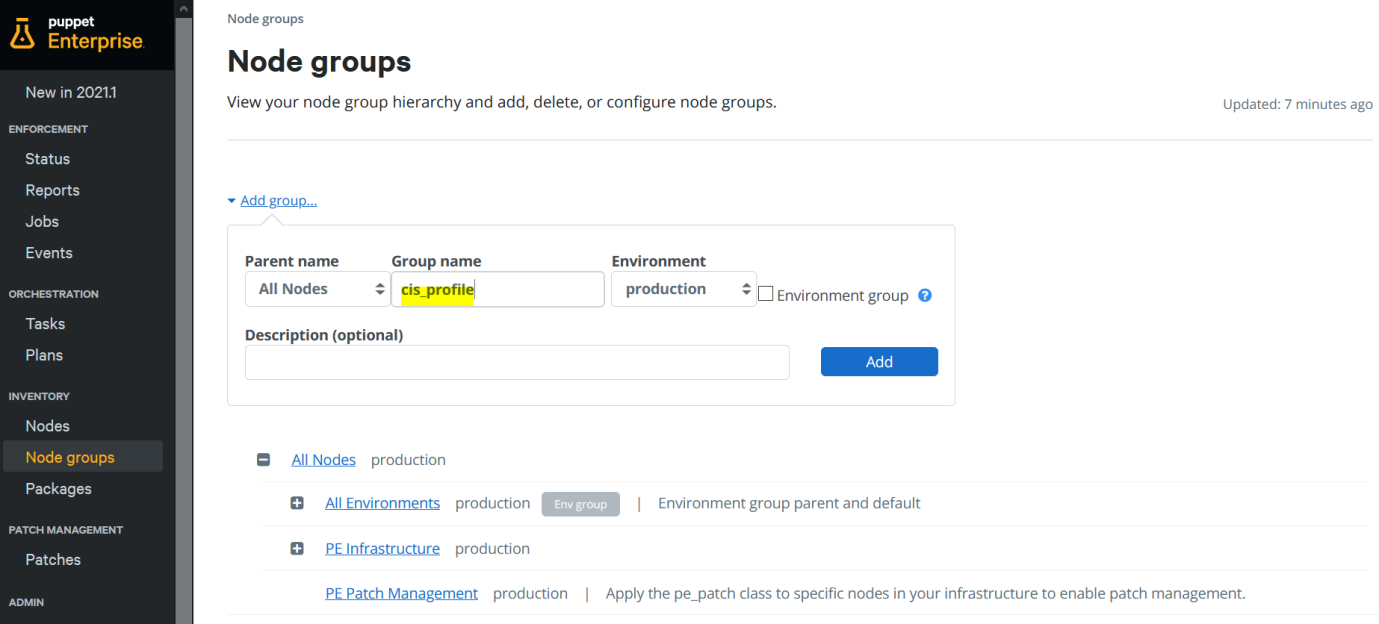
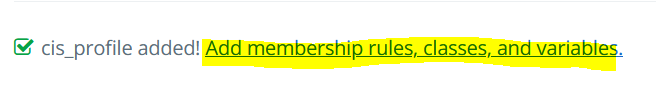
**How to perform Cyber-Hygiene using Puppet Enterprise 2021.1**

Login to Puppet Enterprise 2021.1 PE Console.

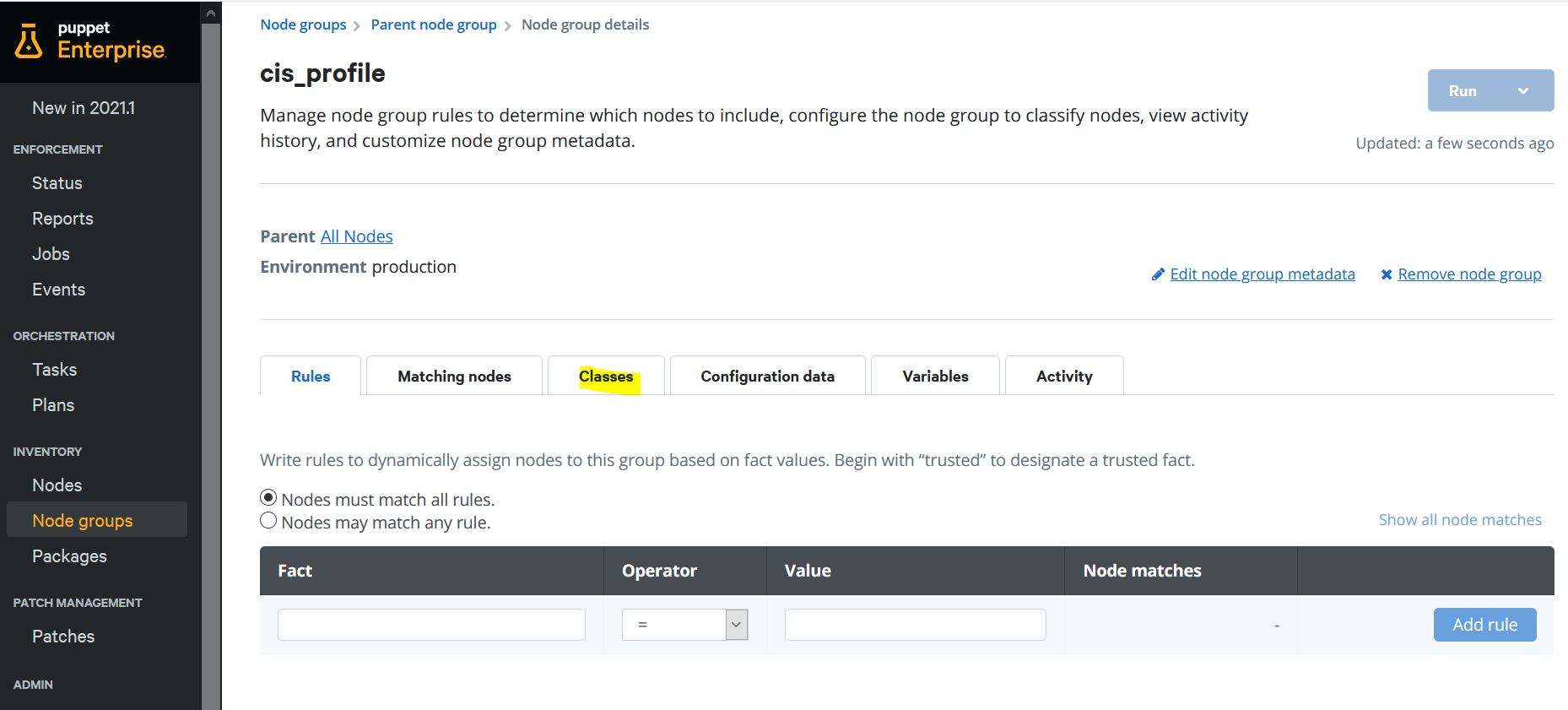
Click ‘**Node groups’ / ‘Add group’.**

Enter **‘cis\_profile’** as Group name, and click ‘**Add**’.

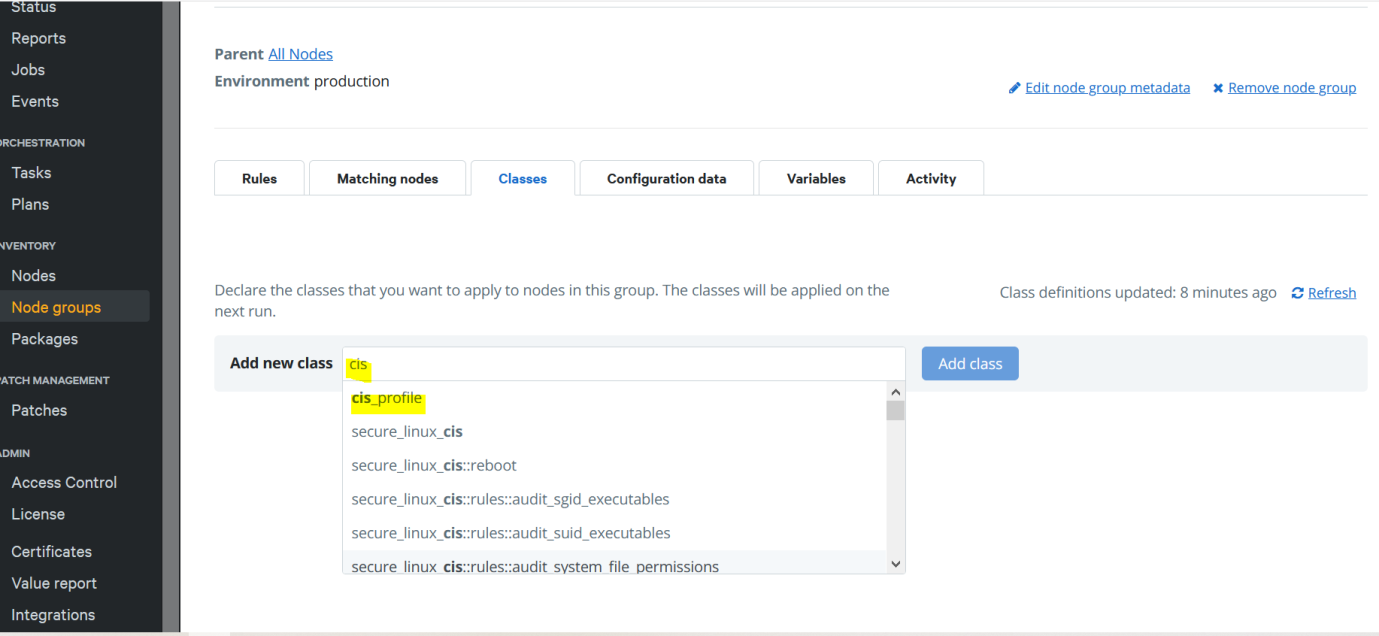




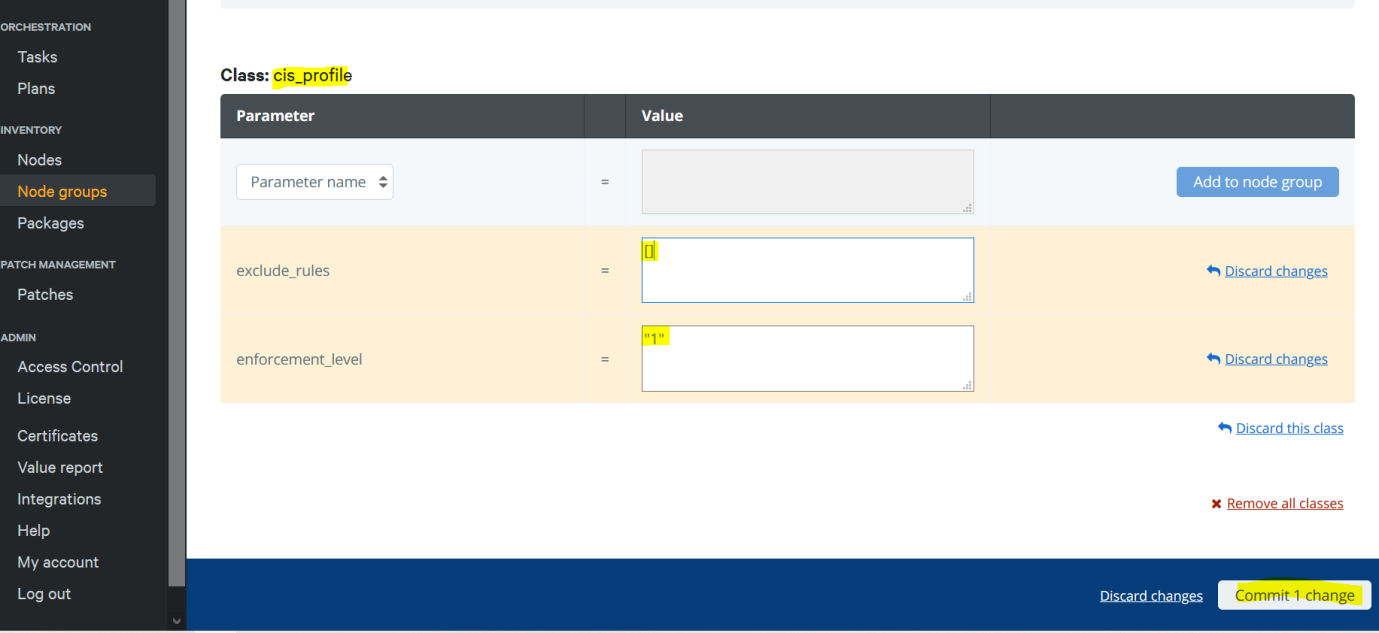
Click ‘**Add membership rules, classes, and variables**’.



Click ‘**Classes’** tab.



Enter ‘**cis\_profile**’ as ‘Add new classs’ and click ‘**Add class**’. You would notice the type-ahead search feature automatically presents you with a drop list of search result, you could select the ‘cis\_profile’ and ‘Add class’.



**Optionally**, you may add two parameters with preferred (example CIS Enforcement Level is 1 ) or default (example exclude\_rules is a blank array) values.

**enforcement \_level: ‘1’**

**exclude\_rules: []**

Don’t forget to click ‘**Commit 1 change**’ to save your changes.

Click ‘**Configuration data’** tab.

Add four parameters with desired values.

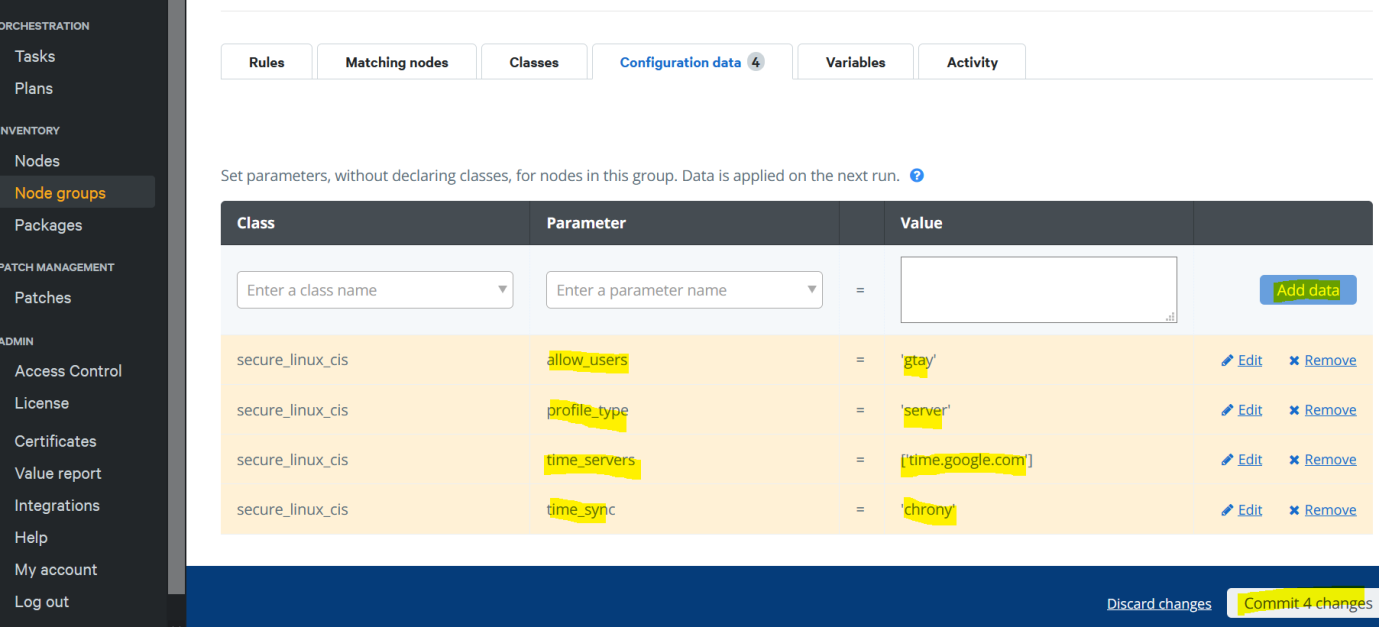
**time\_sync: ‘chrony’**

**time\_servers: [‘time.google.com’]**

**profile\_type: ‘server’**

**allow\_users: ‘gtay’**

Actually, if you disable the ‘**ensure\_ssh\_access\_is\_limited’** rules, the allow\_users parameter will be meaningless and could just be any dummy values.



Don’t forget to click ‘**Commit 4 changes**’ to save your changes.

Click ‘**Rules’** tab.

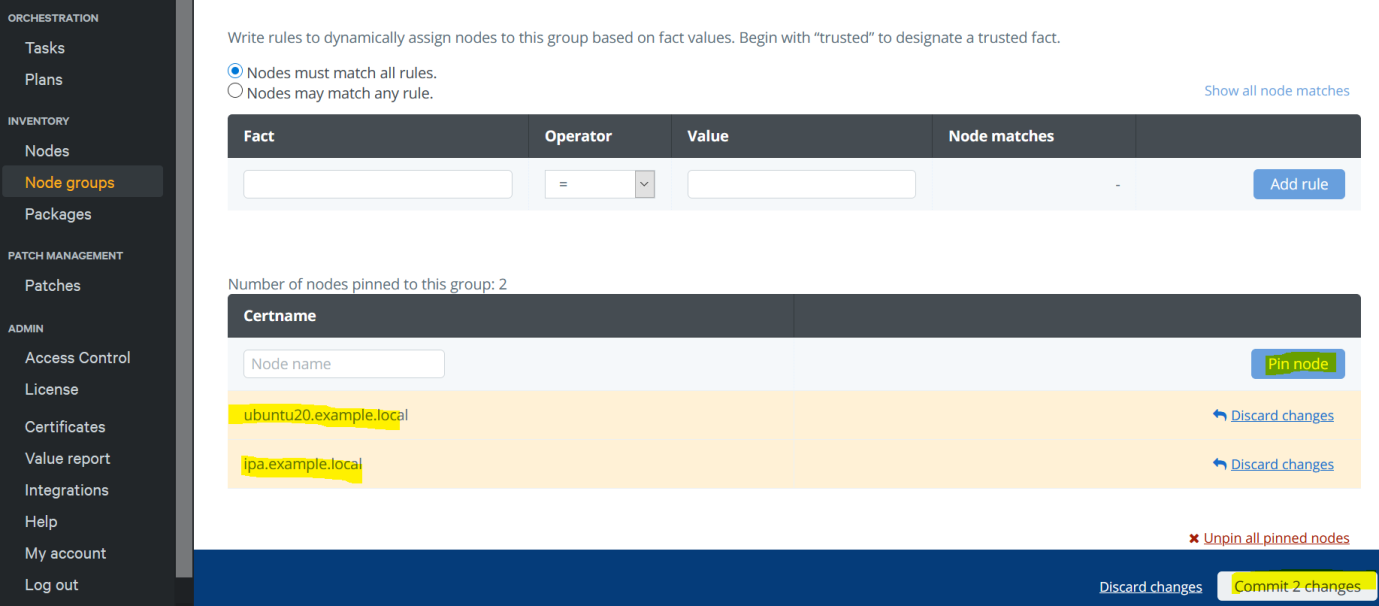
Look at the section ‘Pin specific nodes to the group.’

Under ‘Certname’, select and enter two nodes for POC (Proof Of Concept) of Cyber-Hygiene run.

. ipa.example.local

. ubuntu20.example.local

For each selection, click ‘**Pin node**’ to complete it.



Don’t forget to click ‘**Commit 2 changes**’ to save your changes.

Here it is, you are done with the configuration.

Login as **root** to Puppet Enterprise 2021.1 Agent node (server or workstation)

Run a few rounds of:

**# puppet agent -t -d --noop | tee dry\_run.log**

**# puppet agent -t -d | tee actual\_and\_debug\_run.log**

**# puppet agent -t | tee actual\_run.log**

Tips:

After each run, you may check the content of these two text files for the enforced\_rules selection and the available classes in the system.

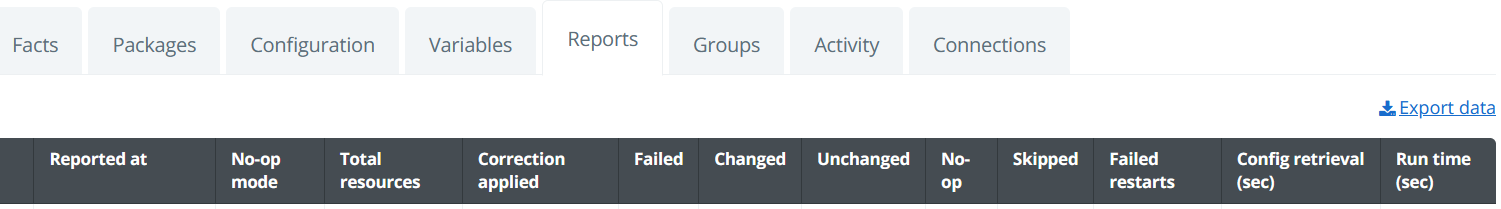
**$ cat /usr/share/cis\_scripts/enforced\_rules.txt**

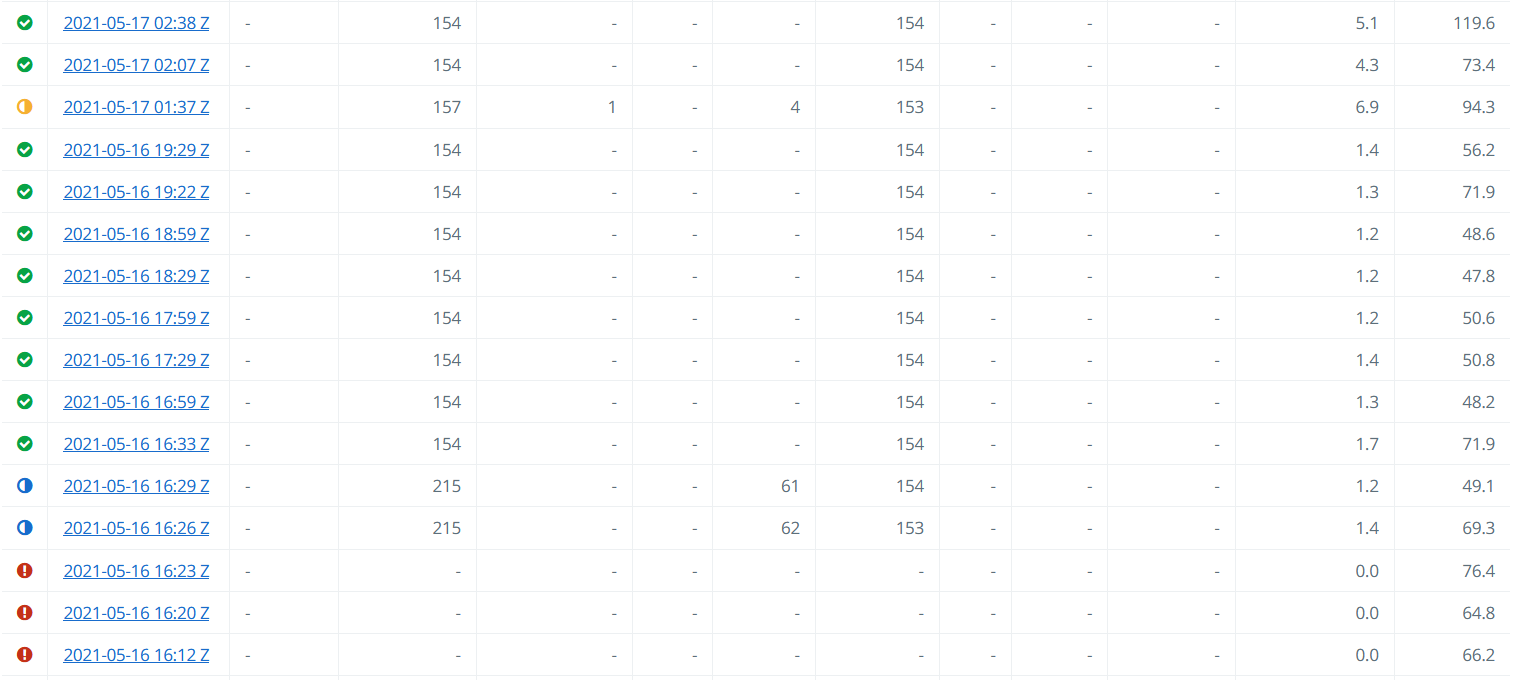
**$ sudo cat /opt/puppetlabs/puppet/cache/state/classes.txt**

After that login to PE Console, click ‘**Nodes**’ / select a node / ‘**Reports**’.

You will notice the change history of **Cyber-Hygiene**, I leave it to you to find-out what those colour codes actually mean?!

Happy Puppeting !!!





=== End of Doc ===