# Aggiornare la password del dispositivo CF in Configurazione Enterprise Manager

## Sommario



## Introduzione

In questo documento viene descritta la procedura per aggiornare la password della periferica StarOS Control-Function (CF) nella configurazione di Element Manager (EM).

Gli operatori potrebbero dover aggiornare regolarmente le password VNF per motivi di sicurezza. Se la password di StarOS CF e la password impostata in EM non sono coerenti, deve essere visualizzato questo allarme su EM che tenta di connettersi al dispositivo CF.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Componenti delle soluzioni Cisco Ultra Virtual Packet Core
- Ultra Automation Services (UAS)
- Gestore elementi
- Elastic Service Controller (ESC)
- Openstack

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

> **Nota:** Se l'operatore utilizza anche AutoVNF, deve aggiornare anche la configurazione di AutoVNF. Ciò è utile per la ridistribuzione di VNF quando si desidera continuare con la stessa password.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

# Verifica e aggiornamento della password in EM

1. Accedere alla CLI NCS di 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. Verificare se l'allarme connessione-guasto allarme è dovuto a password errata.

```
# /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#
```

I dettagli dell'allarme possono essere verificati con il 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. Verificare che il dispositivo sia sincronizzato con EM (ignorare questo passaggio se EM non è in grado di connettersi al dispositivo).

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

4. Verificare la configurazione corrente del gruppo di autenticazione per il 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. Verificare la configurazione del gruppo di autenticazione per i dettagli relativi al nome remoto e alla password 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. Aggiornare la password dell'amministratore umap (cpod-vpc-cpod-mme-cisco-staros-nc-ag) con la nuova password e la nuova password di configurazione 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 volta impostata la password, selezionare dry-run commit per verificare se è stato eseguito il commit delle modifiche (procedere anche se non viene visualizzata alcuna differenza per la modifica della password Authgroup). Tuttavia, accertatevi che non vi siano altre modifiche oltre a quelle previste.

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

8. Prima di eseguire il commit, eseguire una verifica del commit per verificare se le modifiche da eseguire sono sintatticamente corrette

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

9. Se il punto 7 è corretto, confermare le modifiche.

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

10. Verificare se la password utente authgroup config e device config admin è aggiornata.

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

admin@scm(config)# exit
```

11. Verificare la stessa condizione nella configurazione corrente.

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