# Procédure de récupération pour le problème d'allocation de mémoire UAME

## Contenu



## Introduction

Ce document décrit comment récupérer l'Ultra Automation and Monitoring Engine (UAME) à partir du problème de fuite de mémoire dans UAME - CSCvu73187

## Problème

Alarme du contrôleur de services élastiques (ESC) sur le moniteur d'intégrité Ultra M :

```
[root@pod1-ospd ~]# cat /var/log/cisco/ultram-health/*.report | grep -i xxx
 10.10.10.10/vnf-esc          | esc      | XXX      | vnf-esc:(error)
```

## Solution

### Vérification du statut

Étape 1. Connectez-vous à OpenStack Platform Director (OSP-D) et vérifiez les erreurs vnf-esc.

```
[stack@pod1-ospd ~]$ cat /var/log/cisco/ultram-health/*.report | grep -i xxx
[stack@pod1-ospd ~]$ cat /var/log/cisco/ultram-health/*.report | grep -iv ':-)'
```

Étape 2. Confirmez que vous ne pouvez pas vous connecter à UAME via l'adresse IP de gestion 10.241.179.116, mais que l'adresse IP est ping :

```
(pod1) [stack@pod1-ospd ~]$ ssh ubuntu@10.10.10.10
ssh_exchange_identification: read: Connection reset by peer
(pod1) [stack@pod1-ospd ~]$ ping -c 5 10.10.10.10
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
64 bytes from 10.10.10.10: icmp_seq=1 ttl=57 time=0.242 ms
64 bytes from 10.10.10.10: icmp_seq=2 ttl=57 time=0.214 ms
64 bytes from 10.10.10.10: icmp_seq=3 ttl=57 time=0.240 ms
64 bytes from 10.10.10.10: icmp_seq=4 ttl=57 time=0.255 ms
64 bytes from 10.10.10.10: icmp_seq=5 ttl=57 time=0.240 ms
```

```
--- 10.10.10.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.214/0.238/0.255/0.016 ms
```

Étape 3. Vérifiez que les machines virtuelles liées à ESC et UAME sont ACTIVES et s'exécutent sur OSP-D.

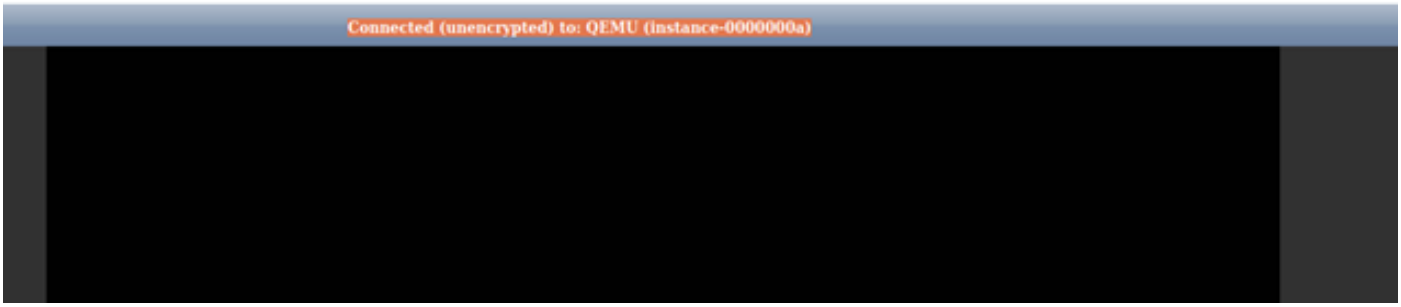
```
[stack@pod1-ospd ~]$ source *core
(pod1) [stack@pod1-ospd ~]$

(pod1) [stack@pod1-ospd ~]$ nova list --field name,status,host,instance_name,power_state | grep
esc
| 31416ffd-0719-4ce5-9e99-a1234567890e | pod1-uame-1 | ACTIVE | - | Running | pod1-AUTOMATION-
ORCH=172.16.180.15; pod1-AUTOMATION-MGMT=172.16.181.33 |
| d6830e97-bd82-4d8e-9467-a1234567890e | pod1-uame-2 | ACTIVE | - | Running | pod1-AUTOMATION-
ORCH=172.16.180.8; pod1-AUTOMATION-MGMT=172.16.181.12

(pod1) [stack@pod1-ospd ~]$ nova list --field name,status,host,instance_name,power_state | grep
uame
| 0c1596bc-e50f-4374-9098-a1234567890e | pod1-esc-vnf-esc-core-esc-1 | ACTIVE | - | Running |
pod1-AUTOMATION-ORCH=172.16.180.10; pod1-AUTOMATION-MGMT=172.16.181.10 |
| 3875618d-dcbe-4748-b196-a1234567890e | pod1-esc-vnf-esc-core-esc-2 | ACTIVE | - | Running |
pod1-AUTOMATION-ORCH=172.16.180.18; pod1-AUTOMATION-MGMT=172.16.181.5
```

Étape 4. Vérifiez que vous êtes en mesure de vous connecter à l'ESC principal et de secours. Vérifiez que l'état ESC est également correct.

```
[admin@pod1-esc-vnf-esc-core-esc-2 ~]$ cat /opt/cisco/esc/keepalived_state

[admin@pod1-esc-vnf-esc-core-esc-2 ~]$ health.sh
============== ESC HA with DRBD =================
vimmanager (pgid 14654) is running
monitor (pgid 14719) is running
mona (pgid 14830) is running
snmp is disabled at startup
etsi is disabled at startup
pgsql (pgid 15130) is running
keepalived (pgid 13083) is running
portal is disabled at startup
confd (pgid 15027) is running
filesystem (pgid 0) is running
escmanager (pgid 15316) is running
====================================
ESC HEALTH PASSED

[admin@pod1-esc-vnf-esc-core-esc-2 ~]$ ssh admin@172.16.180.12
########################################################################
# ESC on pod1-esc-vnf-esc-core-esc-2 is in BACKUP state.
########################################################################

[admin@pod1-esc-vnf-esc-core-esc-1 ~]$ cat /opt/cisco/esc/keepalived_state
BACKUP
```

## Étapes de récupération

Étape 1. Connectez-vous à la console Horizon Dashboard pour l'instance pod1-uame-2.




Étape 2. Redémarrez doucement l'instance de machine virtuelle pod1-uame-2 à partir du tableau de bord Horizon. Observez les messages du journal de console de l'instance.

Étape 3. Une fois que l'invite de connexion est affichée dans la console de l'instance de machine virtuelle pod1-uame-2 à partir du tableau de bord Horizon, lancez SSH dans l'UAME via son IP de gestion 10.10.10.10

```
(pod1) [stack@pod1-ospd ~]$ ssh ubuntu@10.10.10.10
```

**Note**: Passez à l'étape suivante uniquement si cette étape a réussi.

Étape 4. Vérifiez l'espace disque en particulier pour le système de fichiers **/dev/vda3** sur **principal** UAME.

```
ubuntu@pod1-uame-1:~$ df -kh
```

Étape 5. Tronquer le fichier syslog ou syslog.1 (taille de fichier plus grande sur les deux fichiers, généralement en Mo ou en Go) sur le système UAME **principal**.

```
ubuntu@pod1-uame-1:~$ sudo su -
root@pod1-uame-1:~#
root@pod1-uame-1:~# cd /var/log
root@pod1-uame-1:/var/log# ls -lrth *syslog*
root@pod1-uame-1:/var/log# > syslog.1 or > syslog
```

Étape 6. Assurez-vous que la taille du fichier syslog ou syslog.1 est désormais de 0 octets sur le système UAME **principal**.

```
root@pod1-uame-1:/var/log# ls -lrth *syslog*
```

Étape 7. Assurez-vous que df -kh doit avoir suffisamment d'espace libre pour la partition du système de fichiers sur le système UAME **principal**.

```
ubuntu@pod1-uame-1:~$ df -kh
```

SSH dans UAME secondaire.

```
ubuntu@pod1-uame-1:~$ ssh ubuntu@172.16.180.8
password:
...
ubuntu@pod1-uame-2:~$
```

Étape 8. Tronquer le fichier syslog ou syslog.1 (taille de fichier plus grande sur les deux fichiers, généralement en Mo ou en Go) sur le système UAME secondaire.

```
ubuntu@pod1-uame-2:~$ sudo su -
root@pod1-uame-2:~#
root@pod1-uame-2:~# cd /var/log
root@pod1-uame-2:/var/log# ls -lrth *syslog*
root@pod1-uame-2:/var/log# > syslog.1 or > syslog
```

Étape 9. Assurez-vous que la taille du fichier syslog ou syslog.1 est désormais de 0 octets sur le système UAME secondaire.

```
root@pod1-uame-2:/var/log# ls -lrth *syslog*
```

Étape 10. Assurez-vous que df -kh doit avoir suffisamment d'espace libre pour la partition du système de fichiers sur l'UAME secondaire.

```
ubuntu@pod1-uame-2:~$ df -kh
```

## Après vérification de l'état de récupération

Étape 1. Attendez au moins une itération du moniteur d'intégrité Ultra M pour confirmer qu'aucune erreur vnf-esc n'a été détectée dans le rapport d'intégrité.

```
[stack@pod1-ospd ~]$ cat /var/log/cisco/ultram-health/*.report | grep -i xxx
[stack@pod1-ospd ~]$ cat /var/log/cisco/ultram-health/*.report | grep -iv ':-)'
```

Étape 2. Confirmez que les machines virtuelles ESC et UAME sont ACTIVES et en cours d'exécution sur OSPD.

```
[stack@pod1-ospd ~]$ source *core
(pod1) [stack@pod1-ospd ~]$ nova list --field name,status,host,instance_name,power_state | grep
esc
(pod1) [stack@pod1-ospd ~]$ nova list --field name,status,host,instance_name,power_state | grep
uame
```

Étape 3. SSH dans l'ESC primaire et secondaire et confirmer que l'état de santé de l'ESC est également passé.

```
[admin@pod1-esc-vnf-esc-core-esc-2 ~]$ cat /opt/cisco/esc/keepalived_state
```

```
[admin@pod1-esc-vnf-esc-core-esc-2 ~]$ health.sh
============== ESC HA with DRBD =================
vimmanager (pgid 14638) is running
monitor (pgid 14703) is running
mona (pgid 14759) is running
snmp is disabled at startup
etsi is disabled at startup
pgsql (pgid 15114) is running
keepalived (pgid 13205) is running
portal is disabled at startup
confd (pgid 15011) is running
filesystem (pgid 0) is running
escmanager (pgid 15300) is running
=====================================
ESC HEALTH PASSED

[admin@pod1-esc-vnf-esc-core-esc-2 ~]$ ssh admin@
admin@172.16.181.26's password:
```

```
Last login: Fri May 1 10:28:12 2020 from 172.16.180.13

########################################################################
# ESC on scucs501-esc-vnf-esc-core-esc-2 is in BACKUP state.
########################################################################

[admin@pod1-esc-vnf-esc-core-esc-2 ~]$ cat /opt/cisco/esc/keepalived_state
BACKUP
```

Étape 4. Confirmez dans UAME que la valeur ESC vnfd est à l'état ALIVE.

```
ubuntu@pod1-uame-1:~$ sudo su
ubuntu@pod1-uame-1:~$ confd_cli -u admin -C
pod1-uame-1# show vnfr state
```