

Wiederherstellungsverfahren für das UAME-Speicherzuweisungsproblem

Inhalt

[Einführung](#)

[Problem](#)

[Lösung](#)

[Statusprüfung](#)

[Wiederherstellungsschritte](#)

[Nach Prüfung des Wiederherstellungsstatus](#)

Einführung

In diesem Dokument wird beschrieben, wie Sie die Ultra Automation and Monitoring Engine (UAME) aus dem Speicherlecks in UAME - [CSCvu73187](#) - wiederherstellen.

Problem

Der Alarm Elastic Services Controller (ESC) auf dem Ultra M-Statusmonitor:

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

Lösung

Statusprüfung

Schritt 1: Melden Sie sich bei OpenStack Platform Director (OSP-D) an, und überprüfen Sie die vnf-esc-Fehler.

```
[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 ':-)'
```

Schritt 2: Bestätigen Sie, dass Sie sich nicht über die Verwaltungs-IP 10.241.179.116 bei UAME anmelden können, IP jedoch pingfähig ist:

```
(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
```

Schritt 3: Bestätigen Sie, dass VMs im Zusammenhang mit ESC und UAME aktiv sind und auf OSP-D ausgeführt werden.

```
[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
```

Schritt 4: Stellen Sie sicher, dass Sie eine Verbindung zum primären und Backup-ESC herstellen können. Stellen Sie sicher, dass die ESC-Statusanzeige ebenfalls erfolgreich ist.

```
[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
```

Wiederherstellungsschritte

Schritt 1: Melden Sie sich bei der Horizon Dashboard Console für die Instanz POD1-UAM-2 an.

Schritt 2: Soft starten Sie die POD1-uame-2 VM-Instanz vom Horizon Dashboard neu. Beobachten Sie die Konsolenprotokollmeldungen der Instanz.

Schritt 3: Sobald die Anmeldeaufforderung in der Konsole der POD1-uame-2 VM-Instanz vom Horizon Dashboard angezeigt wird, starten Sie SSH über die Management-IP 10.10.10.10 in das UAME.

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

Hinweis: Fahren Sie nur dann mit dem nächsten Schritt fort, wenn dieser Schritt erfolgreich war.

Schritt 4: Überprüfen Sie den Speicherplatz speziell für `/dev/vda3` Dateisystem auf **primärem** UAME.

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

Schritt 5: Kürzen Sie die Syslog- oder Syslog.1-Datei (größere Dateigröße aus den beiden Dateien, in der Regel in MB oder GB) auf dem **primären** UAME.

```
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
```

Schritt 6: Stellen Sie sicher, dass die Dateigröße von syslog oder syslog.1 jetzt 0 Byte auf dem **primären** UAME beträgt.

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

Schritt 7: Stellen Sie sicher, dass `df -kh` genügend freien Speicherplatz für die Dateisystempartition auf dem **primären** UAME haben sollte.

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

SSH in sekundäres UAME.

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

```
...
```

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

Schritt 8: Abschneiden der Syslog- oder Syslog.1-Datei (größere Dateigröße von den beiden Dateien, in der Regel in MB oder GB) auf sekundärem UAME.

```
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
```

Schritt 9: Stellen Sie sicher, dass die Dateigröße von syslog oder syslog.1 jetzt 0 Byte auf dem sekundären UAME beträgt.

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

Schritt 10: Stellen Sie sicher, dass df -kh genügend freien Speicherplatz für Dateisystempartition auf sekundärem UAME haben sollte.

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

Nach Prüfung des Wiederherstellungsstatus

Schritt 1: Warten Sie mindestens eine Iteration des Ultra M Health Monitors, um sicherzustellen, dass im Gesundheitsbericht keine VNF-esc-Fehler aufgetreten sind.

```
[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 ':-)'
```

Schritt 2: Bestätigen Sie, dass ESC- und UAME-VMs aktiv sind und auf OSPD ausgeführt werden.

```
[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
```

Schritt 3: SSH in den primären und den Backup-ESC einlegen und sicherstellen, dass auch der ESC-Status übergeben wird.

```
[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
```

Schritt 4: Bestätigen Sie in UAME, dass ESC vnfd den Status "ALIVE" hat.

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