Table of Contents

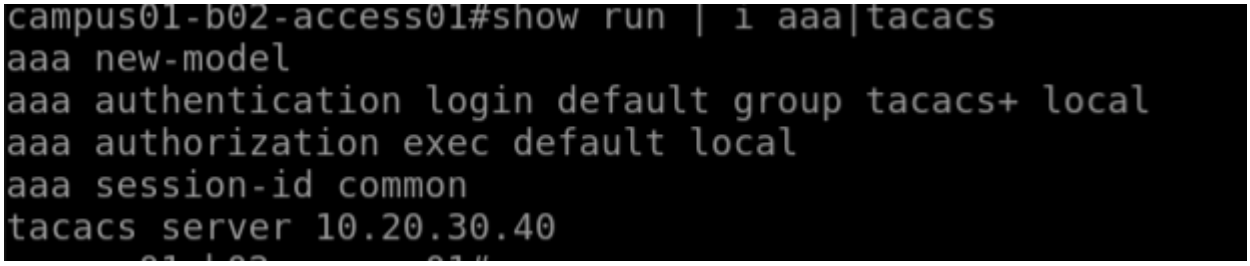
Verify if tacacs is configured

TACACS+ is a security application that provides centralized validation of users attempting to gain access to a router or network access server. Below example helps in validating tacacs configuration using NetYCE Compliance module

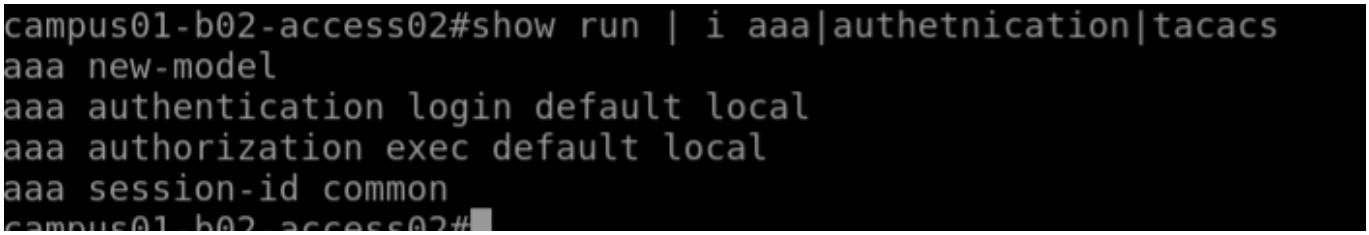
Example config

campus01-b02-access01 and campus01-b02-access02 are the two reference devices which we are using for this example. One has tacacs configuration and other does not.

campus01-b02-access01#

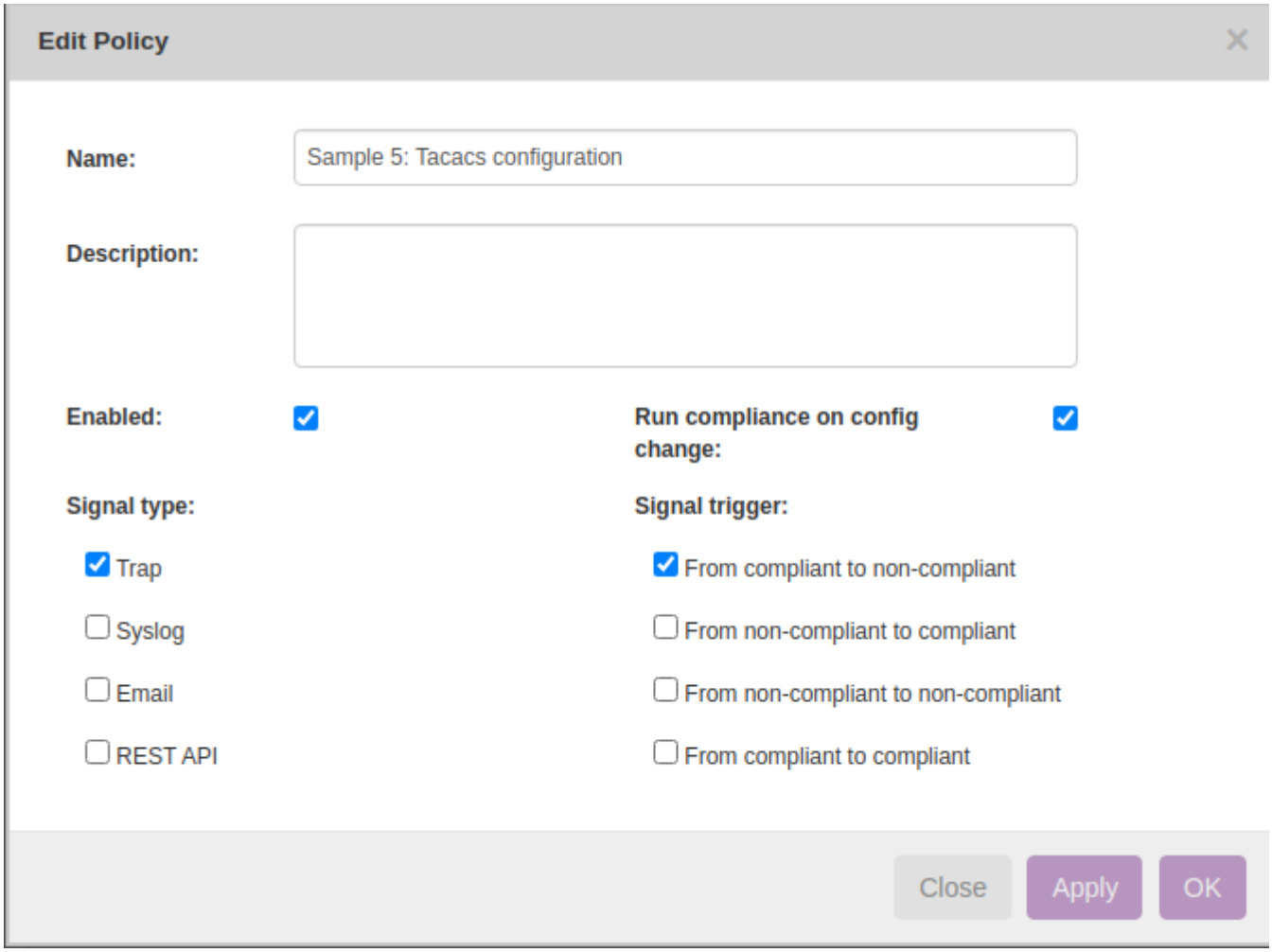


campus01-b02-access02#



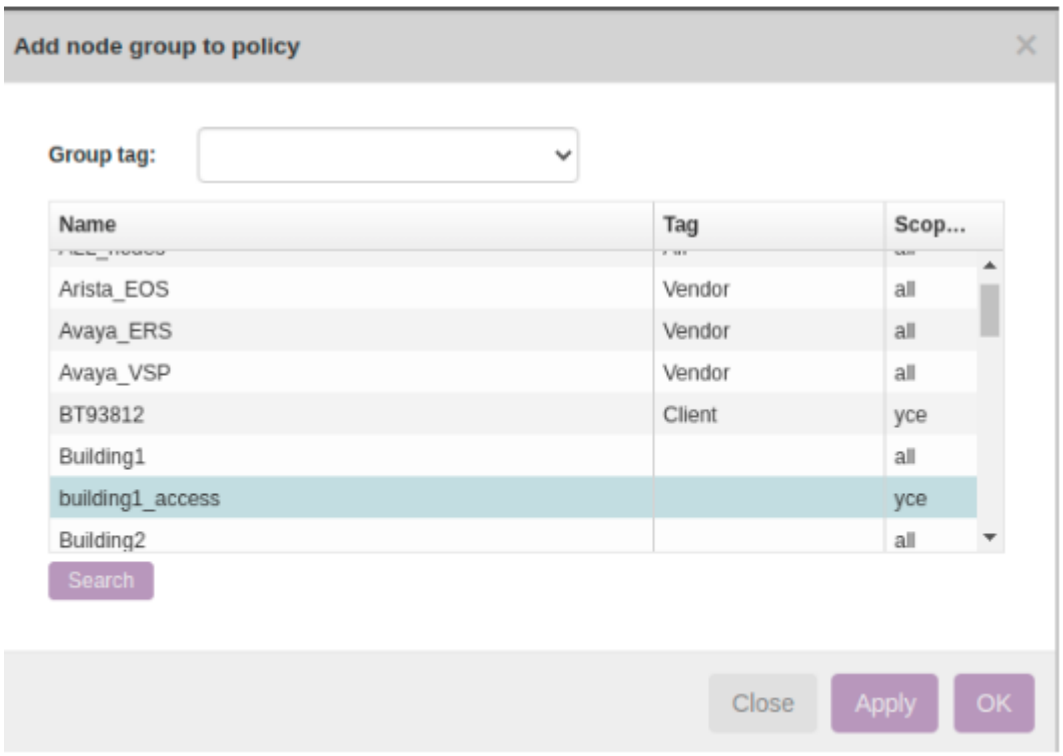
How its done

Below are the steps to create new policy. *Operate → Compliance → Policies → New→*

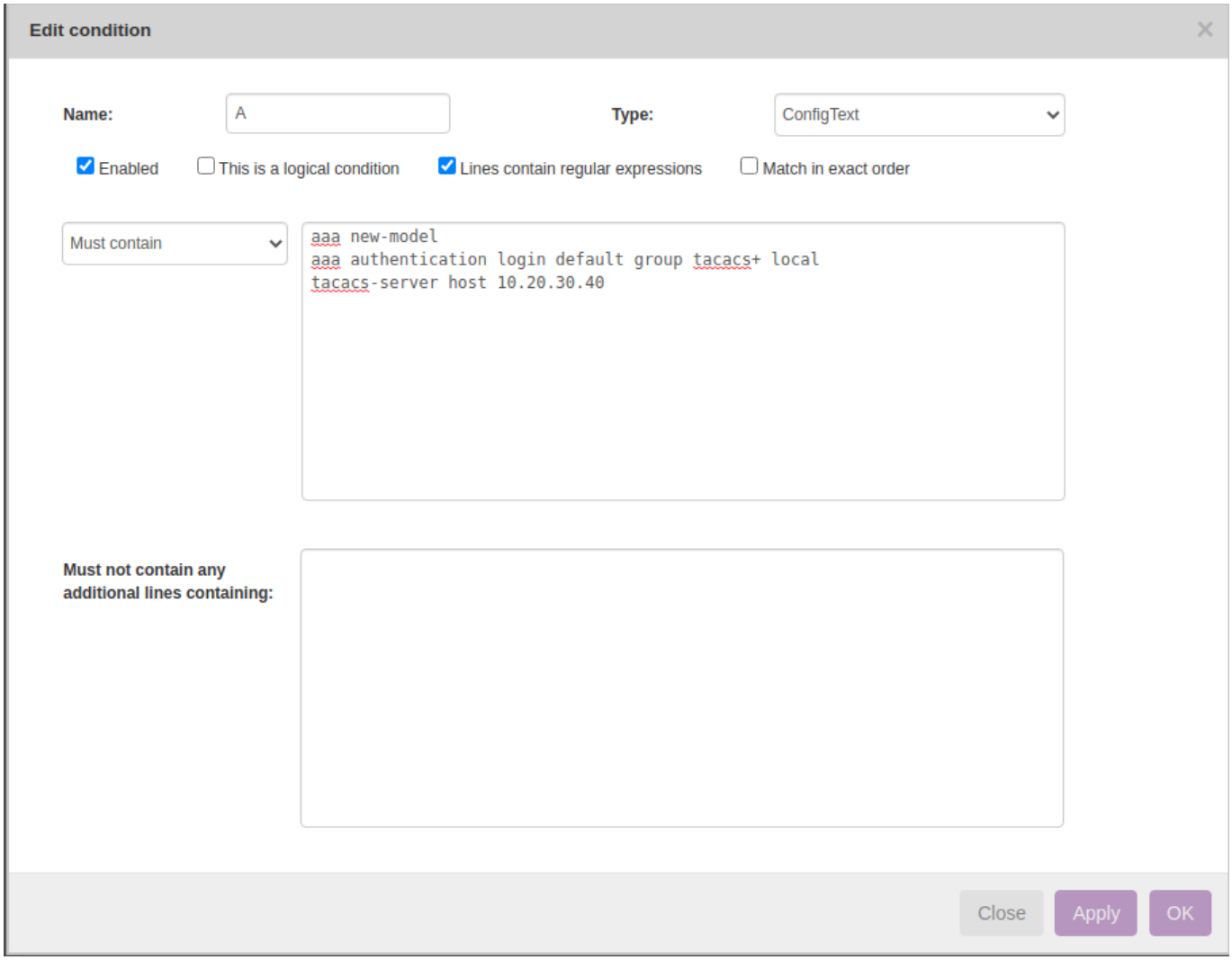


Click on the Node Group to select the relevant group of devices to add. Node group named “building2_access” holds the nodes of both the nodes:


Node group
Tag
Scope
New
Delete


Add node group to policy
Group tag:
Name
Tag
Scop...
Arista_EOS
Vendor
all
Avaya_ERS
Vendor
all
Avaya_VSP
Vendor
all
BT93812
Client
yce
Building1
all
building1_access
yce
Building2
all
Search
Close
Apply
OK

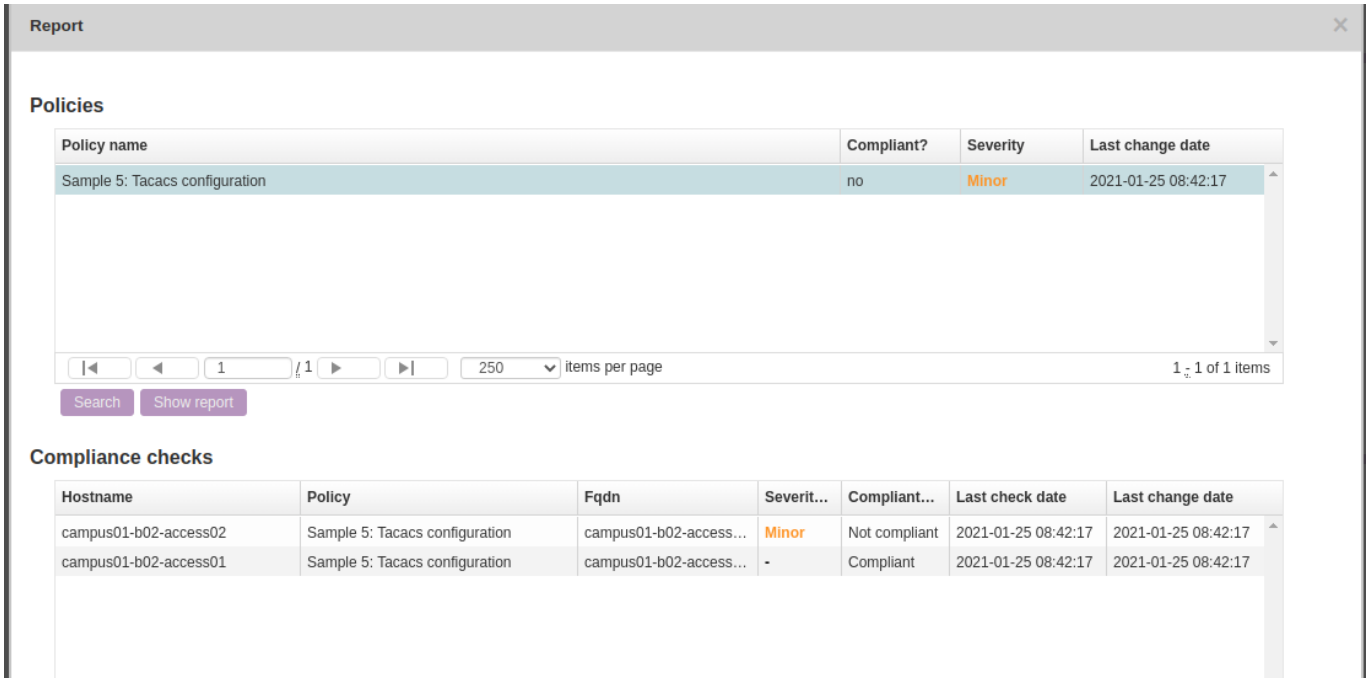
Rule → New



Report/test results:

Below is how to create reports to see the results of the compliance policies.

Operate → Compliance → Reports → New → Report Name "test" → Report type "Policies" → Policy Name "Sample5 : TACACS Configuration" → Show Report



This was a simple example to understand how to implement compliance policy to verify tacacs configuration.