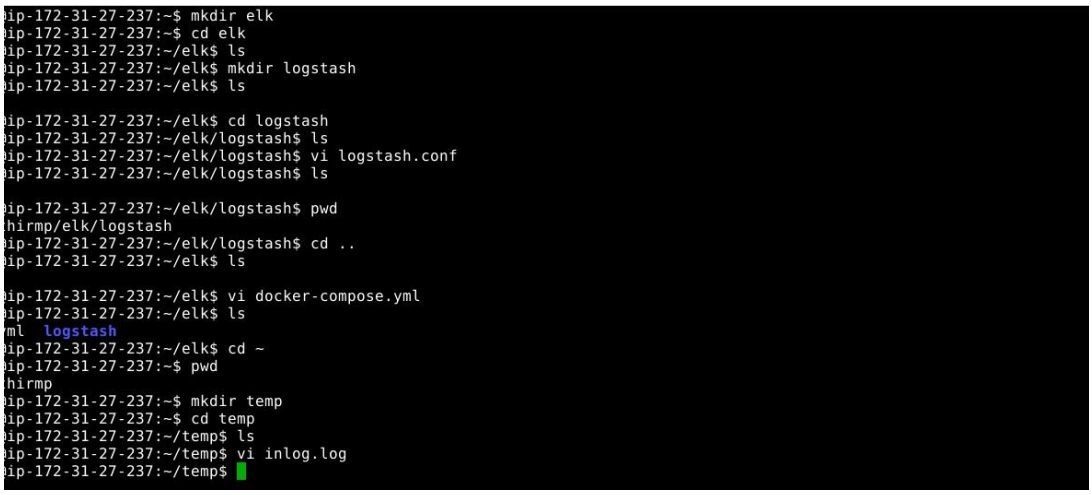
Phase 5: (Practice Project)

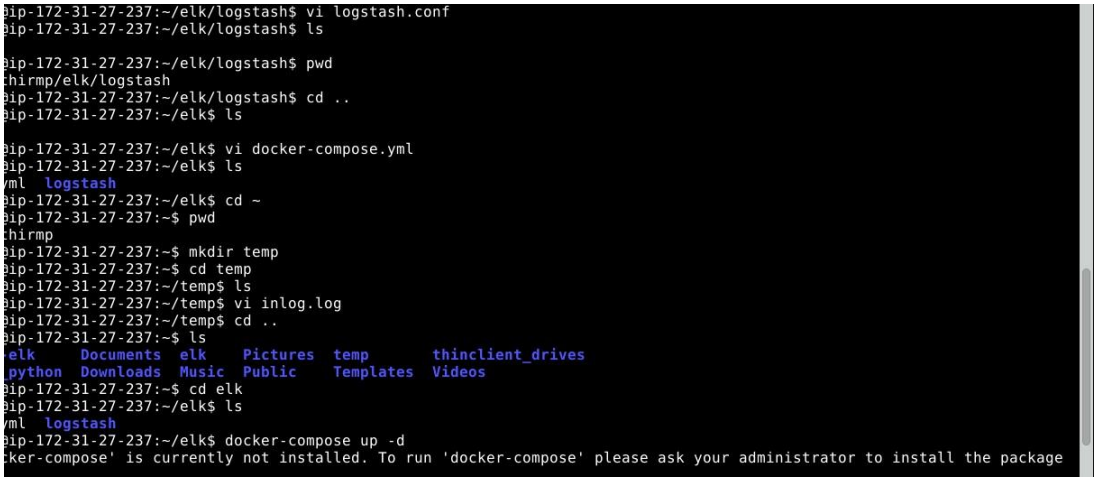
Screen shots for Deploying ELK Stack on Docker Container..

(Developed By: Ullas H P)

1. Run docker Container

2. Creating yml and log files:

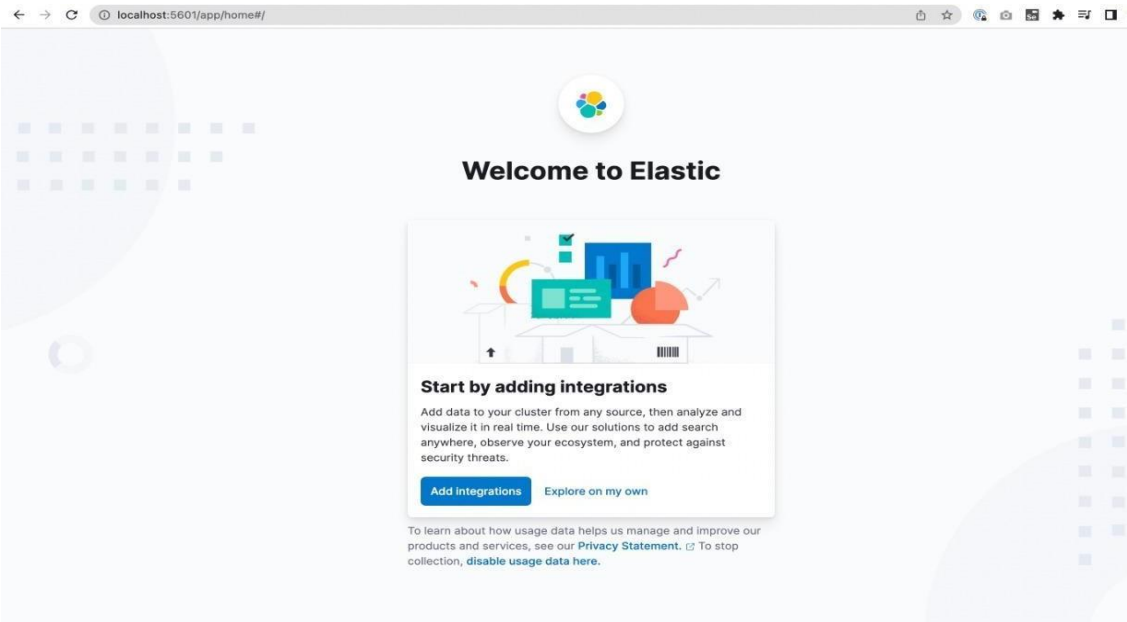




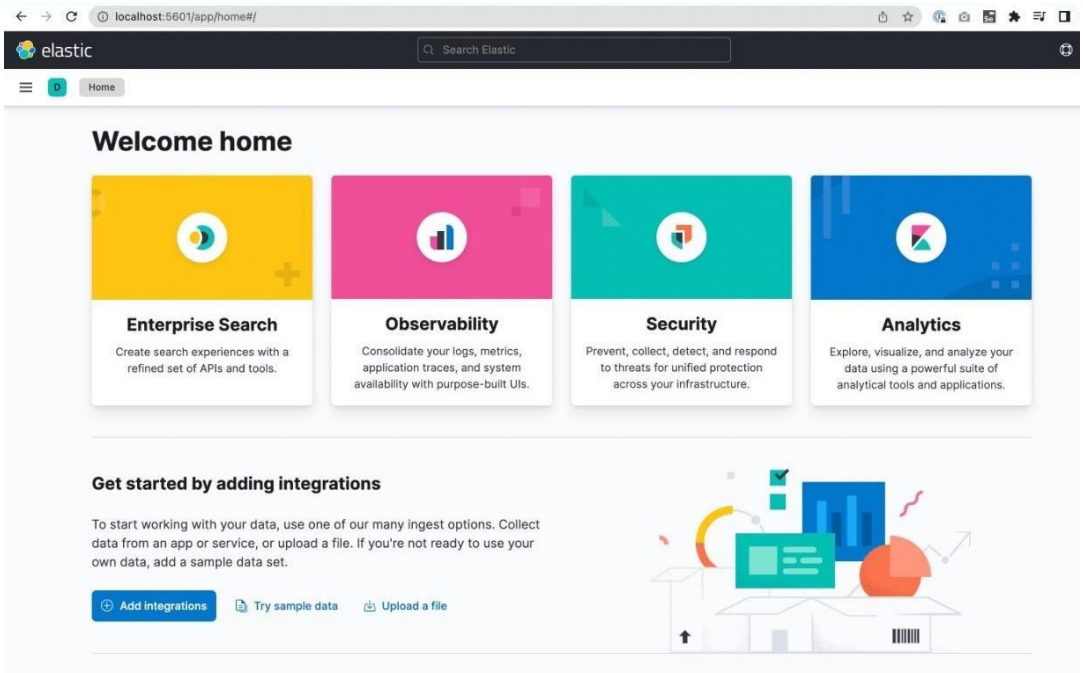
3. Installing ELK stack

ng_alert_logstash_version_mismatch\",\"alerting:monitoring_alert_kibana_version_mismatch\",\"alerting:monitoring_alert_elasticsearch_version_mismatch\",\"alerting:monitoring_ccr_read_exceptions\",\"alert
ng:monitoring_shard_size\",\"alerting:apm.transaction_duration\",\"alerting:apm.transaction_duration_anomaly\",\"alerting:apm.error_rate\",\"alerting:apm.transaction_error_rate\"],\"skippedTaskTypes\":[\"
report:execute\"],\"taskMaxAttempts\":{\"session_cleanup\":3,\"reports:monitor\":1,\"search_sessions_monitor\":3,\"search_sessions_cleanup\":3,\"search_sessions_expire\":3,\"actions:.email\":1,\"actions:.
index\":1,\"actions:.pagerduty\":1,\"actions:.swimlane\":1,\"actions:.server-log\":1,\"actions:.slack\":1,\"actions:.webhook\":1,\"actions:.servicenow\":1,\"actions:.servicenow-sir\":1,\"actions:.servicen
ow-itom\":1,\"actions:.jira\":1,\"actions:.resilient\":1,\"actions:.teams\":1,\"actions_telemetry\":3,\"cleanup_failed_action_executions\":3,\"alerting_telemetry\":3,\"alerts_invalidate_api_keys\":3,\"ale
rting_health_check\":3,\"lens_telemetry\":3,\"endpoint:user-artifact-packager\":3,\"security:endpoint-diagnostics\":3,\"security:endpoint-meta-telemetry\":3,\"security:telemetry-lists\":3,\"security:telem
etry-detection-rules\":3,\"endpoint:metadata-check-transforms-task\":3,\"apm-telemetry-task\":3,\"alerting:transform_health\":3,\"alerting:.index-threshold\":3,\"alerting:.geo-containment\":3,\"alerting:.
es-query\":3,\"alerting:xpack.ml.anomaly_detection_alert\":3,\"alerting:xpack.ml.anomaly_detection_jobs_health\":3,\"alerting:xpack.uptime.alerts.monitorStatus\":3,\"alerting:xpack.uptime.alerts.tlsCertif
icate\":3,\"alerting:xpack.uptime.alerts.durationAnomaly\":3,\"alerting:xpack.uptime.alerts.tls\":3,\"alerting:siem.signals\":3,\"alerting:siem.notifications\":3,\"alerting:metrics.alert.anomaly\":3,\"ale
rting:logs.alert.document.count\":3,\"alerting:metrics.alert.inventory.threshold\":3,\"alerting:metrics.alert.threshold\":3,\"alerting:monitoring_alert_cluster_health\":3,\"alerting:monitoring_alert_licen
se_expiration\":3,\"alerting:monitoring_alert_cpu_usage\":3,\"alerting:monitoring_alert_missing_monitoring_data\":3,\"alerting:monitoring_alert_disk_usage\":3,\"alerting:monitoring_alert_thread_pool_searc
h_rejections\":3,\"alerting:monitoring_alert_thread_pool_write_rejections\":3,\"alerting:monitoring_alert_jvm_memory_usage\":3,\"alerting:monitoring_alert_nodes_changed\":3,\"alerting:monitoring_alert_log
stash_version_mismatch\":3,\"alerting:monitoring_alert_kibana_version_mismatch\":3,\"alerting:monitoring_alert_elasticsearch_version_mismatch\":3,\"alerting:monitoring_ccr_read_exceptions\":3,\"alerting:m
onitoring_shard_size\":3,\"alerting:apm.transaction_duration\":3,\"alerting:apm.transaction_duration_anomaly\":3,\"alerting:apm.error_rate\":3,\"alerting:apm.transaction_error_rate\":3}}},\"sort\":[{\"_sc
ript\":{\"type\":\"number\",\"order\":\"asc\",\"script\":{\"lang\":\"painless\",\"source\":\"\\nif (doc['task.retryAt'].size()!=0) {\\n return doc['task.retryAt'].value.toInstant().toEpochMilli();\\n}\\n
if (doc['task.runAt'].size()!=0) {\\n return doc['task.runAt'].value.toInstant().toEpochMilli();\\n}\\n   \"}}}],\"max_docs\":10}"}
kibana | {"type":"log","@timestamp":"2022-10-09T13:52:26+00:00","tags":["info","elasticsearch","deprecation"],"pid":6,"message":"Elasticsearch deprecation: 299 Elasticsearch-7.16.2-2b937c44140b655
9905130a8650c64dbd0879cfb \"Elasticsearch built-in security features are not enabled. Without authentication, your cluster could be accessible to anyone. See https://www.elastic.co/guide/en/elasticsearch/
reference/7.16/security-minimal-setup.html to enable security.\"\nOrigin:kibana\nQuery:\n200\nPOST /.kibana_task_manager/_update_by_query?ignore_unavailable=true&refresh=true&conflicts=proceed\n{\"query\"
:{\"bool\":{\"must\":[{\"term\":{\"type\":\"task\"}},{\"bool\":{\"must\":[{\"bool\":{\"should\":[{\"bool\":{\"must\":[{\"term\":{\"task.status\":\"idle\"}},{\"range\":{\"task.runAt\":{\"lte\":\"now\"}}}]}
},{\"bool\":{\"must\":[{\"bool\":{\"should\":[{\"term\":{\"task.status\":\"running\"}},{\"term\":{\"task.status\":\"claiming\"}}]}},{\"range\":{\"task.retryAt\":{\"lte\":\"now\"}}}]}}]}}]}},\"filter\":[{\"b
ool\":{\"must_not\":[{\"bool\":{\"should\":[{\"term\":{\"task.status\":\"running\"}},{\"term\":{\"task.status\":\"claiming\"}}],\"must\":{\"range\":{\"task.retryAt\":{\"gt\":\"now\"}}}}}}]}}],\"script
\":{\"source\":\"\\n   if (params.claimableTaskTypes.contains(ctx._source.task.taskType)) {\\n   if (ctx._source.task.schedule != null || ctx._source.task.attempts < params.taskMaxAttempts[ctx._source
.task.taskType] || params.claimTasksById.contains(ctx._id)) {\\n   ctx._source.task.status = \\\"claiming\\\"; ctx._source.task.ownerId=params.fieldUpdates.ownerId; ctx._source.task.retryAt=params.fi
eldUpdates.retryAt;\\n   } else {\\n   ctx._source.task.status = \\\"failed\\\";\\n   }\\n   } else if (params.skippedTaskTypes.contains(ctx._source.task.taskType) && params.claimTasksById.con
tains(ctx._id)) {\\n   ctx._source.task.status = \\\"claiming\\\"; ctx._source.task.ownerId=params.fieldUpdates.ownerId; ctx._source.task.retryAt=params.fieldUpdates.retryAt;\\n   } else if (!params.s
kippedTaskTypes.contains(ctx._source.task.taskType)) {\\n   ctx._source.task.status = \\\"unrecognized\\\";\\n   } else {\\n   ctx.op = \\\"noop\\\";\\n   }\",\"lang\":\"painless\",\"params\":{\"f
ieldUpdates\":{\"ownerId\":\"kibana:5913500c-a11d-4b26-8e7a-ee8cc25a1376\",\"retryAt\":\"2022-10-09T13:52:56.257Z\"},\"claimTasksById\":[],\"claimableTaskTypes\":[\"report:execute\"],\"skippedTaskTypes\":
[\"session_cleanup\",\"reports:monitor\",\"search_sessions_monitor\",\"search_sessions_cleanup\",\"search_sessions_expire\",\"actions:.email\",\"actions:.index\",\"actions:.pagerduty\",\"actions:.swimlane
\",\"actions:.server-log\",\"actions:.slack\",\"actions:.webhook\",\"actions:.servicenow\",\"actions:.servicenow-sir\",\"actions:.servicenow-itom\",\"actions:.jira\",\"actions:.resilient\",\"actions:.team
s\",\"actions_telemetry\",\"cleanup_failed_action_executions\",\"alerting_telemetry\",\"alerts_invalidate_api_keys\",\"alerting_health_check\",\"lens_telemetry\",\"endpoint:user-artifact-packager\",\"secu
rity:endpoint-diagnostics\",\"security:endpoint-meta-telemetry\",\"security:telemetry-lists\",\"security:telemetry-detection-rules\",\"endpoint:metadata-check-transforms-task\",\"apm-telemetry-task\",\"al
erting:transform_health\",\"alerting:.index-threshold\",\"alerting:.geo-containment\",\"alerting:.es-query\",\"alerting:xpack.ml.anomaly_detection_alert\",\"alerting:xpack.ml.anomaly_detection_jobs_health
\",\"alerting:xpack.uptime.alerts.monitorStatus\",\"alerting:xpack.uptime.alerts.tlsCertificate\",\"alerting:xpack.uptime.alerts.durationAnomaly\",\"alerting:xpack.uptime.alerts.tls\",\"alerting:siem.sign
als\",\"alerting:siem.notifications\",\"alerting:metrics.alert.anomaly\",\"alerting:logs.alert.document.count\",\"alerting:metrics.alert.inventory.threshold\",\"alerting:metrics.alert.threshold\",\"alerti
ng:monitoring_alert_cluster_health\",\"alerting:monitoring_alert_license_expiration\",\"alerting:monitoring_alert_cpu_usage\",\"alerting:monitoring_alert_missing_monitoring_data\",\"alerting:monitoring_al
ert_disk_usage\",\"alerting:monitoring_alert_thread_pool_search_rejections\",\"alerting:monitoring_alert_thread_pool_write_rejections\",\"alerting:monitoring_alert_jvm_memory_usage\",\"alerting:monitoring
_alert_nodes_changed\",\"alerting:monitoring_alert_logstash_version_mismatch\",\"alerting:monitoring_alert_kibana_version_mismatch\",\"alerting:monitoring_alert_elasticsearch_version_mismatch\",\"alerting
:monitoring_ccr_read_exceptions\",\"alerting:monitoring_shard_size\",\"alerting:apm.transaction_duration\",\"alerting:apm.transaction_duration_anomaly\",\"alerting:apm.error_rate\",\"alerting:apm.transact
ion_error_rate\"],\"taskMaxAttempts\":{\"report:execute\":1}}},\"sort\":[{\"_script\":{\"type\":\"number\",\"order\":\"asc\",\"script\":{\"lang\":\"painless\",\"source\":\"\\nif (doc['task.retryAt'].size(
)!=0) {\\n return doc['task.retryAt'].value.toInstant().toEpochMilli();\\n}\\nif (doc['task.runAt'].size()!=0) {\\n return doc['task.runAt'].value.toInstant().toEpochMilli();\\n}\\n   \"}}},\"max_docs
\":1}"}
kibana | {"type":"log","@timestamp":"2022-10-09T13:52:28+00:00","tags":["info","elasticsearch","deprecation"],"pid":6,"message":"Elasticsearch deprecation: 299 Elasticsearch-7.16.2-2b937c44140b655
9905130a8650c64dbd0879cfb \"Elasticsearch built-in security features are not enabled. Without authentication, your cluster could be accessible to anyone. See https://www.elastic.co/guide/en/elasticsearch/
reference/7.16/security-minimal-setup.html to enable security.\"\nOrigin:kibana\nQuery:\n200\nGET /_nodes?filter_path=nodes.*.version%2Cnodes.*.http.publish_address%2Cnodes.*.ip"}
^CGracefully stopping... (press Ctrl+C again to force)
[+] Running 3/3
 ⠿ Container logstash   Stopped

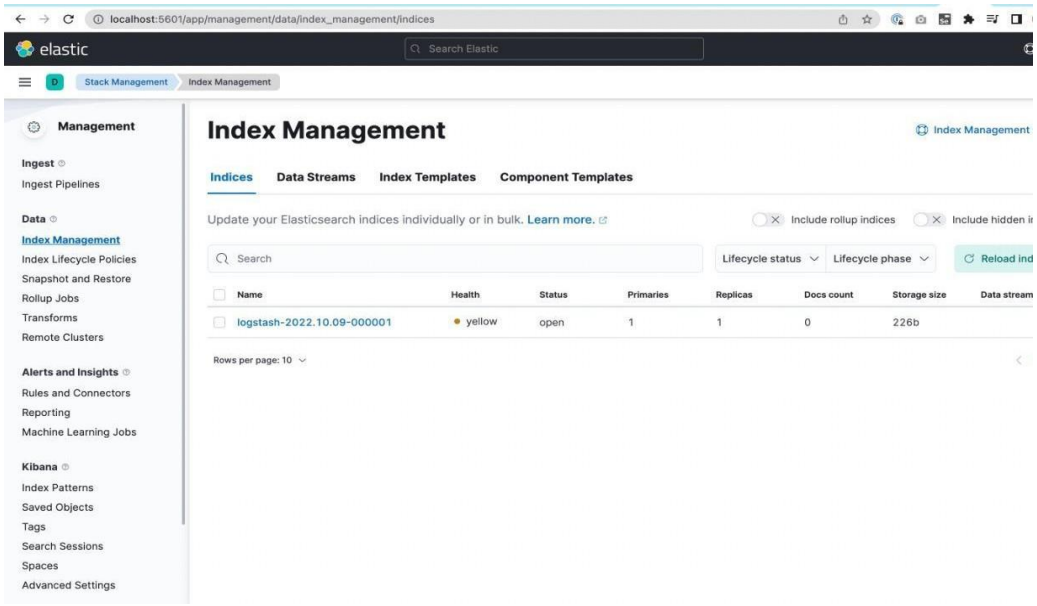
4. Run Localhost:5601 to connect with Elastic:



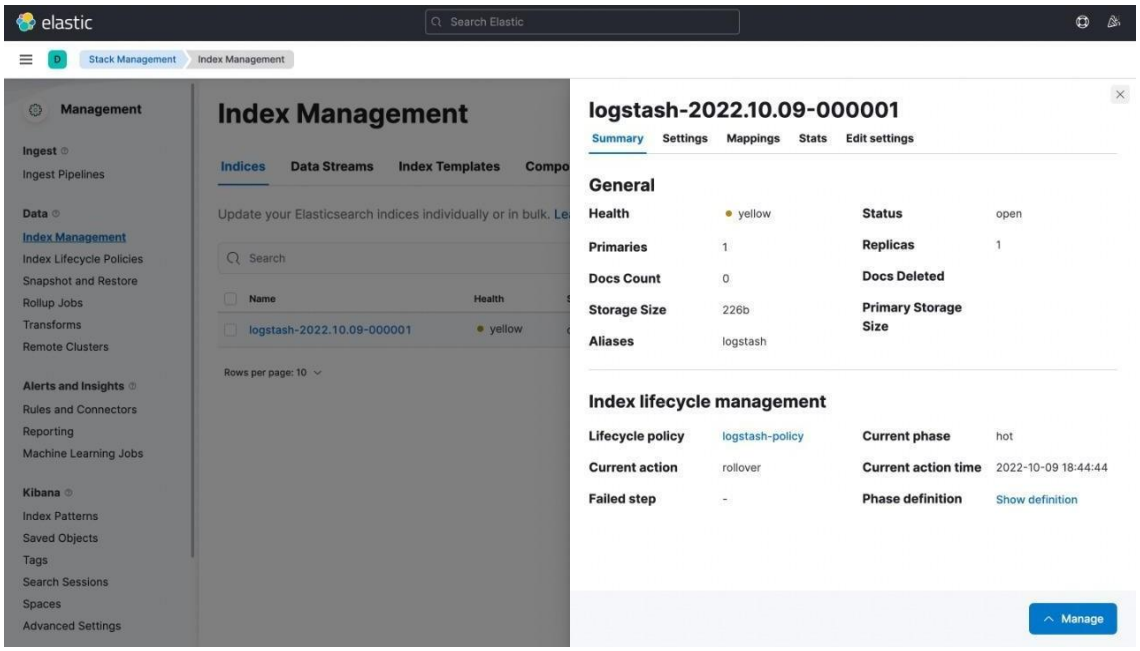
5. Explore the integrations:

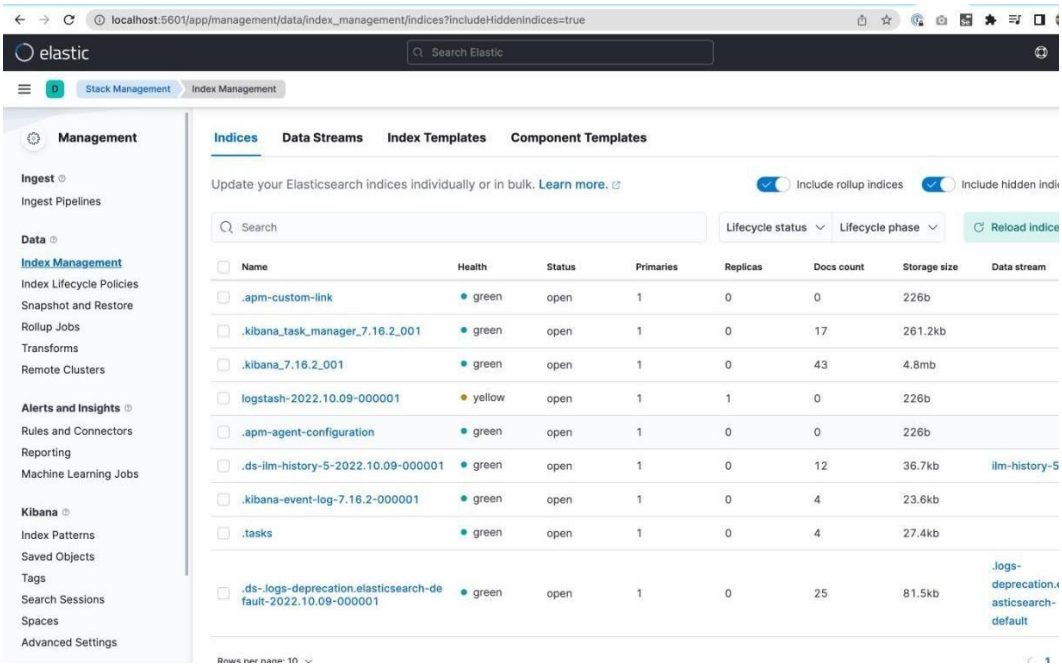


6. Index Management:



7. Check Status of log file:




localhost:5601/app/management/data/index_management/indices?includeHiddenIndices=true
elastic
Search Elastic
Stack Management
Index Management
Management
Ingest
Ingest Pipelines
Data
Index Management
Index Lifecycle Policies
Snapshot and Restore
Rollup Jobs
Transforms
Remote Clusters
Alerts and Insights
Rules and Connectors
Reporting
Machine Learning Jobs
Kibana
Index Patterns
Saved Objects
Tags
Search Sessions
Spaces
Advanced Settings
Indices
Data Streams
Index Templates
Component Templates
Update your Elasticsearch indices individually or in bulk. Learn more.
Include rollup indices
Search
Lifecycle status
Lifecycle phase
Reload indice
Name
Health
Status
Primaries
Replicas
Docs count
Storage size
Data stream
.apm-custom-link
green
open
1
0
0
226b
.kibana_task_manager_7.16.2_001
green
open
1
0
17
261.2kb
.kibana_7.16.2_001
green
open
1
0
43
4.8mb
logstash-2022.10.09-000001
yellow
open
1
1
0
226b
.apm-agent-configuration
green
open
1
0
0
226b
.ds-ilm-history-5-2022.10.09-000001
green
open
1
0
12
36.7kb
ilm-history-5
.kibana-event-log-7.16.2-000001
green
open
1
0
4
23.6kb
.tasks
green
open
1
0
4
27.4kb
.ds-.logs-deprecation.elasticsearch-default-2022.10.09-000001
green
open
1
0
25
81.5kb
.logs-deprecation.elasticsearch-default