Aktualisieren des CF-Gerätekennworts in der EM-Konfiguration

Inhalt

[Einführung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Überprüfen und Aktualisieren des Kennworts im EM](#)

Einführung

Dieses Dokument beschreibt das Verfahren zur Aktualisierung des Gerätekennworts der StarOS Control-Function (CF) in der Element Manager (EM)-Konfiguration.

Aus Sicherheitsgründen müssen Betreiber die VNF-Passwörter regelmäßig aktualisieren. Wenn das Kennwort des StarOS CF und das in EM festgelegte Kennwort inkonsistent sind, muss dieser Alarm im EM angezeigt werden, der versucht, eine Verbindung zum CF-Gerät herzustellen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Komponenten der Cisco Ultra Virtual Packet Core-Lösungen
- Ultra Automation Services (UAS)
- Element Manager (EM)
- Elastic Service Controller (ESC)
- OpenStack

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- USP 6.4
- EM 6.4.0
- ESC: 121
- StarOS: 70597
- Cloud - CVIM 2.4.17

> **Hinweis**: Wenn der Operator auch AutoVNF verwendet, muss auch die AutoVNF-Konfiguration aktualisiert werden. Dies ist hilfreich bei der erneuten Bereitstellung von VNF, wenn Sie mit demselben Kennwort fortfahren möchten.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Überprüfen und Aktualisieren des Kennworts im EM

1. Melden Sie sich bei der NCS CLI von EM an.

```
/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. Überprüfen Sie, ob der Alarm für einen Verbindungsausfall auf ein falsches Kennwort zurückzuführen ist.

```
# /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#
```

Details zum Alarm können mithilfe des Befehls **show alarm (Alarme) überprüft** werden:

```
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. Überprüfen Sie, ob das Gerät mit EM synchronisiert ist (ignorieren Sie diesen Schritt, wenn das EM keine Verbindung zum Gerät herstellen kann).

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

4. Überprüfen Sie die aktuelle Authentifizierungsgruppenkonfiguration für das CF-Gerät.

```
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. Überprüfen Sie die Konfiguration der Authentifizierungsgruppe für UMap-Details zu Remote-Namen und Remote-Passwörtern.

```
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. Aktualisieren Sie das Kennwort für den **umap-Admin** authgroup (**cpod-vpc-cpod-mme-cisco-staros-nc-ag**) mit dem neuen Kennwort und dem Gerätekonfigurationskennwort.

```
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. Wenn das Kennwort festgelegt ist, überprüfen Sie, ob die Änderungen übernommen wurden oder nicht (fahren Sie fort, auch wenn bei der Kennwortänderung für die Authentifizierungsgruppe kein Unterschied angezeigt wird). Stellen Sie jedoch sicher, dass außer den beabsichtigten Änderungen keine weiteren Änderungen vorgenommen werden.

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

8. Überprüfen Sie vor dem Commit, ob die vorgenommenen Änderungen syntaktisch korrekt sind.

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

9. Wenn die Schritte 7 in Ordnung sind, verpflichten Sie sich, die Änderungen vorzunehmen.

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

10. Überprüfen Sie, ob die Benutzerkennwörter für die authgroup-Konfiguration und die Gerätekonfiguration aktualisiert wurden.

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

admin@scm(config)# exit
```

11. Überprüfen Sie das Gleiche in der aktuellen Konfiguration.

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