Compliance and Client Run Reports Migration

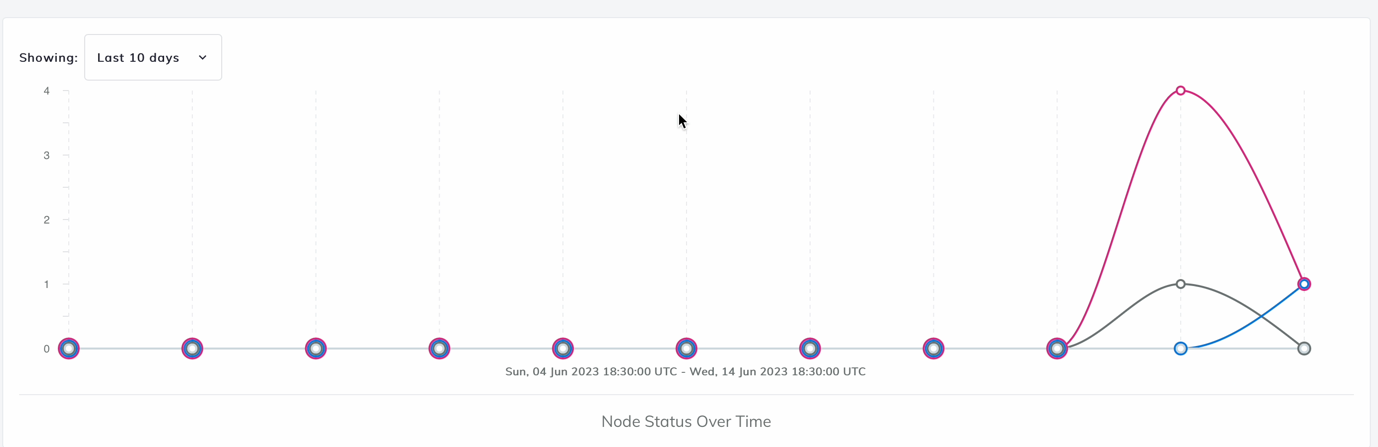
Compliance Report:

* Export Reports in JSON. We have API to download reports for a given date and with filters.
  + API- `api/v0/compliance/reporting/export` with the filters
  + {"type":"json","filters":[{"type":"start\_time","values":["2023-06-12T00:00:00Z"]},{"type":"end\_time","values":["2023-06-15T23:59:59Z"]}]}
* The API needs to be called with smaller intervals but multiple times to fetch all the reports from DB
* Structure the JSON data using script
  + Add `type:inspec\_report` field to the node
  + Modify node\_id as node\_uuid
  + Modidy id as report\_uuid
  + Change control tags from empty string to array of empty strings.
  + Change endTime from seconds to utc format ex:` 2006-01-02T15:04:05Z`
* Call */datacollector* API to push the data to the new system
  + With the API endpoint api/v0/events/data-collector
  + Using api-token make an http request and get response.

Trends API behaviour changes if we push data through /datacollector API

A screen shot of a graph

Description automatically generated with medium confidence



Example of the JSON struct:

{

"id": "547c9645-de1e-4754-a2ad-c5328b17a4d5",

"node\_id": "ff6556d1-0965-4b0f-bf1b-e37680c85280",

"node\_name": "chef-test-violet-waxwing-yellow-EUWDWX",

"end\_time": {

"seconds": 1686718598

},

"status": "passed",

"environment": "DevSec QWN NAKQP",

"version": "2.2.20",

"platform": {

"name": "debian",

"release": "8.18",

"full": "debian 8.18"

},

"statistics": {

"duration": 0.001481

},

"profiles": [

{

"name": "DevSec Apache BaselineKBAQKK",

"title": "DevSec Apache BaselineKBAQKK",

"copyright": "DevSec Hardening Framework Team",

"copyright\_email": "hello@dev-sec.io",

"summary": "Test-suite for best-practice apache hardening",

"version": "2.1.0",

"full": "DevSec Apache BaselineKBAQKK, v2.1.0",

"sha256": "3e1310b071dc4d706263e9d07083e10a92b4b69e4a36cffa1eda7eaecIDMTM",

"controls": [

{

"id": "apache-10",

"code": "control 'apache-10' do\n impact 1.0\n title 'Disable insecure HTTP-methods'\n desc 'Disable insecure HTTP-methods and allow only necessary methods.'\n\n describe file(File.join(apache.conf\_dir, '/conf-enabled/hardening.conf')) do\n its('content') { should match(/^\\s\*?\u003cLimitExcept\\s+?GET\\s+?POST\u003e/) }\n end\n\n # open bug https://github.com/chef/inspec/issues/786, if the bug solved use this test\n # describe apache\_conf do\n # its('LimitExcept') { should eq ['GET','POST'] }\n # end\nend\n",

"desc": "Disable insecure HTTP-methods and allow only necessary methods.",

"impact": 1,

"title": "Disable insecure HTTP-methods",

"source\_location": {

"ref": "apache-baseline-2.0.2/controls/apache\_spec.rb",

"line": 179

},

"results": [

{

"status": "skipped",

"code\_desc": "Operating System Detection",

"run\_time": 0.000004,

"skip\_message": "Skipped control due to only\_if condition."

}

],

"tags": "{}",

"waived\_str": "no"

},

{

"id": "apache-14",

"code": "control 'apache-14' do\n impact 1.0\n title 'Enable Apache Logging'\n desc 'Apache allows you to logging independently of your OS logging. It is wise to enable Apache logging, because it provides more information, such as the commands entered by users that have interacted with your Web server.'\n\n sites\_enabled\_path = File.join(apache.conf\_dir, '/sites-enabled/')\n loaded\_sites = command('ls ' \u003c\u003c sites\_enabled\_path).stdout.split.keep\_if { |file\_name| /.conf/.match(file\_name) }\n\n loaded\_sites.each do |id|\n describe file(File.join(sites\_enabled\_path, id)).content.gsub(/#.\*$/, '').scan(%r{\u003cvirtualhost(.\*?)\u003c\\/virtualhost\u003e}im).flatten do\n it { should include(/CustomLog.\*$/i) }\n end\n end\nend\n",

"desc": "Apache allows you to logging independently of your OS logging. It is wise to enable Apache logging, because it provides more information, such as the commands entered by users that have interacted with your Web server.",

"impact": 1,

"title": "Enable Apache Logging",

"source\_location": {

"ref": "apache-baseline-2.0.2/controls/apache\_spec.rb",

"line": 235

},

"results": [

{

"status": "skipped",

"code\_desc": "Operating System Detection",

"run\_time": 0.000003,

"skip\_message": "Skipped control due to only\_if condition."

}

],

"tags": "{}",

"waived\_str": "no"

}

],

"status": "passed"

}

],

"roles": [

"base\_windowsFBRWY",

"windows-hardeningSZGKO",

"best.role.everJMNQI"

]

}

Modified Struct to push to another Automate instance:

{

"end\_time": "2023-06-14T04:56:38Z",

"environment": "DevSec QWN NAKQP",

"node\_id": "ff6556d1-0965-4b0f-bf1b-e37680c85280",

"node\_name": "chef-test-violet-waxwing-yellow-EUWDWX",

"node\_uuid": "ff6556d1-0965-4b0f-bf1b-e37680c85280",

"platform": {

"full": "debian 8.18",

"name": "debian",

"release": "8.18"

},

"profiles": [

{

"controls": [

{

"code": "control 'apache-10' do\n impact 1.0\n title 'Disable insecure HTTP-methods'\n desc 'Disable insecure HTTP-methods and allow only necessary methods.'\n\n describe file(File.join(apache.conf\_dir, '/conf-enabled/hardening.conf')) do\n its('content') { should match(/^\\s\*?\u003cLimitExcept\\s+?GET\\s+?POST\u003e/) }\n end\n\n # open bug https://github.com/chef/inspec/issues/786, if the bug solved use this test\n # describe apache\_conf do\n # its('LimitExcept') { should eq ['GET','POST'] }\n # end\nend\n",

"desc": "Disable insecure HTTP-methods and allow only necessary methods.",

"id": "apache-10",

"impact": 1,

"results": [

{

"code\_desc": "Operating System Detection",

"run\_time": 0.000004,

"skip\_message": "Skipped control due to only\_if condition.",

"status": "skipped"

}

],

"source\_location": {

"line": 179,

"ref": "apache-baseline-2.0.2/controls/apache\_spec.rb"

},

"title": "Disable insecure HTTP-methods",

"waived\_str": "no"

},

{

"code": "control 'apache-14' do\n impact 1.0\n title 'Enable Apache Logging'\n desc 'Apache allows you to logging independently of your OS logging. It is wise to enable Apache logging, because it provides more information, such as the commands entered by users that have interacted with your Web server.'\n\n sites\_enabled\_path = File.join(apache.conf\_dir, '/sites-enabled/')\n loaded\_sites = command('ls ' \u003c\u003c sites\_enabled\_path).stdout.split.keep\_if { |file\_name| /.conf/.match(file\_name) }\n\n loaded\_sites.each do |id|\n describe file(File.join(sites\_enabled\_path, id)).content.gsub(/#.\*$/, '').scan(%r{\u003cvirtualhost(.\*?)\u003c\\/virtualhost\u003e}im).flatten do\n it { should include(/CustomLog.\*$/i) }\n end\n end\nend\n",

"desc": "Apache allows you to logging independently of your OS logging. It is wise to enable Apache logging, because it provides more information, such as the commands entered by users that have interacted with your Web server.",

"id": "apache-14",

"impact": 1,

"results": [

{

"code\_desc": "Operating System Detection",

"run\_time": 0.000003,

"skip\_message": "Skipped control due to only\_if condition.",

"status": "skipped"

}

],

"source\_location": {

"line": 235,

"ref": "apache-baseline-2.0.2/controls/apache\_spec.rb"

},

"title": "Enable Apache Logging",

"waived\_str": "no"

}

],

"copyright": "DevSec Hardening Framework Team",

"copyright\_email": "hello@dev-sec.io",

"full": "DevSec Apache BaselineKBAQKK, v2.1.0",

"name": "DevSec Apache BaselineKBAQKK",

"sha256": "3e1310b071dc4d706263e9d07083e10a92b4b69e4a36cffa1eda7eaecIDMTM",

"status": "passed",

"summary": "Test-suite for best-practice apache hardening",

"title": "DevSec Apache BaselineKBAQKK",

"version": "2.1.0"

}

],

"report\_uuid": "547c9645-de1e-4754-a2ad-c5328b17a4d5",

"roles": [

"base\_windowsFBRWY",

"windows-hardeningSZGKO",

"best.role.everJMNQI"

],

"statistics": {

"duration": 0.001481

},

"status": "passed",

"type": "inspec\_report",

"version": "2.2.20"

}