status = error

# log action execution errors for easier debugging

logger.action.name = org.elasticsearch.action

logger.action.level = info

appender.rolling.type = Console

appender.rolling.name = rolling

appender.rolling.layout.type = ESJsonLayout

appender.rolling.layout.type\_name = server

rootLogger.level = info

rootLogger.appenderRef.rolling.ref = rolling

appender.deprecation\_rolling.type = Console

appender.deprecation\_rolling.name = deprecation\_rolling

appender.deprecation\_rolling.layout.type = ESJsonLayout

appender.deprecation\_rolling.layout.type\_name = deprecation

logger.deprecation.name = org.elasticsearch.deprecation

logger.deprecation.level = warn

logger.deprecation.appenderRef.deprecation\_rolling.ref = deprecation\_rolling

logger.deprecation.additivity = false

appender.index\_search\_slowlog\_rolling.type = Console

appender.index\_search\_slowlog\_rolling.name = index\_search\_slowlog\_rolling

appender.index\_search\_slowlog\_rolling.layout.type = ESJsonLayout

appender.index\_search\_slowlog\_rolling.layout.type\_name = index\_search\_slowlog

logger.index\_search\_slowlog\_rolling.name = index.search.slowlog

logger.index\_search\_slowlog\_rolling.level = trace

logger.index\_search\_slowlog\_rolling.appenderRef.index\_search\_slowlog\_rolling.ref = index\_search\_slowlog\_rolling

logger.index\_search\_slowlog\_rolling.additivity = false

appender.index\_indexing\_slowlog\_rolling.type = Console

appender.index\_indexing\_slowlog\_rolling.name = index\_indexing\_slowlog\_rolling

appender.index\_indexing\_slowlog\_rolling.layout.type = ESJsonLayout

appender.index\_indexing\_slowlog\_rolling.layout.type\_name = index\_indexing\_slowlog

logger.index\_indexing\_slowlog.name = index.indexing.slowlog.index

logger.index\_indexing\_slowlog.level = trace

logger.index\_indexing\_slowlog.appenderRef.index\_indexing\_slowlog\_rolling.ref = index\_indexing\_slowlog\_rolling

logger.index\_indexing\_slowlog.additivity = false

appender.audit\_rolling.type = Console

appender.audit\_rolling.name = audit\_rolling

appender.audit\_rolling.layout.type = PatternLayout

appender.audit\_rolling.layout.pattern = {\

"type": "audit", \

"timestamp":"%d{yyyy-MM-dd'T'HH:mm:ss,SSSZ}"\

%varsNotEmpty{, "node.name":"%enc{%map{node.name}}{JSON}"}\

%varsNotEmpty{, "node.id":"%enc{%map{node.id}}{JSON}"}\

%varsNotEmpty{, "host.name":"%enc{%map{host.name}}{JSON}"}\

%varsNotEmpty{, "host.ip":"%enc{%map{host.ip}}{JSON}"}\

%varsNotEmpty{, "event.type":"%enc{%map{event.type}}{JSON}"}\

%varsNotEmpty{, "event.action":"%enc{%map{event.action}}{JSON}"}\

%varsNotEmpty{, "user.name":"%enc{%map{user.name}}{JSON}"}\

%varsNotEmpty{, "user.run\_by.name":"%enc{%map{user.run\_by.name}}{JSON}"}\

%varsNotEmpty{, "user.run\_as.name":"%enc{%map{user.run\_as.name}}{JSON}"}\

%varsNotEmpty{, "user.realm":"%enc{%map{user.realm}}{JSON}"}\

%varsNotEmpty{, "user.run\_by.realm":"%enc{%map{user.run\_by.realm}}{JSON}"}\

%varsNotEmpty{, "user.run\_as.realm":"%enc{%map{user.run\_as.realm}}{JSON}"}\

%varsNotEmpty{, "user.roles":%map{user.roles}}\

%varsNotEmpty{, "origin.type":"%enc{%map{origin.type}}{JSON}"}\

%varsNotEmpty{, "origin.address":"%enc{%map{origin.address}}{JSON}"}\

%varsNotEmpty{, "realm":"%enc{%map{realm}}{JSON}"}\

%varsNotEmpty{, "url.path":"%enc{%map{url.path}}{JSON}"}\

%varsNotEmpty{, "url.query":"%enc{%map{url.query}}{JSON}"}\

%varsNotEmpty{, "request.method":"%enc{%map{request.method}}{JSON}"}\

%varsNotEmpty{, "request.body":"%enc{%map{request.body}}{JSON}"}\

%varsNotEmpty{, "request.id":"%enc{%map{request.id}}{JSON}"}\

%varsNotEmpty{, "action":"%enc{%map{action}}{JSON}"}\

%varsNotEmpty{, "request.name":"%enc{%map{request.name}}{JSON}"}\

%varsNotEmpty{, "indices":%map{indices}}\

%varsNotEmpty{, "opaque\_id":"%enc{%map{opaque\_id}}{JSON}"}\

%varsNotEmpty{, "x\_forwarded\_for":"%enc{%map{x\_forwarded\_for}}{JSON}"}\

%varsNotEmpty{, "transport.profile":"%enc{%map{transport.profile}}{JSON}"}\

%varsNotEmpty{, "rule":"%enc{%map{rule}}{JSON}"}\

%varsNotEmpty{, "event.category":"%enc{%map{event.category}}{JSON}"}\

}%n

# "node.name" node name from the `elasticsearch.yml` settings

# "node.id" node id which should not change between cluster restarts

# "host.name" unresolved hostname of the local node

# "host.ip" the local bound ip (i.e. the ip listening for connections)

# "event.type" a received REST request is translated into one or more transport requests. This indicates which processing layer generated the event "rest" or "transport" (internal)

# "event.action" the name of the audited event, eg. "authentication\_failed", "access\_granted", "run\_as\_granted", etc.

# "user.name" the subject name as authenticated by a realm

# "user.run\_by.name" the original authenticated subject name that is impersonating another one.

# "user.run\_as.name" if this "event.action" is of a run\_as type, this is the subject name to be impersonated as.

# "user.realm" the name of the realm that authenticated "user.name"

# "user.run\_by.realm" the realm name of the impersonating subject ("user.run\_by.name")

# "user.run\_as.realm" if this "event.action" is of a run\_as type, this is the realm name the impersonated user is looked up from

# "user.roles" the roles array of the user; these are the roles that are granting privileges

# "origin.type" it is "rest" if the event is originating (is in relation to) a REST request; possible other values are "transport" and "ip\_filter"

# "origin.address" the remote address and port of the first network hop, i.e. a REST proxy or another cluster node

# "realm" name of a realm that has generated an "authentication\_failed" or an "authentication\_successful"; the subject is not yet authenticated

# "url.path" the URI component between the port and the query string; it is percent (URL) encoded

# "url.query" the URI component after the path and before the fragment; it is percent (URL) encoded

# "request.method" the method of the HTTP request, i.e. one of GET, POST, PUT, DELETE, OPTIONS, HEAD, PATCH, TRACE, CONNECT

# "request.body" the content of the request body entity, JSON escaped

# "request.id" a synthentic identifier for the incoming request, this is unique per incoming request, and consistent across all audit events generated by that request

# "action" an action is the most granular operation that is authorized and this identifies it in a namespaced way (internal)

# "request.name" if the event is in connection to a transport message this is the name of the request class, similar to how rest requests are identified by the url path (internal)

# "indices" the array of indices that the "action" is acting upon

# "opaque\_id" opaque value conveyed by the "X-Opaque-Id" request header

# "x\_forwarded\_for" the addresses from the "X-Forwarded-For" request header, as a verbatim string value (not an array)

# "transport.profile" name of the transport profile in case this is a "connection\_granted" or "connection\_denied" event

# "rule" name of the applied rulee if the "origin.type" is "ip\_filter"

# "event.category" fixed value "elasticsearch-audit"

logger.xpack\_security\_audit\_logfile.name = org.elasticsearch.xpack.security.audit.logfile.LoggingAuditTrail

logger.xpack\_security\_audit\_logfile.level = info

logger.xpack\_security\_audit\_logfile.appenderRef.audit\_rolling.ref = audit\_rolling

logger.xpack\_security\_audit\_logfile.additivity = false

logger.xmlsig.name = org.apache.xml.security.signature.XMLSignature

logger.xmlsig.level = error

logger.samlxml\_decrypt.name = org.opensaml.xmlsec.encryption.support.Decrypter

logger.samlxml\_decrypt.level = fatal

logger.saml2\_decrypt.name = org.opensaml.saml.saml2.encryption.Decrypter

logger.saml2\_decrypt.level = fatal