Ponga al día la contraseña del dispositivo de los CF en la configuración EM

Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Verifique y ponga al día la contraseña en el EM](#)

Introducción

Este documento describe el procedimiento para poner al día la contraseña del dispositivo de la función de control de StarOS (CF) en la configuración del encargado del elemento (EM).

Los operadores pueden tener que poner al día las contraseñas VNF en una base normal por razones de seguridad. Si la contraseña de los CF de StarOS y la contraseña definida en el EM son contrarias, usted debe ver esta alarma en el EM que intenta conectar con el dispositivo de los CF.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Componentes ultra virtuales de las soluciones de la base del paquete de Cisco
- Ultra servicios de la automatización (UAS)
- Elemento Manager(EM)
- Reguladores elásticos del servicio (salida)
- Openstack

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- USP 6.4
- EM 6.4.0
- Salida: 4.3.0(121)
- StarOS: 21.10.0 (70597)
- Nube - CVIM 2.4.17

> Nota: Si el operador también utiliza AutoVNF, necesitan poner al día la configuración de AutoVNF también. Esto es útil en el despliegue de VNF cuando usted desea continuar con

la misma contraseña.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Verifique y ponga al día la contraseña en el EM

1. Ábrase una sesión al NCS CLI 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. Verifique si la alarma del conexión-error de la alarma es debido a la mala contraseña.

```
# /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#
```

Los detalles de la alarma se pueden verificar a través del comando 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. Controle si el dispositivo está en sincronización con el EM (ignore este paso si el EM no puede conectar con el dispositivo).

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

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

4. Verifique la configuración actual del authgroup para el dispositivo de los 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. Verifique la configuración del authgroup para los detalles del nombre remoto y de la remoe-contraseña del umap.

```
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. Ponga al día la contraseña para el umap admin del authgroup (cpod-VPC-cpod-MME-Cisco-staros-nc-AG) con la nueva contraseña de la contraseña y de los config del dispositivo.

```
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. Una vez que se fija la contraseña, controle el cometer de plazo seco para ver si los cambios que están confiados o no (proceda incluso si no visualizan ninguna diferencia para el cambio de la contraseña del authgroup). Sin embargo, asegúrese que no haya otros cambios aparte de los cambios previstos.

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

8. Antes del cometer, haga un control del cometer para validar si los cambios a confiar hecho están sintácticamente correctos

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

9. Si autorización de los pasos 7, cometer a los cambios.

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

10. Verifique si la contraseña del usuario admin de los config del authgroup y de los config del dispositivo sea actualizada o no.

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

admin@scm(config)# exit
```

11. Verifique lo mismo en los ejecutar-config.

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