Atualize a senha do dispositivo CF na configuração EM

Contents

Introduction

Este documento descreve o procedimento para atualizar a senha do dispositivo StarOS Control-Function (CF) na configuração do Element Manager (EM).

Os operadores podem ter que atualizar as senhas de VNF regularmente por motivos de segurança. Se a senha do CF do StarOS e a senha definidas em EM forem inconsistentes, você deverá ver esse alarme no EM que tenta se conectar ao dispositivo CF.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Componentes das soluções Cisco Ultra Virtual Packet Core
- Ultra Automation Services (UAS)
- Gerenciador de Elementos (EM)
- Controladores de serviço elásticos (ESC)
- Openstack

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

> **Note**: Se o operador também usar o AutoVNF, ele também precisará atualizar a configuração do AutoVNF. Isso é útil na reimplantação do VNF quando você deseja continuar com a mesma senha.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Verifique e atualize a senha no EM

1. Faça login na CLI do NCS da 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 se o alarme de falha de conexão do alarme é devido a uma senha incorreta.

```
# /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#
```

Os detalhes do alarme podem ser verificados por meio do 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. Verifique se o dispositivo está em sincronia com o EM (ignore esta etapa se o EM não puder se conectar ao dispositivo).

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

4. Verifique a configuração atual do grupo de autenticação para o 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 a configuração do grupo de autenticação para obter detalhes de nome remoto e senha remota 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. Atualize a senha para o admin umap do authgroup (**cpod-vpc-cpod-mme-cisco-staros-nc-ag**) com a nova senha e a nova senha de configuração do 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. Depois que a senha for definida, verifique a confirmação de execução para ver se as alterações foram confirmadas ou não (continue mesmo se ela não exibir nenhuma diferença para a alteração da senha do grupo de autenticação). No entanto, certifique-se de que não há outras alterações além das alterações pretendidas.

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

8. Antes de confirmar, faça uma verificação de confirmação para validar se as alterações a serem confirmadas foram sintacticamente corretas

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

9. Se as etapas 7 estiverem ok, confirme as alterações.

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

10. Verifique se a senha de usuário do admin de configuração do grupo de autenticação e do

dispositivo está atualizada ou não.

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

admin@scm(config)# exit
```

11. Verifique o mesmo em running-config.

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