Wachtwoord voor toegangsapparaat bijwerken in EM-configuratie

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Controleer en update het wachtwoord in EM](#)

Inleiding

In dit document wordt de procedure beschreven om het wachtwoord voor het StarOS-Control-Functie (CF)-apparaat in de configuratie van Element Manager (EM) bij te werken.

Exploitanten kunnen de VPN-wachtwoorden om veiligheidsredenen regelmatig moeten bijwerken. Als het wachtwoord van de StarOS CF en het wachtwoord dat in EM is ingesteld niet met elkaar in overeenstemming zijn, moet u dit alarm op EM zien dat probeert verbinding te maken met het CF-apparaat.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Componenten voor Cisco Ultra Virtual Packet Core-oplossingen
- Ultra Automation Services (UAS)
- Element-beheer (EM)
- Elastic Service Control-controllers (ESC)
- Openstack

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

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

> Opmerking: Als de operator AutoVNF ook gebruikt, moet de configuratie ook worden aangepast. Dit is handig om VPN opnieuw in te zetten als u met hetzelfde wachtwoord wilt doorgaan.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Controleer en update het wachtwoord in EM

1. Meld u aan bij 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. Controleer of het alarm dat de verbinding uitvalt te wijten is aan een slecht wachtwoord.

```
# /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#
```

Alarmgegevens kunnen worden geverifieerd met de opdracht Alarm tonen:

```
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. Controleer of het apparaat in-sync is met EM (negeer deze stap als het EM niet op het apparaat kan aansluiten).

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

4. Controleer de huidige groepsconfiguratie voor het CF-apparaat.

```
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. Controleer de configuratie van de auteur voor multi-name-naam en verwijder-wachtwoordgegevens.

```
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 het wachtwoord voor de **auteur** (**cpod-vpc-cpod-mme-cisco-staros-nc-ag**) map admin met het nieuwe wachtwoord en het wachtwoord voor apparaatconfiguratie.

```
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. Zodra het wachtwoord is ingesteld, controleer dan of de wijzigingen die al dan niet zijn aangebracht (Ga verder, ook als er geen verschil is voor de wijziging van het wachtwoord van de groep). Zorg er echter voor dat er geen andere wijzigingen zijn dan de voorgenomen wijzigingen.

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

8. Alvorens zich te engageren, moet u een controle uitvoeren om te valideren of de aangebrachte wijzigingen syntactisch correct zijn

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

9. Als stap 7 goed is, onderbreek dan de wijzigingen.

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

10. Controleer of de autorgroup configuratie en device configuratie beheerder het gebruikerswachtwoord wordt bijgewerkt of niet.

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

admin@scm(config)# exit
```

11. Controleer het zelfde in in werking stellen-configuratie.

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