Update the CF Device Password in EM Configuration

Contents

Introduction

This document describes the procedure to update the StarOS Control-Function (CF) device password in the Element Manager (EM) configuration.

Operators may have to update the VNF passwords on a regular basis for security reasons. If the password of the StarOS CF and password set in EM are inconsistent, you must see this alarm on EM that tries to connect to the CF device.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Ultra Virtual Packet Core solutions components
- Ultra Automation Services (UAS)
- Element Manager(EM)
- Elastic Service Controllers (ESC)
- Openstack

Components Used

The information in this document is based on these software and hardware versions:

- USP 6.4
- EM 6.4.0
- ESC: 4.3.0(121)
- StarOS : 21.10.0 (70597)
- Cloud - CVIM 2.4.17

> **Note**: If the operator also uses AutoVNF, they need to update the AutoVNF configuration as well. This is helpful in re-deployment of VNF when you wish to continue with the same password.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Verify and Update the Password in EM

1. Log in to EM's NCS CLI.

```
/opt/cisco/usp/packages/nso/ncs-<version>/bin/ncs_cli -u admin -C

Example:
/opt/cisco/usp/packages/nso/ncs-4.1.1/bin/ncs_cli -u admin -C
```

2. Verify if the alarm connection-failure alarm is due to Bad password.

```
# /opt/cisco/usp/packages/nso/ncs-4.1.1/bin/ncs_cli -u admin -C
admin@scm# devices device cpod-vpc-cpod-mme-cf-nc connect
  result false
  info Failed to authenticate towards device cpod-vpc-cpod-mme-cf-nc: Bad password for
local/remote user admin/admin
admin@scm# *** ALARM connection-failure: Failed to authenticate towards device cpod-vpc-cpod-
mme-cf-nc: Bad password for local/remote user admin/admin
admin@scm#
```

Alarm details can be verified through **show alarms** command:

```
admin@scm# show alarms
alarms summary indeterminates 0
alarms summary criticals 0
alarms summary majors 0
alarms summary minors 0
alarms summary warnings 0
alarms alarm-list number-of-alarms 1
alarms alarm-list last-changed 2020-03-22T16:27:52.582486+00:00
  alarms alarm-list alarm cpod-vpc-cpod-mme-cf-nc connection-failure /devices/device[name='cpod-
vpc-cpod-mme-cf-nc'] ""
  is-cleared false
  last-status-change 2020-03-22T16:27:52.582486+00:00
last-perceived-severity major
  last-alarm-text "Failed to authenticate towards device cpod-vpc-cpod-mme-cf-nc: Bad password
for local/remote user admin/admin "
status-change 2020-03-22T16:26:38.439971+00:00
received-time 2020-03-22T16:26:38.439971+00:00
perceived-severity major
alarm-text "Connected as admin"
admin@scm#
```

3. Check if the device is in-sync with EM (ignore this step if the EM is not able to connect to the device).

```
admin@scm(config)# devices device cpod-vpc-cpod-mme-cf-nc check-sync
result in-sync
admin@scm(config)#
```

4. Verify the current authgroup configuration for the CF device.

```
admin@scm(config)# show full-configuration devices device cpod-vpc-cpod-mme-cf-nc authgroup
devices device cpod-vpc-cpod-mme-cf-nc
authgroup cpod-vpc-cpod-mme-cisco-staros-nc-ag
!
admin@scm(config)#
```

5. Verify the authgroup configuration for umap remote-name and remoe-password details.

```
admin@scm(config)# show full-configuration devices authgroups group cpod-vpc-cpod-mme-cisco-
staros-nc-ag
devices authgroups group cpod-vpc-cpod-mme-cisco-staros-nc-ag
umap admin
remote-name admin
remote-password $4$EeINS2rZCbXdh6ZY+VEXkQ==
!
umap oper
remote-name admin
remote-password $4$EeINS2rZCbXdh6ZY+VEXkQ==
!
umap security-admin
remote-name admin
remote-password $4$EeINS2rZCbXdh6ZY+VEXkQ==
!
!
admin@scm(config)#
```

6. Update the password for the authgroup (**cpod-vpc-cpod-mme-cisco-staros-nc-ag**) umap admin with the new password and device config password.

```
admin@scm(config)# devices authgroups group cpod-vpc-cpod-mme-cisco-staros-nc-ag umap admin
remote-password <new-password>

admin@scm(config-umap-admin)# top
```

7. Once the password is set, check dry-run commit to see whether the changes that are committed or not (proceed even if it doesn't display any difference for the authgroup password change). However, ensure there are no other changes apart from the intended changes.

```
admin@scm(config)# commit dry-run
admin@scm(config)#
```

8. Before commit, do a commit check to validate if the changes to commit made are syntactically correct

```
admin@scm(config)# commit check
Validation complete
admin@scm(config)#
```

9. If steps 7 okay, commit to the changes.

```
admin@scm(config)# commit
```

10. Verify whether the authgroup config and device config admin user password is updated or not.

```
admin@scm(config)# show full-configuration devices authgroups group cpod-vpc-cpod-mme-cisco-staros-nc-ag

admin@scm(config)# exit
```

11. Verify the same in running-config.

```
admin@scm# show running-config devices authgroups group cpod-vpc-cpod-mme-cisco-staros-nc-ag
```