vagrant@vagrant:~/10-monitoring-04-elk/elk2$ docker-compose down

Stopping filebeat ... done

Stopping logstash ... done

Stopping kibana ... done

Stopping some\_app ... done

Removing filebeat ... done

Removing logstash ... done

Removing kibana ... done

Removing es-hot ... done

Removing es-warm ... done

Removing some\_app ... done

Removing network elk2\_elastic

Removing network elk2\_default

vagrant@vagrant:~/10-monitoring-04-elk/elk2$ docker-compose up --d

Creating network "elk2\_elastic" with driver "bridge"

Creating network "elk2\_default" with the default driver

Creating es-warm ... done

Creating some\_app ... done

Creating es-hot ... done

Creating logstash ... done

Creating kibana ... done

Creating filebeat ... done

vagrant@vagrant:~/10-monitoring-04-elk/elk2$ docker exec -it es-hot /bin/bash

elasticsearch@f993591b13b4:~$ cd /usr/share/elasticsearch

elasticsearch@f993591b13b4:~$ bin/elasticsearch-create-enrollment-token --scope kibana

WARNING: Owner of file [/usr/share/elasticsearch/config/users] used to be [root], but now is [elasticsearch]

WARNING: Owner of file [/usr/share/elasticsearch/config/users\_roles] used to be [root], but now is [elasticsearch]

ERROR: Failed to determine the health of the cluster.

elasticsearch@f993591b13b4:~$ exit

exit

vagrant@vagrant:~/10-monitoring-04-elk/elk2$ docker logs --details es-hot

Created elasticsearch keystore in /usr/share/elasticsearch/config/elasticsearch.keystore

{"@timestamp":"2024-02-03T12:47:20.034Z", "log.level": "INFO", "message":"version[8.7.0], pid[178], build[docker/09520b59b6bc1057340b55750186466ea715e30e/2023-03-27T16:31:09.816451435Z], OS[Linux/5.4.0-135-generic/amd64], JVM[Oracle Corporation/OpenJDK 64-Bit Server VM/19.0.2/19.0.2+7-44]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.node.Node","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:47:20.069Z", "log.level": "INFO", "message":"JVM home [/usr/share/elasticsearch/jdk], using bundled JDK [true]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.node.Node","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:47:20.076Z", "log.level": "INFO", "message":"JVM arguments [-Des.networkaddress.cache.ttl=60, -Des.networkaddress.cache.negative.ttl=10, -Djava.security.manager=allow, -XX:+AlwaysPreTouch, -Xss1m, -Djava.awt.headless=true, -Dfile.encoding=UTF-8, -Djna.nosys=true, -XX:-OmitStackTraceInFastThrow, -Dio.netty.noUnsafe=true, -Dio.netty.noKeySetOptimization=true, -Dio.netty.recycler.maxCapacityPerThread=0, -Dlog4j.shutdownHookEnabled=false, -Dlog4j2.disable.jmx=true, -Dlog4j2.formatMsgNoLookups=true, -Djava.locale.providers=SPI,COMPAT, --add-opens=java.base/java.io=ALL-UNNAMED, -Des.cgroups.hierarchy.override=/, -XX:+UseG1GC, -Djava.io.tmpdir=/tmp/elasticsearch-9773168984894802824, -XX:+HeapDumpOnOutOfMemoryError, -XX:+ExitOnOutOfMemoryError, -XX:HeapDumpPath=data, -XX:ErrorFile=logs/hs\_err\_pid%p.log, -Xlog:gc\*,gc+age=trace,safepoint:file=logs/gc.log:utctime,level,pid,tags:filecount=32,filesize=64m, -Xms1g, -Xmx1g, -XX:MaxDirectMemorySize=536870912, -XX:G1HeapRegionSize=4m, -XX:InitiatingHeapOccupancyPercent=30, -XX:G1ReservePercent=15, -Des.distribution.type=docker, --module-path=/usr/share/elasticsearch/lib, --add-modules=jdk.net, -Djdk.module.main=org.elasticsearch.server]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.node.Node","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:15.359Z", "log.level": "INFO", "message":"Package versions: jackson-core=2.13.4, jackson-databind=2.13.4-2, jackson-dataformat-xml=2.13.4, jackson-datatype-jsr310=2.13.4, azure-core=1.34.0, Troubleshooting version conflicts: https://aka.ms/azsdk/java/dependency/troubleshoot", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"com.azure.core.implementation.jackson.JacksonVersion","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.607Z", "log.level": "INFO", "message":"loaded module [aggregations]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.619Z", "log.level": "INFO", "message":"loaded module [analysis-common]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.637Z", "log.level": "INFO", "message":"loaded module [apm]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.638Z", "log.level": "INFO", "message":"loaded module [blob-cache]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.642Z", "log.level": "INFO", "message":"loaded module [constant-keyword]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.645Z", "log.level": "INFO", "message":"loaded module [data-streams]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.650Z", "log.level": "INFO", "message":"loaded module [frozen-indices]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.652Z", "log.level": "INFO", "message":"loaded module [ingest-attachment]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.652Z", "log.level": "INFO", "message":"loaded module [ingest-common]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.666Z", "log.level": "INFO", "message":"loaded module [ingest-geoip]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.672Z", "log.level": "INFO", "message":"loaded module [ingest-user-agent]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.675Z", "log.level": "INFO", "message":"loaded module [kibana]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.676Z", "log.level": "INFO", "message":"loaded module [lang-expression]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.678Z", "log.level": "INFO", "message":"loaded module [lang-mustache]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.714Z", "log.level": "INFO", "message":"loaded module [lang-painless]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.717Z", "log.level": "INFO", "message":"loaded module [legacy-geo]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.718Z", "log.level": "INFO", "message":"loaded module [mapper-extras]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.723Z", "log.level": "INFO", "message":"loaded module [mapper-version]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.726Z", "log.level": "INFO", "message":"loaded module [old-lucene-versions]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.735Z", "log.level": "INFO", "message":"loaded module [parent-join]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"} {"@timestamp":"2024-02-03T12:48:50.736Z", "log.level": "INFO", "message":"loaded module [percolator]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.737Z", "log.level": "INFO", "message":"loaded module [rank-eval]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.744Z", "log.level": "INFO", "message":"loaded module [reindex]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.746Z", "log.level": "INFO", "message":"loaded module [repositories-metering-api]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.749Z", "log.level": "INFO", "message":"loaded module [repository-azure]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.753Z", "log.level": "INFO", "message":"loaded module [repository-gcs]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.756Z", "log.level": "INFO", "message":"loaded module [repository-s3]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.762Z", "log.level": "INFO", "message":"loaded module [repository-url]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.766Z", "log.level": "INFO", "message":"loaded module [runtime-fields-common]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.769Z", "log.level": "INFO", "message":"loaded module [search-business-rules]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.771Z", "log.level": "INFO", "message":"loaded module [searchable-snapshots]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.790Z", "log.level": "INFO", "message":"loaded module [snapshot-based-recoveries]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.795Z", "log.level": "INFO", "message":"loaded module [snapshot-repo-test-kit]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.797Z", "log.level": "INFO", "message":"loaded module [spatial]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.798Z", "log.level": "INFO", "message":"loaded module [transform]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.809Z", "log.level": "INFO", "message":"loaded module [transport-netty4]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.818Z", "log.level": "INFO", "message":"loaded module [unsigned-long]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.819Z", "log.level": "INFO", "message":"loaded module [vector-tile]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"} {"@timestamp":"2024-02-03T12:48:50.822Z", "log.level": "INFO", "message":"loaded module [wildcard]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.824Z", "log.level": "INFO", "message":"loaded module [x-pack-aggregate-metric]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.828Z", "log.level": "INFO", "message":"loaded module [x-pack-analytics]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.829Z", "log.level": "INFO", "message":"loaded module [x-pack-async]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.831Z", "log.level": "INFO", "message":"loaded module [x-pack-async-search]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.837Z", "log.level": "INFO", "message":"loaded module [x-pack-autoscaling]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.850Z", "log.level": "INFO", "message":"loaded module [x-pack-ccr]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.852Z", "log.level": "INFO", "message":"loaded module [x-pack-core]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"} {"@timestamp":"2024-02-03T12:48:50.854Z", "log.level": "INFO", "message":"loaded module [x-pack-deprecation]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.858Z", "log.level": "INFO", "message":"loaded module [x-pack-enrich]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.885Z", "log.level": "INFO", "message":"loaded module [x-pack-eql]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.886Z", "log.level": "INFO", "message":"loaded module [x-pack-fleet]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.890Z", "log.level": "INFO", "message":"loaded module [x-pack-graph]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.891Z", "log.level": "INFO", "message":"loaded module [x-pack-identity-provider]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.893Z", "log.level": "INFO", "message":"loaded module [x-pack-ilm]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.893Z", "log.level": "INFO", "message":"loaded module [x-pack-logstash]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.894Z", "log.level": "INFO", "message":"loaded module [x-pack-ml]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.894Z", "log.level": "INFO", "message":"loaded module [x-pack-monitoring]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.898Z", "log.level": "INFO", "message":"loaded module [x-pack-profiling]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.900Z", "log.level": "INFO", "message":"loaded module [x-pack-ql]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.902Z", "log.level": "INFO", "message":"loaded module [x-pack-rollup]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.908Z", "log.level": "INFO", "message":"loaded module [x-pack-security]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.920Z", "log.level": "INFO", "message":"loaded module [x-pack-shutdown]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.926Z", "log.level": "INFO", "message":"loaded module [x-pack-sql]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.941Z", "log.level": "INFO", "message":"loaded module [x-pack-stack]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.946Z", "log.level": "INFO", "message":"loaded module [x-pack-text-structure]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.947Z", "log.level": "INFO", "message":"loaded module [x-pack-voting-only-node]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.950Z", "log.level": "INFO", "message":"loaded module [x-pack-watcher]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.951Z", "log.level": "INFO", "message":"loaded module [x-pack-write-load-forecaster]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:50.952Z", "log.level": "INFO", "message":"no plugins loaded", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:49:40.401Z", "log.level": "WARN", "message":"Feb 03, 2024 12:49:40 PM org.apache.lucene.store.MemorySegmentIndexInputProvider <init>", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"stderr","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:49:40.507Z", "log.level": "INFO", "message":"using [1] data paths, mounts [[/usr/share/elasticsearch/data (/dev/mapper/ubuntu--vg-ubuntu--lv)]], net usable\_space [18.4gb], net total\_space [30.3gb], types [ext4]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.env.NodeEnvironment","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:49:40.514Z", "log.level": "INFO", "message":"heap size [1gb], compressed ordinary object pointers [true]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.env.NodeEnvironment","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:49:41.223Z", "log.level": "INFO", "message":"node name [es-hot], node ID [14YcXtMjTJKPBt2IXLmjsQ], cluster name [es-docker-cluster], roles [data\_hot, data\_content, master]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.node.Node","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:16.298Z", "log.level": "INFO", "message":"[controller/198] [Main.cc@123] controller (64 bit): Version 8.7.0 (Build e4e1c23721e58c) Copyright (c) 2023 Elasticsearch BV", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"ml-cpp-log-tail-thread","log.logger":"org.elasticsearch.xpack.ml.process.logging.CppLogMessageHandler","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:19.389Z", "log.level": "INFO", "message":"Security is disabled", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.xpack.security.Security","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:23.259Z", "log.level": "INFO", "message":"Profiling is enabled", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.xpack.profiler.ProfilingPlugin","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:33.375Z", "log.level": "INFO", "message":"creating NettyAllocator with the following configs: [name=unpooled, suggested\_max\_allocation\_size=1mb, factors={es.unsafe.use\_unpooled\_allocator=null, g1gc\_enabled=true, g1gc\_region\_size=4mb, heap\_size=1gb}]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.transport.netty4.NettyAllocator","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:33.867Z", "log.level": "INFO", "message":"using rate limit [40mb] with [default=40mb, read=0b, write=0b, max=0b]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.indices.recovery.RecoverySettings","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:34.611Z", "log.level": "INFO", "message":"using discovery type [multi-node] and seed hosts providers [settings]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.discovery.DiscoveryModule","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:52.793Z", "log.level": "INFO", "message":"initialized", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.node.Node","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:52.870Z", "log.level": "INFO", "message":"starting ...", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.node.Node","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:53.117Z", "log.level": "INFO", "message":"persistent cache index loaded", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.xpack.searchablesnapshots.cache.full.PersistentCache","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:53.128Z", "log.level": "INFO", "message":"deprecation component started", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.xpack.deprecation.logging.DeprecationIndexingComponent","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:54.565Z", "log.level": "INFO", "message":"publish\_address {172.27.0.3:9300}, bound\_addresses {0.0.0.0:9300}", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.transport.TransportService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:56.407Z", "log.level": "INFO", "message":"bound or publishing to a non-loopback address, enforcing bootstrap checks", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.bootstrap.BootstrapChecks","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:56.439Z", "log.level": "INFO", "message":"this node has not joined a bootstrapped cluster yet; [cluster.initial\_master\_nodes] is set to [es-hot, es-warm]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.cluster.coordination.ClusterBootstrapService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:58.278Z", "log.level": "INFO", "message":"setting initial configuration to VotingConfiguration{WM9JgsGPTNC1PryuLiIAfg,14YcXtMjTJKPBt2IXLmjsQ}", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][generic][T#3]","log.logger":"org.elasticsearch.cluster.coordination.Coordinator","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:59.285Z", "log.level": "INFO", "message":"elected-as-master ([2] nodes joined)[\_FINISH\_ELECTION\_, {es-hot}{14YcXtMjTJKPBt2IXLmjsQ}{ohuXwgHLQ6Ce\_Pb\_0Ek3Bg}{es-hot}{172.27.0.3}{172.27.0.3:9300}{hms}{8.7.0} completing election, {es-warm}{WM9JgsGPTNC1PryuLiIAfg}{snnw\_jM6QLW8ZuzgCObl4w}{es-warm}{172.27.0.2}{172.27.0.2:9300}{mw}{8.7.0} completing election], term: 2, version: 1, delta: master node changed {previous [], current [{es-hot}{14YcXtMjTJKPBt2IXLmjsQ}{ohuXwgHLQ6Ce\_Pb\_0Ek3Bg}{es-hot}{172.27.0.3}{172.27.0.3:9300}{hms}{8.7.0}]}, added {{es-warm}{WM9JgsGPTNC1PryuLiIAfg}{snnw\_jM6QLW8ZuzgCObl4w}{es-warm}{172.27.0.2}{172.27.0.2:9300}{mw}{8.7.0}}", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.service.MasterService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:59.836Z", "log.level": "INFO", "message":"cluster UUID set to [tWR1H9pRTNaGswZlhLBwhA]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][cluster\_coordination][T#1]","log.logger":"org.elasticsearch.cluster.coordination.CoordinationState","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:00.283Z", "log.level": "INFO", "message":"master node changed {previous [], current [{es-hot}{14YcXtMjTJKPBt2IXLmjsQ}{ohuXwgHLQ6Ce\_Pb\_0Ek3Bg}{es-hot}{172.27.0.3}{172.27.0.3:9300}{hms}{8.7.0}]}, added {{es-warm}{WM9JgsGPTNC1PryuLiIAfg}{snnw\_jM6QLW8ZuzgCObl4w}{es-warm}{172.27.0.2}{172.27.0.2:9300}{mw}{8.7.0}}, term: 2, version: 1, reason: Publication{term=2, version=1}", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][clusterApplierService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.service.ClusterApplierService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:01.040Z", "log.level": "INFO", "message":"starting file settings watcher ...", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][clusterApplierService#updateTask][T#1]","log.logger":"org.elasticsearch.reservedstate.service.FileSettingsService","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:01.299Z", "log.level": "INFO", "message":"node-join: [{es-hot}{14YcXtMjTJKPBt2IXLmjsQ}{ohuXwgHLQ6Ce\_Pb\_0Ek3Bg}{es-hot}{172.27.0.3}{172.27.0.3:9300}{hms}{8.7.0}] with reason [completing election]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.coordination.NodeJoinExecutor","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:01.302Z", "log.level": "INFO", "message":"node-join: [{es-warm}{WM9JgsGPTNC1PryuLiIAfg}{snnw\_jM6QLW8ZuzgCObl4w}{es-warm}{172.27.0.2}{172.27.0.2:9300}{mw}{8.7.0}] with reason [completing election]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.coordination.NodeJoinExecutor","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:01.342Z", "log.level": "INFO", "message":"file settings service up and running [tid=48]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[file-settings-watcher]","log.logger":"org.elasticsearch.reservedstate.service.FileSettingsService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:01.561Z", "log.level": "INFO", "message":"publish\_address {172.27.0.3:9200}, bound\_addresses {0.0.0.0:9200}", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.http.AbstractHttpServerTransport","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:01.567Z", "log.level": "INFO", "message":"started {es-hot}{14YcXtMjTJKPBt2IXLmjsQ}{ohuXwgHLQ6Ce\_Pb\_0Ek3Bg}{es-hot}{172.27.0.3}{172.27.0.3:9300}{hms}{8.7.0}{xpack.installed=true}", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.node.Node","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:02.063Z", "log.level": "INFO", "message":"node-join: [{es-warm}{WM9JgsGPTNC1PryuLiIAfg}{snnw\_jM6QLW8ZuzgCObl4w}{es-warm}{172.27.0.2}{172.27.0.2:9300}{mw}{8.7.0}] with reason [joining]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.coordination.NodeJoinExecutor","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:05.829Z", "log.level": "INFO", "message":"recovered [0] indices into cluster\_state", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.gateway.GatewayService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:07.916Z", "log.level": "INFO", "message":"adding index template [.monitoring-ent-search-mb] for index patterns [.monitoring-ent-search-8-\*]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:08.049Z", "log.level": "INFO", "message":"adding index template [.monitoring-kibana-mb] for index patterns [.monitoring-kibana-8-\*]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:08.292Z", "log.level": "INFO", "message":"adding index template [.ml-anomalies-] for index patterns [.ml-anomalies-\*]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:08.359Z", "log.level": "INFO", "message":"adding template [.monitoring-beats] for index patterns [.monitoring-beats-7-\*]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:08.378Z", "log.level": "INFO", "message":"adding template [.monitoring-kibana] for index patterns [.monitoring-kibana-7-\*]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:08.428Z", "log.level": "INFO", "message":"adding template [.monitoring-logstash] for index patterns [.monitoring-logstash-7-\*]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:08.480Z", "log.level": "INFO", "message":"adding template [.monitoring-es] for index patterns [.monitoring-es-7-\*]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:08.497Z", "log.level": "INFO", "message":"adding index template [.ml-state] for index patterns [.ml-state\*]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:08.565Z", "log.level": "INFO", "message":"adding index template [.monitoring-logstash-mb] for index patterns [.monitoring-logstash-8-\*]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"} {"@timestamp":"2024-02-03T12:51:08.601Z", "log.level": "INFO", "message":"adding index template [.ml-stats] for index patterns [.ml-stats-\*]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:08.625Z", "log.level": "INFO", "message":"adding template [.monitoring-alerts-7] for index patterns [.monitoring-alerts-7]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:08.654Z", "log.level": "INFO", "message":"adding index template [.ml-notifications-000002] for index patterns [.ml-notifications-000002]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:08.833Z", "log.level": "INFO", "message":"adding index template [.monitoring-es-mb] for index patterns [.monitoring-es-8-\*]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:08.976Z", "log.level": "INFO", "message":"adding index template [.monitoring-beats-mb] for index patterns [.monitoring-beats-8-\*]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:09.024Z", "log.level": "INFO", "message":"adding index template [ilm-history] for index patterns [ilm-history-5\*]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:09.074Z", "log.level": "INFO", "message":"adding index template [.watch-history-16] for index patterns [.watcher-history-16\*]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:09.105Z", "log.level": "INFO", "message":"adding index template [.slm-history] for index patterns [.slm-history-5\*]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:09.126Z", "log.level": "INFO", "message":"adding index template [.fleet-file-data] for index patterns [.fleet-file-data-\*-\*]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:09.164Z", "log.level": "INFO", "message":"adding index template [.fleet-files] for index patterns [.fleet-files-\*-\*]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:09.241Z", "log.level": "INFO", "message":"adding component template [data-streams-mappings]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:09.255Z", "log.level": "INFO", "message":"adding component template [.deprecation-indexing-settings]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:09.276Z", "log.level": "INFO", "message":"adding component template [.deprecation-indexing-mappings]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:09.292Z", "log.level": "INFO", "message":"adding component template [logs-settings]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:09.303Z", "log.level": "INFO", "message":"adding component template [logs-mappings]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:09.319Z", "log.level": "INFO", "message":"adding component template [synthetics-settings]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:09.326Z", "log.level": "INFO", "message":"adding component template [metrics-mappings]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:09.359Z", "log.level": "INFO", "message":"adding component template [metrics-settings]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:09.369Z", "log.level": "INFO", "message":"adding component template [synthetics-mappings]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:10.449Z", "log.level": "INFO", "message":"adding index template [logs] for index patterns [logs-\*-\*]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:10.511Z", "log.level": "INFO", "message":"adding index template [synthetics] for index patterns [synthetics-\*-\*]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:10.558Z", "log.level": "INFO", "message":"adding index template [metrics] for index patterns [metrics-\*-\*]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:10.684Z", "log.level": "INFO", "message":"adding index template [.deprecation-indexing-template] for index patterns [.logs-deprecation.\*]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:11.058Z", "log.level": "INFO", "message":"adding index lifecycle policy [ml-size-based-ilm-policy]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.xpack.ilm.action.TransportPutLifecycleAction","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:11.581Z", "log.level": "INFO", "message":"adding index lifecycle policy [.monitoring-8-ilm-policy]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.xpack.ilm.action.TransportPutLifecycleAction","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:12.029Z", "log.level": "INFO", "message":"adding index lifecycle policy [logs]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.xpack.ilm.action.TransportPutLifecycleAction","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:12.645Z", "log.level": "INFO", "message":"adding index lifecycle policy [metrics]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.xpack.ilm.action.TransportPutLifecycleAction","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:13.141Z", "log.level": "INFO", "message":"adding index lifecycle policy [synthetics]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.xpack.ilm.action.TransportPutLifecycleAction","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:13.570Z", "log.level": "INFO", "message":"adding index lifecycle policy [7-days-default]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.xpack.ilm.action.TransportPutLifecycleAction","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:14.053Z", "log.level": "INFO", "message":"adding index lifecycle policy [30-days-default]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.xpack.ilm.action.TransportPutLifecycleAction","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:14.461Z", "log.level": "INFO", "message":"adding index lifecycle policy [90-days-default]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.xpack.ilm.action.TransportPutLifecycleAction","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:14.793Z", "log.level": "INFO", "message":"adding index lifecycle policy [180-days-default]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.xpack.ilm.action.TransportPutLifecycleAction","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:15.194Z", "log.level": "INFO", "message":"adding index lifecycle policy [365-days-default]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.xpack.ilm.action.TransportPutLifecycleAction","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:15.546Z", "log.level": "INFO", "message":"adding index lifecycle policy [watch-history-ilm-policy-16]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.xpack.ilm.action.TransportPutLifecycleAction","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:15.947Z", "log.level": "INFO", "message":"adding index lifecycle policy [ilm-history-ilm-policy]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.xpack.ilm.action.TransportPutLifecycleAction","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:16.376Z", "log.level": "INFO", "message":"adding index lifecycle policy [slm-history-ilm-policy]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.xpack.ilm.action.TransportPutLifecycleAction","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:16.837Z", "log.level": "INFO", "message":"adding index lifecycle policy [.deprecation-indexing-ilm-policy]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.xpack.ilm.action.TransportPutLifecycleAction","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:17.227Z", "log.level": "INFO", "message":"adding index lifecycle policy [.fleet-actions-results-ilm-policy]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.xpack.ilm.action.TransportPutLifecycleAction","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:17.794Z", "log.level": "INFO", "message":"adding index lifecycle policy [.fleet-files-ilm-policy]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.xpack.ilm.action.TransportPutLifecycleAction","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:18.344Z", "log.level": "INFO", "message":"adding index lifecycle policy [.fleet-file-data-ilm-policy]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.xpack.ilm.action.TransportPutLifecycleAction","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:19.607Z", "log.level": "INFO", "message":"Node [{es-hot}{14YcXtMjTJKPBt2IXLmjsQ}] is selected as the current health node.", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][management][T#1]","log.logger":"org.elasticsearch.health.node.selection.HealthNodeTaskExecutor","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:22.710Z", "log.level": "INFO", "message":"license [d5b05723-266e-453e-92a1-fb602b8fa179] mode [basic] - valid", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][clusterApplierService#updateTask][T#1]","log.logger":"org.elasticsearch.license.LicenseService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:38.883Z", "log.level": "INFO", "message":"adding index template [ecs-logstash] for index patterns [ecs-logstash-\*]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataIndexTemplateService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:40.766Z", "log.level": "INFO", "message":"[logstash-2023.12.03] creating index, cause [auto(bulk api)], templates [], shards [1]/[1]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataCreateIndexService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:41.204Z", "log.level": "INFO", "message":"[logstash-2023.12.11] creating index, cause [auto(bulk api)], templates [], shards [1]/[1]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataCreateIndexService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:41.218Z", "log.level": "INFO", "message":"[logstash-2023.12.10] creating index, cause [auto(bulk api)], templates [], shards [1]/[1]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataCreateIndexService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:41.238Z", "log.level": "INFO", "message":"[logstash-2024.02.03] creating index, cause [auto(bulk api)], templates [], shards [1]/[1]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataCreateIndexService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:41.247Z", "log.level": "INFO", "message":"[logstash-2023.12.06] creating index, cause [auto(bulk api)], templates [], shards [1]/[1]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataCreateIndexService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:44.756Z", "log.level": "INFO", "message":"[logstash-2023.12.10/6YsSp7IYTn22jH3\_byP3zQ] create\_mapping", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataMappingService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:45.150Z", "log.level": "INFO", "message":"[logstash-2023.12.03/oRYPxcfgQ\_6XcP2mdbt36A] create\_mapping", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataMappingService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:45.338Z", "log.level": "INFO", "message":"[logstash-2024.02.03/sOiCU7AqSGCyVnJhP80Q8g] create\_mapping", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataMappingService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:46.326Z", "log.level": "INFO", "message":"[logstash-2023.12.11/F\_K\_OUF6S5WRyqT-SaZwjQ] create\_mapping", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataMappingService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:46.332Z", "log.level": "INFO", "message":"[logstash-2023.12.06/klXXTjPLQZmlL-T760s-cw] create\_mapping", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataMappingService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:47.175Z", "log.level": "INFO", "message":"[logstash-2024.02.03/sOiCU7AqSGCyVnJhP80Q8g] update\_mapping [\_doc]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataMappingService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:48.174Z", "log.level": "INFO", "message":"[logstash-2024.02.03/sOiCU7AqSGCyVnJhP80Q8g] update\_mapping [\_doc]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataMappingService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:48.703Z", "log.level": "INFO", "message":"[logstash-2024.02.03/sOiCU7AqSGCyVnJhP80Q8g] update\_mapping [\_doc]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataMappingService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:49.120Z", "log.level": "INFO", "message":"[logstash-2024.02.03/sOiCU7AqSGCyVnJhP80Q8g] update\_mapping [\_doc]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataMappingService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:49.696Z", "log.level": "INFO", "message":"[logstash-2024.02.03/sOiCU7AqSGCyVnJhP80Q8g] update\_mapping [\_doc]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataMappingService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:50.824Z", "log.level": "INFO", "message":"[logstash-2024.02.03/sOiCU7AqSGCyVnJhP80Q8g] update\_mapping [\_doc]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataMappingService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:52.005Z", "log.level": "INFO", "message":"[logstash-2024.02.03/sOiCU7AqSGCyVnJhP80Q8g] update\_mapping [\_doc]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataMappingService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:52.595Z", "log.level": "INFO", "message":"[logstash-2024.02.03/sOiCU7AqSGCyVnJhP80Q8g] update\_mapping [\_doc]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataMappingService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:53.133Z", "log.level": "INFO", "message":"[logstash-2024.02.03/sOiCU7AqSGCyVnJhP80Q8g] update\_mapping [\_doc]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataMappingService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:52:01.032Z", "log.level": "INFO", "message":"[logstash-2023.12.04] creating index, cause [auto(bulk api)], templates [], shards [1]/[1]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataCreateIndexService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:52:03.240Z", "log.level": "INFO", "message":"[gc][69] overhead, spent [434ms] collecting in the last [1s]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][scheduler][T#1]","log.logger":"org.elasticsearch.monitor.jvm.JvmGcMonitorService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:52:04.020Z", "log.level": "INFO", "message":"[logstash-2023.12.04/UweUmywARY-yLxeTPbkjqg] create\_mapping", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataMappingService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:52:05.461Z", "log.level": "INFO", "message":"[logstash-2023.12.27] creating index, cause [auto(bulk api)], templates [], shards [1]/[1]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataCreateIndexService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:52:06.402Z", "log.level": "INFO", "message":"[logstash-2023.12.26] creating index, cause [auto(bulk api)], templates [], shards [1]/[1]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataCreateIndexService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:52:06.450Z", "log.level": "INFO", "message":"[logstash-2023.12.12] creating index, cause [auto(bulk api)], templates [], shards [1]/[1]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataCreateIndexService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:52:09.767Z", "log.level": "INFO", "message":"[logstash-2023.12.27/lpnTvbegTymO1rxr\_C-3Qg] create\_mapping", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataMappingService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:52:10.745Z", "log.level": "INFO", "message":"[logstash-2023.12.26/fhpnr98XTG-hQRrnuva75Q] create\_mapping", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataMappingService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:52:12.716Z", "log.level": "INFO", "message":"[logstash-2023.12.12/G6DGg2KCT9OjRXgnrwJAxA] create\_mapping", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataMappingService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:52:22.458Z", "log.level": "INFO", "message":"[logstash-2023.12.18] creating index, cause [auto(bulk api)], templates [], shards [1]/[1]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataCreateIndexService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:52:25.088Z", "log.level": "INFO", "message":"[logstash-2023.12.18/uviE-7IgRr27PulqqPh1Yg] create\_mapping", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataMappingService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:52:34.929Z", "log.level": "INFO", "message":"[logstash-2024.02.03/sOiCU7AqSGCyVnJhP80Q8g] update\_mapping [\_doc]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataMappingService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:52:38.587Z", "log.level": "INFO", "message":"[logstash-2024.02.03/sOiCU7AqSGCyVnJhP80Q8g] update\_mapping [\_doc]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataMappingService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:52:42.442Z", "log.level": "INFO", "message":"[logstash-2024.02.03/sOiCU7AqSGCyVnJhP80Q8g] update\_mapping [\_doc]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataMappingService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:52:43.296Z", "log.level": "INFO", "message":"[logstash-2024.02.03/sOiCU7AqSGCyVnJhP80Q8g] update\_mapping [\_doc]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-hot][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.metadata.MetadataMappingService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"14YcXtMjTJKPBt2IXLmjsQ","elasticsearch.node.name":"es-hot","elasticsearch.cluster.name":"es-docker-cluster"}

vagrant@vagrant:~/10-monitoring-04-elk/elk2$ docker logs --details es-warm

Created elasticsearch keystore in /usr/share/elasticsearch/config/elasticsearch.keystore

{"@timestamp":"2024-02-03T12:47:19.904Z", "log.level": "INFO", "message":"version[8.7.0], pid[169], build[docker/09520b59b6bc1057340b55750186466ea715e30e/2023-03-27T16:31:09.816451435Z], OS[Linux/5.4.0-135-generic/amd64], JVM[Oracle Corporation/OpenJDK 64-Bit Server VM/19.0.2/19.0.2+7-44]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.node.Node","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:47:20.039Z", "log.level": "INFO", "message":"JVM home [/usr/share/elasticsearch/jdk], using bundled JDK [true]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.node.Node","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:47:20.041Z", "log.level": "INFO", "message":"JVM arguments [-Des.networkaddress.cache.ttl=60, -Des.networkaddress.cache.negative.ttl=10, -Djava.security.manager=allow, -XX:+AlwaysPreTouch, -Xss1m, -Djava.awt.headless=true, -Dfile.encoding=UTF-8, -Djna.nosys=true, -XX:-OmitStackTraceInFastThrow, -Dio.netty.noUnsafe=true, -Dio.netty.noKeySetOptimization=true, -Dio.netty.recycler.maxCapacityPerThread=0, -Dlog4j.shutdownHookEnabled=false, -Dlog4j2.disable.jmx=true, -Dlog4j2.formatMsgNoLookups=true, -Djava.locale.providers=SPI,COMPAT, --add-opens=java.base/java.io=ALL-UNNAMED, -Des.cgroups.hierarchy.override=/, -XX:+UseG1GC, -Djava.io.tmpdir=/tmp/elasticsearch-6633252673285148493, -XX:+HeapDumpOnOutOfMemoryError, -XX:+ExitOnOutOfMemoryError, -XX:HeapDumpPath=data, -XX:ErrorFile=logs/hs\_err\_pid%p.log, -Xlog:gc\*,gc+age=trace,safepoint:file=logs/gc.log:utctime,level,pid,tags:filecount=32,filesize=64m, -Xms1g, -Xmx1g, -XX:MaxDirectMemorySize=536870912, -XX:G1HeapRegionSize=4m, -XX:InitiatingHeapOccupancyPercent=30, -XX:G1ReservePercent=15, -Des.distribution.type=docker, --module-path=/usr/share/elasticsearch/lib, --add-modules=jdk.net, -Djdk.module.main=org.elasticsearch.server]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.node.Node","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:02.520Z", "log.level": "INFO", "message":"Package versions: jackson-core=2.13.4, jackson-databind=2.13.4-2, jackson-dataformat-xml=2.13.4, jackson-datatype-jsr310=2.13.4, azure-core=1.34.0, Troubleshooting version conflicts: https://aka.ms/azsdk/java/dependency/troubleshoot", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"com.azure.core.implementation.jackson.JacksonVersion","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.286Z", "log.level": "INFO", "message":"loaded module [aggregations]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.291Z", "log.level": "INFO", "message":"loaded module [analysis-common]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.292Z", "log.level": "INFO", "message":"loaded module [apm]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.292Z", "log.level": "INFO", "message":"loaded module [blob-cache]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.299Z", "log.level": "INFO", "message":"loaded module [constant-keyword]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.301Z", "log.level": "INFO", "message":"loaded module [data-streams]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.302Z", "log.level": "INFO", "message":"loaded module [frozen-indices]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.302Z", "log.level": "INFO", "message":"loaded module [ingest-attachment]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.303Z", "log.level": "INFO", "message":"loaded module [ingest-common]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.342Z", "log.level": "INFO", "message":"loaded module [ingest-geoip]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.343Z", "log.level": "INFO", "message":"loaded module [ingest-user-agent]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.345Z", "log.level": "INFO", "message":"loaded module [kibana]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.346Z", "log.level": "INFO", "message":"loaded module [lang-expression]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.346Z", "log.level": "INFO", "message":"loaded module [lang-mustache]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.358Z", "log.level": "INFO", "message":"loaded module [lang-painless]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.362Z", "log.level": "INFO", "message":"loaded module [legacy-geo]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.367Z", "log.level": "INFO", "message":"loaded module [mapper-extras]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.375Z", "log.level": "INFO", "message":"loaded module [mapper-version]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.383Z", "log.level": "INFO", "message":"loaded module [old-lucene-versions]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.386Z", "log.level": "INFO", "message":"loaded module [parent-join]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.394Z", "log.level": "INFO", "message":"loaded module [percolator]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.408Z", "log.level": "INFO", "message":"loaded module [rank-eval]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.415Z", "log.level": "INFO", "message":"loaded module [reindex]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.425Z", "log.level": "INFO", "message":"loaded module [repositories-metering-api]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.427Z", "log.level": "INFO", "message":"loaded module [repository-azure]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.437Z", "log.level": "INFO", "message":"loaded module [repository-gcs]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.438Z", "log.level": "INFO", "message":"loaded module [repository-s3]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.440Z", "log.level": "INFO", "message":"loaded module [repository-url]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.441Z", "log.level": "INFO", "message":"loaded module [runtime-fields-common]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.441Z", "log.level": "INFO", "message":"loaded module [search-business-rules]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.444Z", "log.level": "INFO", "message":"loaded module [searchable-snapshots]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.445Z", "log.level": "INFO", "message":"loaded module [snapshot-based-recoveries]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.445Z", "log.level": "INFO", "message":"loaded module [snapshot-repo-test-kit]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.447Z", "log.level": "INFO", "message":"loaded module [spatial]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.449Z", "log.level": "INFO", "message":"loaded module [transform]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.457Z", "log.level": "INFO", "message":"loaded module [transport-netty4]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.459Z", "log.level": "INFO", "message":"loaded module [unsigned-long]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.461Z", "log.level": "INFO", "message":"loaded module [vector-tile]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.461Z", "log.level": "INFO", "message":"loaded module [wildcard]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.482Z", "log.level": "INFO", "message":"loaded module [x-pack-aggregate-metric]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.485Z", "log.level": "INFO", "message":"loaded module [x-pack-analytics]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.491Z", "log.level": "INFO", "message":"loaded module [x-pack-async]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.496Z", "log.level": "INFO", "message":"loaded module [x-pack-async-search]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.498Z", "log.level": "INFO", "message":"loaded module [x-pack-autoscaling]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.503Z", "log.level": "INFO", "message":"loaded module [x-pack-ccr]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.511Z", "log.level": "INFO", "message":"loaded module [x-pack-core]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.513Z", "log.level": "INFO", "message":"loaded module [x-pack-deprecation]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.514Z", "log.level": "INFO", "message":"loaded module [x-pack-enrich]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.517Z", "log.level": "INFO", "message":"loaded module [x-pack-eql]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.519Z", "log.level": "INFO", "message":"loaded module [x-pack-fleet]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.520Z", "log.level": "INFO", "message":"loaded module [x-pack-graph]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.522Z", "log.level": "INFO", "message":"loaded module [x-pack-identity-provider]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.523Z", "log.level": "INFO", "message":"loaded module [x-pack-ilm]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.525Z", "log.level": "INFO", "message":"loaded module [x-pack-logstash]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.533Z", "log.level": "INFO", "message":"loaded module [x-pack-ml]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.535Z", "log.level": "INFO", "message":"loaded module [x-pack-monitoring]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.544Z", "log.level": "INFO", "message":"loaded module [x-pack-profiling]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.547Z", "log.level": "INFO", "message":"loaded module [x-pack-ql]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.556Z", "log.level": "INFO", "message":"loaded module [x-pack-rollup]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.562Z", "log.level": "INFO", "message":"loaded module [x-pack-security]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.573Z", "log.level": "INFO", "message":"loaded module [x-pack-shutdown]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.577Z", "log.level": "INFO", "message":"loaded module [x-pack-sql]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.577Z", "log.level": "INFO", "message":"loaded module [x-pack-stack]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.581Z", "log.level": "INFO", "message":"loaded module [x-pack-text-structure]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.586Z", "log.level": "INFO", "message":"loaded module [x-pack-voting-only-node]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.587Z", "log.level": "INFO", "message":"loaded module [x-pack-watcher]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.589Z", "log.level": "INFO", "message":"loaded module [x-pack-write-load-forecaster]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:48:33.590Z", "log.level": "INFO", "message":"no plugins loaded", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.plugins.PluginsService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:49:35.510Z", "log.level": "WARN", "message":"Feb 03, 2024 12:49:35 PM org.apache.lucene.store.MemorySegmentIndexInputProvider <init>", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"stderr","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:49:35.648Z", "log.level": "INFO", "message":"using [1] data paths, mounts [[/usr/share/elasticsearch/data (/dev/mapper/ubuntu--vg-ubuntu--lv)]], net usable\_space [18.4gb], net total\_space [30.3gb], types [ext4]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.env.NodeEnvironment","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:49:35.653Z", "log.level": "INFO", "message":"heap size [1gb], compressed ordinary object pointers [true]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.env.NodeEnvironment","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:49:36.267Z", "log.level": "INFO", "message":"node name [es-warm], node ID [WM9JgsGPTNC1PryuLiIAfg], cluster name [es-docker-cluster], roles [data\_warm, master]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.node.Node","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:16.284Z", "log.level": "INFO", "message":"[controller/189] [Main.cc@123] controller (64 bit): Version 8.7.0 (Build e4e1c23721e58c) Copyright (c) 2023 Elasticsearch BV", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"ml-cpp-log-tail-thread","log.logger":"org.elasticsearch.xpack.ml.process.logging.CppLogMessageHandler","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:19.344Z", "log.level": "INFO", "message":"Security is disabled", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.xpack.security.Security","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:23.183Z", "log.level": "INFO", "message":"Profiling is enabled", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.xpack.profiler.ProfilingPlugin","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:33.357Z", "log.level": "INFO", "message":"creating NettyAllocator with the following configs: [name=unpooled, suggested\_max\_allocation\_size=1mb, factors={es.unsafe.use\_unpooled\_allocator=null, g1gc\_enabled=true, g1gc\_region\_size=4mb, heap\_size=1gb}]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.transport.netty4.NettyAllocator","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:33.848Z", "log.level": "INFO", "message":"using rate limit [40mb] with [default=40mb, read=0b, write=0b, max=0b]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.indices.recovery.RecoverySettings","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:34.622Z", "log.level": "INFO", "message":"using discovery type [multi-node] and seed hosts providers [settings]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.discovery.DiscoveryModule","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:52.747Z", "log.level": "INFO", "message":"initialized", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.node.Node","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:52.754Z", "log.level": "INFO", "message":"starting ...", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.node.Node","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:53.008Z", "log.level": "INFO", "message":"persistent cache index loaded", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.xpack.searchablesnapshots.cache.full.PersistentCache","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:53.011Z", "log.level": "INFO", "message":"deprecation component started", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.xpack.deprecation.logging.DeprecationIndexingComponent","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:54.459Z", "log.level": "INFO", "message":"publish\_address {172.27.0.2:9300}, bound\_addresses {0.0.0.0:9300}", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.transport.TransportService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:56.367Z", "log.level": "INFO", "message":"bound or publishing to a non-loopback address, enforcing bootstrap checks", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.bootstrap.BootstrapChecks","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:56.388Z", "log.level": "INFO", "message":"this node has not joined a bootstrapped cluster yet; [cluster.initial\_master\_nodes] is set to [es-hot, es-warm]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.cluster.coordination.ClusterBootstrapService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:58.248Z", "log.level": "INFO", "message":"setting initial configuration to VotingConfiguration{14YcXtMjTJKPBt2IXLmjsQ,WM9JgsGPTNC1PryuLiIAfg}", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-warm][generic][T#4]","log.logger":"org.elasticsearch.cluster.coordination.Coordinator","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:59.305Z", "log.level": "INFO", "message":"elected-as-master ([2] nodes joined)[\_FINISH\_ELECTION\_, {es-hot}{14YcXtMjTJKPBt2IXLmjsQ}{ohuXwgHLQ6Ce\_Pb\_0Ek3Bg}{es-hot}{172.27.0.3}{172.27.0.3:9300}{hms}{8.7.0} completing election, {es-warm}{WM9JgsGPTNC1PryuLiIAfg}{snnw\_jM6QLW8ZuzgCObl4w}{es-warm}{172.27.0.2}{172.27.0.2:9300}{mw}{8.7.0} completing election], term: 1, version: 1, delta: master node changed {previous [], current [{es-warm}{WM9JgsGPTNC1PryuLiIAfg}{snnw\_jM6QLW8ZuzgCObl4w}{es-warm}{172.27.0.2}{172.27.0.2:9300}{mw}{8.7.0}]}, added {{es-hot}{14YcXtMjTJKPBt2IXLmjsQ}{ohuXwgHLQ6Ce\_Pb\_0Ek3Bg}{es-hot}{172.27.0.3}{172.27.0.3:9300}{hms}{8.7.0}}", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-warm][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.service.MasterService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:50:59.338Z", "log.level": "WARN", "message":"failing [elected-as-master ([2] nodes joined)[\_FINISH\_ELECTION\_, {es-hot}{14YcXtMjTJKPBt2IXLmjsQ}{ohuXwgHLQ6Ce\_Pb\_0Ek3Bg}{es-hot}{172.27.0.3}{172.27.0.3:9300}{hms}{8.7.0} completing election, {es-warm}{WM9JgsGPTNC1PryuLiIAfg}{snnw\_jM6QLW8ZuzgCObl4w}{es-warm}{172.27.0.2}{172.27.0.2:9300}{mw}{8.7.0} completing election]]: failed to commit cluster state version [1]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-warm][masterService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.service.MasterService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster","error.type":"org.elasticsearch.cluster.coordination.FailedToCommitClusterStateException","error.message":"node is no longer master for term 1 while handling publication","error.stack\_trace":"org.elasticsearch.cluster.coordination.FailedToCommitClusterStateException: node is no longer master for term 1 while handling publication\n\tat org.elasticsearch.server@8.7.0/org.elasticsearch.cluster.coordination.Coordinator.publish(Coordinator.java:1427)\n\tat org.elasticsearch.server@8.7.0/org.elasticsearch.cluster.service.MasterService.publish(MasterService.java:470)\n\tat org.elasticsearch.server@8.7.0/org.elasticsearch.cluster.service.MasterService.publishClusterStateUpdate(MasterService.java:361)\n\tat org.elasticsearch.server@8.7.0/org.elasticsearch.cluster.service.MasterService.runTasks(MasterService.java:298)\n\tat org.elasticsearch.server@8.7.0/org.elasticsearch.cluster.service.MasterService$Batcher.run(MasterService.java:170)\n\tat org.elasticsearch.server@8.7.0/org.elasticsearch.cluster.service.TaskBatcher.runIfNotProcessed(TaskBatcher.java:110)\n\tat org.elasticsearch.server@8.7.0/org.elasticsearch.cluster.service.TaskBatcher$BatchedTask.run(TaskBatcher.java:148)\n\tat org.elasticsearch.server@8.7.0/org.elasticsearch.common.util.concurrent.ThreadContext$ContextPreservingRunnable.run(ThreadContext.java:891)\n\tat org.elasticsearch.server@8.7.0/org.elasticsearch.common.util.concurrent.PrioritizedEsThreadPoolExecutor$TieBreakingPrioritizedRunnable.runAndClean(PrioritizedEsThreadPoolExecutor.java:257)\n\tat org.elasticsearch.server@8.7.0/org.elasticsearch.common.util.concurrent.PrioritizedEsThreadPoolExecutor$TieBreakingPrioritizedRunnable.run(PrioritizedEsThreadPoolExecutor.java:223)\n\tat java.base/java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1144)\n\tat java.base/java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:642)\n\tat java.base/java.lang.Thread.run(Thread.java:1589)\n"}

{"@timestamp":"2024-02-03T12:50:59.831Z", "log.level": "INFO", "message":"cluster UUID set to [tWR1H9pRTNaGswZlhLBwhA]", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-warm][cluster\_coordination][T#1]","log.logger":"org.elasticsearch.cluster.coordination.CoordinationState","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:00.031Z", "log.level": "INFO", "message":"master node changed {previous [], current [{es-hot}{14YcXtMjTJKPBt2IXLmjsQ}{ohuXwgHLQ6Ce\_Pb\_0Ek3Bg}{es-hot}{172.27.0.3}{172.27.0.3:9300}{hms}{8.7.0}]}, added {{es-hot}{14YcXtMjTJKPBt2IXLmjsQ}{ohuXwgHLQ6Ce\_Pb\_0Ek3Bg}{es-hot}{172.27.0.3}{172.27.0.3:9300}{hms}{8.7.0}}, term: 2, version: 1, reason: ApplyCommitRequest{term=2, version=1, sourceNode={es-hot}{14YcXtMjTJKPBt2IXLmjsQ}{ohuXwgHLQ6Ce\_Pb\_0Ek3Bg}{es-hot}{172.27.0.3}{172.27.0.3:9300}{hms}{8.7.0}{xpack.installed=true}}", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-warm][clusterApplierService#updateTask][T#1]","log.logger":"org.elasticsearch.cluster.service.ClusterApplierService","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:00.261Z", "log.level": "INFO", "message":"publish\_address {172.27.0.2:9200}, bound\_addresses {0.0.0.0:9200}", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.http.AbstractHttpServerTransport","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"WM9JgsGPTNC1PryuLiIAfg","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:00.262Z", "log.level": "INFO", "message":"started {es-warm}{WM9JgsGPTNC1PryuLiIAfg}{snnw\_jM6QLW8ZuzgCObl4w}{es-warm}{172.27.0.2}{172.27.0.2:9300}{mw}{8.7.0}{xpack.installed=true}", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"main","log.logger":"org.elasticsearch.node.Node","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"WM9JgsGPTNC1PryuLiIAfg","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}

{"@timestamp":"2024-02-03T12:51:21.683Z", "log.level": "INFO", "message":"license [d5b05723-266e-453e-92a1-fb602b8fa179] mode [basic] - valid", "ecs.version": "1.2.0","service.name":"ES\_ECS","event.dataset":"elasticsearch.server","process.thread.name":"elasticsearch[es-warm][clusterApplierService#updateTask][T#1]","log.logger":"org.elasticsearch.license.LicenseService","elasticsearch.cluster.uuid":"tWR1H9pRTNaGswZlhLBwhA","elasticsearch.node.id":"WM9JgsGPTNC1PryuLiIAfg","elasticsearch.node.name":"es-warm","elasticsearch.cluster.name":"es-docker-cluster"}