

Verwendung des Konfigurationsleitfadens für die Integration von DRAs verschiedener Anbieter

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurationsschritte und Best Practices](#)

[Schritt 1: Ermitteln des DRA-Verbindungsmodus \(eingehender und ausgehende Peers\)](#)

[Phase 2: Eingehende Peers im Richtlinien-Generator konfigurieren](#)

[Schritt 3: AVP für Host-IP-Adresse konfigurieren](#)

[Schritt 4: Überprüfung des Austauschs von Peer-Funktionen](#)

[Schritt 5: Stellen Sie sicher, dass der eindeutige Quellhostname für den Durchmesser an jedem Peerknoten für den Durchmesser definiert ist.](#)

[Schritt 6: Konfigurieren der Next-Hop-Routing-Tabelle für DRA-Peers](#)

Einleitung

In diesem Dokument werden die Konfigurationsschritte und Best Practices für die Integration von DRA mit Cisco Policy Suite (CPS)-PCRF-Clustern aus Komponenten verschiedener Hersteller beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Techniker, die mit dieser Lösung arbeiten, mit den folgenden Themen vertraut sind:

- Linux-Betriebssystem
- Cisco Policy Suite (CPS)-Plattform und Cluster-Architektur
- Policy and Charging Rules Function (PCRF)
- Verwendung des Vi-Editors
- Wireshark Netzwerk-Analyse-Tool

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der CPS 25.1-Version und AlmaLinux 8.10.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurationsschritte und Best Practices

Schritt 1: Ermitteln des DRA-Verbindungsmodus (eingehender und ausgehende Peers)

- **Eingehende Peers:** Die PCRF-Instanz ist so konfiguriert, dass sie Verbindungsanforderungen von festgelegten Diameter-Peers akzeptiert. Der Peer-Knoten initiiert die Diameter Capabilities-Exchange-Request (CER)-Anfrage an die PCRF-Instanz.
- **Ausgehende Peers:** Die PCRF-Instanz wird so konfiguriert, dass sie den CER zu seinen Peers initiiert.

Best Practice:

Bei den meisten DRA-Integrationen mit Komponenten verschiedener Hersteller muss der DRA als eingehender Peer konfiguriert werden, wobei der DRA den CER zur PCRF-Instanz initiiert.

Phase 2: Eingehende Peers im Richtlinien-Generator konfigurieren

Konfigurieren Sie in der GUI von Policy Builder den Namen des eingehenden Peers und den Peer-Bereich, und verweisen Sie dabei auf die Tabellen für eingehende Peers und Bereiche.



Anmerkung: Ausführliche Parameterbeschreibungen finden Sie im CPS Mobile Configuration Guide, Release 25.1.0, im Abschnitt Diameter Stack Configuration.

Diese Parameter können unter "Inbound Peers" (Eingehende Peers) konfiguriert werden:

Peers-Tabelle

Parameter	Beschreibung
Peers	Definiert, welche Peernamen Verbindungen zu PCRF initiieren dürfen.
Lokaler Hostname	Identifiziert den lokalen Hostnamen des Richtlinien-Directors (Load Balancer), der identifiziert eine eingehende Verbindung vom Peer und lässt sie zu.
Instanznummer	Gibt die zugewiesene Nummer des Policy Server (QNS)-Prozesses an, der stellt eine Verbindung mit dem ausgehenden Peer her.  Anmerkung: Lokaler Hostname und Instanznummer müssen angegeben werden, wenn nur ein einziger Policy Server (QNS)-Prozess auf Policy Builder (Load Balancer) eine Verbindung mit dem Peer zulassen/initiieren soll. Andernfalls kann die Instanznummer als 0 beibehalten werden. In diesem Fall müssen alle Policy Server (QNS)-Prozesse auf Policy Director (Load Balancer) eine Verbindung mit dem Peer versuchen/zulassen. Der Standardwert ist 0.
Bewertung	Priorität, die diesem Peer für die Zustellung einer PCRF-initiierten Anforderung zugewiesen wird. Die Fehlermeldung Je höher der Bewertungswert, desto höher ist die Priorität, die dem Peer zugewiesen wird. Der Standardwert ist 1.
Port-Bereich	Nur angeben, wenn die zugrunde liegende Transportverbindung SCTP ist und nicht erforderlich, wenn TCP identisch ist.

Antwort-Timeout	Cisco empfiehlt, diesen Parameter nicht zu verwenden.
Namensmuster	Herkunft - Host Ein VP-Wert in CER muss anhand dieses Musters validiert werden in Reihenfolge für die Herstellung der Verbindung. Sollte dies nicht geschehen, wird der CER wird stillschweigend verworfen und die TCP-Verbindung wird durch PCRF zurückgesetzt. Die Namensmusterprüfung findet nicht statt, wenn die Option "Undefinierten Peer akzeptieren" aktiviert ist. unter "Diameter Stack Configuration" beschrieben. Das Namensmuster muss der reguläre Java-Standardausdruck sein. Syntax, die hier beschrieben wird.

Bereichstabelle

Parameter	Beschreibung
Bereiche	Definiert, auf welchen Peer-Realms Verbindungen initiiert werden dürfen. PCRF
Peer-Typ	Wird nicht für eingehende Bereiche verwendet.
Verarbeitungsprotokoll	Zuordnung zwischen dem Bereichsnamen und der spezifischen PCRF-Logik, die für die Nachricht angewendet werden, um weitere Informationen über das Verarbeitungsprotokoll zu erhalten. Wenn ein Durchmesserstapel mit einem Durchmesserbereich ohne Protokoll importiert wird zugewiesen, wird der Standardwert als GX_TGPP verwendet.
Bewertung	Die diesem Bereich zugewiesene Priorität für die Zustellung einer PCRF-

	initiierten Anforderung. Diese wird nur mit dem Verarbeitungsprotokoll SY_PRIME verwendet. Der Standardwert ist 0. Je niedriger der Bewertungswert, desto höher ist die dem Bereich zugewiesene Priorität. Beispielsweise wird ein Bereich mit Rating = 10 verwendet, nachdem ein Bereich mit Bewertung=1.
Stats-Alias	Unabhängig davon, welche Statistiken für den jeweiligen Bereich generiert werden, erhalten Sie die Name, der im Statistikalias konfiguriert und an diese Statistiken angehängt ist. Dies gilt nur für die mbean-Statistik von com.Broadhop.message.
Namensmuster	Origin-Realm Ein VP-Wert in CER muss für dieses Muster validiert werden in Reihenfolge für die Verarbeitung der eingehenden Nachricht. Wenn das nicht geschieht, Die Nachricht wird stillschweigend verworfen, und die TCP-Verbindung wird durch PCRF zurückgesetzt. Das Namensmuster muss der reguläre Java-Standardausdruck sein. Syntax, die hier beschrieben wird.

Best Practice:

Um eine detailliertere Kontrolle zu erhalten, konfigurieren Sie je nach Anforderung bestimmte Peer- und Bereichseinträge, damit die Peerererstellung nur von bestimmten Peers aus möglich ist, und deaktivieren Sie die Option Undefineden Peer akzeptieren ausPeer entfernen.

Beispiel:

Abbildung 1: Tabelle der eingehenden Peers

REFERENCE DATA

File Tools

Systems

- Summary
- system-1
 - Plugin Configurations
 - cluster-1
 - Plugin Configurations
 - Diameter Configuration
 - Lab-PCRF
 - USuM Configuration

- Account Balance Templates
- Custom Reference Data Tables
- Diameter Agents
- Diameter Clients
- Diameter Defaults
- Fault List
- Notifications
- Policy Enforcement Points
- Rule Retry Profiles
- Subscriber Data Sources
- Tariff Times

Diameter Stack

*Name

Lab-PCRF

*Realm

pcrf.mnc.mcc.3gppnetwork

☐ Accept Undefined Peer

Settings

Inbound Peers

Peers

Local Host Name	Instance Number	*Rating	Port Range	*Response Timeout	*Name Pattern
	0	1			.*

Add Remove

Realms

Peer Type	*Processing Protocol	Rating	Stats Alias	*Name Pattern
	GX_TGPP	0		.*
	RX_TGPP	0		.*

Abbildung 1: Tabelle der eingehenden Peers

Schritt 3: AVP für Host-IP-Adresse konfigurieren

Der Diameter Host-IP-Adresse AVP gibt die IP-Adresse des Knotens während CER/CEA-Austauschvorgängen (RFC 3588) für SCTP-basierte Verbindungen an. In Cisco CPS PCRF ist diese Adresse standardmäßig die interne Schnittstellen-IP, die sich von der erwarteten Diameter Service-IP für bestimmte DRA-Anbieter unterscheidet.

In Cisco CPS PCRF können Sie entweder die virtuelle Load Balancer-IP (LbVIP) oder die physische IP der virtuellen Load Balancer-Rechner als IP-Adresse für Durchmesser, Quelle und Endpunkt verwenden.

Standardmäßig wird die interne Schnittstellen-IP als Host-IP-Adresse in den CER/CEA-Nachrichten im Durchmesser kommuniziert, wie in der Abbildung dargestellt, wobei man sehen kann, dass die Quell-IP in der Erfassung anders ist als die IP in der Host-IP-Adresse AVP.

Abbildung 2: CEA-Nachricht mit interner IP als Host-IP-Adresse

No.	Time	Source	Destination	Protocol	Length	Info
28	11.542641	DRA IP	PCRF Service IP	DIAME...	264	cmd=Capabilities-Exchange Request(257) flags=R--- appl=Diameter Common Message
30	11.794483	PCRF Service IP	DRA IP	DIAME...	592	cmd=Capabilities-Exchange Answer(257) flags=---- appl=Diameter Common Messages

Frame 30: 592 bytes on wire (4736 bits), 592 bytes captured (4736 bits)

> Linux cooked capture v1

> Internet Protocol Version 4, Src: PCRF Service IP (10.130.130.130), Dst: DRA IP (10.18.18.18)

> Transmission Control Protocol, Src Port: 3868, Dst Port: 49151, Seq: 1, Ack: 197, Len: 524

> Diameter Protocol

Version: 0x01

Length: 524

Flags: 0x00

Command Code: Capabilities-Exchange (257)

ApplicationId: Diameter Common Messages (0)

Hop-by-Hop Identifier: 0x5992d592

End-to-End Identifier: 0x071fbd73

[Request In: 28]

[Response Time: 0.251842000 seconds]

> AVP: Origin-Host(264) l=63 f=M- val=pcrf.mnc.mcc.3gppnetwork.org

> AVP: Origin-Realm(296) l=42 f=M- val=pcrf.mnc046.mcc404.3gppnetwork.org

> AVP: Host-IP-Address(257) l=14 f=M- val=192.12 (192.12)

> AVP: Vendor-Id(266) l=12 f=M- val=26878

> AVP: Supported-Vendor-Id(265) l=12 f=M- val=10415

> AVP: Vendor-Specific-Application-Id(260) l=32 f=M-

> AVP: Auth-Application-Id(258) l=12 f=M- val=3GPP Gx (16777238)

> AVP: Supported-Vendor-Id(265) l=12 f=M- val=8164

> AVP: Vendor-Specific-Application-Id(260) l=32 f=M-

> AVP: Supported-Vendor-Id(265) l=12 f=M- val=9

> AVP: Vendor-Specific-Application-Id(260) l=32 f=M-

> AVP: Supported-Vendor-Id(265) l=12 f=M- val=7898

> AVP: Vendor-Specific-Application-Id(260) l=32 f=M-

> AVP: Supported-Vendor-Id(265) l=12 f=M- val=5535

> AVP: Vendor-Specific-Application-Id(260) l=32 f=M-

> AVP: Vendor-Specific-Application-Id(260) l=32 f=M-

> AVP: Auth-Application-Id(258) l=12 f=M- val=3GPP Rx (16777236)

> AVP: Supported-Vendor-Id(265) l=12 f=M- val=13019

> AVP: Vendor-Specific-Application-Id(260) l=32 f=M-

> AVP: Product-Name(269) l=21 f= val=Cisco Quantum

> AVP: Result-Code(268) l=12 f=M- val=DIAMETER_SUCCESS (2001)

Abbildung 2: CEA-Nachricht mit interner IP als Host-IP-Adresse

Obwohl dieser AVP nicht obligatorisch ist, wenn TCP als Transportprotokoll verwendet wird (siehe RFC 3588), beziehen sich einige DRA-Anbieter beim Herstellen der Diameter-Verbindung auf diesen AVP und erwarten den Diameter-Service IP von PCRF anstelle von interner IP. Wenn diese Erwartung nicht erfüllt wird, können sich die Peers nicht etablieren.

Best Practice:

Um die Diameter-Service-IP in der Host-IP-Adresse AVP von PCRF anzukündigen, aktualisieren Sie die Datei /etc/hosts mit einem Eintrag, der den PCRF-Quell-FQDN (wie in den lokalen Endpunkten des Diameter Stack definiert) der gewünschten IP-Adresse zuordnet.



Anmerkung: Weitere Informationen finden Sie in den Tabellen mit lokalen Endpunkten im CPS Mobile Configuration Guide, Release 25.1.0, im Abschnitt Diameter Stack Configuration (Stack-Konfiguration mit Durchmessern).

So aktualisieren Sie zusätzliche Host-Einträge in OpenStack-basierten CPS PCRF:

- Überprüfen Sie, ob sich der CPS-Cluster im bereitgestellten Zustand befindet.

curl -X GET [installer API-System](#).

- Abrufen und Aktualisieren der Datei additional-hosts.yaml über die REST-API.

```
curl -X GET http://<Cluster Manager IP>:8458/api/system/config/additional-hosts >> additional-hosts.yaml
```

- Wenden Sie die Änderungen mit den Curl-Befehlen an, wie in der Produktdokumentation beschrieben.

```
curl -X PUT API-System zusätzliche Hosts -H "Inhaltstyp: application/yaml" —data-binary @additional-hosts.yaml
```

Nach Abschluss dieses API-Aufrufs wird der Cluster Manager mit der neuen /etc/hostsfile konfiguriert, und alle anderen bereitgestellten VMs werden asynchron aktualisiert.



Anmerkung: Ausführliche Anweisungen finden Sie im CPS-Installationshandbuch für OpenStack im Abschnitt Orchestrierungs-API.

So aktualisieren Sie zusätzliche Host-Einträge in VMware-basierter CPS PCRF:

- Fügen Sie den Eintrag in der Datei AdditionalHosts.csv unter dem Pfad /var/qps/config/deploy/csv/ hinzu.
- So importieren Sie Änderungen in die Cluster Manager-VM:

```
/var/qps/install/current/scripts/import/import_deploy.sh
```

- Änderungen vom Cluster-Manager übernehmen:

```
/var/qps/install/current/scripts/build_all.sh
```

```
/var/qps/install/current/scripts/upgrade/reinit.sh
```



Anmerkung: Ausführliche Anweisungen finden Sie im CPS-Installationshandbuch für VMware im Abschnitt Konfiguration zusätzlicher Hosts.

Beispiel:

Abbildung 3: GUI-Durchmesser Stack - Lokale Endpunkte

*Local End Points						
*Local Host Name	Instance Number	*Advertised Diameter F Q D N	*Listening Port	Local Bind Ip	*Transport Protocol	Multi Homing Hosts
HOSTNAME-lb01	0	HOSTNAME.pcrf.mncXXX.mccYYY.3gppnetwork.org	3868		TCP	
HOSTNAME-lb02	0	HOSTNAME.pcrf.mncXXX.mccYYY.3gppnetwork.org	3868		TCP	

Add Remove ↕ ↕

Abbildung 3: GUI-Durchmesser Stack - Lokale Endpunkte

Beispiel für /etc/hosts-Eintrag:

<#root>

10.x.x.130 HOSTNAME.pcrf.mncXXX.mccYYY.3gppnetwork.org HOSTNAME.pcrf.mncXXX.mccYYY.3gppnetwork.org

```
192.x.x.16 HOSTNAME-cluman installer
#END_QPS_OTHER_HOSTS
[root@Hostname-cluman ~]#
```

Schritt 4: Überprüfung des Austauschs von Peer-Funktionen

Die DRA muss explizit angeben, dass Diameter-Anwendungen wie Gx (16777238) und Rx (16777236) in CER- (Capabilities-Exchange-Request) und CEA-Nachrichten (Capabilities-Exchange-Answer) unterstützt werden.

Die Relay-Anwendung mit Application Identifier 0xffffffff wird von Cisco PCRF nicht unterstützt. Wenn nur die Relay-Anwendung (4294967295) und nicht Gx/Rx ausgetauscht wird, wird die Peer-Verbindung als Nur-Relay-Modus eingerichtet, und PCRF antwortet nicht auf CCR-I-Nachrichten.

Weitere Informationen finden Sie im Abschnitt Next Hop Routing im CPS Mobile Configuration Guide.

Best Practice:

Erfassen Sie während der Herstellung der Peer-Verbindung immer die pcap auf PCRF, um sicherzustellen, dass DRA eine CER-Nachricht (Capabilities-Exchange-Request) mit dem AVP-Auth-Application-ID-Wertesatz sendet Diameter-Anwendungen wie Gx (16777238) oder Rx (16777236) oder beide, und PCRF antwortet mit ähnlichen Werten in der CEA-Nachricht

(Capabilities-Exchange-Answer).

Abbildung 4: CER-Nachricht mit falschem Wert in Authentifizierungsanwendung-ID als Relay

```

Diameter Protocol
  Version: 0x01
  Length: 196
  > Flags: 0x80, Request
  Command Code: Capabilities-Exchange (257)
  ApplicationId: Diameter Common Messages (0)
  Hop-by-Hop Identifier: 0x5b2c55d3
  End-to-End Identifier: 0x171b0936
  [Answer In: 409]
  > AVP: Origin-Host(264) l=59 f=-M- val=[redacted]01ors.mnc[redacted].mcc[redacted].3gppnetwork.org
  > AVP: Origin-Realm(296) l=41 f=-M- val=epc.mnc084.mcc404.3gppnetwork.org
  > AVP: Host-IP-Address(257) l=14 f=-M- val=10.[redacted].[redacted].146
  > AVP: Vendor-Id(266) l=12 f=-M- val=323
  > AVP: Product-Name(269) l=20 f=--- val=Eagle XG DSR
  > AVP: Auth-Application-Id(258) l=12 f=-M- val=Relay (4294967295)
    AVP Code: 258 Auth-Application-Id
    > AVP Flags: 0x40, Mandatory: Set
    AVP Length: 12
    Auth-Application-Id: Relay (4294967295)
  > AVP: Firmware-Revision(267) l=12 f=--- val=6491648
```

Abbildung 4: CER-Nachricht mit falschem Wert in Authentifizierungs-Anwendungs-ID als Relay

Abbildung 5: CER-Meldung mit korrekten Werten in Auth-Anwendungs-ID: Gx und Rx

Command Code: Capabilities-Exchange (257)

ApplicationId: Diameter Common Messages (0)

Hop-by-Hop Identifier: 0x38370427

End-to-End Identifier: 0x0d3fbc01

[Answer In: 30]

```
> AVP: Origin-Host(264) l=60 f=-M- val=[REDACTED]drax01c[REDACTED].mnc084.mcc404.3gppnetwork.org
> AVP: Origin-Realm(296) l=41 f=-M- val=epc.mnc084.mcc404.3gppnetwork.org
> AVP: Host-IP-Address(257) l=14 f=-M- val=10.[REDACTED].[REDACTED].151
> AVP: Vendor-Id(266) l=12 f=-M- val=323
> AVP: Product-Name(269) l=20 f=--- val=Eagle XG DSR
✓ AVP: Vendor-Specific-Application-Id(260) l=32 f=-M-
  AVP Code: 260 Vendor-Specific-Application-Id
  > AVP Flags: 0x40, Mandatory: Set
  AVP Length: 32
  ✓ Vendor-Specific-Application-Id: 0000010a4000000c000028af000001024000000c01000014
    > AVP: Vendor-Id(266) l=12 f=-M- val=10415
    ✓ AVP: Auth-Application-Id(258) l=12 f=-M- val=3GPP Rx (16777236)
      AVP Code: 258 Auth-Application-Id
      > AVP Flags: 0x40, Mandatory: Set
      AVP Length: 12
      Auth-Application-Id: 3GPP Rx (16777236)
  ✓ AVP: Vendor-Specific-Application-Id(260) l=32 f=-M-
    AVP Code: 260 Vendor-Specific-Application-Id
    > AVP Flags: 0x40, Mandatory: Set
    AVP Length: 32
    ✓ Vendor-Specific-Application-Id: 0000010a4000000c000028af000001024000000c01000016
      > AVP: Vendor-Id(266) l=12 f=-M- val=10415
      > AVP: Auth-Application-Id(258) l=12 f=-M- val=3GPP Gx (16777238)
> AVP: Firmware-Revision(267) l=12 f=--- val=6557952
```

Abbildung 5: CER-Meldung mit korrekten Werten in Auth-Application-Id: Gx und Rx

Schritt 5: Stellen Sie sicher, dass der eindeutige Quellhostname für den Durchmesser an jedem Peerknoten für den Durchmesser definiert ist.

Cisco CPS PCRF unterstützt eine Umgebung, in der jeder verbundene Peer-Knoten einen eindeutigen Quellhostnamen mit Durchmesser benötigt.

Wenn die Migration für Durchmesser-Peer-Verbindungen von bestehenden direkten Gx- oder Rx-Verbindungen zu DRA-vermittelten Verbindungen erfolgen soll, muss die DRA-Verbindung für jede Diameter-Schnittstelle (Gx oder Rx) zwischen PCEF oder P-CSCF und DRA idealerweise einen eindeutigen Quell-Hostnamen für die Durchmesseranwendung (den Wert des AVP Origin-Hosts) verwenden, der sich von dem unterscheidet, der für direkte PCRF-Verbindungen mit demselben Peer-Knoten verwendet wird.

Dadurch wird sichergestellt, dass Anfragen von Peer-Knoten über die richtige DRA-Peer-Verbindung weitergeleitet werden und nicht verworfen werden, wenn in der Liste "PCRF show_peers.py" alte Einträge für direkte Verbindungen vorhanden sind.

Best Practice:

Wenn es nicht möglich ist, den Hostnamen für DRA-Verbindungen auf dem Peer zu ändern, führen Sie einen vollständigen Neustart aller vier QNS-Dienste nacheinander auf jeder VM des Lastenausgleichs durch, nachdem Sie direkte Peer-Verbindungen entfernt haben.

Dies würde sicherstellen, dass alte veraltete (Origin Host:) Einträge von Peers, die früher für die direkte Durchmesserschnittstelle (Gx/Rx) zwischen PCEF/P-CSCF und PCRF verwendet wurden, nicht mehr in der PCRF-Durchmesser-Peer-Verbindungsliste vorhanden sind und die Ausgabe von `show_peers.py` nur DRA-Peer-Verbindungen und somit eine ordnungsgemäße Weiterleitung von Durchmesseranwendungsnachrichten (z. B.: Gx_CCA-I, Gx_CCA-T) aus neu erzeugten Durchmesserverbindungen zwischen DRA und PCRF.



Anmerkung: Das Neustarten von QNS-Services auf LB-VMs beeinträchtigt den Datenverkehr und setzt alle Diameter-Peer-Verbindungen auf diesen QNS-Instanzen zurück. Führen Sie diesen Schritt während eines geplanten Wartungsfensters durch.

Schritt 6: Konfigurieren der Next-Hop-Routing-Tabelle für DRA-Peers

Diese Funktion ermöglicht die Zusammenarbeit mit einem DRA, der sich nicht im Topologie-Versteckmodus befindet. Wenn ein DRA eine Verbindung herstellt, meldet er seine eigenen Origin-Host- und Realm-Werte. Diameter-Anwendungsmeldungen verwenden jedoch den Ursprungs-Host und -Bereich (z. B. PCEF, TDF, AF) des tatsächlichen Anwendungshosts, sodass PCRF ermitteln muss, welche DRA-Verbindung für die Zustellung von Nachrichten an den richtigen Host verwendet werden soll.



Anmerkung: Die Next-Hop-Routing-Tabelle wird nur für PCRF-initiierte Anforderungen verwendet. Antworten auf eingehende Anfragen werden immer über die gleiche Verbindung gesendet, auf der sie empfangen wurden, um ein asymmetrisches Routing zu verhindern.

Diese Parameter können in der Next-Hop-Routing-Tabelle konfiguriert werden:

Parameter	Beschreibung
Next-Hop-Bereich	DRA-Bereichsname wie in Origin-Realm AVP in CER oder CEA empfangen Nachricht.

	 Anmerkung: Alle nächsten Hop-Realms (Next Hop Realm) müssen mit dem Wert für Origin-Realm A VP in der eingehenden CER/CEA-Nachricht übereinstimmen.
Next-Hop-Hosts	Namensliste des DRA-Hosts, wie in Origin-Host AVP in CER oder CEA empfangen Nachricht.  Anmerkung: Alle Next-Hop-Hostnamen (Next-Hop-Hosts) müssen mit dem Wert für Origin-Host A VP in der eingehenden CER/CEA-Nachricht übereinstimmen.
Anwendungs-ID	ID der Durchmesseranwendung, die von der DRA unterstützt wird. Es enthält Informationen, die den bestimmten Dienst identifizieren, den der Dienst Sitzung gehört zu.
Muster für Zielbereiche	Tatsächliches Namensmuster des Zielbereichs, wie in Origin-Realm AVP empfangen in AAR-Nachricht. Das Muster muss der Standard-Java-Standard sein. Ausdruckssyntax
Ziel-Host-Muster	Tatsächliches Muster des Ziel-Hostnamens, wie in Origin-Host AVP empfangen in AAR-Meldung. Das Muster muss ein Java-Standardmuster sein. konventionen. Das Muster muss der Standard-Java-Standard sein. Ausdruckssyntax

Best Practice:

Versuchen Sie stets, das richtige Regex-Muster (Platzhalterabgleich) zu verwenden, während Sie Einträge in der Spalte Zielrealmmuster und Zielhostmuster in

Next-Hop-Routing-Tabelle, um die Konfigurationseinträge für Gx- und Rx-Peers mit mehreren Verbindungen zu minimieren und Konfigurationsfehler zu vermeiden.



Anmerkung: Detaillierte Konfigurationsanleitungen finden Sie im CPS Mobile Configuration Guide, Release 25.1.0, im Abschnitt Next Hop Routing.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.