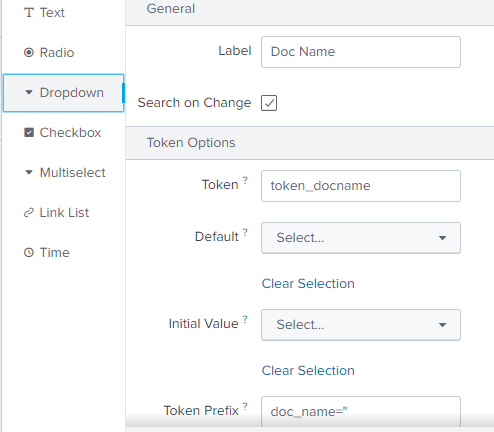
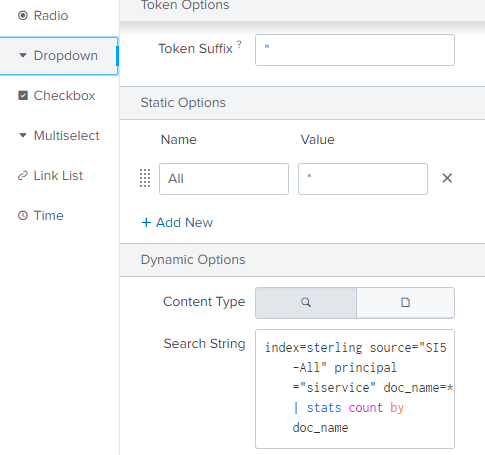
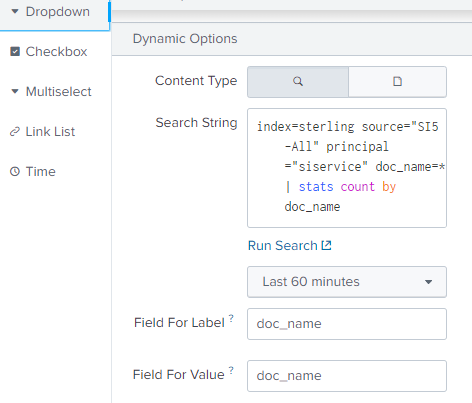
Splunk dropdown syntax:







index=sterling source="SI5-All" principal="siservice" doc\_name=\* | stats count by doc\_name

index=sterling sourcetype="SI5\*" source="SI5-All" doc\_name="\*" $token\_docname$

| eval FileSize(KB)=round(fileSizeBytes/1024,2)

| table connection\_start\_time principal doc\_name FileSize(KB) state

| sort - connection\_start-time

(index=sterling host="ms-si0-d01" sourcetype="SI5:Jobs" file\_name="PX\*") | stats count by file\_name

index=sterling sourcetype="SI5\*" source="SI5-All" doc\_name="\*" $token\_docname$

| eval FileSize(KB)=round(fileSizeBytes/1024,2)

| table connection\_start\_time principal doc\_name FileSize(KB) state

| sort - connection\_start-time