**Use Cases**

**User Account Log In Activity**

1.1: Detect when a user logs in too many times in a time window.

1.2: Detect when a user logs in on a weekend.

1.3: Detect when a user logs in late at night.

1.4: Detect when a user logs into a machine they have never accessed before.

**Use Case 2: Software Verification**

2.1: Detect when external media (USB, floppy disk (seriously), or CDROM) are inserted into machine

2.2: Detect when RPM (or other native package) are installed.

~~2.3: Detect if upgrades are needed.~~

**TODO (In Progress):**

1. Transform WebHook Data (Parse Text in LS)
2. Develop Visual Display in Kibana and Email Standard Template
3. ~~Percolate User Activity~~
4. Set Email Server and Messages[NOTE: Discussion Board started with Elasticsearch]
5. ~~Develop Use Cases~~
6. USB (hips index)\* [NOTE: need to replace index]

Use Case 3: User Activities

3.1: Detect whether use has performed 2 or more actions from list of potentially risky activities (change of permissions, FTP/SCP, sudo, Access to critical system Information)

3.2: Detect Top 10 most active users from past hour, on an hourly basis.

3.3: Scan for abnormal user activities 24, 48, and/or 72 hour time-based intervals.

Use Case 4: Routine System Administration

4.1: Collect index data based upon Severity and Priority levels and render that in displays (such as Pie Chart) for easy identification of system status

4.2: Collect and Track Failure notices and Errors associated with each system to determine system status and if potentially compromised

4.3: Conduct routine systems check using ssh to access each system and verify critical applications and servers are operational. Report back stsatus off all systems.

**Sources:**

<http://www.bigdatapaper.com/2015/12/16/implementing-a-statistical-anomaly-detector-in-elasticsearch-part-3/>

<https://discuss.elastic.co/t/cannot-find-default-email-account-as-no-accounts-have-been-configured/60121/11>

<https://www.elastic.co/blog/when-and-how-to-percolate-1>

<https://www.elastic.co/guide/en/x-pack/current/condition-script.html>

**//////////////////////////\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*COMMANDS**

//Execute Watch

curl -XPOST elastic:changeme@bb16:9200/\_xpack/watcher/watch/severity/\_execute?pretty

curl -XPOST elastic:changeme@128.63.27.63:9200/\_xpack/watcher/watch/user-activity/\_execute?pretty

//GET Specific Watch

curl –XGET elastic:changeme@bb16:9200/\_xpack/watcher/watch/severity

//Search ALL watches

curl -XGET elastic:changeme@bb16:9200/.watches/\_search?pretty | less

//Search Watch History

~~curl -XGET elastic:changeme@bb16:9200/.watcher\_history/\_search?pretty~~

//ES5 Search Watches

~~curl -XGET elastic:changeme@bb16:9200/\_xpack/.watches/\_search~~

//Standard ES2 Search Watches command

curl -XGET elastic:changeme@bb16:9200/.watches/\_search?pretty

//Delete command

curl -XDELETE 'http://elastic:changeme@bb16:9200/\_watcher/watch/severity'

curl -XDELETE 'http://elastic:changeme@bb16:9200/\_watcher/watch/user-activity'

**//////////////////////////\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*HBSS INDEX MESSAGE QUERY**

curl -XPUT 'elastic:changeme@bb11:9205/\_watcher/watch/hbsslogin' -d '

{

"trigger": {

"schedule": {

"interval": "1m"

}

},

"input" : {

"search" : {

"request" : {

"indices" : [ "hbss-audit-\*" ],

"body" : {

"query" : {

"bool" : {

"must" : { "match" : {"message": ".\*Failed Logon for user.\* AND .\*incorrect password.\*"}},

"filter" : {

"range" : {"@timestamp" : {"gte" : "now-10m"}}}

}

}

}

}

}

},

"condition" : {

"compare" : { "ctx.payload.hits.total" : { "gt" : 3 }}

},

"actions" : {

"hbsslogin" : {

"webhook" : {

"method" : "POST",

"host" : "128.63.27.245",

"port" : 9609,

"body" : "{{ctx.payload.hits.total}}:{{ctx.payload.hits }}"

}}

}

}

'

**///////////////\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*PRIORITY LABEL MATCH**

curl -XPUT 'elastic:changeme@bb11:9205/\_watcher/watch/priority' -d '

{

"trigger": {

"schedule": {

"interval": "10m"

}

},

"input" : {

"search" : {

"request" : {

"indices" : [ "hbss\*" ],

"body" : {

"size" : 0,

"query" : {

"bool": {

"filter": [

{

"range": {

"@timestamp": {

"gte": "now-15m"

}

}

}

],

"should" : [

{

"match" : { "priority" : "High" }

},

{

"match" : { "priority" : 1 }

}

],

"minimum\_should\_match" : 1,

"boost" : 1.0

} } }}

}},

"condition" : {

"compare" : { "ctx.payload.hits.total" : { "gt" : 0 }}

},

"actions" : {

"index-alert" : {

"index" : {

"index" : "watcher-alerts",

"doc\_type" : "Priority alert"

}

}}

}

'

**///////////////\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*SEVERITY LABEL MATCH**

curl -XPUT 'elastic:changeme@bb16:9200/\_watcher/watch/severity' -d '

{

"trigger": {

"schedule": {

"interval": "1h"

}

},

"input" : {

"search" : {

"request" : {

"indices" : [ "pipeline-auth\*" ],

"body" : {

"query" : {

"bool" : {

"must" : { "match" : {"severity\_label": "Error"}},

"filter" : {

"range" : {"@timestamp" : {"gte" : "now-30d"}}}

}

}

}

}

}

},

"condition" : {

"compare" : { "ctx.payload.hits.total" : { "gt" : 0 }}

},

"actions" : {

"index-alert" : {

"index" : {

"index" : "watcher-alerts",

"doc\_type" : "Severity alert"

}

},

"my-webhook" : {

"webhook" : {

"method" : "POST",

"host" : "bigbrother3.arl.army.mil",

"port" : 9612,

"body" : { "inline" : "{{ctx.payload.hits}}"},

"headers" : {

"Authorization" : "elastic",

"Content-Type": "application/json"

},

"body" : {

"inline" : { "message" : "{{ctx.payload.hits.hits}}" }

} }

}

}}

'

**///////////////\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*USER ACTIVITY MATCH**

curl -XPUT 'elastic:changeme@bigbrother3.arl.army.mil:9200/\_watcher/watch/user-activity' -d '

{

"metadata": {

"watch" : "user activity"

},

"trigger": {

"schedule": {

"interval": "1m"}},

"input" : {

"search" : {

"request" : {

"indices" : [ "pipeline-\*" ],

"body" : {

"query" : {

"bool" : {

"must" : { "match" : {"cmdname": ".\*New.\*"}},

"filter" : {

"range" : {"@timestamp" : {"gte" : "now-30d"}}}

}},

"aggs": {

"group\_by\_username": {

"terms": {

"field": "username.keyword"

}}}

}}}},

"actions" : {

"watcher-alerts" : {

"index" : {

"index" : "watcher-alerts",

"doc\_type" : "USER ACTIVITY Alert"

}},

"my-webhook": {

"transform" : {

"script" : "return ctx.id"

},

"webhook" : {

"method" : "POST",

"host" : "bigbrother3",

"port" : 9612,

"body" : "{{ctx.id}}"

}}

}

}'

**///////////////\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*USER 30-DAY LOGIN MATCH**

curl -XPUT 'elastic:changeme@bigbrother3.arl.army.mil:9200/\_watcher/watch/user-30day-login' -d '

{

"metadata": {

"watch" : "user 30 day login activity"

},

"trigger": {

"schedule": {

"interval": "1m"}},

"input" : {

"search" : {

"request" : {

"indices" : [ "pipeline-hbss-audit-\*" ],

"body" : {

"query":{

"bool" : {

"must" : { "match" : { "cmdname.keyword" : "Logon Attempt" }}

}},

"size": 0,

"aggs":{

"by\_user":{

"terms":{

"field":"username.keyword",

"min\_doc\_count": 0,

"order" : { "\_count" : "asc" },

"size":10000

} ,

"aggs": {

"by\_date": {

"date\_histogram": {

"field": "starttime",

"interval": "30d",

"order" : { "\_count" : "asc" },

"min\_doc\_count": 0,

"extended\_bounds": {

"min": "now-3M",

"max": "now"

}

}

},

"categories": {

"terms": {

"field": "\_count"

}

},

"min\_bucket\_selector": {

"bucket\_selector": {

"buckets\_path": {

"count": "categories.\_bucket\_count"

},

"script": {

"inline": "params.count != 0"

}

}

}

}

}

} } }}},

"actions" : {

"watcher-alerts" : {

"index" : {

"index" : "watcher-alerts",

"doc\_type" : "USER 30 DAY LOGIN ACTIVITY ALERT"

}},

"my-webhook": {

"webhook" : {

"method" : "POST",

"host" : "bigbrother3",

"port" : 9612,

"body" : "{{ctx.id}}"

}},

"send\_email" : {

"email" : {

"to" : "ian.t.robertson.ctr@mail.mil",

"subject" : "Testing USER signal",

"body": "USER ACTIVITY DETECTED. TESTING BODY. "

}

}

}}

'

**///////////////\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*USER CARDINALITY MATCH**

curl -XPUT 'elastic:changeme@bb11:9205/\_watcher/watch/user-login-ip' -d '

{

"trigger": {

"schedule": {

"interval": "10m"

}

},

"input" : {

"search" : {

"request" : {

"indices" : [ "pipeline-\*" ],

"body" : {

"query" : {

"bool" : {

"must" : { "match" : {"tag": "LOGIN"}},

"filter" : {

"range" : {"@timestamp" : {"gte" : "now-60d"}}}

}

},

"aggs": {

"group\_by\_username": {

"terms": {

"field": "username.keyword"

}

}

}

}

}

}

},

"actions" : {

"watcher-alerts" : {

"throttle\_period": "5m",

"index" : {

"index" : "watcher-alerts",

"doc\_type" : "USER ACTIVITY Alert"

}

},

"send\_email" : {

"email" : {

"to" : "ian.t.robertson.ctr@mail.mil",

"subject" : "Testing HBSS signal",

"body": "HBSS USER MATCH DETECTED. TESTING BODY."

}

}

}

}

'

**///////////////\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*USER ACTIVITY CHECK**

curl -XPUT 'elastic:changeme@bb11:9205/\_watcher/watch/user' -d '

{

"trigger": {

"schedule": {

"interval": "1m"

}

},

"input" : {

"search" : {

"request" : {

"indices" : [ "pipeline-syslog\*" ],

"body" : {

"query" : {

"bool" : {

"must" : { "exists" : {"field": "username"}},

"filter" : {

"range" : {"@timestamp" : {"gte" : "now-1m"}}}

}

}

}

}

}

},

"condition" : {

"compare" : { "ctx.payload.hits.total" : { "gt" : 0 }}

},

"actions" : {

"my-webhook" : {

"webhook" : {

"method" : "POST",

"host" : "128.63.27.245",

"port" : 9609,

"body" : "{{ctx.payload.hits.total}}:{{ctx.payload.hits }}"

}}

}

}

}'

**////////////////////////\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*INACTIVE USER ALERT**

POST \_xpack/watcher/watch/\_execute

{

"watch": {

"trigger": {

"schedule": {

"daily": {

"at": {

"hour": 5,

"minute": 0

}

}

}

},

"input": {

"search": {

"request": {

"indices": [

"pipeline-hbss-audit\*"

],

"body": {

"query": {

"bool": {

"must": [

{

"range": {

"starttime": {

"gt": "now-1y"

}

}

},

{

"exists": {

"field": "username"

}

},

{

"term": {

"cmdname.keyword": {

"value": "Logon Attempt"

}

}

},

{

"term": {

"message": {

"value": "successful"

}

}

}

]

}

},

"size": 0,

"aggs": {

"by\_user": {

"terms": {

"field": "username.keyword",

"size": 1000000

},

"aggs": {

"inactive\_periods": {

"scripted\_metric": {

"init\_script": "params.\_agg.logins = []",

"map\_script": "params.\_agg.logins.add(doc.starttime.value)",

"reduce\_script": {"file":"reduce-inactiveusers"}

}

}

}

}

}

}

}

}

},

"condition": {

"script": {

"file": "condition"

}

},

"transform": {

"script": {

"file": "transform-inactiveusers"

}

},

"actions": {

"send\_email" : {

"email" : {

"to" : [ "ian.t.robertson.ctr@mail.mil"],

"subject" : "TESTING (RAW Data): 30-Day Inactive Users List",

"body": "The following users had periods of inactivity greater than 30 days within the past year:\n\nThe payload is formatted into a dictionary containing user names mapped to an array of inactivity periods.\n{ \n\tuserX: { \n\t\tlogin: <date>,\n\t\t\tnext\_login: <date>,\n\t\t\tduration\_iso8601: <duration between logins in ISO 8601 format>\n\t}\n}\n\n{{ctx.payload}}\n\nDATA: \n\n{{#ctx.payload}}{{key}}: {{if(inactive\_periods != 0) {inactive\_periods} else{} }}\n{{/ctx.payload}}\n\n"

}

}

}

}

}

**//////////////////////////////\*\*\*\*\*\*\*\*\*\*\*\*\*\*CRITICAL ERRORS ALERT**

PUT /\_watcher/watch/critical-errors

{

"trigger": {

"schedule": {

"interval": "24h"

}

},

"input": {

"search": {

"request": {

"indices": [

"pipeline-auth\*"

],

"body": {

"query": {

"bool": {

"must": [

{

"range": {

"@timestamp": {

"gte": "now-24h"

}}},

{

"term": {

"severity\_label.keyword" : { "value" : "Critical"

}

}

}

]

}

},

"sort": [

{

"@timestamp": {

"order": "desc"

}

}

]

}

}

}

},

"condition": {

"compare": {

"ctx.payload.hits.total": {

"gt": 0

}

}

},

"actions": {

"send\_email" : {

"email" : {

"to" : ["ian.t.robertson.ctr@mail.mil", "david.d.jaccard.ctr@mail.mil", "kenneth.d.renard.ctr@mail.mil"],

"subject" : "Critical Auth Results",

"body": "{{ctx.payload.hits.total}} Critical Errors have occured in Auth Pipeline within past 24 hours\n\n{{#ctx.payload.hits.hits}}MESSAGE: {{\_source.message}}TIME: {{\_source.@timestamp}}\nHOST: {{\_source.host}}\nSOURCE: {{\_source.logsource}}\n\n{{/ctx.payload.hits.hits}}\n"

}

}

}

}

**//////////\*\*\*\*\*\*\*\*(TRANSFORM INTO PERCOLATOR) USER ACTIVITY CHECK FOR EXECUTION = 100% SUCCESS**

curl -XPUT 'elastic:changeme@bb11:9205/\_xpack/watcher/watch/userexe' -d '

{

"trigger": {

"schedule": {

"interval": "20h"

}

},

"input" : {

"search" : {

"request" : {

"indices" : [ "pipeline-syslog\*" ],

"body" : {

"query" : {

"bool" : {

"must" : { "exists" : {"field": "username"}},

"filter" : {

"range" : {"@timestamp" : {"gte" : "now-1080m"}}}

}

}

}}

}

},

"actions" : {

"my-webhook" : {

"webhook" : {

"method" : "POST",

"host" : "128.63.27.245",

"port" : 9612,

"body" : "{{ctx.payload.hits.total}}:{{ctx.payload.hits }}"

}}

}}

}'

**///////////////////\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*SYSTEMS REPORTING**

PUT /\_watcher/watch/inactive-users

{

"metadata": {

"window\_period": "3d",

"last\_period":"24h"

},

"trigger": {

"schedule": {

"interval": "24h"

}

},

"input": {

"search": {

"request": {

"indices": "pipeline-auth\*",

"body": {

"query": {

"bool": {

"must": [

{

"range": {

"@timestamp": {

"gte": "now-{{ctx.metadata.window\_period}}"

}}

}]}

},

"aggs": {

"periods": {

"filters": {

"filters": {

"history": {

"range": {

"@timestamp": {

"gte": "now-{{ctx.metadata.window\_period}}"

}

}

},

"last\_period": {

"range": {

"@timestamp": {

"gte": "now-{{ctx.metadata.last\_period}}"

}

}

}

}

},

"aggs": {

"hosts": {

"terms": {

"field": "client\_addr",

"size": 10000

}

}

}

}

},

"size": 0

}

}

}

},

"condition" : {

"script": "return ctx.payload.aggregations.periods.buckets.history.hosts.buckets.size() > ctx.payload.aggregations.periods.buckets.last\_period.hosts.buckets.size();"

},

"transform": {

"script": "def last\_period=ctx.payload.aggregations.periods.buckets.last\_period.hosts.buckets.stream().map(e -> e.key).collect(Collectors.toList()); return ctx.payload.aggregations.periods.buckets.history.hosts.buckets.stream().map(e -> e.key).filter(p -> !last\_period.contains(p)).collect(Collectors.toList());"

},

"actions": {

"send\_email" : {

"email" : {

"to" : ["ian.t.robertson.ctr@mail.mil"],

"subject" : "Systems Reporting Status (Alpha)",

"body": "Pipeline Auth Logs\n@author: Ian Robertson\n\n The following systems have not reported logs in the last {{ctx.metadata.last\_period}} hours using a {{ctx.metadata.window\_period}} window.\nUSE CASE: Verify Systems Reporting, Systems connectivity, and/or Data Validation \nDo per each index type.\n\n {{#ctx.payload.\_value}}{{.}} \n \n {{/ctx.payload.\_value}}\n"

}

}

}

}

**///////////////\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*BARE COMPONENTS FOR MANUAL EXECUTION**

curl -XPUT 'elastic:changeme@bb16:9205/\_xpack/watcher/watch/my-watch' -d '

{

"trigger": {

"schedule": {

"interval": "20h"

}

},

"actions": {

"send\_email": {

"email": {

"from": "root@bb11.iscm.arl.army.mil",

"to": "ian.t.robertson.ctr@mail.mil",

"subject": "Testing Email Delivery Alerting",

"body": "Body content goes here",

"account" : "standard\_account"

}

}

}

}

'

PUT \_xpack/watcher/watch/my-watch/\_execute

curl -XPOST elastic:changeme@bb11:9205/\_xpack/watcher/watch/my-watch/\_execute?pretty

**///////////////////\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*ADDITIONAL ACTION**

"send\_email" : {

"throttle\_period": "5m",

"email" : {

"to" : "elasticsearch@bb11",

"subject" : "Received Wakeup signal",

"body" : "Your Queue is full - dropping event. {{ctx.payload.client}}"

}

},

**//////////////////\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*ROOLING RESTART**

curl -XPUT 'elastic:changeme@128.63.27.63:9200/\_cluster/settings' -d '

{

"transient" : {

"cluster.routing.allocation.enable" : "none"

}

}

'

**////////////////////\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*RESTART ES**

./bin/elasticsearch.sh restart && tail –f log/Oceania-v5.log

curl -XPUT 'elastic:changeme@128.63.27.61:9200/\_cluster/settings' -d '

{

"transient" : {

"cluster.routing.allocation.enable" : "all"

}

}

'

**/////////////////////////\*\*\*\*\*\*\*\*\*\*\*\*\*FLUSH SYNCED**

curl -XPOST elastic:changeme@bb16:9200/\_flush/synced

**/////////////////////////\*\*\*\*\*\*\*\*\*\*\*\*\*LICENSE**

curl -XPUT -u elasticsearch bb11:9205/\_xpack/license -d @{army-research-lab-b925c19f-ce62-4851-b95a-6f0efec26fee-v2.json}

**////////////////\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*SNAPSHOT AND RESTORE**

curl -XPUT elastic:changeme@bb10:9205/\_snapshot/backup -d '{

"type": "fs",

"settings": {

"compress": true,

"location": "/srv/backup"

}

}

'

curl -XPOST elastic:changeme@bb16:9200/\_cluster/reroute?pretty -d '{ "commands" : [ { "allocate" : { "index" : ".monitoring", "shard" : 0, "node" :"bb16", "allow\_primary": "true" } } ] }'

///////////////////\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*CHANGE FIELDDATA

PUT pipeline-windows-\*/\_mapping/timestamp?update\_all\_types

{

"properties": {

"timestamp": {

"type": "text",

"fielddata": true

}

}

}

//////////////////\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*ADD TIMESTAMP

curl -XPUT elastic:changeme@bigbrother3:9200/watcher-alerts -d '{

"mappings" : {

"date\_field":{

"properties": {

"date": {

"type": "date"

}

}}

}

}'

curl -XPUT elastic:changeme@bigbrother2:9200/pip -d '{

"mappings" : {

"date\_field":{

"properties": {

"date": {

"type": "date"

}

}}

}

}'

node.name: "bb14"

cluster.name: "Oceania"

path.logs: "log"

network.host: "\_global\_, \_local\_"

discovery.zen.ping.unicast.hosts: "bigbrother", "bigbrother2", "bigbrother3", "bigbrother4"

discovery.zen.minimum\_master\_nodes: 1

node.master: false

node.data: true

node.ingest: false

elasticsearch/bin/elasticsearch -d \

-Edefault.node.name=${HOSTNAME} \

-Edefault.cluster.name="Oceania" \

-Edefault.path.data="/data/es\_data" \

-Edefault.path.logs="/home/elastic/v5/log" \

-Edefault.network.host="\_global\_, \_local\_" \

-Edefault.discovery.zen.ping.unicast.hosts=bigbrother,bigbrother2,bigbrother3,bigbrother4 \

-Edefault.node.master=false \

-Edefault.node.data=true \

-Edefault.node.ingest=false \

-Edefault.xpack.notification.email.account.standard\_account.profile=standard \

-Edefault.xpack.notification.email.account.standard\_account.smtp.auth=false \

-Edefault.xpack.notification.email.account.standard\_account.smtp.starttls.enable=false \

-Edefault.xpack.notification.email.account.standard\_account.smtp.starttls.required=false \

-Edefault.xpack.notification.email.account.standard\_account.smtp.host=localhost \

-Edefault.xpack.notification.email.account.standard\_account.smtp.port=25

mkdir elasticsearch; chown -R elasticsearch:elasticsearch data; chmod -R 750 data;

curl -k --cert "/etc/pki/private/iscmprod38.iscm.arl.army.mil.pem":changeit -XGET 'https://10.100.12.138:9200/\_cluster/settings'

ln -s /opt/elasticsearch /data01

service elasticsearch start && tail -f /var/log/elasticsearch/iscmprod38.iscm.arl.army.mil\_elasticsearch.log

curl -k --cert "/etc/pki/private/iscmprod38.iscm.arl.army.mil.pem":changeit -XGET 'https://10.100.12.138:9200/\_cluster/settings' -d '

{

"transient" : {

"cluster.routing.allocation.enable" : "all"

}}'

for shard in $( curl -k --cert "/etc/pki/private/iscmprod38.iscm.arl.army.mil.pem":changeit -XGET 'https://10.100.12.138:9200/\_cat/shards' | grep UNASSIGNED | awk '{print $2}'); do

curl -k --cert "/etc/pki/private/iscmprod40.iscm.arl.army.mil.pem":changeit -XPOST 'https://10.100.12.140:9200/\_cluster/reroute' -d '{

"commands" : [ {

"allocate" : {

"index" : "iscm\_assets\_4.4.0-snapshot\_2016dec17\_0800",

"shard" : 1,

"node" : "iscmprod40.iscm.arl.army.mil",

"allow\_primary" : true

}

}

]

}'

; sleep 5; done

curl -XPOST 'rdkdev46:9200/\_cluster/reroute' -d '{

"commands": [ {

"allocate": {

"index": "interrogator\_2015-10-20",

"shard": 1,

"node": "elk47",

"allow\_primary": true

}

}

]

}'