Data stream :

Create data stream :PUT \_data\_stream/logs-test

Check the data stream status:GET \_data\_stream/logs-tes

Output:

{

"data\_streams": [

{

"name": "logs-test",

"timestamp\_field": {

"name": "@timestamp"

},

"indices": [

{

"index\_name": ".ds-logs-test-000001",

"index\_uuid": "Yr2UXtg1RUqTVhmtn9i4XQ"

},

{

"index\_name": ".ds-logs-test-000002",

"index\_uuid": "i838VkbYQMmjNfUyqQSrBg"

}

],

"generation": 2,

"status": "YELLOW",

"template": "logs-test"

}

]

}

Create Index pattern:

PUT \_index\_template/logs-test

{

"index\_patterns":[

"logs-test"

],

"data\_stream":{

"timestamp\_field": {

"name":"@timestamp"

}

},

"priority":200,

"template":{

"settings":{

"number\_of\_shards":2

}

}

}

Check the template :GET /\_index\_template/logs-test

Output:

{

"index\_templates": [

{

"name": "logs-test",

"index\_template": {

"index\_patterns": [

"logs-test"

],

"template": {

"settings": {

"index": {

"number\_of\_shards": "2"

}

}

},

"composed\_of": [],

"priority": 200,

"data\_stream": {

"timestamp\_field": {

"name": "@timestamp"

}

}

}

}

]

}

Ingest data to data stream:

POST logs-test/\_doc

{

"message":"login not success",

"@timestamp":"2023-04-09T00:00:00"

}

Bulk Ingest :

PUT /logs-test/\_bulk?refresh

{"create":{ }}

{ "@timestamp": "2023-04-06T11:04:05.000Z", "message": "Login attempt failed" }

{"create":{ }}

{ "@timestamp": "2099-04-06T12:06:07.000Z", "message": "login successful" }

{"create":{ }}

{ "@timestamp": "2099-04-06T06:07:08.000Z", "message": "logout successful" }

Check the data ingestion status:

GET logs-test/\_search

{

"size": 20

}

Delete data stream:DELETE /\_index\_template/template\_3

Data rollover: POST logs-test/\_rollover

Output:

{

"acknowledged": true,

"shards\_acknowledged": true,

"old\_index": ".ds-logs-test-000001",

"new\_index": ".ds-logs-test-000002",

"rolled\_over": true,

"dry\_run": false,

"conditions": {}

}

///Split index///

PUT .ds-logs-test-000002/\_split/.ds-logs-test-000002-target

{

"settings":{

"index.number\_of\_shards": 4

}

}

Get error of this:

{

"error": {

"root\_cause": [

{

"type": "illegal\_state\_exception",

"reason": "index .ds-logs-test-000002 must be read-only to resize index. use \"index.blocks.write=true\""

}

],

"type": "illegal\_state\_exception",

"reason": "index .ds-logs-test-000002 must be read-only to resize index. use \"index.blocks.write=true\""

},

"status": 500

}

Reseaon: Your index need to make an index read-only

To change it to read only :

PUT .ds-logs-test-000002/\_settings

{

"index": {

"blocks.read\_only": true

}

}

Then try to split command again and get the result as:

{

"acknowledged": true,

"shards\_acknowledged": true,

"index": ".ds-logs-test-000002-target"

}

Shrink

PUT .ds-logs-test-000002-target/\_shrink/.ds-logs-test-000002-target-shrink1

{

"settings": {

"index.number\_of\_replicas": 2,

"index.number\_of\_shards": 2

}

}

GET .ds-logs-test-000002-target-shrink1/\_search\_shards

Condition of data rollover:

POST logs-test/\_rollover

{

"conditions": {

"max\_docs": 1,

"max\_age": "10m",

"max\_size": "5gb"

}

}

Output:

{

"acknowledged": true,

"shards\_acknowledged": true,

"old\_index": ".ds-logs-test-000004",

"new\_index": ".ds-logs-test-000005",

"rolled\_over": true,

"dry\_run": false,

"conditions": {

"[max\_age: 10m]": false,

"[max\_docs: 1]": true,

"[max\_size: 5gb]": false

}

}