CPAR Health Check-Handbuch

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie den Status von Cisco Prime Access Registrar (CPAR) vor und nach der Ausführung eines Wartungsfensters überprüfen.

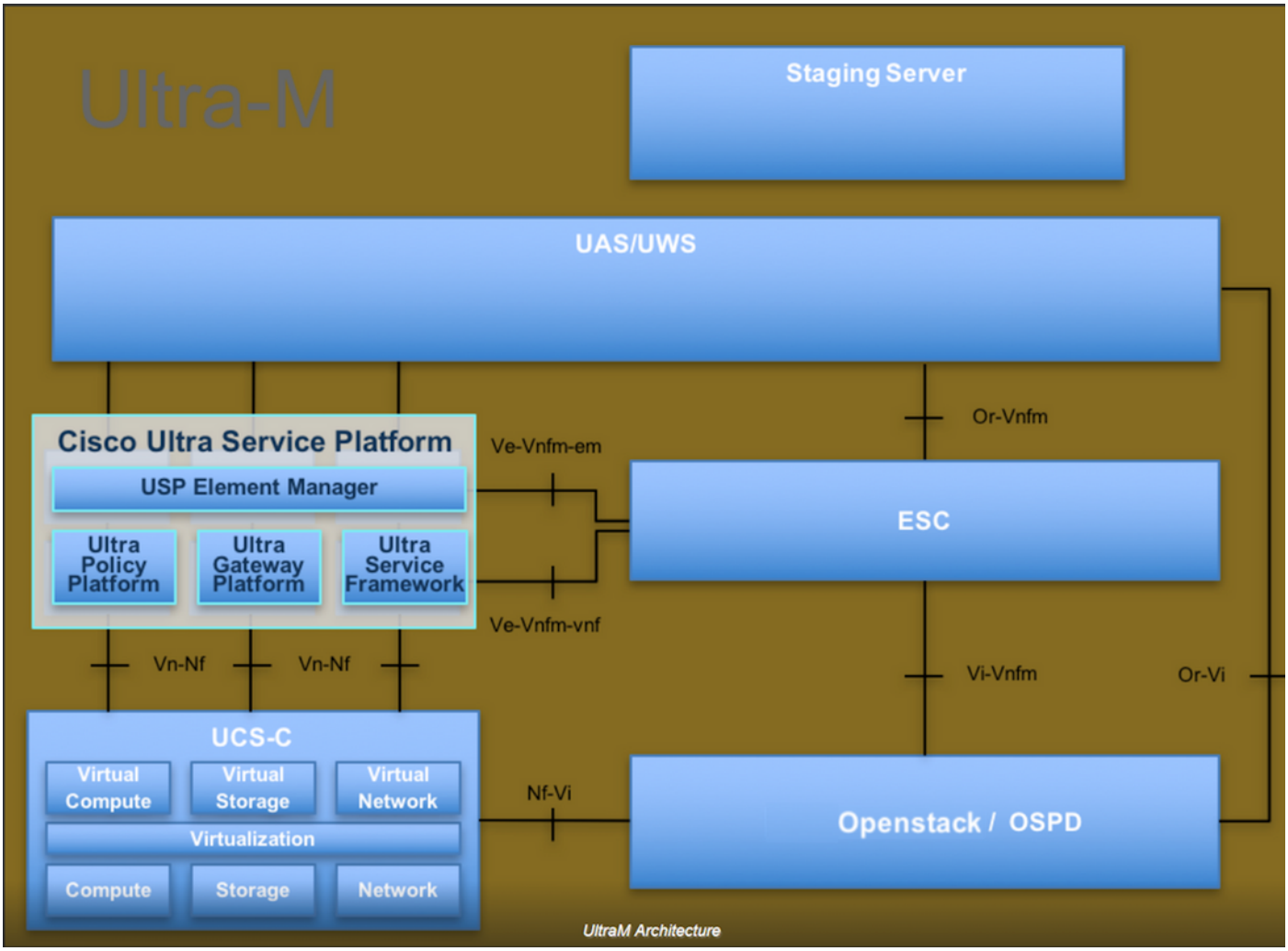
Dieses Verfahren gilt für eine OpenStack-Umgebung, in der die NEWTON-Version verwendet wird, in der der ESC CPAR nicht verwaltet und direkt auf dem auf OpenStack bereitgestellten virtuellen System installiert wird.

Hintergrundinformationen

Ultra-M ist eine vorkonfigurierte und validierte Kernlösung für virtualisierte mobile Pakete, die die Bereitstellung von VNFs vereinfacht. OpenStack ist der Virtualized Infrastructure Manager (VIM) für Ultra-M und besteht aus den folgenden Knotentypen:

- Computing
- Object Storage Disk - Computing (OSD - Computing)
- Controller
- OpenStack-Plattform - Director (OSPD)

Die High-Level-Architektur von Ultra-M und die beteiligten Komponenten sind in diesem Bild dargestellt:



Dieses Dokument richtet sich an Mitarbeiter von Cisco, die mit der Cisco Ultra-M-Plattform vertraut sind. Es beschreibt die Schritte, die für OpenStack und Redhat OS erforderlich sind.

Hinweis: Ultra M 5.1.x wird zur Definition der Verfahren in diesem Dokument berücksichtigt.

Auswirkungen auf das Netzwerk

Es bestehen keine Unterbrechungen oder Interferenzen mit Netzwerk- oder CPAR-Services.

Alarme

Dieses Verfahren löst keine Alarme aus.

Integritätsüberprüfung

Stellen Sie über Secure Shell (SSH) eine Verbindung zum Server her.

Führen Sie alle diese Schritte vor und nach der Aktivität aus.

Schritt 1: Führen Sie den Befehl **/opt/CSCOar/bin/arstatus** auf Betriebssystemebene aus.

```
[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 ~]#
```

Schritt 2: Führen Sie den Befehl **/opt/CSCOar/bin/aregcmd** auf Betriebssystemebene aus, und geben Sie die Administratorberechtigungen ein. Stellen Sie sicher, dass CPAr Health 10 von 10 und die CPAR-CLI-Option für das Beenden ist.

```
[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
```

Schritt 3: Führen Sie den Befehl **netstat** aus. **| grep-Durchmesser** und überprüfen, ob alle DRA-Verbindungen hergestellt sind.

Die unten erwähnte Ausgabe ist für eine Umgebung vorgesehen, in der Durchmesser-Verbindungen erwartet werden. Wenn weniger Links angezeigt werden, stellt dies eine Trennung von DRA dar, die analysiert werden muss.

```
[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
```

Schritt 4: Überprüfen Sie, ob das TPS-Protokoll Anforderungen anzeigt, die von CPAR verarbeitet werden. Die fett hervorgehobenen Werte repräsentieren den TPS, und genau diese Werte müssen wir beachten.

Der TPS-Wert darf 1500 nicht überschreiten.

```
[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
```

Schritt 5: Suchen Sie in **name_radius_1_log nach** Fehler- oder Warnmeldungen.

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

Schritt 6: Mit diesem Befehl wird die Speichergröße überprüft, die vom CPAR-Prozess verwendet wird.

```
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
```

Der hervorgehobene Wert sollte kleiner sein als: 7 Gb, das ist der maximal zulässige Wert auf Anwendungsebene.

Schritt 7: Mit diesem Befehl wird die Festplattenauslastung überprüft:

```
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
```

Dieser Gesamtwert sollte kleiner sein als: 80 % der Befragten identifizieren bei mehr als 80 % die unnötigen Dateien und säubern sie.

Schritt 8: Stellen Sie sicher, dass keine **Core-**Datei generiert wurde.

Die Core-Datei wird im Fall eines Anwendungsabsturzes generiert, wenn CPAR eine Ausnahme nicht behandeln kann und diese an diesen beiden Standorten generiert wird.

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

In den beiden oben genannten Speicherorten sollten keine Core-Dateien vorhanden sein. Wenn diese gefunden werden, wird ein Cisco TAC-Vorgang ausgelöst, um die Ursache für diese Ausnahme zu ermitteln und die Core-Dateien zum Debuggen anzufügen.