在EM配置中更新CF裝置密碼

目錄

簡介

本文檔介紹在元素管理器(EM)配置中更新StarOS控制功能(CF)裝置密碼的過程。

出於安全原因，操作員可能必須定期更新VNF密碼。如果StarOS CF的密碼和EM中設定的密碼不一致，您必須在嘗試連線到CF裝置的EM上看到此警報。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Ultra虛擬封包核心解決方案元件
- Ultra自動化服務(UAS)
- 元素管理器(EM)
- 彈性服務控制器(ESC)
- Openstack

採用元件

本文中的資訊係根據以下軟體和硬體版本：

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

> **附註**：如果操作員也使用AutoVNF，則他們也需要更新AutoVNF配置。當您希望繼續使用同一密碼時，這對VNF的重新部署很有幫助。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

驗證並更新EM中的密碼

1.登入到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.驗證警報連線失敗警報是否由於密碼錯誤。

```
# /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#
```

警報詳細資訊可通過**show alarms**命令驗證：

```
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.檢查裝置是否與EM同步（如果EM無法連線到裝置，請忽略此步驟）。

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

4.檢驗CF裝置的當前authgroup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.驗證umap remote-name和remote-password details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.使用新密碼和裝置配置密碼更新authgroup(**cpod-vpc-cpod-mme-cisco-staros-nc-ag**)umap admin的密碼。

```
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.設定密碼後，檢查乾式運行提交以檢視是否已提交更改（即使對authgroup密碼更改未顯示任何差異仍繼續操作）。 但是，請確保除預期更改外沒有其他更改。

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

8.提交之前，執行提交檢查以驗證對提交所做的更改是否語法正確

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

9.如果步驟7正常，則確認更改。

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

10.驗證authgroup config和device config admin使用者密碼是否已更新。

```
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中驗證相同內容。

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