更新EM配置中的CF设备密码

目录

简介

本文档介绍在元素管理器(EM)配置中更新StarOS控制功能(CF)设备密码的过程。

出于安全原因，操作人员可能必须定期更新VNF密码。如果StarOS CF的密码和EM中设置的密码不一致，您必须在尝试连接到CF设备的EM上看到此警报。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科超虚拟数据包核心解决方案组件
- 超自动化服务(UAS)
- 元素管理器(EM)
- 弹性服务控制器(ESC)
- OpenStack

使用的组件

本文档中的信息基于以下软件和硬件版本：

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

> **注意**：如果操作员也使用AutoVNF，则他们还需要更新AutoVNF配置。当您希望使用相同密码继续时，这有助于重新部署VNF。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

验证并更新EM中的密码

1.登录EM的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.验证警报连接故障警报是否由于密码错误而引起。

```
# /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#
```

警报详细信息可通过show alarms**命令**验证：

```
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.检查设备是否与EM同步（如果EM无法连接到设备，请忽略此步骤）。

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

4.检验CF设备的当前授权组配置。

```
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.验证umap remote-name和remoe-password详细信息的authgroup配置。

```
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.使用新密码和设备配置密码更新authgroup(**cpod-vpc-cpod-mme-cisco-staros-nc-ag**)umap admin的密码。

```
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.设置密码后，检查dry-run commit以查看是否提交了更改（即使没有显示身份验证组密码更改的任何差异，也继续操作）。 但是，请确保除预期更改外没有其他更改。

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

8.提交前，执行提交检查以验证对提交所做的更改是否在语法上正确

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

9.如果步骤7正确，则确定更改。

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

10.验证是否更新了authgroup config和device config admin用户密码。

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

admin@scm(config)# exit
```

11.在running-config中检验相同情况。

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