Manual de verificação de integridade do CPAR

Contents

Introduction

Este documento descreve como verificar a integridade do Cisco Prime Access Registrar (CPAR) antes e depois da execução de uma janela de manutenção.

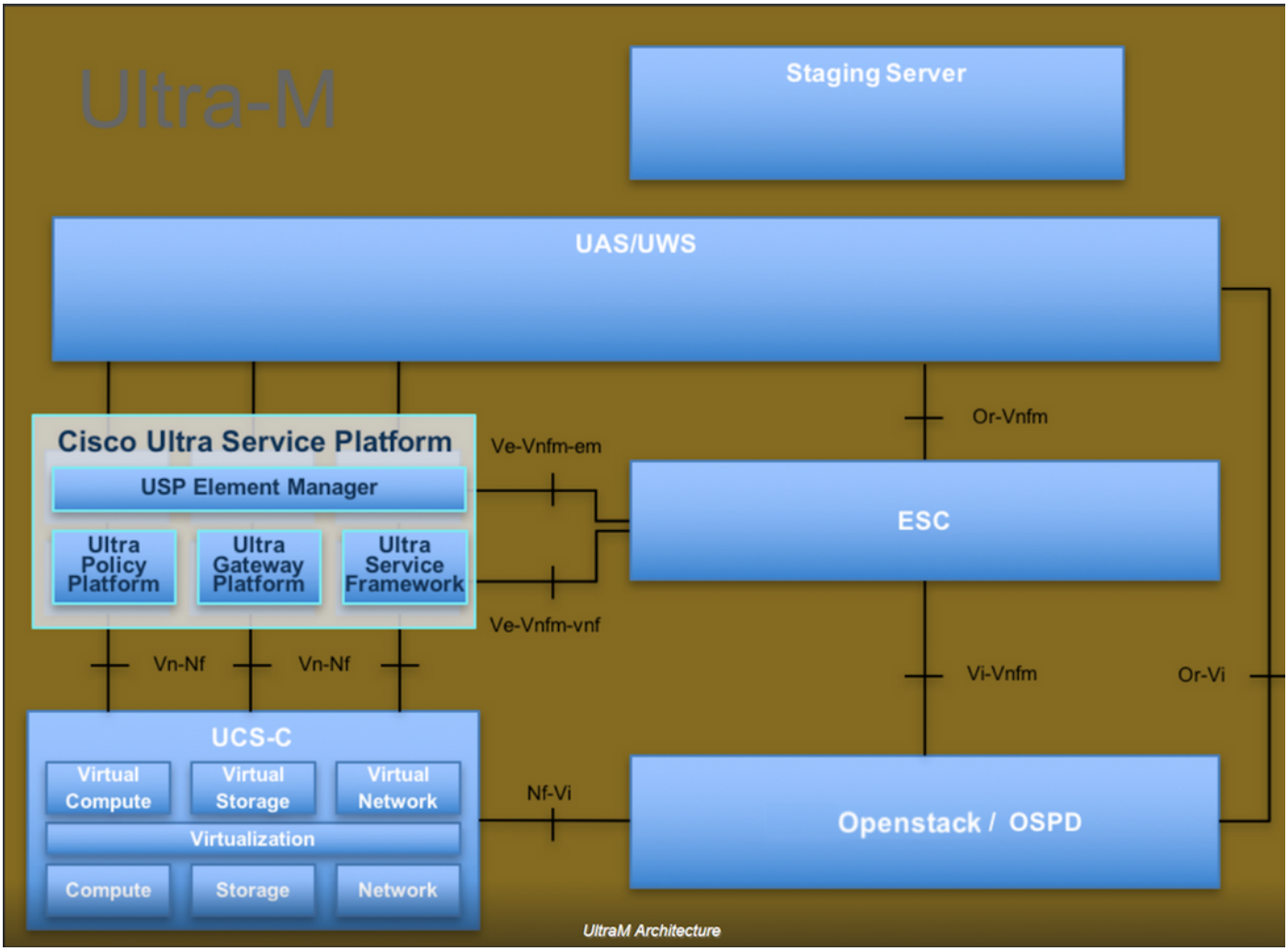
Este procedimento aplica-se a um ambiente Openstack usando a versão NEWTON em que o ESC não gerencia o CPAR e é instalado diretamente na VM implantada no Openstack.

Informações de Apoio

O Ultra-M é uma solução de núcleo de pacotes móveis virtualizados pré-embalada e validada, projetada para simplificar a implantação de VNFs. O OpenStack é o Virtualized Infrastructure Manager (VIM) para Ultra-M e consiste nos seguintes tipos de nó:

- Computação
- Disco de Armazenamento de Objeto - Computação (OSD - Compute)
- Controlador
- Plataforma OpenStack - Diretor (OSPD)

A arquitetura de alto nível da Ultra-M e os componentes envolvidos são mostrados nesta imagem:



Este documento destina-se aos funcionários da Cisco que estão familiarizados com a plataforma Cisco Ultra-M e detalha as etapas necessárias para serem executadas no OpenStack e no sistema operacional Redhat.

Note: A versão Ultra M 5.1.x é considerada para definir os procedimentos neste documento.

Impacto na rede

Não há interrupção ou interferência com serviços de rede ou CPAR.

Alarmes

Esse procedimento não dispara alarmes.

Verificação de integridade

Conecte-se ao servidor por meio do Secure Shell (SSH).

Execute todas essas etapas antes e depois da atividade.

Etapa 1. Execute o comando **/opt/CSCOar/bin/arstatus** no nível do SO.

```
[root@aaa04 ~]# /opt/CSCOar/bin/arstatus
Cisco Prime AR RADIUS server running       (pid: 24834)
Cisco Prime AR Server Agent running        (pid: 24821)
Cisco Prime AR MCD lock manager running    (pid: 24824)
Cisco Prime AR MCD server running          (pid: 24833)
Cisco Prime AR GUI running                 (pid: 24836)
SNMP Master Agent running                (pid: 24835)
[root@wscaaa04 ~]#
```

Etapa 2. Execute o comando **/opt/CSCOar/bin/aregcmd** no nível do SO e insira as credenciais de administrador. Verifique se CPAr Health é 10 em 10 e se a CLI CPAR de saída é CLI.

```
[root@aaa02 logs]# /opt/CSCOar/bin/aregcmd
Cisco Prime Access Registrar 7.3.0.1 Configuration Utility
Copyright (C) 1995-2017 by Cisco Systems, Inc.  All rights reserved.
Cluster:
User: admin
Passphrase:
Logging in to localhost

[ //localhost ]
    LicenseInfo = PAR-NG-TPS 7.2(100TPS:)
                  PAR-ADD-TPS 7.2(2000TPS:)
                  PAR-RDDR-TRX 7.2()
                  PAR-HSS 7.2()
    Radius/
    Administrators/

Server 'Radius' is Running, its health is 10 out of 10

--> exit
```

Etapa 3. Execute o comando **netstat | diâmetro de grep** e verifique se todas as conexões DRA estão estabelecidas.

A saída mencionada abaixo destina-se a um ambiente em que são esperados links de diâmetro. Se menos links forem exibidos, isso representa uma desconexão do DRA que precisa ser analisada.

```
[root@aa02 logs]# netstat | grep diameter
tcp        0            0 aaa02.aaa.epc.:77 mp1.dra01.d:diameter ESTABLISHED
tcp        0            0 aaa02.aaa.epc.:36 tsa6.dra01:diameter ESTABLISHED
tcp        0            0 aaa02.aaa.epc.:47 mp2.dra01.d:diameter ESTABLISHED
tcp        0            0 aaa02.aaa.epc.:07 tsa5.dra01:diameter ESTABLISHED
tcp        0            0 aaa02.aaa.epc.:08 np2.dra01.d:diameter ESTABLISHED
```

Etapa 4. Verifique se o registro TPS mostra solicitações sendo processadas pelo CPAR. Os valores destacados em negrito representam o TPS, e esses são os que precisamos prestar atenção.

O valor do TPS não deve exceder 1500.

```
[root@aaa04 ~]# tail -f /opt/CSCOar/logs/tps-11-21-2017.csv
11-21-2017,23:57:35,263,0
11-21-2017,23:57:50,237,0
11-21-2017,23:58:05,237,0
```

```
11-21-2017,23:58:20,257,0
11-21-2017,23:58:35,254,0
11-21-2017,23:58:50,248,0
11-21-2017,23:59:05,272,0
11-21-2017,23:59:20,243,0
11-21-2017,23:59:35,244,0
11-21-2017,23:59:50,233,0
```

Etapa 5. Procure mensagens de erro ou alarme em **name_radius_1_log**.

```
[root@aaa02 logs]# grep -E "error|alarm" name_radius_1_log
```

Etapa 6. Este é o comando para verificar a quantidade de memória que o processo CPAR usa.

```
top | grep radius
```

```
[root@aaa02 ~]# top | grep radius
27008 root      20   0 20.228g 2.413g  11408 S 128.3  7.7   1165:41 radius
```

Este valor destacado deve ser inferior a: 7 Gb, que é o máximo permitido no nível do aplicativo.

Passo 7. Este é o comando para verificar a utilização do disco:

```
df -h
```

```
[root@aaa02 ~]# df -h
Filesystem                                      Size  Used Avail Use% Mounted on
/dev/mapper/vg_arucsvm51-lv_root    26G   21G  4.1G  84% /
tmpfs                                             1.9G  268K  1.9G   1% /dev/shm
/dev/sda1                                        485M   37M  424M   8% /boot
/dev/mapper/vg_arucsvm51-lv_home 23G  4.3G   17G  21% /home
```

Esse valor total deve ser inferior a: 80%, se for mais de 80%, identifique os arquivos desnecessários e limpe-os.

Etapa 8. Verifique se não há nenhum arquivo **principal** gerado.

O arquivo principal é gerado em caso de falha do aplicativo quando o CPAR não consegue lidar com uma exceção e sua geração nesses dois locais.

```
[root@aaa02 ~]# cd /cisco-ar/
[root@aaa02 ~]# cd /cisco-ar/bin
```

Não deve haver nenhum arquivo central localizado nos dois locais acima, se encontrado, crie um caso do Cisco TAC para identificar a causa raiz de tal exceção e anexe os arquivos principais para depuração.