POST \_xpack/watcher/watch/\_execute

{

"watch": {

"metadata": {

"window\_period": "7d",

"last\_period":"24h"

},

"trigger": {

"schedule": {

"interval": "24h"

}

},

"input": {

"search": {

"request": {

"indices": "bb-hbss-audit-\*",

"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": "server.hostname.keyword",

"size": 10000

},

"aggs": {

"hostaddress": {

"terms": {

"field": "server.ip.keyword",

"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();"

},

"actions": {

"watcher-alerts" : {

"index" : {

"index" : "watcher",

"execution\_time\_field" : "triggered\_time",

"doc\_type" : "HBSS SYSTEMS REPORTING LOSS OF CONNECTIVITY ALERT. "

}},

"send\_email" : {

"email" : {

"to" : ["ian.t.robertson.ctr@mail.mil", "jack.c.swift2.ctr@mail.mil", "david.d.jaccard.ctr@mail.mil", "kenneth.d.renard.ctr@mail.mil", "james.s.herron.ctr@mail.mil", "akhilomen.o.oniha.civ@mail.mil", "daniel.f.baggeroer.ctr@mail.mil", "jason.m.rogowski.ctr@mail.mil", "john.e.shaffer.ctr@mail.mil", "cesar.e.pie.ctr@mail.mil","michael.b.bost.ctr@mail.mil", "mario.barboza.civ@mail.mil", "carlos.j.mateo.ctr@mail.mil", "jesse.d.kurrus.ctr@mail.mil", "usarmy.adelphi.7-sig-cmd.list.cndsp-watch@mail.mil", "phillip.l.tucker.ctr@mail.mil", "stephen.r.neyens.ctr@mail.mil"],

"subject" : "HBSS Systems Reporting Loss of Connectivity",

"body": "Monitoring HBSS Logs\n@author: Ian Robertson\n\n The following systems have not reported logs in the last {{ctx.metadata.last\_period}} hours.\n\nSystems Lost:\n\n {{#ctx.payload.aggregations.periods.buckets.history.hosts.buckets}} \t{{key}} on {{#hostaddress.buckets}} {{key}} {{/hostaddress.buckets}}\n \n {{/ctx.payload.aggregations.periods.buckets.history.hosts.buckets}}\n\n"

}

}

}

}

}

PUT \_xpack/watcher/watch/hbss-systems-reporting

{

"metadata": {

"title" : "List of Down Servers on HBSS",

"description": "The following list of hostnames and IP addresses are the locations of the servers that have not reported connectivity via logs. Using a window of 3 days.",

"window\_period": "3d",

"last\_period":"24h"

},

"trigger": {

"schedule": {

"interval": "24h"

}

},

"input": {

"search": {

"request": {

"indices": "bb-hbss-audit-\*",

"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": "server.hostname.keyword",

"size": 10000

},

"aggs": {

"hostaddress": {

"terms": {

"field": "server.ip.keyword",

"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();"

},

"actions": {

"watcher-alerts" : {

"index" : {

"index" : "watcher",

"execution\_time\_field" : "triggered\_time",

"doc\_type" : "HBSS SYSTEMS REPORTING LOSS OF CONNECTIVITY ALERT. "

}},

"send\_email" : {

"email" : {

"to" : ["ian.t.robertson.ctr@mail.mil", "david.d.jaccard.ctr@mail.mil", "kenneth.d.renard.ctr@mail.mil", "james.s.herron.ctr@mail.mil", "akhilomen.o.oniha.civ@mail.mil", "daniel.f.baggeroer.ctr@mail.mil", "jason.m.rogowski.ctr@mail.mil", "john.e.shaffer.ctr@mail.mil", "cesar.e.pie.ctr@mail.mil","michael.b.bost.ctr@mail.mil", "mario.barboza.civ@mail.mil", "carlos.j.mateo.ctr@mail.mil", "jesse.d.kurrus.ctr@mail.mil", "usarmy.adelphi.7-sig-cmd.list.cndsp-watch@mail.mil", "phillip.l.tucker.ctr@mail.mil", "thomas.a.schreck.ctr@mail.mil","debra.j.smith80.ctr@mail.mil", "peter.t.guarino.civ@mail.mil", "lfrye@keywcorp.com","anna.b.aquino.ctr@mail.mil", "michael.d.rivera2.ctr@mail.mil","thomas.p.bigelow2.ctr@mail.mil","stephen.r.neyens.ctr@mail.mil"],

"subject" : "HBSS Systems Reporting Loss of Connectivity",

"body": "Monitoring HBSS Logs\n@author: Ian Robertson\n\n The following systems have not reported logs in the last {{ctx.metadata.last\_period}} hours.\n\nSystems Lost:\n\n {{#ctx.payload.aggregations.periods.buckets.history.hosts.buckets}} \t{{key}} on {{#hostaddress.buckets}} {{key}} {{/hostaddress.buckets}}\n \n {{/ctx.payload.aggregations.periods.buckets.history.hosts.buckets}}\n\n"

}

}

}

}