Actualizar la contraseña del dispositivo CF en la configuración de EM

Contenido

Introducción

Este documento describe el procedimiento para actualizar la contraseña del dispositivo StarOS Control-Function (CF) en la configuración del Administrador de elementos (EM).

Los operadores pueden tener que actualizar las contraseñas de VNF de forma regular por razones de seguridad. Si la contraseña de StarOS CF y la contraseña establecida en EM no son consistentes, debe ver esta alarma en EM que intenta conectarse al dispositivo CF.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Componentes de las soluciones Cisco Ultra Virtual Packet Core
- Servicios de automatización (UAS)
- Administrador de elementos (EM)
- Controladores de servicio elásticos (ESC)
- 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
- ESC: 4.3.0(121)
- StarOS : 21.10.0 (70597)
- Nube: CVIM 2.4.17

> **Nota:** Si el operador también utiliza AutoVNF, también necesita actualizar la configuración de AutoVNF. Esto es útil para la reimplementación de VNF cuando desea continuar con la misma contraseña.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Verificar y actualizar la contraseña en EM

1. Inicie sesión en la CLI de NCS de 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 de falla de conexión de alarma se debe a una contraseña incorrecta.

```
# /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 mediante el 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. Compruebe si el dispositivo está sincronizado con EM (ignore este paso si el EM no puede conectarse al 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 de authgroup para el dispositivo 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 authgroup para obtener los detalles umap remote-name y 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. Actualice la contraseña para el administrador de umap authgroup (**cpod-vpc-cpod-mme-cisco-staros-nc-ag**) con la nueva contraseña y la contraseña de configuración 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 configurada la contraseña, verifique la confirmación de ejecución en seco para ver si los cambios se han confirmado o no (continúe incluso si no muestra ninguna diferencia para el cambio de contraseña del grupo de autenticación). Sin embargo, asegúrese de que no haya otros cambios aparte de los previstos.

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

8. Antes de realizar la confirmación, realice una comprobación de confirmación para validar si los cambios realizados para la confirmación son sintácticamente correctos

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

9. Si el paso 7 está bien, realice los cambios.

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

10. Verifique si se ha actualizado o no la contraseña de usuario de authgroup config y device

config admin.

```
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 running-config.

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