Mettre à jour le mot de passe du périphérique CF dans la configuration EM

Contenu

Introduction

Ce document décrit la procédure à suivre pour mettre à jour le mot de passe du périphérique de fonction de contrôle (CF) StarOS dans la configuration de Element Manager (EM).

Les opérateurs peuvent devoir mettre à jour régulièrement les mots de passe VNF pour des raisons de sécurité. Si le mot de passe de la CF StarOS et le mot de passe définis dans EM sont incohérents, vous devez voir cette alarme sur EM qui tente de se connecter au périphérique CF.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Composants des solutions Cisco Ultra Virtual Packet Core
- Ultra Automation Services (UAS)
- Gestionnaire d'éléments (EM)
- Contrôleurs de service élastiques (ESC)
- OpenStack

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

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

> **Note**: Si l'opérateur utilise également AutoVNF, il doit également mettre à jour la configuration AutoVNF. Ceci est utile pour le redéploiement de VNF lorsque vous souhaitez continuer avec le même mot de passe.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Vérification et mise à jour du mot de passe dans EM

1. Connectez-vous à l'interface de ligne de commande NCS d'EM.

```
/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. Vérifiez si l'alarme de défaillance de connexion est due à un mot de passe incorrect.

```
# /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#
```

Les détails des alarmes peuvent être vérifiés à l'aide de la commande **show alarms** :

```
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. Vérifiez si le périphérique est synchronisé avec le module EM (ignorez cette étape si le module EM ne peut pas se connecter au périphérique).

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

4. Vérifiez la configuration actuelle du groupe d'authentification pour le périphérique CF.

```
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. Vérifiez la configuration authgroup pour les détails umap remote-name et remoe-password.

```
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. Mettez à jour le mot de passe de l'administrateur umap authgroup (**cpod-vpc-cpod-me-cisco-staros-nc-ag**) avec le nouveau mot de passe et le nouveau mot de passe de configuration du périphérique.

```
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. Une fois le mot de passe défini, cochez la case dry-run commit pour voir si les modifications sont validées ou non (continuez même s'il n'affiche aucune différence pour la modification du mot de passe authgroup). Cependant, assurez-vous qu'il n'y a pas d'autres changements en dehors des changements prévus.

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

8. Avant de valider, effectuez une vérification de validation pour vérifier si les modifications à valider sont correctes syntaxiquement

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

9. Si les étapes 7 sont correctes, assurez-vous de les modifier.

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

10. Vérifiez si le mot de passe utilisateur admin de configuration du groupe d'authentification et du

périphérique est mis à jour ou non.

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

admin@scm(config)# exit
```

11. Vérifiez la même chose dans running-config.

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