Procedimento de recuperação para o problema de alocação de memória UAME

Contents

Introduction

Este documento descreve como recuperar o UAME (Ultra Automation and Monitoring Engine, mecanismo de automação e monitoramento Ultra) do vazamento de memória na edição UAME - CSCvu73187

Problema

O alarme do controlador de serviços elásticos (ESC) no monitor de integridade 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)
```

Solução

Verificação de status

Etapa 1. Faça login no OpenStack Platform Diretor (OSP-D) e verifique os erros de 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 ':-)'
```

Etapa 2. Confirme se você não consegue fazer login no UAME por meio do IP de gerenciamento 10.241.179.116, mas se o IP pode executar 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
```

Etapa 3. Confirme se as VMs relacionadas ao ESC e UAME estão ATIVAS e são executadas no OSP-D.

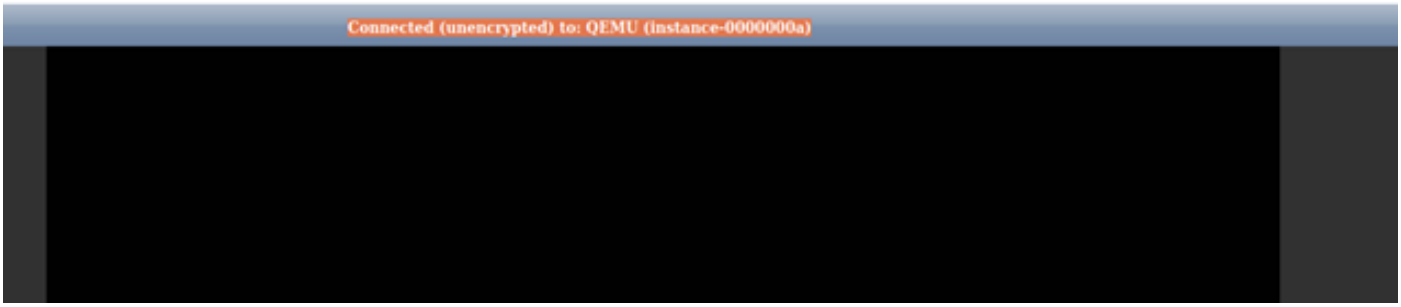
```
[stack@pod1-ospd ~]$ source *core
(pod1) [stack@pod1-ospd ~]$

(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
```

Etapa 4. Confirme se você pode se conectar ao ESC principal e de backup. Verifique se a integridade do ESC também foi passada.

```
[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
```

Etapas de recuperação

Etapa 1. Faça login no console do Horizon Dashboard para uma instância pod1-uame-2.



Etapa 2. Soft Reinicialize a instância da VM pod1-uame-2 no Horizon Dashboard. Observe as mensagens de log do console da instância.

Etapa 3. Quando o prompt de login for exibido no console da instância de VM pod1-uame-2 do Horizon Dashboard, inicie o SSH no UAME por meio do IP de gerenciamento 10.10.10.10

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

Note: Vá para a próxima etapa apenas se esta etapa tiver sido bem-sucedida.

Etapa 4. Verifique o espaço em disco especialmente para **/dev/vda3** filesystem no **principal** UAME.

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

Etapa 5. Trunque o arquivo syslog ou syslog.1 (maior tamanho de arquivo dos dois arquivos, geralmente em MB ou GB) no **principal** 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
```

Etapa 6. Certifique-se de que syslog ou syslog.1 file-size agora seja 0 bytes no UAME **principal**.

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

Passo 7. Verifique se df -kh deve ter espaço livre suficiente para a partição do sistema de arquivos no UAME **primário**.

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

SSH para UAME secundário.

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

Etapa 8. Trunque o arquivo syslog ou syslog.1 (maior tamanho de arquivo dos dois arquivos, geralmente em MB ou GB) no UAME secundário.

```
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
```

Etapa 9. Certifique-se de que syslog ou syslog.1 file-size agora seja 0 bytes em UAME secundário.

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

Etapa 10. Verifique se df -kh deve ter espaço livre suficiente para a partição do sistema de arquivos no UAME secundário.

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

Após a verificação do status da recuperação

Etapa 1. Aguarde pelo menos uma iteração do monitor de integridade do Ultra M para confirmar que nenhum erro de vnf-esc é visto no relatório de integridade.

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

Etapa 2. Confirme se as VMs ESC e UAME estão ATIVAS e em execução no 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
```

Etapa 3. SSH para o ESC principal e de backup e confirme se a integridade do ESC também foi passada.

```
[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
```

Etapa 4. Confirme no UAME se o ESC vnfd está em estado ALIVE.

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