

CPAR-AAA-Konfiguration

Inhalt

[Einführung](#)

[Hintergrundinformationen](#)

[CPAR-Konfiguration](#)

[Globale Konfiguration](#)

[Client-Konfiguration](#)

[Schnelle Regelkonfiguration](#)

[Service-Konfiguration](#)

[Konfiguration von Remote-Servern](#)

[Sitzungsmanager](#)

[Ressourcen-Manager](#)

[Skripte](#)

[Konfiguration der CPAR-Protokollierung](#)

[Timeout-Werte](#)

[Durchmesser Paketgröße](#)

[Sitzungen verwalten in CPAR](#)

[AVP-Attribute im CPAR-AAA für Teilnehmersitzungen zwischengespeichert](#)

[Überprüfen](#)

[Fehlerbehebung](#)

Einführung

In diesem Dokument wird das Verfahren zur Konfiguration der Authentifizierung, Autorisierung und Abrechnung (Authentication, Authorization and Accounting - AAA) von Cisco Prime Access Registrar (CPAR) beschrieben.

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

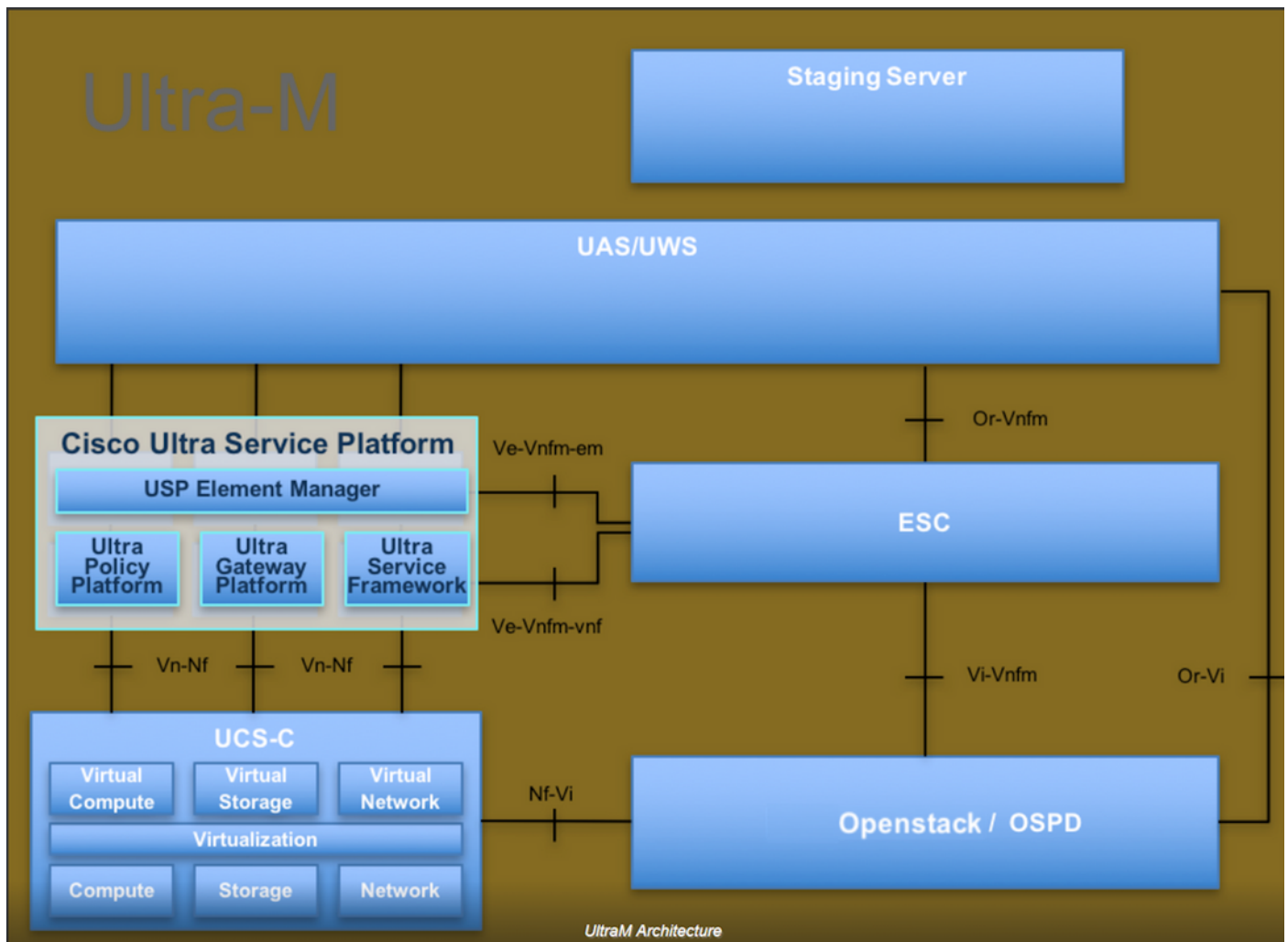
Hintergrundinformationen

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.

CPAR-Konfiguration

Globale Konfiguration

Die globale Diameter-Konfiguration muss mit entsprechenden Werten konfiguriert werden, z. B. mit den Anwendungs-IDs und der Ursprungs-Host-IP-Adresse, Realm usw.

```
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/hosts muss mit der entsprechenden IP-Adresse aktualisiert werden, damit der für das Transportmanagement und den Hostnamen verwendete vollständig qualifizierte AAA-Identitätsdomänenname (Fully Qualified Domain Name, FQDN) aufgelöst werden kann.

Client-Konfiguration

Die Client-Konfiguration ist mit den Diameter-Peers zu konfigurieren, die den Datenverkehr empfangen, in diesem Fall DRA.

```
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
```

Schnelle Regelkonfiguration

FastRules wird verwendet, um den entsprechenden Dienst in der Laufzeit auf der Grundlage bestimmter Bedingungen zuzuordnen. Die Bedingung basiert auf den Attributed Value Pairs (AVP) und den Werten in der Nachricht mit dem Durchmesser. Wenn keine schnellen Regeln zugeordnet wurden, wählt sie den Default-Dienst aus.

```
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/

```

Wenn keine der oben genannten FastRules zugeordnet wurde, wird das Paket als Standarddienst verarbeitet.

```

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

```

Service-Konfiguration

Service Configuration ist der Service, der gemäß Authentifizierung, Autorisierungsanforderung definiert wird:

CD/Radius/Services/

Der verschlüsselte IMSI-Service wird für EAP-AKA-Authentifizierungen verwendet und mit IMSI für Apple-Geräte verschlüsselt. Falls nicht erforderlich, legen Sie den EncryptedIMSI-Parameter auf **False** fest.

```
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 = sml  
DiameterProxyService = dia-proxy  
FetchLocationInformation = False
```

Der Dia-Proxy-Dienst wird zum Auswählen des Remoteservers verwendet und kann Peer-Richtlinien definieren. Die GroupFailover-Option wird als MultiplePeerPolicy verwendet, wenn mehrere Remote-Peers vorhanden sind und dieselben Gruppen erstellen möchten. Definieren Sie

außerdem die GroupTimeOutPolicy für Failover auf mehrere Gruppen.

```
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
```

Die oben genannten ServerGroups sind in **/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
```

Der S6b-Dienst wird für die Verarbeitung der PGW-Update-Prozedur über S6b verwendet.

s6b/

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

Der 3gpp-Reverse-Modus wird für die Verarbeitung von durch HSS initiierten Nachrichten verwendet.

3gpp-reverse/

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

Der Abfragedienst wird während der Re-Authorization-Prozedur verwendet, bei der das aktualisierte Profil direkt aus dem Cache abgerufen wird, basierend auf dem von HSS empfangenen PPR.

query/

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

Der Null-Service besteht darin, einfach mit Erfolg auf den S6b-Terminierungsprozess zu

antworten, da keine Sitzung über S6b zwischengespeichert wird.

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

Konfiguration von Remote-Servern

Remoteserver werden mit Remote-Peer definiert, an den Pakete wie das HSS von AAA gesendet werden. Wenn DRA verwendet wird, definieren Sie die gleichen DRA-Informationen in Clients und Remote-Servern.

```
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 =
```

Sitzungsmanager

Der Sitzungs-Manager definiert die Zwischenspeicherung von Sitzungen. Er arbeitet mit dem Ressourcen-Manager zusammen. Der Sitzungsmanager wird in den Diensten 3gpp-auth, 3gpp-reverse und query bezeichnet.

```
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

```

Ressourcen-Manager

Ressourcen-Manager sind so definiert, dass die Ressourcen zugewiesen und Sitzungsmanagern zugeordnet werden.

Diese drei Ressourcenmanager werden verwendet.

```

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/

```

Skripte

In dieser Tabelle werden alle Skripts angezeigt, die bei der Paketverarbeitung verwendet werden.

Name	Skriptdatei	Einstiegspunkt	Beschreibung
Klicke	Test.tcl	Klippe	Sucht nach der Anwendungs-ID 16777264 und dem Diameter-Befehls-Code 268, ruft den Benutzernamen ab und kopiert ihn in das Attribut call-station-ID von der

Rmserver	Test.tcl	rm_server	<p>eingehenden Anforderung. Dieses Skript wird in Radius Incoming Scriptinpoint (Radius Incoming Scriptinpoint) Sucht nach dem Attribut Server-Assignment-Type, sofern vorhanden, entfernt das Feld Remote-Server aus der eingehenden Anforderung. Dieses Skript wird in einem Dia-Proxy-Dienst als Incoming Scriptinpoint bezeichnet. Das Rex-Skript wird verwendet, um zuerst die empfangenen Informationen von HSS zu überprüfen, insbesondere die "Non-3GPP-IP-Access" und "Non-3GPP-IP-Access-APN" sollten beide den Wert "NON_3GPP_SUBSCRIPTION_ALLOWED (0)" und "Non_3GPP_APNS_ENABLE (0)" aufweisen, da sie ansonsten die Autorisierung fehlschlagen. Im Anschluss daran wird ein einfacher Vergleich des von der SWm DER-Nachricht empfangenen APN-Namens (Service-Selection AVP) mit der von HSS heruntergeladenen APN-Konfiguration durchgeführt. Wenn eine Übereinstimmung vorliegt, werden nur die spezifischen APN-Details kopiert, die unerwünschten AVPs entfernt und die endgültige DEA für die ePDG vorbereitet. Wenn keine Match-Autorisierung fehlschlägt und keine Service-Auswahl AVP in DER vorhanden ist, werden alle APN-Informationen gesendet, jedoch als äußere AVP. Dieses Skript wird in einem ausgehenden Skriptinpoint der 3gpp-auth-Methode referenziert. Das Rex-Skript wird verwendet, um zunächst die erhaltenen Informationen von HSS zu überprüfen, insbesondere die Nicht-3GPP-IP-Zugang und Nicht-3GPP-IP-Access-APN beide den Wert NON_3GPP_SUBSCRIPTION_ALLOWED (0) und Non_3GPP_APNS_ENABLE (0). Im Anschluss daran wird ein einfacher Vergleich des von der SWm DER-</p>
Benutzerdaten	libremoveuserdata.so	removeUserData	<p>Namens (Service-Selection AVP) mit der von HSS heruntergeladenen APN-Konfiguration durchgeführt. Wenn eine Übereinstimmung vorliegt, werden nur die spezifischen APN-Details kopiert, die unerwünschten AVPs entfernt und die endgültige DEA für die ePDG vorbereitet. Wenn keine Match-Autorisierung fehlschlägt und keine Service-Auswahl AVP in DER vorhanden ist, werden alle APN-Informationen gesendet, jedoch als äußere AVP. Dieses Skript wird in einem ausgehenden Skriptinpoint der 3gpp-auth-Methode referenziert. Das Rex-Skript wird verwendet, um zunächst die erhaltenen Informationen von HSS zu überprüfen, insbesondere die Nicht-3GPP-IP-Zugang und Nicht-3GPP-IP-Access-APN beide den Wert NON_3GPP_SUBSCRIPTION_ALLOWED (0) und Non_3GPP_APNS_ENABLE (0). Im Anschluss daran wird ein einfacher Vergleich des von der SWm DER-</p>
Remveuserdataquerie	libremoveuserdataquery.so	removeUserData	<p>Namens (Service-Selection AVP) mit der von HSS heruntergeladenen APN-Konfiguration durchgeführt. Wenn eine Übereinstimmung vorliegt, werden nur die spezifischen APN-Details kopiert, die unerwünschten AVPs entfernt und die endgültige DEA für die ePDG vorbereitet. Wenn keine Match-Autorisierung fehlschlägt und keine Service-Auswahl AVP in DER vorhanden ist, werden alle APN-Informationen gesendet, jedoch als äußere AVP. Dieses Skript wird in einem ausgehenden Skriptinpoint der 3gpp-auth-Methode referenziert. Das Rex-Skript wird verwendet, um zunächst die erhaltenen Informationen von HSS zu überprüfen, insbesondere die Nicht-3GPP-IP-Zugang und Nicht-3GPP-IP-Access-APN beide den Wert NON_3GPP_SUBSCRIPTION_ALLOWED (0) und Non_3GPP_APNS_ENABLE (0). Im Anschluss daran wird ein einfacher Vergleich des von der SWm DER-</p>

			<p>Nachricht empfangenen APN-Namens (Service-Selection AVP) mit der von HSS heruntergeladenen APN-Konfiguration durchgeführt. Wenn eine Übereinstimmung vorliegt, werden nur die spezifischen APN-Details kopiert, die unerwünschten AVPs entfernt und die endgültige DEA für die ePDG vorbereitet. Wenn keine Match-Autorisierung fehlschlägt und keine Service-Auswahl AVP in DER vorhanden ist, werden alle APN-Informationen gesendet, jedoch als äußere AVP.</p> <p>Dieses Skript wird im AbfragedienstAusgehender Skriptinpunkt referenziert</p> <p>Das Proxy Service eingehende Skript - wird verwendet, um den Sticky für die Nachrichten zu deaktivieren, die bereits verarbeitet werden. z. B. Wenn MAR/MAA von DRA1 empfangen wird, verwendet der nachfolgende Benutzer-SAR denselben DRA1, und wenn dieser nicht verfügbar ist und der Verbleib aufrecht erhalten wird, findet kein Failover statt. Damit ein Failover auf eine alternative DRA-Karte möglich ist, muss diese Bindung entfernt werden. Mit dem Skript wird der Visited-Network-Identifier zu S6b SAR(PGW_update) HSS entfernt. Entfernt DestinationHost AVP in Paketen mit DiameterCode 301 und 303.</p> <p>Entfernt AVP der Visited-Network-Identifier in Paketen mit DiameterCode 256 und dem Serverzuweisungstyp ist 13. Ersetzen Sie AVP mit Ergebniscode durch "Test" in Paketen mit DiameterCode 274 und Ergebniscode "Durchmesser-Unbekannte-Sitzungs-ID".</p> <p>Wenn mehrere RTRs für dieselbe Sitzung empfangen werden, werden doppelte Sitzungen gelöscht und protokolliert.</p>
ausschließen	Test.tcl	NewsessionBund esland	
Rmdh	Test.tcl	Rmdh	
rmvnid	Test.tcl	rmvnid	
AAARepReplaceResultCode	Test.tcl	replaceResultCode	
AAARTRCheck	librexblock RTR.so	AAARTRCheck	

Einige der Skripte sind in höherer Version möglicherweise nicht erforderlich, die oben aufgeführten

Skripts sind in CPAR Version 7.3.0.3 zu verwenden

Alle Skripte befinden sich im Pfad `/opt/CSCOar/scripts/radius/`.

Konfiguration der CPAR-Protokollierung

Im Ordner `/opt/CSCOar/logs` werden alle Anwendungsprotokolle gespeichert. Der Dateiname `_radius_1_log` registriert alle verworfenen und abgelehnten Anfragen. Daher ist es wichtig, diese Datei für die Fehlerbehebung zu speichern.

CPAR ermöglicht eine sehr flexible Konfiguration, um dieses Protokoll entsprechend Ihren Anforderungen zu speichern. Je nach Anforderung kann dieser Wert definiert werden, hier werden die neuesten 20 Protokolldateien gespeichert, jede Datei hat eine Größe von 5 MB.

Um diese spezifische Protokollierung zu aktivieren, müssen 2 Parameter im `aregcmd`-Modus konfiguriert werden:

```
/Radius/Advanced
```

```
LogFileSize = "5 Megabyte"
```

```
LogFileCount = 20
```

Die Namenskonvention für Protokolle entspricht der in dieser Tabelle angegebenen Regel:

Beschreibung	Name der Protokolldatei
Aktuelles Protokoll	<code>name_radius_1_log</code>
2. bis aktuelles Protokoll	<code>name_radius_1_log.01</code>
3. bis aktuelles Protokoll	<code>name_radius_1_log.02</code>
...	...
20. bis aktuellstes Protokoll	<code>name_radius_1_log.19</code>

Tabelle 2 Nummerierung der Protokolle

Timeout-Werte

CPAR verfügt über vom Server konfigurierbare Zeitüberschreitungen. Die aktuelle Konfiguration lautet wie folgt:

Allgemeine Timeouts in `/Radius/Advanced`

- **DiameterStaleConnectionDeletionTimeOut** 300000 (ms) Dieser Zeitgeber gibt an, wie lange eine Verbindung mit Durchmesser inaktiv sein kann, bevor CPAR sie als inaktiv kennzeichnet.

Client-Timeouts in `/Radius/Clients/<client_name>`

- **InitialTimeout** 3000 (ms) Die Zeit, die DRA auf eine Antwort wartete, bevor CPAR sie als nicht erreichbar ansah.

Timeouts für Remote-Server in `/Radius/RemoteServers/<remote_server_name>`

- **InitialTimeout** 3000 (ms) Die Zeit, die DRA auf eine Antwort wartete, bevor CPAR sie als nicht erreichbar ansah.
- **DWatchDogTimeout** 2500 (ms) Zeit wartete auf eine Wiederholung von DRA für DiameterWatchDog-Paket, bevor CPAR dies für nicht erreichbar ansieht.
- **ReaktivierungTimerInterval** 30000 (ms) Zeit, die CPAR wartet, bis erneut versucht wird, eine Verbindung mit einem Durchmesser Peer herzustellen.

Durchmesser Paketgröße

In diesem Dokument wird die Bedeutung des Befehls Diameter Packet size und die Gründe erläutert, die Sie dazu veranlasst haben, diesen Parameter auf den Wert 4096 zu setzen.

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

Wie in der obigen Abbildung erläutert, beträgt die Paketgröße mit maximalem Durchmesser, die CPAR erwartet, 4096 Byte zu empfangen. Dieser Wert wird unter der Variable **DiameterPacketSize** im Verzeichnis /Radius/Advanced/Diameter/TransportManagement konfiguriert. Alle Pakete, die diesen Wert nicht erfüllen, werden verworfen. Die Gesamtpaketgröße wird ermittelt, nachdem die Größe der zwischengespeicherten Sitzungsattribute plus die Größe des empfangenen Durchmesser-Pakets addiert wurde.

Betrachten wir zum Beispiel eine PPR-Paketgröße von 4000 Byte, und innerhalb dieser Nachricht hat Non-3GPP-User-Data eine Größe von 3800 Byte. Wenn in der Sitzung bereits Attribute zwischengespeichert wurden und die Größe der zwischengespeicherten Daten 297 Byte beträgt, überschreitet die Sitzunggröße 4096 Byte, und die Nachricht wird von CPAR verworfen.

Während des Projektes und der Analyse von Paketen über 4096 wurde durchgeführt. Die Ergebnisse zeigen, dass durchschnittlich 36 Pakete (SAA) mit einer Kapazität von mehr als 4096 pro CPAR-Instanz pro Tag eintreffen. Diese Anzahl von Paketen ist nicht sinnvoll, da sie sehr klein ist.

Dieser Parameter ist konfigurierbar und kann bei Bedarf erhöht werden. Der Wert wird jedoch über 4096 hinaus erhöht, was einige Nachteile mit sich bringt:

- Wenn DiameterPacketSize auf 5 KB erhöht wird, akzeptiert CPAR SAA-Pakete mit mehr als 4096 Byte. Wenn PPR jedoch für dieselbe Benutzersitzung initiiert wird, da die Größe der Non-3GPP-User-Data 4260 Byte beträgt, schlägt das Sitzungsupdate fehl und führt zu einer Benutzerregistrierung.
- DiameterPacketSize wirkt sich direkt auf den Startspeicher aus, der dem Radius-Prozess zugewiesen ist. Je größer der DurchmesserPacketSize ist, desto größer ist der dem Radius-Prozess beim CPAR-Start zugewiesene Speicherplatz.

Dieses Bild zeigt ein Beispiel für die Ausgabe des obersten Befehls in einer Instanz, in der DiameterPacketSize für 4096 konfiguriert ist:

```
[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

Wenn der Parameter DiameterPackerSize auf 6000 erhöht wird, sieht die Ausgabe des obersten Befehls wie folgt aus:

```
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

- Neben der Speicherzuweisung für den Startspeicher gibt es nach der Verwendung des Systems einen internen dynamischen Speicherpuffer, der im Verhältnis zur Anzahl der Pakete, die CPAR erreichen, wächst. Wenn beispielsweise 1000 Pakete CPAR an einem Punkt erreichen, weist CPAR unabhängig von der Größe der einzelnen Pakete intern im Puffer $1000 * \text{DiameterPacketSize}$ Speicher zu (CPAR weiß, dass DiameterPacketSize die maximale Paketgröße angibt). Dieser interne Speicherpuffer weist mehr Speicher zu, wenn DiameterPacketSize inkrementiert ist, und weniger Speicher, wenn er reduziert wird.

Es wird empfohlen, diesen Parameter als 4096 beizubehalten, da entschieden wurde, dass die Anzahl der Pakete, die größer als 4096 sind, vernachlässigbar ist und die Nachteile unerwünschtes Verhalten darstellen würden.

Sitzungen verwalten in CPAR

Der einzige Mechanismus, der in CPAR vorhanden ist, um die Anzahl der Sitzungen zu überwachen, ist die in diesem Dokument beschriebene Methode. Es gibt keine OID, die über SNMP abgerufen werden kann, das diese Informationen enthält.

CPAR kann Sitzungen verwalten, die CPAR-CLI mit `/opt/CSCOar/bin/aregcmd` eingeben und sich mit Administratorrechten anmelden.

Mit dem Befehl `count-sessions /r` zeigt alle CPAR-Sitzungen alle Sitzungen an, die zu diesem Zeitpunkt an das CPAR angeschlossen sind.

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

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

Um weitere Informationen über die Sitzung(en) zu erhalten, verfügt CPAR über den Befehl query-sessions /r alle, der die Informationen über alle Sitzungen enthält, die an CPAR angehängt sind.

```
--> query-sessions /r all
Sessions for /Radius:
Sessions For /Radius/SessionManagers/sml:
S5 Key: 310310990007655@na1.epc.mcc310.3gppnetwork.org:epgchi01.03.epdg.epc.mcc300.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: epgchi01.03.epdg.epc.mcc300.mcc310.3gppnetwork.org:1522864003:537746744:100, Auth-Application-Id: 16777264, Service-Selection: fms, User-Name: 310310990007655@na1.epc.mcc310.mcc310.3gppnetwork.org, Origin-Realm: epc.mcc300.mcc310.3gppnetwork.org, Origin-Host: epgchi01.03.epdg.epc.mcc300.mcc310.3gppnetwork.org
S6 Key: 310310990007618@na1.epc.mcc310.3gppnetwork.org:epgchi01.06.epdg.epc.mcc300.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: epgchi01.06.epdg.epc.mcc300.mcc310.3gppnetwork.org:1522864820:940397039:100, Auth-Application-Id: 16777264, Service-Selection: fms, User-Name: 310310990007618@na1.epc.mcc310.mcc310.3gppnetwork.org, Origin-Realm: epc.mcc300.mcc310.3gppnetwork.org, Origin-Host: epgchi01.06.epdg.epc.mcc300.mcc310.3gppnetwork.org
S7 Key: 310310990007547@na1.epc.mcc310.3gppnetwork.org:epgchi21.epdg.epc.mcc300.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: epgchi21.epdg.epc.mcc300.mcc310.3gppnetwork.org:1495425783:2890:08002a36040180010100000000, Auth-Application-Id: 16777264, Service-Selection: fms, User-Name: 310310990007547@na1.epc.mcc310.mcc310.3gppnetwork.org, Origin-Realm: epc.mcc300.mcc310.3gppnetwork.org, Origin-Host: epgchi21.epdg.epc.mcc300.mcc310.3gppnetwork.org
S11 Key: 310310990005644@na1.epc.mcc310.3gppnetwork.org:epgchi21.epdg.epc.mcc300.mcc310.3gppnetwork.org:1495425783:2894:088008a1050180010100000000, NAS: 10.169.48.235, NAS-Port: 0, User-Name: 310310990005644, Time: 00:01:16, USL: 1, Session-Id: epgchi21.epdg.epc.mcc300.mcc310.3gppnetwork.org:1495425783:2894:088008a1050180010100000000, Auth-Application-Id: 16777264, Service-Selection: fms, User-Name: 310310990005644@na1.epc.mcc310.mcc310.3gppnetwork.org, Origin-Realm: epc.mcc300.mcc310.3gppnetwork.org, Origin-Host: epgchi21.epdg.epc.mcc300.mcc310.3gppnetwork.org
```

Um nur die Informationen einer bestimmten Sitzung anzuzeigen, kann der Befehl geändert und der USER-Wert verwendet werden, d. h.: query-sessions /r mit dem Benutzer 310310990007655

```
--> query-sessions /r with-user 310310990007655
Sessions with-user 310310990007655 for /Radius:
Sessions For /Radius/SessionManagers/sml:
S5 Key: 310310990007655@na1.epc.mcc310.3gppnetwork.org:epgchi01.03.epdg.epc.mcc300.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: epgchi01.03.epdg.epc.mcc300.mcc310.3gppnetwork.org:1522864003:537746744:100, Auth-Application-Id: 16777264, Service-Selection: fms, User-Name: 310310990007655@na1.epc.mcc310.mcc310.3gppnetwork.org, Origin-Realm: epc.mcc300.mcc310.3gppnetwork.org, Origin-Host: epgchi01.03.epdg.epc.mcc300.mcc310.3gppnetwork.org
```

Diese Liste enthält alle möglichen Filter für den Befehl "query sessions":

- Alle
- with-ID
- mit NAS
- Mit-Benutzer
- Mit-Taste
- mit Alter+
- with-Attribute.

Um Sitzungen von CPAR zu trennen, verwenden Sie schließlich die Befehlsfreigabesitzungen /r all, und alle Sitzungen, die zu diesem Zeitpunkt angehängt wurden, werden getrennt.

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

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

Zum Trennen einer bestimmten Sitzung kann ein Filter angewendet werden.

AVP-Attribute im CPAR-AAA für Teilnehmersitzungen zwischengespeichert

Prime Access Registrar unterstützt das Zwischenspeichern von Attributen bei Session Manager, die zum Abfragen von Daten verwendet werden können. Dieser Diameter-Abfrage-Dienst enthält eine Liste der Session-Manager, von denen eine Abfrage durchgeführt werden soll, und eine Liste der (zwischengespeicherten) Attribute, die als Antwort auf eine DIAMETER-Abfrage im Access-Accept-Paket zurückgegeben werden sollen. Dies wird durch ein Erweiterungspunktsskript oder durch die Rule Engine (Regel) und die Policy Engine (Policy Engine) initiiert, indem diese auf eine neue Umgebungsvariable mit dem Namen Query-Service festgelegt wird.

Der DIAMETER-Abfragedienst sollte durch ein Erweiterungspunkt-Skript oder durch die Rule

Engine und Policy Engine ausgewählt werden, indem dieser auf eine neue Umgebungsvariable mit dem Namen Query-Service festgelegt wird. Der Grund dafür ist, dass die DIAMETER-Abfrage als Access-Request eingeht und der Server nicht weiß, ob es sich um eine DIAMETER-Abfrage-Anfrage oder eine normale Authentifizierungsanfrage handelt. Durch Festlegen der Abfrage-Service-Umgebungsvariable wird dem Prime Access Registrar-Server mitgeteilt, dass die Anforderung eine DIAMETER-Abfrage-Anforderung ist, sodass der Prime Access Registrar-Server die Anforderung mit dem Abfragedurchsatzdienst in der Umgebungsvariable Abfrage-Dienst verarbeiten kann.

Wenn ein DIAMETER-Abfragedienst ausgewählt wird, um eine Zugriffsanforderung zu verarbeiten, fragt er die konfigurierte Liste der Session Manager mithilfe des QueryKey-Werts ab, der im Ressourcen-Manager des Sitzungscaches konfiguriert ist, auf den unter diesen Session Manager als Schlüssel verwiesen wird. Wenn ein übereinstimmender Datensatz gefunden wird, wird eine Access-Accept-Datei, die eine Liste der zwischengespeicherten Attribute enthält, die (basierend auf der Konfiguration) im zugeordneten Datensatz vorhanden sind, an den Client zurückgesendet. Wenn der Sitzungscache ein mehrwertiges Attribut enthält, werden alle Werte dieses Attributs in der Antwort als mehrwertiges Attribut zurückgegeben. Wenn kein übereinstimmender Datensatz vorhanden ist, wird ein Access-Reject-Paket an den Client gesendet.

Prime Access Registrar führt Scripting-Punkte auf Session Manager-Ebene zusammen mit automatisierten programmierbaren Schnittstellen (APIs) ein, um auf die im Sitzungsdatensatz enthaltenen zwischengespeicherten Informationen zuzugreifen. Sie können diese Skriptpunkte und APIs verwenden, um Erweiterungspunktskripts zu schreiben, um die zwischengespeicherten Informationen zu ändern.

Derzeit verfügt unsere Bereitstellung über keine schriftlichen Skripts oder nutzt programmierbare APIs, um auf diese Daten zuzugreifen. Die Option ist jedoch vorhanden.

Die Attribute, die unser Sitzungsmanager derzeit speichert, sind:

Codiert bei `/radius/resourcemanagers/swmcache/AttributesToBeCached`:

- Nicht-3GPP-Benutzerdaten
- Serviceauswahl

Standardmäßig:

- Benutzername (IMSI)
- Quelle - Host
- Auth-Anwendungs-ID
- Ursprungsbereich
- Sitzungs-ID

Solche Attribute sind pro Sitzung sichtbar, wenn dieser Befehl **query-sessions** für die CLI verwendet wird.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.