

Table of Contents

Verify if tacacs is configured 3

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-access01#show run | i aaa|tacacs
aaa new-model
aaa authentication login default group tacacs+ local
aaa authorization exec default local
aaa session-id common
tacacs server 10.20.30.40
```

campus01-b02-access02#

```
campus01-b02-access02#show run | i aaa|authetnrication|tacacs
aaa new-model
aaa authentication login default local
aaa authorization exec default local
aaa session-id common
campus01-b02-access02#
```

How its done

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

Edit Policy

Name:

Sample 5: Tacacs configuration

Description:

Enabled:

☒

Run compliance on config change:

☒

Signal type:

☒ Trap

☐ Syslog

☐ Email

☐ REST API

Signal trigger:

☒ From compliant to non-compliant

☐ From non-compliant to compliant

☐ From non-compliant to non-compliant

☐ From compliant to compliant

Close

Apply

OK

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

Edit condition

Name:

A

Type:

ConfigText

☒ Enabled

☐ This is a logical condition

☒ Lines contain regular expressions

☐ Match in exact order

Must contain

aaa new-model
aaa authentication login default group tacacs+ local
tacacs-server host 10.20.30.40

Must not contain any
additional lines containing:

Close

Apply

OK

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

Report

Policies

Policy name	Compliant?	Severity	Last change date
Sample 5: Tacacs configuration	no	Minor	2021-01-25 08:42:17

1

/ 1

250

items per page

1 of 1 items

Search

Show report

Compliance checks

Hostname	Policy	Fqdn	Severit...	Compliant...	Last check date	Last change date
campus01-b02-access02	Sample 5: Tacacs configuration	campus01-b02-access...	Minor	Not compliant	2021-01-25 08:42:17	2021-01-25 08:42:17
campus01-b02-access01	Sample 5: Tacacs configuration	campus01-b02-access...	-	Compliant	2021-01-25 08:42:17	2021-01-25 08:42:17

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

From:
<https://wiki.netyce.com/> - **Technical documentation**

Permanent link:
<https://wiki.netyce.com/doku.php/guides:user:compliance:examples:tacacs>

Last update: **2022/04/29 08:39**

