aruba
a Hewlett Packard Enterprise company

CPPM-JUNIPER TACACS+ INTEGRATION

Chaitanya DNSS
cdnss@hpe.com

Contents

INTRODUCTION

This document talks about the Juniper Switch Integration with CPPM for TACACS Administration and is tested on Junos OS 18.4 and CPPM 6.9.5

JUNIPER SWITCH CONFIGURATION

On the Juniper Switch we need to define the TACACS+ Server and mention the authentication order to be TACACS+.

```
set system authentication-order tacplus
set system tacplus-server 10.10.1.162 secret "$9$ikqfQF/uBEjHqfTQn6reK8Nd"
set system tacplus-server 10.10.1.162 timeout 10
set system tacplus-server 10.10.1.162 single-connection
set system tacplus-server 10.10.1.162 source-address 10.10.11.100
set system tacplus-options timestamp-and-timezone
```

Make sure that your Switch Time is in Sync with the CPPM Time to avoid errors.

Now that we have configured the TACACS+ Server next step is to configure the following Classes along with the user templates.

In Juniper world the Local User Templates (SU, RO,OP) are tied to the class inside which the level of access is defined. By default, Juniper Network Devices will have four types of Login Classes with preset Permissions: **operator, Read-only, superuser/super-user, unauthorized**. So all we have to make sure the Login Templates are tied to respective classes.

```
juniperSwitch> show configuration | display set | match class
set system login user OP class operator
set system login user RO class read-only
set system login user SU class super-user
set system login user remote class read-only
```

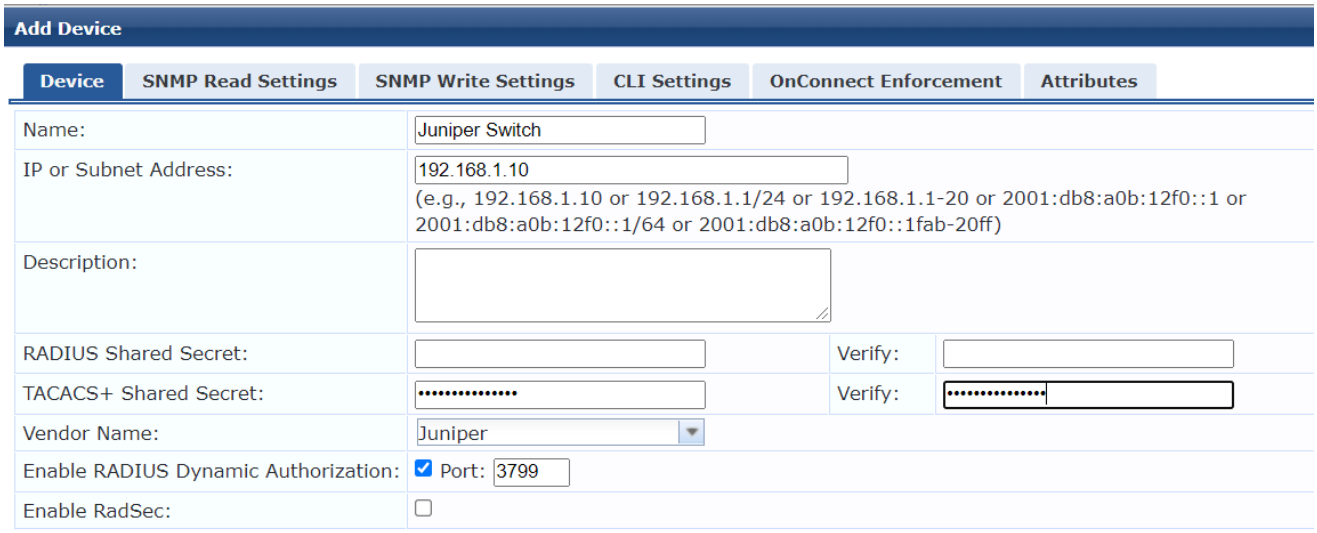
Configuring the Custom Class is beyond the Scope of this document and can be referred to below article.

https://www.juniper.net/documentation/us/en/software/junos/user-access/topics/topic-map/junos-os-login-class.html

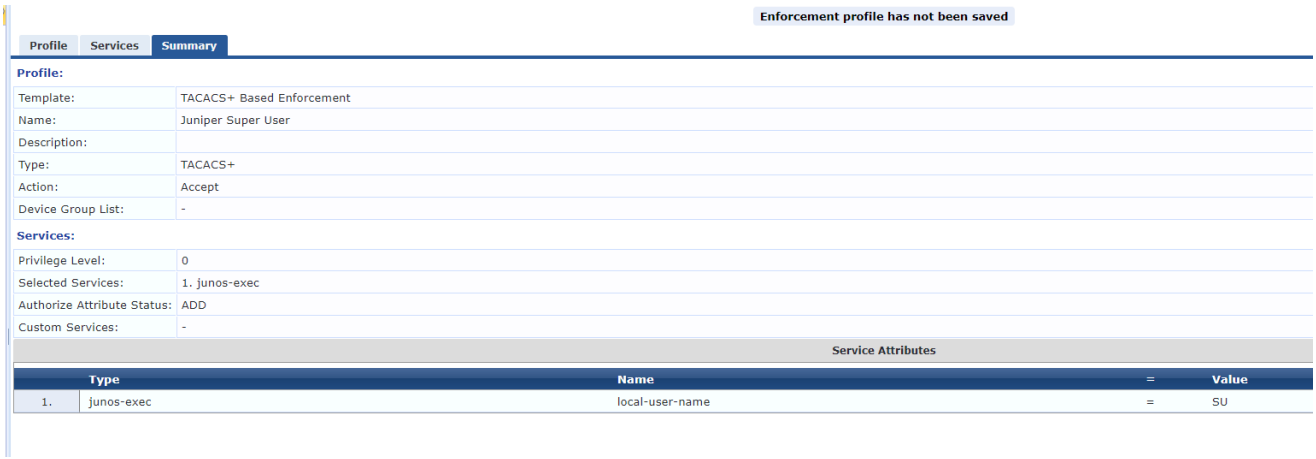
CLEARPASS TACACS+ CONFIGURATION:

Adding Juniper Device

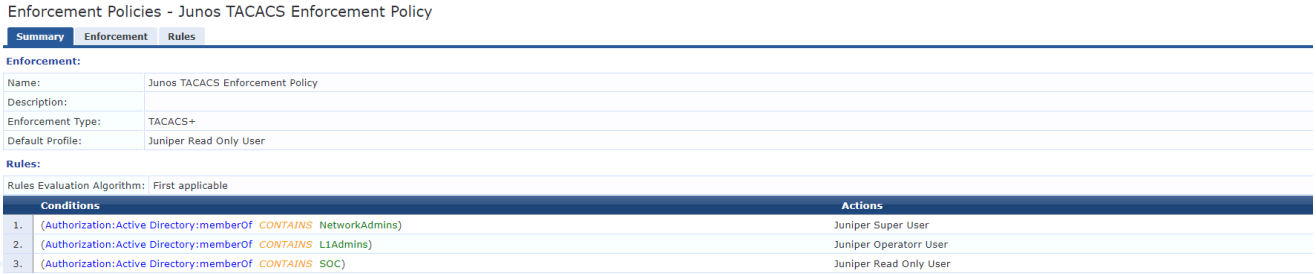
In Order to authenticate the Device the first step is to add the Juniper Device as the Network Device as below.



After you add the Device create the Enforcement Profiles that would return the Local User Templates Created on the Juniper Switch that is SU for superuser, RO for Read-Only, OP for Operator. Please note that these are case-sensitive.



After Creating the Profiles, we need to map the profiles to Enforcement Conditions post which Enforcement Policy can be included in the Service.



Map the Enforcement in the Service Created for Juniper TACACS+ Authentication and it would work as expected.
Starting 18.4 you can enable Accounting on Juniper