

# CPAR AAA 컨피그레이션

## 목차

---

[소개](#)

[배경 정보](#)

[CPAR 컨피그레이션](#)

[전역 컨피그레이션](#)

[클라이언트 컨피그레이션](#)

[빠른 규칙 컨피그레이션](#)

[서비스 컨피그레이션](#)

[원격 서버 컨피그레이션](#)

[세션 관리자](#)

[리소스 관리자](#)

[스크립트](#)

[CPAR 로깅 컨피그레이션](#)

[시간 초과 값](#)

[지름 패킷 크기](#)

[CPAR에서 세션 관리](#)

[가입자 세션에 대해 CPAR AAA에 캐시된 특성\(AVP\)](#)

[다음을 확인합니다.](#)

[문제 해결](#)

---

## 소개

이 문서에서는 CPAR(Cisco Prime Access Registrar) AAA(Authentication, Authorization, Accounting) 컨피그레이션의 절차에 대해 설명합니다.

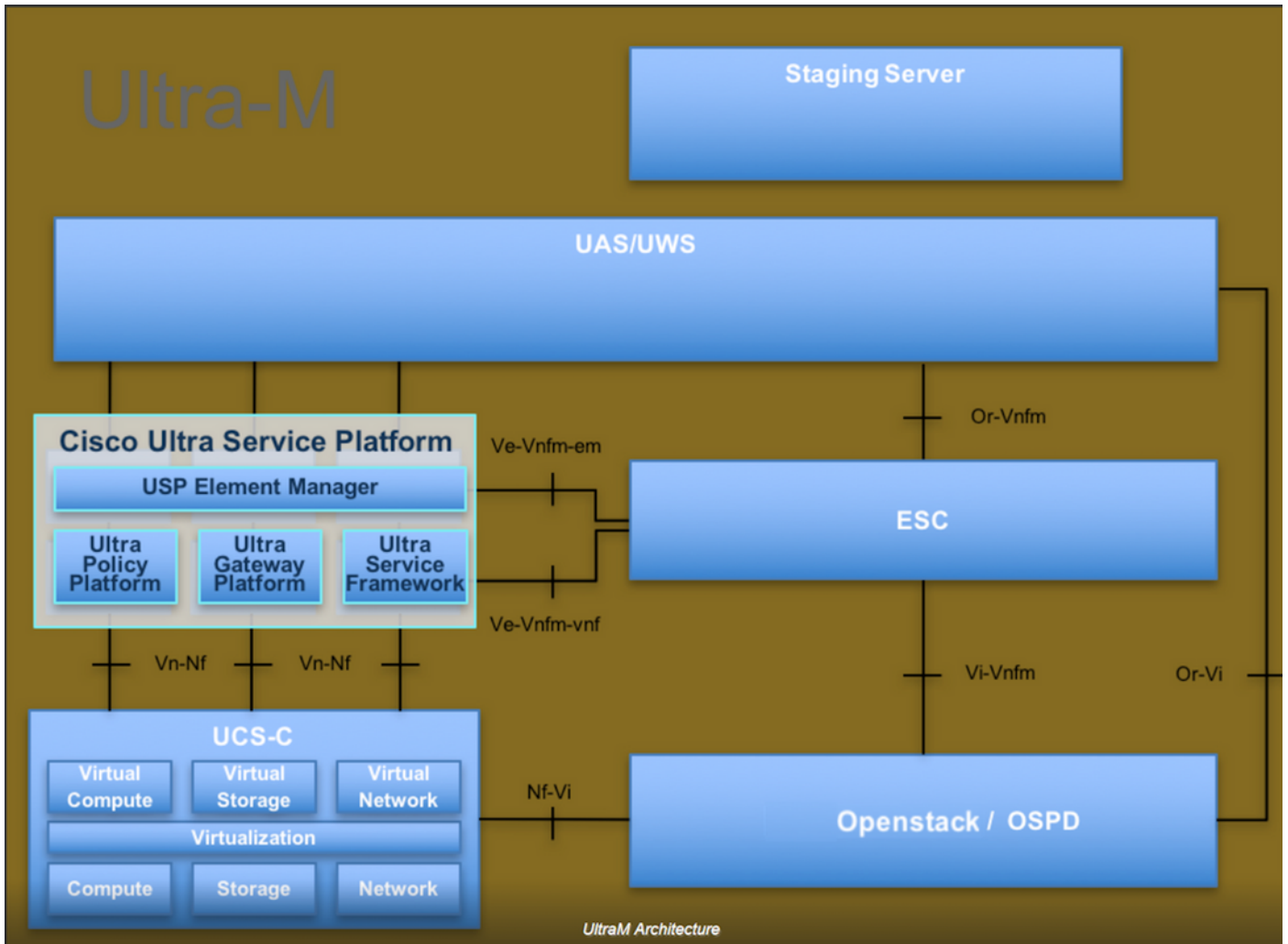
이 절차는 ESC가 CPAR을 관리하지 않고 CPAR이 Openstack에 구축된 VM에 직접 설치되는 NEWTON 버전을 사용하는 Openstack 환경에 적용됩니다.

## 배경 정보

Ultra-M은 VNF의 구축을 간소화하기 위해 설계된, 사전 패키징되고 검증된 가상화된 모바일 패킷 코어 솔루션입니다. OpenStack은 Ultra-M용 VIM(Virtualized Infrastructure Manager)이며 다음 노드 유형으로 구성됩니다.

- 컴퓨팅
- 개체 스토리지 디스크 - 컴퓨팅(OSD - 컴퓨팅)
- 컨트롤러
- OpenStack 플랫폼 - 디렉터(OSPD)

이 그림에는 Ultra-M의 고급 아키텍처와 관련 구성 요소가 나와 있습니다.



이 문서는 Cisco Ultra-M 플랫폼에 대해 잘 알고 있는 Cisco 직원을 대상으로 하며 OpenStack 및 Redhat OS에서 수행해야 하는 단계에 대해 자세히 설명합니다.

 참고: 이 문서의 절차를 정의하기 위해 Ultra M 5.1.x 릴리스가 고려됩니다.

## CPAR 컨피그레이션

### 전역 컨피그레이션

Diameter Global 컨피그레이션은 Application-ID, Origin Host IP-Address, Realm 등과 같은 적절한 값으로 구성됩니다.

```
Cd /Radius/Advanced/Diameter/
Diameter/
```

```
IsDiameterEnabled = TRUE
General/
  Product = CPAR
  Version = 7.3.0.3
  AuthApplicationIdList = 1:5:16777264:16777265:16777272:16777250
```

```
AcctApplicationIdList = 3
TransportManagement/
  Identity = aaa01.aaa.epc.mncxx.mccxx.3gppnetwork.org
  Realm = epc.mncxx.mccxx.3gppnetwork.org
  WatchdogTimeout = 500
  ValidateIncomingMessages = FALSE
  ValidateOutgoingMessages = TRUE
  MaximumNumberOfDiameterPackets = 8192
  ReserveDiameterPacketPool = 0
  DiameterPacketSize = 4096
  AdvertisedHostName/
    1. aaa01.aaa.epc.mncxx.mccxx.3gppnetwork.org
```

/etc/hosts는 전송 관리에 사용되는 AAA FQDN(정규화된 도메인 이름) 및 확인할 호스트 이름에 대해 확인할 해당 IP 주소로 업데이트해야 합니다.

## 클라이언트 컨피그레이션

클라이언트 컨피그레이션은 트래픽이 수신된 Diameter 피어(이 경우 DRA)로 구성됩니다.

```
Cd /Radius/Clients/
DRA01/
```

```
Name = DRA01
Description =
Protocol = diameter
HostName = x.x.x.x
PeerPort = 3868
Vendor =
IncomingScript~ =
OutgoingScript~ =
AdvertisedHostName =
UserLogEnabled = FALSE
AdvertisedRealm =
InitialTimeout = 3000
MaxIncomingRequestRate = 0
KeepAliveTime = 0
AuthSessionStateInASR = No-State-Maintained
SCTP-Enabled = FALSE
TLS-Enabled = FALSE
```

## 빠른 규칙 컨피그레이션

FastRules는 특정 조건에 따라 런타임에 해당 서비스를 매핑하는 데 사용되며, 조건은 AVP(특성 값 쌍) 및 지름 메시지에 있는 해당 값을 기반으로 합니다. 일치하는 빠른 규칙이 없으면 기본 서비스를 선택합니다.

Cd /Radius/FastRules/

FastRules/

RuleDefinitions/

Entries 1 to 5 from 5 total entries

Current filter: <all>

r1/

Name = r1

Description = Used for HSS initiated Flows

Protocol = diameter

Condition = "1 OR 2"

Success = author(3gpp-reverse)

Failure = Rule(r2)

Attributes/

Entries 1 to 2 from 2 total entries

Current filter: <all>

1/

Name = 1

Description =

Dictionary = environment

Attribute = Diameter-Command-Code

Value = 304

2/

Name = 2

Description =

Dictionary = environment

Attribute = Diameter-Command-Code

Value = 305

r2/

Name = r2

Description = Used for PGW Update procedure over S6b

Protocol = diameter

Condition = "1 AND 2"

Success = author(s6b)

Failure = Rule(r3)

Attributes/

Entries 1 to 2 from 2 total entries

Current filter: <all>

1/

Name = 1

Description =

Dictionary = Request

Attribute = Auth-Application-Id

Value = 16777272

2/

Name = 2

Description =

Dictionary = request

Attribute = Diameter-Command-Code

Value = 265

r3/

Name = r3

Description = OPTIONAL used for PGW Termination procedure

Protocol = diameter

Condition = "1 and 2"

Success = author(null)

Failure = Rule(r4)

Attributes/

Entries 1 to 2 from 2 total entries

Current filter: <all>

1/

Name = 1  
Description =  
Dictionary = Request  
Attribute = Auth-Application-Id  
Value = 16777272

2/

Name = 2  
Description =  
Dictionary = environment  
Attribute = Diameter-Command-Code  
Value = 275

r4/

Name = r4  
Description = Used for SWm Termination procedure  
Protocol = diameter  
Condition = "1 and 2"  
Success = author(3gpp-auth)  
Failure = Rule(r5)  
Attributes/

Entries 1 to 2 from 2 total entries  
Current filter: <all>

1/

Name = 1  
Description =  
Dictionary = request  
Attribute = Auth-Application-Id  
Value = 16777264

2/

Name = 2  
Description =  
Dictionary = environment  
Attribute = Diameter-Command-Code  
Value = 275

r5/

Name = r5  
Description = Used for SWm ReAuthorization  
Protocol = diameter  
Condition = "1 and 2"  
Success = Query(query)  
Failure =  
Attributes/

Entries 1 to 2 from 2 total entries  
Current filter: <all>

1/

Name = 1  
Description =  
Dictionary = environment  
Attribute = Diameter-Command-Code  
Value = 265

2/

Name = 2  
Description =  
Dictionary = request  
Attribute = Auth-Application-Id  
Value = 16777264

Order/

Radius/

```
Diameter/  
  1. r1  
Tacacs/
```

위의 FastRules 중 일치하는 것이 없는 경우 패킷은 기본 서비스에 따라 처리됩니다.

```
Cd /Radius/  
DefaultAuthenticationService~ = encrypted-imsi-service  
DefaultAuthorizationService~ = 3gpp-auth
```

## 서비스 컨피그레이션

Service Configuration(서비스 컨피그레이션)에서 서비스는 인증, 권한 부여 요구 사항에 따라 정의됩니다.

```
Cd /Radius/Services/
```

Encrypted-IMSI-Service는 EAP-AKA 인증에 사용되며 Apple 디바이스에 대해 IMSI가 암호화됩니다. 필요하지 않은 경우 EncryptedIMSI 매개변수를 False로 설정합니다

```
encrypted-imsi-service/  
  Name = encrypted-imsi-service  
  Description =  
  Type = eap-aka  
  NumberOfQuintets = 1  
  AlwaysRequestIdentity = True  
  EnableIdentityPrivacy = False  
  EnableRollingPseudonymSecret = False  
  PseudonymSecret = <encrypted>  
  PseudonymRenewtime = "24 Hours"  
  PseudonymLifetime = Forever  
  NotificationService =  
  Generate3GPPCompliantPseudonym = False  
  EnableReauthentication = False  
  UseOutagePolicyForReauth = False  
  MaximumReauthentications = 16  
  ReauthenticationTimeout = 3600  
  ReauthenticationRealm =  
  EnableEncryptedIMSI = True  
  EncryptedIMSIDelimiter = NULL  
  EncryptedIMSIKeyIdDelimiter = ,  
  DefaultPrivateKey = xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx  
  QuintetCacheTimeout = 0  
  AuthenticationTimeout = 120  
  QuintetGenerationScript~ =  
  UseProtectedResults = False  
  SendReAuthIDInAccept = False  
  Subscriber_DBLookup = DiameterDB  
  DiameterInterface = SWx
```

```
ProxyService = dia-proxy
```

The 3GPP service is used for Registration/Profiledownload from HSS over SWx;  
3gpp-auth/

```
Name = 3gpp-auth
Description =
Type = 3gpp-authorization
Protocol = diameter
IncomingScript~ =
OutgoingScript~ = removeuserdata
SessionManager = sm1
DiameterProxyService = dia-proxy
FetchLocationInformation = False
```

dia-proxy 서비스는 원격 서버를 선택하는 데 사용되며 피어 정책을 정의할 수 있습니다. 여러 원격 피어가 있고 동일한 피어를 그룹화하려는 경우 GroupFailover 옵션은 MultiplePeerPolicy로 사용됩니다. 또한 여러 그룹에 대한 장애 조치를 수행할 GroupTimeOutPolicy를 정의합니다

```
dia-proxy/
```

```
Name = dia-proxy
Description =
Type = diameter
IncomingScript~ = rmserver
OutgoingScript~ =
MultiplePeersPolicy = GroupFailover
GroupTimeOutPolicy = FailOver
ServerGroups/
  Entries 1 to 2 from 2 total entries
  Current filter: <all>

  Group_Primary_DRA/
    Name = Group_Primary_DRA
    Metric = 0
    IsActive = TRUE
  Group_Secondary_DRA/
    Name = Group_Secondary_DRA
    Metric = 1
    IsActive = TRUE
```

위에서 언급 한 서버 그룹은 /Radius/GroupServers/

```
GroupServers/
```

```
Entries 1 to 2 from 2 total entries
Current filter: <all>

Group_Primary_DRA/
  Name = Group_Primary_DRA
```

```
Description =
MultiplePeersPolicy = RoundRobin
PeerTimeOutPolicy = FailOver
DiaRemoteServers/
  Entries 1 to 2 from 2 total entries
  Current filter: <all>
```

DRA01/

```
Name = DRA01
Metric = 0
Weight = 0
IsActive = TRUE
```

DRA02/

```
Name = DRA02
Metric = 1
Weight = 0
IsActive = TRUE
```

Group\_Secondary\_DRA/

```
Name = Group_Secondary_DRA
Description =
MultiplePeersPolicy = RoundRobin
PeerTimeOutPolicy = FailOver
DiaRemoteServers/
  Entries 1 to 4 from 4 total entries
  Current filter: <all>
```

DRA03/

```
Name = DRA03
Metric = 0
Weight = 0
IsActive = TRUE
```

DRA04/

```
Name = DRA04
Metric = 2
Weight = 0
IsActive = TRUE
```

DRA05/

```
Name = DRA05
Metric = 1
Weight = 0
IsActive = TRUE
```

S6b 서비스는 S6b를 통해 PGW 업데이트 절차를 처리하는 데 사용됩니다.

s6b/

```
Name = s6b
Description =
Type = 3gpp-authorization
Protocol = diameter
IncomingScript~ =
OutgoingScript~ =
SessionManager =
DiameterProxyService = dia-proxy
FetchLocationInformation = False
```



3gpp-reverse는 HSS가 개시한 메시지가 처리되도록 사용된다.

3gpp-reverse/

```
Name = 3gpp-reverse
Description =
Type = 3gpp-reverse-authorization
IncomingScript~ = AAARTRCheck
OutgoingScript~ =
SessionManager = sm1
TranslationService =
```

쿼리 서비스는 HSS에서 수신한 PPR을 기반으로 캐시에서 업데이트된 프로파일을 직접 가져오는 Re-Authorization 절차 중에 사용됩니다.

query/

```
Name = query
Description =
Type = diameter-query
IncomingScript~ =
OutgoingScript~ = removeuserdataquery
UpdateSessionLastAccessTime = False
SessionManagersToBeQueried/
  1. sm1
AttributesToBeReturned/
  1. Non-3GPP-User-Data
  2. Service-Selection
```

Null 서비스는 S6b에 캐시된 세션이 없으므로 S6b 종료 프로세스에 대한 성공으로 회신하는 것입니다.

null/

```
Name = null
Description =
Type = null
IncomingScript~ =
OutgoingScript~ =
```

## 원격 서버 컨피그레이션

원격 서버는 HSS와 같이 AAA에서 패킷이 전송되는 원격 피어로 정의됩니다. DRA를 사용하는 경우 클라이언트와 원격 서버 모두에서 동일한 DRA 정보를 정의합니다.

RemoteServers/

DRA01/

```
Name = DRA01
Description =
Protocol = diameter
HostName = 10.169.48.235
DestinationPort = 3868
DestinationRealm = epc.mnc300.mcc310.3gppnetwork.org
ReactivateTimerInterval = 300000
Vendor =
IncomingScript~ = AAAReplaceResultCode
OutgoingScript~ = rmdh
MaxTries = 3
MaxTPSLimit = 0
MaxSessionLimit = 0
InitialTimeout = 3000
LimitOutstandingRequests = FALSE
MaxPendingPackets = 0
MaxOutstandingRequests = 0
DWatchDogTimeout = 2500
SCTP-Enabled = FALSE
TLS-Enabled = FALSE
AdvertiseHostName =
AdvertiseRealm =
```

## 세션 관리자

세션 관리자는 세션 캐싱에 대해 정의할 수 있으며 리소스 관리자와 함께 작동합니다. 세션 관리자는 3gpp-auth, 3gpp-reverse 및 query services에서 언급된다.

Cd /Radius/SessionManagers/

sm1/

```
Name = sm1
Description =
Type = local
EnableDiameter = True
IncomingScript =
OutgoingScript =
AllowAccountingStartToCreateSession = FALSE
SessionTimeout =
PhantomSessionTimeout =
SessionKey = User-Name:Session-Id
SessionCreationCmdList = 268||305
SessionDeletionCmdList = 275
SessionRestorationTimeout = 24h
ResourceManagers/
  1. 3gpp
  2. swmcache
  3. per-user
```

## 리소스 관리자

리소스 관리자는 리소스를 할당하도록 정의되며 세션 관리자에 매핑됩니다.

이 세 가지 리소스 관리자가 사용됩니다.

```

Cd /Radius/ResourceManagers/
ResourceManagers/
    3gpp/
        Name = 3gpp
        Description =
        Type = 3gpp
        EnableRegistrationFlow = TRUE
        EnableSessionTermination = false
        ReuseExistingSession = True
        HSSProxyService = dia-proxy

Per-User/
        Name = Per-User
        Description =
        Type = user-session-limit
        UserSessionLimit = 0

swmcache/
        Name = swmcache
        Description =
        Type = session-cache
        OverwriteAttributes = FALSE
        QueryKey = Session-Id
        PendingRemovalDelay = 10
        AttributesToBeCached/
            1. Non-3GPP-User-Data
            2. Service-Selection
        QueryMappings/
    
```

## 스크립트

이 표에는 패킷 처리 중에 사용되는 모든 스크립트가 표시됩니다.

| 이름  | 스크립트 파일  | 진입점 | 설명   |
|-----|----------|-----|--|
| 클리드 | test.tcl | 클리드 | <p>Application-Id 16777264 및 Diameter-Command Code 268을 찾고, 사용자 ID를 가져온 다음 수신 요청에서 calling-ID 특성으로 복사합니다.</p> <p>이 스크립트는 Radius 수신 스크립팅 포에서 참조됩니다.</p> |

|                     |                           |           |   |
|---------------------|---------------------------|-----------|---|
| rmserver            | test.tcl                  | rm_server | <p>Server-Assignment-Type 특성이 있는 이 특성이 있으면 수신 요청에서 Remove Server 필드를 제거합니다.</p> <p>이 스크립트는 dia-proxy service Incoming scriptinpoint에서 참조됩니다.</p>  |
| removeuserdata      | libremoveuserdata.so      | 사용자데이터 제거 | <p>Rex 스크립트는 먼저 HSS로부터 받은 정보를 확인하는 데 사용됩니다. 특히 'Non-3GPP-IP-Access' 및 'Non-3GPP-IP-Access-APN' 모두 'NON_3GPP_SUBSCRIPTION_ALLOW(0)' 및 'Non_3GPP_APNS_ENABLE(0)' 가져야 합니다. 그렇지 않으면 권한 부여가 실패합니다. SWm DER 메시지(service-selection AVP)에서 수신한 APN 이름을 HSS에서 다운로드한 APN 구성과 간단히 비교한 다음, 일치하는 항목이 있을 경우 APN 세부 정보만 복사하고 원치 않는 APN 제거하고 ePDG를 향한 최종 DEA를 준비합니다. 일치 권한 부여가 실패하고 서비스 AVP가 DER에 없는 경우 모든 APN 정보가 외부 AVP로 전송됩니다.</p> <p>이 스크립트는 3gpp-auth Outgoing scriptinpoint에서 참조됩니다</p> |
| removeuserdataquery | libremoveuserdataquery.so | 사용자데이터 제거 | <p>Rex 스크립트는 먼저 HSS에서 받은 정보를 확인하는 데 사용됩니다. 특히 Non-3GPP-IP-Access 및 Non-3GPP-IP-Access-APN NON_3GPP_SUBSCRIPTION_ALLOW 및 Non_3GPP_APNS_ENABLE(0)의 값 가져야 합니다. 그렇지 않으면 권한 부여가 실패합니다. SWm DER 메시지(서비스 선택 AVP)에서 수신된 이름(서비스 선택 AVP)과 HSS에서 다운로드한 APN 컨피그레이션을 간단히 비교한 다음, 일치하는 항목이 있을 경우 특정 APN 세부 정보만 복사하고 원치 않는 AVP를 제거하고 ePDG를 향한 최종 DEA를 준비합니다. 권한 부여가 실패하고 서비스 선택 AVP가 DER에 없는 경우 모든 APN 정보가 외부 AVP로 전송됩니다.</p> <p>이 스크립트는 query serviceOutgoing scriptinpoint에서 참조됩니다.</p>    |

|                      |                   |              |  |
|----------------------|-------------------|--------------|--|
| 발신                   | test.tcl          | 새 세션 상태      | Dia 프록시 서비스 수신 스크립트 - 이미 수신된 메시지에 대한 스티커 설정을 해제하여 사용됩니다. 예를 들어, MAR/MAA가 DRA1에서 수신된 경우 후속 사용자 SA와 동일한 DRA1을 사용하며, DRA1을 사용할 수 없고 고착성이 유지되는 경우 장애 조치하지 않습니다. 대체 DRA로 장애 조치하려면 이 스티커를 제거해야 합니다. 이 스크립트는 S6b SAR(PGW_update) HSS로 향하는 Visited-Network-Identifier를 제거하는 데 사용됩니다. |
| RMDH                 | test.tcl          | RMDH         | DiameterCode 301 및 303의 패킷에서 DestinationHost AVP를 제거합니다.   |
| rmvnid               | test.tcl          | rmvnid       | DiameterCode 256 및 Server-Assignment-Type이 13인 패킷에서 Visited-Network-Identifier AVP를 제거합니다.   |
| AAAReplaceResultCode | test.tcl          | replace결과 코드 | DiameterCode 274 및 Result-Code "Diameter-Unknown-Session-Id"로 패킷의 Result-Code AVP를 "Test"로 교체  |
| AARTRC체크             | librexblockRTR.so | AARTRC체크     | 동일한 세션에 대해 여러 RTR이 수신되면 RTR이 삭제되고 기록됩니다.   |

상위 버전에서는 일부 스크립트가 필요하지 않을 수 있습니다. 나열된 스크립트는 CPAR 버전 7.3.0.3에서 사용됩니다.

모든 스크립트는 /opt/CSCOar/scripts/radius/경로에 있습니다.

## CPAR 로깅 컨피그레이션

/opt/CSCOar/logs 폴더는 모든 애플리케이션 로그를 저장합니다. name\_radius\_1\_log 파일은 모든 삭제 및 거부된 요청을 등록하므로 문제 해결을 위해 이 파일을 저장하는 것이 중요합니다.

CPAR을 사용하면 매우 유연한 컨피그레이션을 통해 요구 사항에 따라 이 로그를 저장할 수 있습니다. 요구 사항에 따라 이 값을 정의할 수 있습니다. 최신 로그 파일 20개가 보관되며 각 파일의 크기는 5Mb입니다.

이 특정 로깅을 활성화하려면 aregcmd 모드에서 2개의 매개변수를 구성해야 합니다.

/Radius/Advanced

LogFileSize = "5메가바이트"

LogFileCount = 20

로그 명명 규칙은 이 표에 지정된 규칙을 따릅니다.

|              |                      |
|--------------|----------------------|
| 설명           | 로그 파일의 이름            |
| 최신 로그        | name_radius_1_log    |
| 두 번째에서 최신 로그 | name_radius_1_log.01 |
| 세 번째에서 최신 로그 | name_radius_1_log.02 |
| ...          | ...                  |
| 20번째에서 최신 로그 | name_radius_1_log.19 |

표 2 로그 번호 매기기

## 시간 초과 값

CPAR에는 서버 구성 가능한 시간 제한이 있습니다. 현재 설정에는 다음 컨피그레이션이 있습니다.

/Radius/Advanced에 있는 일반 시간 제한

- DiameterStaleConnectionDeletionTimeout 300000(ms) 이 타이머는 CPAR이 연결을 아래로 표시하기 전에 지름 연결이 비활성 상태일 수 있는 기간을 나타냅니다.

/Radius/Clients/<client\_name>에 있는 클라이언트 시간 초과

- InitialTimeout 3000(ms) CPAR에서 연결할 수 없다고 간주하기 전에 DRA의 응답을 대기한 시간입니다.

/Radius/RemoteServers/<remote\_server\_name>에 있는 원격 서버 시간 초과

- InitialTimeout 3000(ms) CPAR에서 연결할 수 없다고 간주하기 전에 DRA의 응답을 대기한 시간입니다.
- DWatchDogTimeout 2500(ms) CPAR에서 DiameterWatchDog 패킷에 연결할 수 없는 것으로 간주하기 전에 DRA에서 다시 시작하기를 기다린 시간입니다.

- ReactivateTimerInterval 300000(ms) CPAR이 지름 피어와의 연결을 다시 설정할 때까지 대기하는 시간입니다.

## 지름 패킷 크기

이 문서에서는 Diameter Packet size 명령의 의미와 이 매개변수를 값 4096으로 유지하게 된 이유를 설명합니다.

|                    |  |
|--------------------|--|
| DiameterPacketSize | Required; the Diameter packet size that can be processed.<br>An incoming Diameter packet with a packet size more than the value set in this field will be dropped. |
|--------------------|--|

위 그림에서 설명한 것처럼 CPAR에서 수신할 것으로 예상되는 최대 직경 패킷 크기는 4096바이트입니다. 이 값은 /Radius/Advanced/Diameter/TransportManagement 디렉토리에 있는 DiameterPacketSize 변수 아래에 구성됩니다. 이 값을 준수하지 않는 모든 패킷은 삭제됩니다. 총 패킷 크기는 세션 캐시된 특성의 크기와 수신된 지름 패킷의 크기를 더한 후에 얻습니다.

예를 들어 PPR 패킷 크기가 4000바이트이고 이 메시지 내에서 Non-3GPP-User-Data의 크기는 3800바이트입니다. 세션이 이미 일부 특성을 캐시했으며 캐시된 데이터 크기가 297바이트이면 세션 크기가 4096바이트를 초과하고 메시지가 CPAR에 의해 삭제됩니다.

프로젝트 도중 4096개보다 큰 패킷의 분석 및 분석이 수행되었습니다. 이 결과는 하루 평균 36개의 패킷(SAA)이 4096개보다 큰 경우 각 CPAR 인스턴스에 도착함을 나타냅니다. 이러한 패킷 수는 매우 작기 때문에 의미가 없습니다.

이 매개변수는 구성 가능하며 필요한 경우 늘릴 수 있습니다. 그러나 값이 4096을 초과하여 증가하면 몇 가지 단점이 있습니다.

- DiameterPacketSize가 5KB로 증가하면 CPAR는 4096바이트보다 큰 SAA 패킷을 수락합니다. 그러나 동일한 사용자 세션에 대해 PPR이 시작되면 Non-3GPP-User-Data의 크기가 4260바이트이므로 세션 업데이트가 실패하고 사용자 등록 취소가 발생합니다.
- DiameterPacketSize는 RADIUS 프로세스에 할당된 시작 메모리에 직접 영향을 줍니다. DiameterPacketSize가 클수록 CPAR 시작 시 Radius 프로세스에 할당된 RES 메모리의 양이 커집니다.

이 그림에서는 DiameterPacketSize가 4096으로 구성된 인스턴스에서 top 명령의 출력 예를 보여줍니다.

```
[root@snqaaa07 ~]# top
top - 21:29:25 up 49 days, 20:21, 1 user, load average: 0.81, 0.28, 0.14
Tasks: 348 total, 1 running, 347 sleeping, 0 stopped, 0 zombie
%cpu(s):  2.8 us,  0.0 sy,  0.0 ni, 97.2 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem: 32777520 total, 5219052 used, 27558468 free, 1328 buffers
KiB Swap: 30408700 total, 0 used, 30408700 free. 2354304 cached Mem

  PID USER      PR  NI   VIRT   RES   SHR  S  %CPU  %MEM     TIME+ COMMAND
16721 root        20   0 18.726g 174648 10608  S 100.1  0.5   1:07.34 radius
```

DiameterPackerSize 매개 변수를 6000으로 늘리면 top 명령의 출력은 다음과 같습니다.

```
top - 22:57:50 up 49 days, 21:49, 1 user, load average: 1.00, 1.01, 1.00
Tasks: 348 total, 1 running, 347 sleeping, 0 stopped, 0 zombie
%Cpu(s): 2.8 us, 0.0 sy, 0.0 ni, 97.2 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem: 32777520 total, 5383328 used, 27394192 free, 1328 buffers
KiB Swap: 30408700 total, 0 used, 30408700 free. 2355000 cached Mem

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 18455 root        20   0 18.741g 210788 10756 S 100.1  0.6   87:00.67 radius
```

- 시작 메모리 할당 외에, 시스템이 사용되면 CPAR에 도달하는 패킷 수와 관련하여 증가하는 내부 동적 메모리 버퍼가 있습니다. 예를 들어 한 지점에서 1000개의 패킷이 CPAR에 도달하면 CPAR은 개별 패킷의 크기와 상관없이 버퍼 내부에 1000 \* DiameterPacketSize의 메모리 값을 할당합니다(CPAR은 DiameterPacketSize가 최대 패킷 크기를 나타낸다는 것을 알고 있음). 이 내부 메모리 버퍼는 DiameterPacketSize가 증가하면 더 많은 메모리를 할당하고 감소하면 더 적은 메모리를 할당합니다.

4096보다 큰 패킷 수는 무시할 수 있으며 이러한 단점이 원치 않는 동작을 유발한다고 결정되었으므로 이 매개변수를 4096으로 유지하는 것이 좋습니다.

## CPAR에서 세션 관리

CPAR에서 세션 수를 모니터링하는 유일한 메커니즘은 이 문서에 설명된 방법을 사용하는 것입니다. 이 정보가 포함된 SNMP를 통해 검색할 수 있는 OID가 없습니다.

CPAR은 세션을 관리할 수 있습니다. CPAR CLI에 /opt/CSCCOar/bin/aregcmd를 입력하고 관리자 자격 증명으로 로그인합니다.

count-sessions /r 명령을 사용하면 모든 CPAR에 해당 시점에 연결된 모든 세션이 표시됩니다.

```
--> count-sessions /r all

Total 3 session(s) in /Radius/SessionManagers
```

세션에 대한 자세한 내용을 보려면 CPAR에 연결된 모든 세션에 대한 정보를 제공하는 query-sessions /r all 명령을 사용합니다.

```
--> query-sessions /r all

Sessions for /radius:
Sessions for /Radius/SessionManagers/smi:
S3 Key: 3103109900076558nai.epc.mnc310.3gppnetwork.org:epgch101.03.epdg.epc.mnc300.mcc310.3gppnetwork.org:1522864003:537746744:100, NAS: 10.169.48.75, NAS-Port: 0, User-Name: 310310990007655, Time: 00:28:10, USL: 1, Session-Id: epgch101.03.epdg.epc.mnc300.mcc310.3gppnetwork.org:1522864003:537746744:100, Auth-Application-Id: 16777264, Service-Selection: fms, User-Name: 3103109900076558nai.epc.mnc310.3gppnetwork.org, Origin-Realm: epc.mnc300.mcc310.3gppnetwork.org, Origin-Host: epgch101.03.epdg.epc.mnc300.mcc310.3gppnetwork.org
S0 Key: 310310990007618nai.epc.mnc310.3gppnetwork.org:epgch101.06.epdg.epc.mnc300.mcc310.3gppnetwork.org:1522864820:940397039:100, NAS: 10.169.48.238, NAS-Port: 0, User-Name: 310310990007618, Time: 00:14:34, USL: 1, Session-Id: epgch101.06.epdg.epc.mnc300.mcc310.3gppnetwork.org:1522864820:940397039:100, Auth-Application-Id: 16777264, Service-Selection: fms, User-Name: 310310990007618nai.epc.mnc310.3gppnetwork.org, Origin-Realm: epc.mnc300.mcc310.3gppnetwork.org, Origin-Host: epgch101.06.epdg.epc.mnc300.mcc310.3gppnetwork.org
S1 Key: 310310990007547nai.epc.mnc310.3gppnetwork.org:epgch121.epdg.epc.mnc300.mcc310.3gppnetwork.org:1495425783:2890:08002a36040180010100000000, NAS: 10.169.48.78, NAS-Port: 0, User-Name: 310310990007547, Time: 00:07:04, USL: 1, Session-Id: epgch121.epdg.epc.mnc300.mcc310.3gppnetwork.org:1495425783:2890:08002a36040180010100000000, Auth-Application-Id: 16777264, Service-Selection: fms, User-Name: 310310990007547nai.epc.mnc310.3gppnetwork.org, Origin-Realm: epc.mnc300.mcc310.3gppnetwork.org, Origin-Host: epgch121.epdg.epc.mnc300.mcc310.3gppnetwork.org
S11 Key: 310310990005644nai.epc.mnc310.3gppnetwork.org:1495425783:2894:08002a36040180010100000000, NAS: 10.169.48.235, NAS-Port: 0, User-Name: 310310990005644, Time: 00:01:16, USL: 1, Session-Id: epgch121.epdg.epc.mnc300.mcc310.3gppnetwork.org:1495425783:2894:08002a36040180010100000000, Auth-Application-Id: 16777264, Service-Selection: fms, User-Name: 310310990005644nai.epc.mnc310.3gppnetwork.org, Origin-Realm: epc.mnc300.mcc310.3gppnetwork.org, Origin-Host: epgch121.epdg.epc.mnc300.mcc310.3gppnetwork.org
```



특정 세션의 정보만 표시하려면 명령을 변경하고 USER 값(예: query-sessions /r with-User 310310990007655)을 사용할 수 있습니다.

```
--> query-sessions /r with-User 310310990007655
Sessions with-User 310310990007655 for /Radius
Session-Id : 310310990007655, User-Name : 310310990007655, Time : 00:30:22, USL : 1, Session-Id : epgch101.03.epdg.epc.mcc310.3gppnetwork.org:1522864003:537746744:100, NAS : 10.169.48.75, NAS-Port : 0, user-name : 310310990007655, Time : 00:30:22, USL : 1, Session-Id : epgch101.03.epdg.epc.mcc310.3gppnetwork.org:1522864003:537746744:100, Auth-Application-Id : 16777264, Service-Selection : ims, User-Name : 310310990007655@nat.epc.mcc310.mcc310.3gppnetwork.org, Origin-Realm : epc.mcc310.mcc310.3gppnetwork.org, Origin-Host : epgch101.03.epdg.epc.mcc310.3gppnetwork.org
```

이 목록에는 query-sessions 명령에 사용할 수 있는 모든 필터가 포함되어 있습니다.

- 모두
- ID 포함
- NAS 사용
- 사용자 포함
- 키 포함
- with-age+
- with-Attribute입니다.

마지막으로, CPAR에서 세션을 분리하려면 release-sessions /r all 명령을 사용하고 해당 시점에 연결된 모든 세션이 분리됩니다.

```
--> release-sessions /r all
```

```
Released 4 session(s) in /Radius/SessionManagers
```

특정 세션을 분리하기 위해 필터를 적용할 수 있습니다.

## 가입자 세션에 대해 CPAR AAA에 캐시된 특성(AVP)

Prime Access Registrar는 데이터를 쿼리하는 데 사용할 수 있는 세션 관리자에서 특성 캐싱을 지원합니다. 이 Diameter-query 서비스에는 쿼리할 세션 관리자 목록과 DIAMETER 쿼리 요청에 대한 응답으로 Access-Accept 패킷에서 반환할 (캐시된) 특성 목록이 포함되어 있습니다. 이 작업은 확장 지점 스크립트를 통해 시작되거나 Query-Service라는 새 환경 변수로 설정하여 규칙 및 정책 엔진을 통해 시작됩니다.

DIAMETER 쿼리 서비스는 확장 지점 스크립트를 통해 선택하거나 Query-Service라는 새 환경 변수로 설정하여 규칙 및 정책 엔진을 통해 선택해야 합니다. 그 이유는 DIAMETER Query 요청이 Access-Request로 들어오는데 서버가 DIAMETER Query 요청인지 일반 인증 요청인지 알 방법이 없기 때문입니다. Query-Service 환경 변수를 설정하면 Prime Access Registrar 서버에 요청이 DIAMETER 쿼리 요청임을 알려 Prime Access Registrar 서버가 Query-Service 환경 변수에 설정된 diameter-query 서비스로 요청을 처리할 수 있도록 합니다.

DIAMETER 쿼리 서비스가 액세스 요청을 처리하도록 선택된 경우, 이 세션 관리자 아래에서 키로 참조되는 세션 캐시 리소스 관리자에 구성된 QueryKey 값을 사용하여 구성된 세션 관리자 목록에

일치하는 레코드를 쿼리합니다. 일치하는 레코드가 있는 경우 일치하는 레코드에 있는 캐시된 특성 목록(컨피그레이션에 따라)을 포함하는 Access-Accept가 클라이언트로 다시 전송됩니다. 세션 캐시에 다중값 특성이 포함되어 있으면 해당 특성의 모든 값이 응답에서 다중값 특성으로 반환됩니다. 일치하는 레코드가 없는 경우 액세스 거부 패킷이 클라이언트로 전송됩니다.

Prime Access Registrar는 세션 레코드에 있는 캐시된 정보에 액세스하기 위해 자동화된 프로그래밍 가능 인터페이스(API)와 함께 세션 관리자 레벨의 스크립팅 포인트를 도입합니다. 이러한 스크립팅 지점 및 API를 사용하여 확장 지점 스크립트를 작성하여 캐시된 정보를 수정할 수 있습니다.

현재 Cisco 구축에는 스크립트를 작성하지 않았거나 프로그래밍 가능한 API를 사용하여 이러한 데이터에 액세스하지만 옵션은 여기에 있습니다.

현재 세션 관리자가 저장하는 속성은 다음과 같습니다.

/radius/resourcemanagers/swmcache/AttributesToBeCached에서 하드코딩됨:

- Non-3GPP-사용자-데이터
- 서비스 선택

기본적으로:

- 사용자 이름(IMSI)
- 원천 호스트
- 인증 애플리케이션 ID
- 원천 영역
- 세션 ID

이러한 특성은 CLI에서 이 명령 query-sessions를 사용할 때 세션별로 표시됩니다.

**다음을 확인합니다.**

현재 이 설정에 사용 가능한 확인 절차는 없습니다.

## 문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.