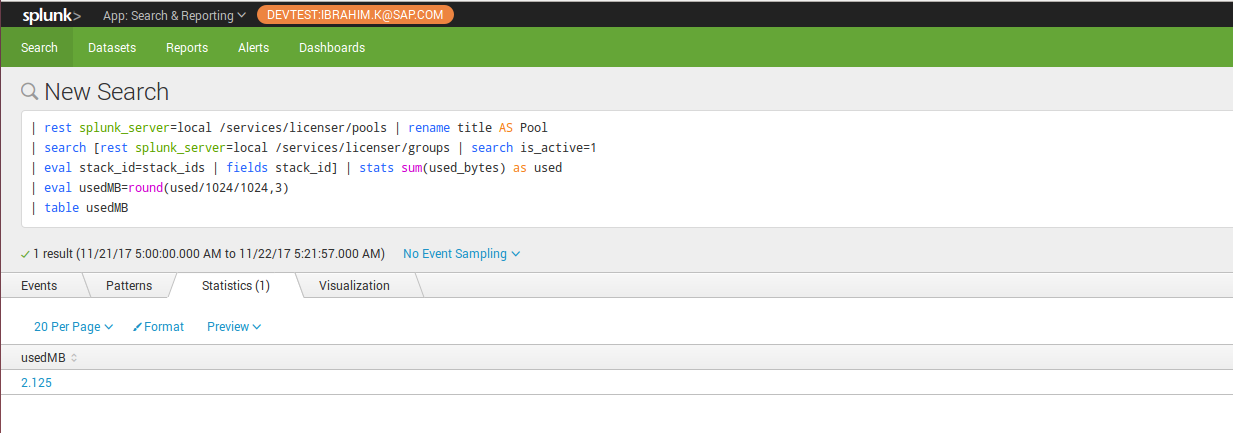
rest splunk\_server=local /services/licenser/pools | rename title AS Pool

| search [rest splunk\_server=local /services/licenser/groups | search is\_active=1

| eval stack\_id=stack\_ids | fields stack\_id] | stats sum(used\_bytes) as used

| eval usedMB=round(used/1024/1024,3)

| table usedMB



Above search fetches the overall license usage for all active license groups and this can be used as an alert to be generated when the value is zero. It means that there is no license usage reported by any of the Slave machine from mid-night till now.

This alert can be scheduled for a custom trigger condition where the usedMB is less than 1.

1. b. License Usage per Pool is 0 MB

| rest splunk\_server=local /services/licenser/pools | rename title AS Pool

| search [rest splunk\_server=local /services/licenser/groups | search is\_active=1

| eval stack\_id=stack\_ids | fields stack\_id] | table Pool

| join type=outer Pool

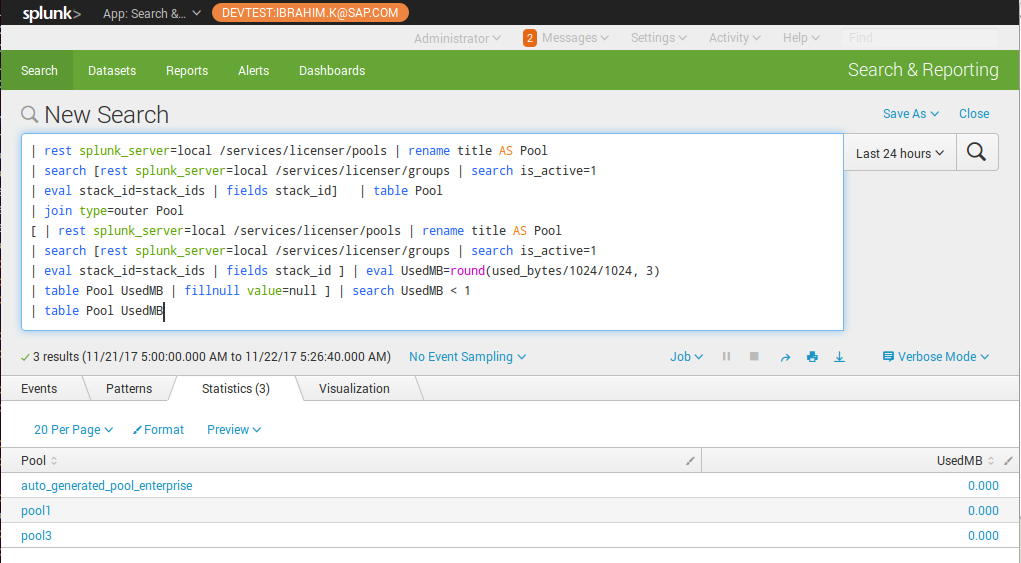
[ | rest splunk\_server=local /services/licenser/pools | rename title AS Pool

| search [rest splunk\_server=local /services/licenser/groups | search is\_active=1

| eval stack\_id=stack\_ids | fields stack\_id ] | eval UsedMB=round(used\_bytes/1024/1024, 3)

| table Pool UsedMB | fillnull value=null ] | search UsedMB < 1

| table Pool UsedMB



Above search fetches all the pools and its usage of license from mid-night, and if there is any pool which have zero license usage (no license usage value).

This alert can be triggered per pool when there is no license usage reported from mid-night until the alert scheduled time.

This alert can be scheduled for a custom trigger condition where the usedMB value is null for each pool.

1. c. Issue with the REST based search:

In the REST API endpoint, we have the license usage information from the mid-night to the present time. This will give you an alert when you do not have any license usage from mid-night, means there are no logs reported from the licensing Slave indexers.

If the license slaves sent license information to the License master after mid-night and it stopped sending in the middle of the day, the license usage will be there until the next day. In this case the zero-license usage check will not be triggered.

REST and Internal Logs:

This approach will use both the REST API details and the internal logs to check the overall license usage and per pool license usage.

1. a. Overall license Usage on the license Master is 0 MB (Internal logs)

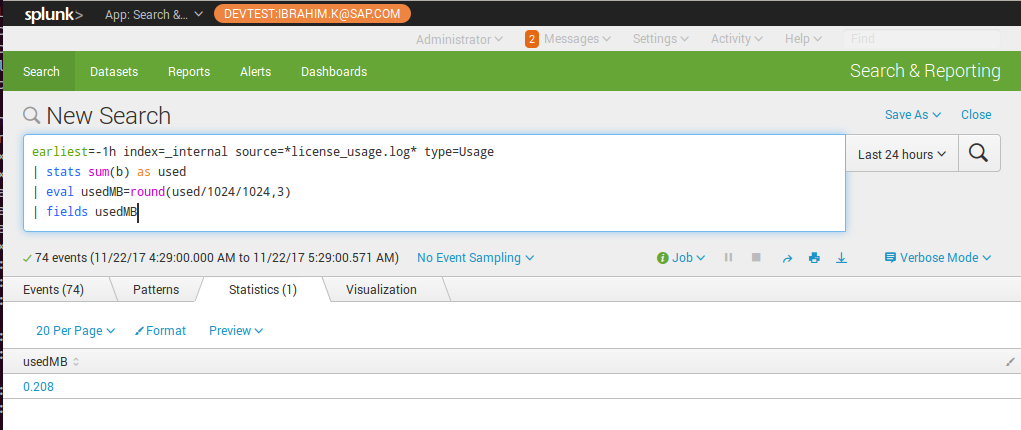
For the overall license usage check for a period, we do not need the information from the Splunk REST API. Check the license\_usage.log for the last few hours for the license usage data. If there is no license information for a period, indicates none of the Slave indexers have sent the license information to the License Master for that period.

earliest=-1h index=\_internal source=\*license\_usage.log\* type=Usage

| stats sum(b) as used

| eval usedMB=round(used/1024/1024,3)

| fields usedMB



This alert can be triggered when the usedMB is nearly zero, which indicates that none of the slaves have reported license usage for last one hour.

1. b. License Usage per Pool is 0 MB (with REST & Internal logs)

Fetch the active pool information from the REST and compare this with the license information received from the Slave for each active pool. If there is no data available for any active pools, license usage information is missing for some active pools, it will trigger an alert with the pool details.

| rest splunk\_server=local /services/licenser/pools | rename title AS Pool

| search [rest splunk\_server=local /services/licenser/groups | search is\_active=1

| eval stack\_id=stack\_ids

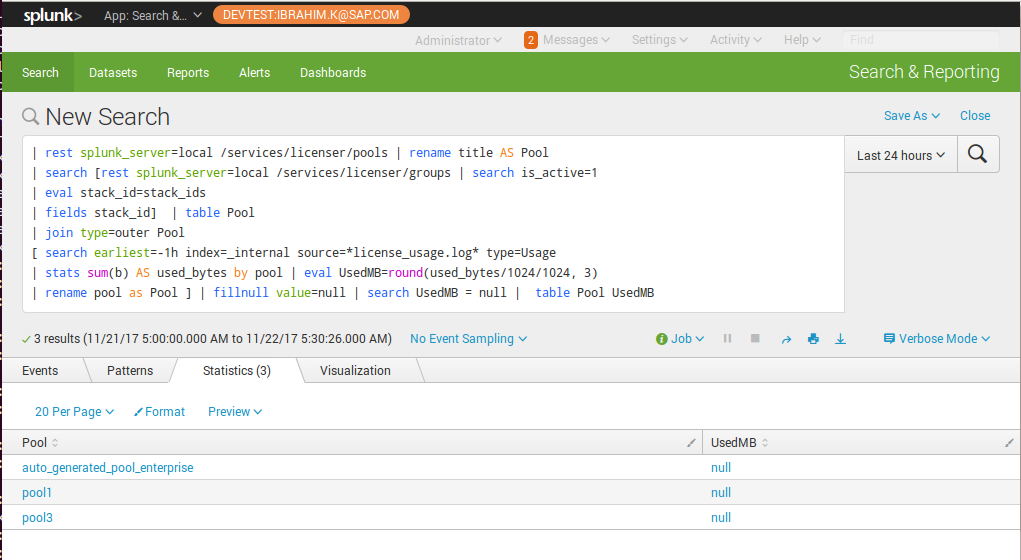
| fields stack\_id] | table Pool

| join type=outer Pool

[ search earliest=-1h index=\_internal source=\*license\_usage.log\* type=Usage

| stats sum(b) AS used\_bytes by pool | eval UsedMB=round(used\_bytes/1024/1024, 3)

| rename pool as Pool ] | fillnull value=null | search UsedMB = null | table Pool UsedMB



This alert can be triggered for each pool where usedMB is null, which indicates that there are no license usage reported for the particular pool for the last one hour.