Manuale di verifica dello stato di CPAR

Sommario

Introduzione

Questo documento descrive come controllare lo stato di Cisco Prime Access Registrar (CPAR) prima e dopo l'esecuzione di una finestra di manutenzione.

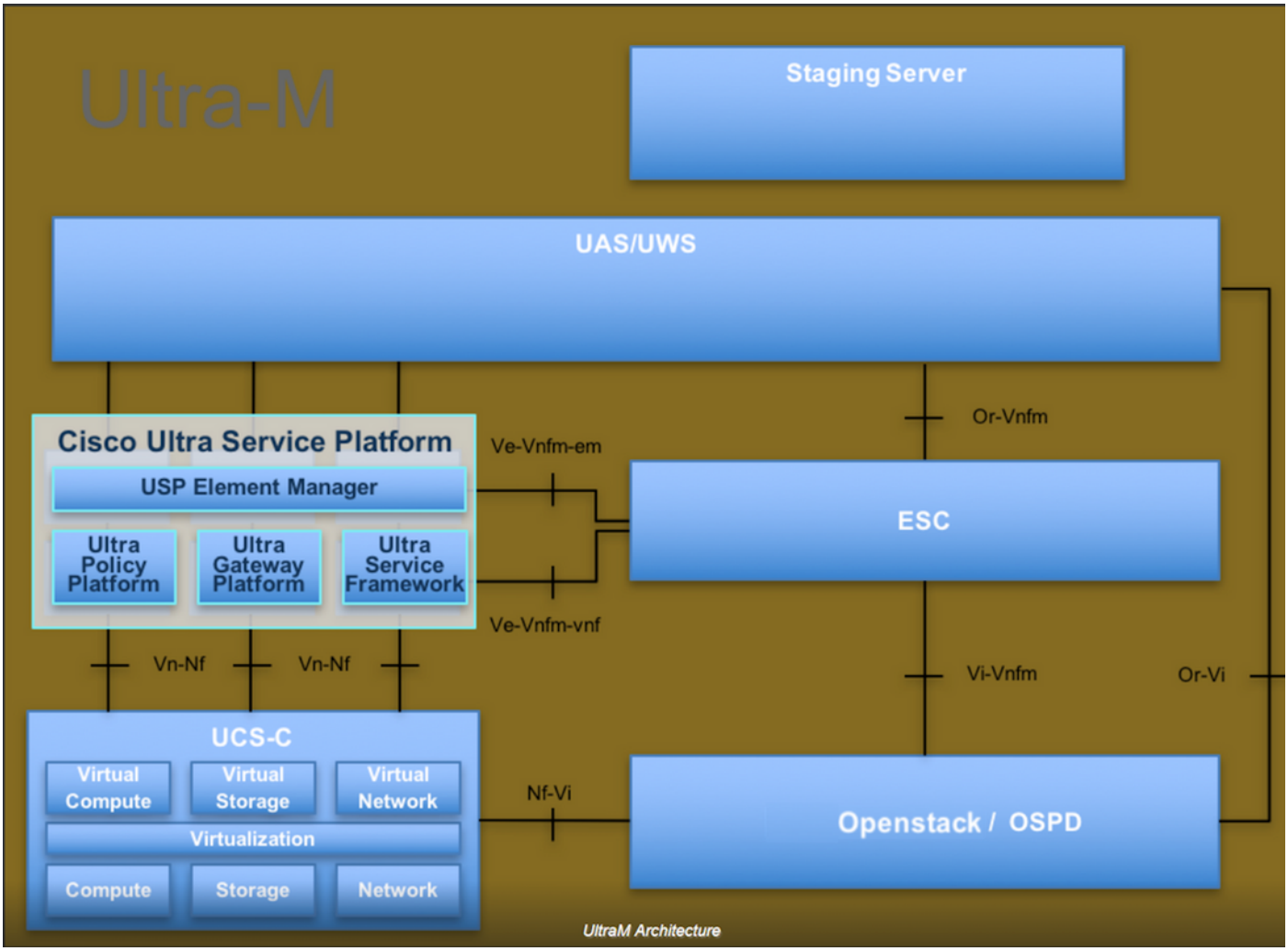
Questa procedura è valida per un ambiente Openstack che utilizza la versione NEWTON in cui ESC non gestisce CPAR e viene installato direttamente sulla VM distribuita in Openstack.

Premesse

Ultra-M è una soluzione di base di pacchetti mobili preconfezionata e convalidata, progettata per semplificare l'installazione di VNF. OpenStack è Virtualized Infrastructure Manager (VIM) per Ultra-M ed è costituito dai seguenti tipi di nodi:

- Calcola
- Disco Object Storage - Compute (OSD - Compute)
- Controller
- Piattaforma OpenStack - Director (OSPD)

L'architettura di alto livello di Ultra-M e i componenti coinvolti sono mostrati in questa immagine:



Questo documento è destinato al personale Cisco che ha familiarità con la piattaforma Cisco Ultra-M e descrive in dettaglio i passaggi richiesti da eseguire in OpenStack e Redhat OS.

> **Nota:** Per definire le procedure descritte in questo documento, viene presa in considerazione la release di Ultra M 5.1.x.

Impatto sulla rete

Non vi sono interruzioni o interferenze con la rete o i servizi CPAR.

Allarmi

Questa procedura non attiva alcun allarme.

Controllo dello stato

Connettersi al server tramite Secure Shell (SSH).

Eseguire tutti questi passaggi prima e dopo l'attività.

Passaggio 1. Eseguire il comando **/opt/CSCOar/bin/arstatus** a livello di sistema operativo.

```
[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 ~]#
```

Passaggio 2. Eseguire il comando **/opt/CSCOar/bin/aregcmd** a livello di sistema operativo e immettere le credenziali dell'amministratore. Verificare che CPAr Health sia 10 su 10 e che esista dalla CLI di CPAR.

```
[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
```

Passaggio 3. Eseguire il comando **netstat | diametro grep** e verificare che tutte le connessioni DRA siano stabilite.

L'output riportato di seguito è relativo a un ambiente in cui sono previsti collegamenti con diametro. Se vengono visualizzati meno collegamenti, si tratta di una disconnessione da DRA che deve essere analizzata.

```
[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
```

Passaggio 4. Verificare che nel registro TPS siano visualizzate le richieste elaborate da CPAR. I valori evidenziati in grassetto rappresentano i TPS e quelli a cui dobbiamo prestare attenzione.

Il valore di TPS non deve superare 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
```

Passaggio 5. Cercare eventuali messaggi di errore o di allarme in **name_radius_1_log**.

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

Passaggio 6. Questo comando consente di verificare la quantità di memoria utilizzata dal processo CPAR.

```
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
```

Il valore evidenziato deve essere inferiore a: 7 Gb, il massimo consentito a livello di applicazione.

Passaggio 7. Questo è il comando per verificare l'utilizzo del 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
```

Questo valore complessivo deve essere inferiore a: L'80%, se supera l'80%, identifica i file non necessari e li pulisce.

Passaggio 8. Verificare che non sia stato generato alcun file di **base**.

Il file di base viene generato in caso di arresto anomalo dell'applicazione quando CPAR non è in grado di gestire un'eccezione e viene generato in queste due posizioni.

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

Non dovrebbero esserci file di base nel percorso sopra indicato, se trovati, per individuare la causa principale di tale eccezione e allegare i file di base per il debug, sollevare una richiesta TAC di Cisco.