

Usa guida alla configurazione per l'integrazione DRA multifornitore

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Procedura di configurazione e best practice](#)

[Passaggio 1: Determinare la modalità di connettività DRA \(peer in entrata e in uscita\)](#)

[Passaggio 2: Configura peer in ingresso in Generatore criteri](#)

[Passaggio 3: Configurazione di AVP Host-IP-Address](#)

[Passaggio 4: Convalida funzionalità peer Exchange](#)

[Passaggio 5: Accertarsi che il nome host di origine univoco del diametro sia definito in ogni nodo peer del diametro](#)

[Passaggio 6: configurare la tabella di routing dell'hop successivo per i peer DRA](#)

Introduzione

In questo documento vengono descritti i passaggi della configurazione e le best practice per l'integrazione DRA multi-vendor con cluster PCRF Cisco Policy Suite (CPS).

Prerequisiti

Requisiti

Cisco consiglia ai tecnici che utilizzano questa soluzione di avere familiarità con gli argomenti seguenti:

- Sistema operativo Linux
- Piattaforma Cisco Policy Suite (CPS) e architettura cluster
- Funzione PCRF (Policy and Charging Rules)
- Uso del direttore Vi
- Strumento di analisi della rete Wireshark

Componenti usati

Il riferimento delle informazioni contenute in questo documento è la versione CPS 25.1 e AlmaLinux 8.10.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Procedura di configurazione e best practice

Passaggio 1: Determinare la modalità di connettività DRA (peer in entrata e in uscita)

- Peer in ingresso: Il PCRF è configurato per accettare le richieste di connessione dai peer Diameter designati. Il nodo peer avvia Diameter Capabilities-Exchange-Request (CER) per il PCRF.
- Peer in uscita: Il PCRF è configurato per avviare la CER verso i relativi peer.

Procedure ottimali:

Per la maggior parte delle integrazioni DRA multi-vendor, configurare il DRA come un peer in entrata, dove il DRA avvia il CER al PCRF.

Passaggio 2: Configura peer in ingresso in Generatore criteri

Nell'interfaccia utente di Policy Builder, configurare il nome peer in ingresso e l'area di autenticazione peer, facendo riferimento alle tabelle Peer e Aree di autenticazione in ingresso.



Nota: Per una descrizione dettagliata dei parametri, consultate la guida alla configurazione di CPS Mobile, versione 25.1.0, nella sezione Configurazione stack diametro.

Questi parametri possono essere configurati in Peer in ingresso:

Tabella Peer

Parametro	Descrizione
Peer	Definisce i nomi dei peer autorizzati ad avviare connessioni verso PCRF.
Nome host locale	Identifica il nome host locale del Policy Director (load balancer) che identifica e consente una connessione in ingresso dal peer.
Numero istanza	Indica il numero assegnato al processo di Policy Server (QNS) che avvia una connessione con il peer in uscita.
	 Nota: È necessario specificare il nome dell'host locale e il numero dell'istanza se l'intenzione è solo un singolo processo di Policy Server (QNS) in Policy Builder (bilanciamento del carico) per consentire/avviare una connessione con il peer specificato. Il numero dell'istanza può essere mantenuto come 0. In questo caso, tutti i processi di Policy Server (QNS) in Policy Director (bilanciamento del carico) tenteranno/consentiranno la connessione con il peer. Il valore predefinito è 0.
Rating	Priorità assegnata al peer per il recapito di una richiesta avviata da PCRF. OSPF (Open Shortest Path First) più alto è il valore di valutazione, maggiore è la priorità assegnata al peer. Il valore predefinito è 1.
Intervallo porte	Deve essere specificato solo quando la connessione di trasporto sottostante è SCTP e non è obbligatorio quando lo stesso è TCP .

Timeout risposta	Cisco consiglia di non utilizzare questo parametro.
Modello nome	Origin-Host Un valore VP in CER deve essere convalidato in base a questo modello in per stabilire la connessione. Se ciò non accade, la CER viene eliminato automaticamente e la connessione TCP viene reimpostata da PCRF. Il controllo del modello di nome non viene eseguito se l'opzione Accetta peer non definito descritta in Configurazione dello stack del diametro. Il modello di nome deve essere l'espressione regolare Java standard qui descritta.

Tabella Realm

Parametro	Descrizione
Realm	Definisce i realm peer a cui è consentito avviare connessioni PCRF
Tipo peer	Non utilizzata con i realm in ingresso.
Protocollo di elaborazione	Mapping tra il nome dell'area di autenticazione e la logica PCRF specifica in grado di per ulteriori informazioni sul protocollo di elaborazione. Quando si importa uno stack di diametri con un realm di diametro senza protocollo assegnato, il valore predefinito è GX_TGPP.
Rating	Priorità assegnata al realm per il recapito di una richiesta avviata da PCRF. Questo

	viene utilizzato solo con il protocollo di elaborazione SY_PRIME. Il valore predefinito è 0. Più basso è il valore di valutazione, maggiore è la priorità assegnata al realm. Ad esempio, un realm con Rating=10 viene utilizzato dopo un realm con Rating=1.
Alias statistiche	Qualunque siano le statistiche generate per il rispettivo realm, nome configurato nell'alias Statistiche accodato a tali statistiche. Questa opzione è valida solo per le statistiche mbean com.broadhop.message.
Modello nome	Un valore VP nel CER deve essere convalidato rispetto a questo modello in per l'elaborazione del messaggio in ingresso. In caso contrario, il messaggio viene scartato automaticamente e la connessione TCP viene reimpostata da PCRF. Il modello di nome deve essere l'espressione regolare Java standard qui descritta.

Procedure ottimali:

Per un controllo più granulare, configurare voci specifiche di peer e realm in base ai requisiti, inoltre per consentire la creazione di peer solo da peer specifici deselezionare il peer accettato non definito.

Esempio:

Figura 1: Tabella Peer in ingresso

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**

***Realm**

☐ Accept Undefined Peer

Settings

Inbound Peers

Peers

Local Host Name	Instance Number	*Rating	Port Range	*Response Timeout	*Name Pattern
	0	1		[redacted]	*[redacted]*

Realms

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

Figura 1: Tabella Peer in ingresso

Passaggio 3: Configurazione di AVP Host-IP-Address

L'AVP (Diameter Host-IP-Address) comunica l'indirizzo IP del nodo durante gli scambi CER/CEA (RFC 3588) per le connessioni basate su SCTP. In Cisco CPS PCRF, questo indirizzo è per impostazione predefinita l'indirizzo IP dell'interfaccia interna, che è diverso dall'indirizzo IP del servizio del diametro previsto per alcuni fornitori DRA.

In Cisco CPS PCRF, è possibile utilizzare l'indirizzo IP virtuale del load balancer (LbVIP) o l'indirizzo IP fisico delle macchine virtuali del load balancer come indirizzo IP diametro-origine-endpoint.

Per impostazione predefinita, l'indirizzo IP dell'interfaccia interna viene comunicato come indirizzo IP dell'host nei messaggi CER/CEA del diametro, come mostrato nella figura, dove l'indirizzo IP di origine nell'acquisizione è diverso dall'indirizzo IP visualizzato nell'AVP dell'indirizzo IP dell'host.

Figura 2: Messaggio CEA con IP interno come indirizzo IP host

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)						

Figura 2: Messaggio CEA con IP interno come indirizzo IP host

Sebbene questo protocollo AVP non sia obbligatorio quando il protocollo TCP viene utilizzato come protocollo di trasporto (fare riferimento alla RFC 3588), alcuni fornitori DRA fanno riferimento a questo protocollo AVP durante la creazione della connessione Diameter e si aspettano l'IP del servizio Diameter di PCRF invece dell'IP interno. Se questa aspettativa non viene soddisfatta, i pari non riusciranno a stabilire.

Procedure ottimali:

Per annunciare l'IP del servizio Diameter nell'AVP Host-IP-Address da PCRF, aggiornare il file /etc/hosts con una voce che associa l'FQDN di origine PCRF (come definito nello stack del diametro per gli endpoint locali) all'indirizzo IP desiderato.



Nota: Per ulteriori informazioni, fate riferimento alle tabelle degli endpoint locali nella guida alla configurazione di CPS Mobile, versione 25.1.0, nella sezione Configurazione stack diametro (Diameter Stack Configuration).

Per aggiornare le voci di host aggiuntivi in Openstack basato su CPS PCRF:

- Verificare che il cluster CPS sia distribuito.

curl -X GET [programma di installazione API](#).

- Recuperare e aggiornare il file additional-hosts.yaml tramite l'API REST.

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

- Applicare le modifiche con i comandi curl come descritto nella documentazione del prodotto.

```
curl -X PUT API system host aggiuntivi -H "Content-Type: application/yaml" —binario dati @additional-hosts.yaml
```

Al termine di questa chiamata API, Gestione cluster viene configurato con il nuovo file /etc/hostsfile e tutte le altre VM distribuite vengono quindi aggiornate in modo asincrono.



Nota: Per istruzioni dettagliate, consultare la guida all'installazione di CPS per OpenStack, sezione Orchestration API.

Per aggiornare le voci relative agli host aggiuntivi in VMware CPS PCRF:

- Aggiungere la voce nel file AdditionalHosts.csv nel percorso /var/qps/config/deploy/csv/
- Per importare le modifiche nella macchina virtuale di Cluster Manager:

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

- Applica modifiche da Gestione cluster:

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

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



Nota: Per istruzioni dettagliate, fare riferimento alla Guida all'installazione di CPS per VMware, sezione Configurazione host aggiuntivi.

Esempio:

Figura 3: Punti finali locali dello stack di diametro GUI

*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 ↕ ↕

Figura 3: Punti finali locali dello stack di diametro GUI

Esempio di voce /etc/hosts:

<#root>

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

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

Passaggio 4: Convalida funzionalità peer Exchange

DRA deve pubblicizzare esplicitamente il supporto per le applicazioni Diameter come Gx (16777238) e Rx (16777236) nei messaggi Capabilities-Exchange-Request (CER) e Capabilities-Exchange-Answer (CEA).

L'applicazione Relay, con identificatore applicazione 0xffffffff, non è supportata da Cisco PCRF. Se viene scambiata solo l'applicazione Relay (4294967295) e non Gx/Rx, la connessione peer verrà stabilita come modalità solo relay e PCRF non risponderà ai messaggi CCR-I.

Per ulteriori informazioni, consultare la sezione Next Hop Routing nella CPS Mobile Configuration Guide.

Procedure ottimali:

Durante la fase di definizione della connessione peer, acquisire sempre il cappuccio sul PCRF per assicurarsi che DRA invii il messaggio di diametro Capabilities-Exchange-Request (CER) con il valore AVP Auth-Application-ID impostato Applicazioni di diametro come Gx (16777238) o Rx (16777236) o entrambi e PCRF risponda con valori simili nel messaggio Capabilities-Exchange-

Answer (CEA).

Figura 4: Messaggio CER con valore errato in Auth-Application-Id come inoltro

```

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
```

Figura 4: Messaggio CER con valore errato in Auth-Application-Id come Relay

Figura 5: messaggio CER con valori corretti in Auth-Application-Id: Gx e 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]drax016[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
```

Figura 5: messaggio CER con valori corretti in Auth-Application-Id: Gx e Rx

Passaggio 5: Accertarsi che il nome host di origine univoco del diametro sia definito in ogni nodo peer del diametro

Cisco CPS PCRF supporta un ambiente in cui ogni nodo peer connesso richiede un nome host di origine di diametro univoco.

Se la migrazione deve essere eseguita per connessioni peer con diametro da una connettività Gx o Rx diretta esistente a collegamenti DRA, il collegamento DRA per ciascuna interfaccia Diameter (Gx o Rx) tra PCEF o P-CSCF e DRA idealmente deve utilizzare un nome host di origine univoco per l'applicazione del diametro (il valore dell'host di origine AVP) che sia diverso da quello utilizzato per la connettività PCRF diretta con lo stesso nodo peer.

In questo modo, le richieste provenienti dai nodi peer vengono instradate attraverso il collegamento peer DRA corretto e non eliminate se nell'elenco PCRF show_peers.py sono presenti voci di collegamento diretto verso il basso precedenti.

Procedura consigliata:

Se non è possibile modificare il nome host per i collegamenti DRA sul peer, eseguire un riavvio completo di tutti e quattro i servizi QNS in sequenza su ciascuna VM del load balancer dopo aver rimosso i collegamenti peer diretti.

In questo modo le voci obsolete (host origine:) dei peer utilizzate in precedenza per l'interfaccia a diametro diretto (Gx/Rx) tra PCEF/P-CSCF e PCRF non saranno più presenti nell'elenco di connessioni peer con diametro PCRF e l'output `show_peers.py` disporrà solo di connessioni peer DRA e quindi del routing corretto dei messaggi di applicazione del diametro (ad esempio: Gx_CCA-I, Gx_CCA-T) dai collegamenti di diametro appena creati tra DRA e PCRF.



Nota: Il riavvio dei servizi QNS su VM LB ha un impatto sul traffico e reimposta tutte le connessioni peer con diametro su tali istanze QNS. Eseguire questo passaggio durante un intervento di manutenzione pianificato.

Passaggio 6: configurare la tabella di routing dell'hop successivo per i peer DRA

Questa funzionalità consente l'interazione con un DRA che non è in modalità di nascondere la topologia. Quando un DRA stabilisce una connessione, annuncia i propri valori Origin-Host e Realm. Tuttavia, i messaggi dell'applicazione Diameter utilizzano l'host di origine e il realm (ad esempio, PCEF, TDF, AF) dell'host dell'applicazione effettivo, quindi PCRF deve determinare la connessione DRA da utilizzare per il recapito dei messaggi all'host corretto.



Nota: La tabella Route hop successivo viene utilizzata solo per le richieste avviate da PCRF. Le risposte alle richieste in ingresso vengono sempre inviate tramite la stessa connessione su cui sono state ricevute, per evitare il routing asimmetrico.

È possibile configurare questi parametri nella tabella Routing hop successivo:

Parametro	Descrizione
Area autenticazione hop successivo	Nome area DRA ricevuto in Origin-Realm AVP in CER o CEA messaggio.

	Nota: Tutti i realm hop successivi (realm hop successivo) devono corrispondere al valore VP Origin-Realm A nel messaggio CER/CEA in ingresso.
Host hop successivo	Elenco dei nomi host DRA ricevuti in AVP host di origine in CER o CEA messaggio.  Nota: Tutti i nomi host dell'hop successivo (Host hop successivo) devono corrispondere al valore VP Origin-Host A nel messaggio CER/CEA in arrivo.
ID applicazione	ID applicazione Diameter annunciato come supportato da DRA. IT contiene informazioni che identificano il servizio specifico che il servizio sessione di.
Pattern realm di destinazione	Modello nome area di autenticazione di destinazione effettivo ricevuto in AVP area di autenticazione di origine nel messaggio AAR. Il pattern deve essere il normale standard Java sintassi dell'espressione.
Modello host di destinazione	Modello di nome host di destinazione effettivo ricevuto in AVP host di origine in Messaggio AAR. Il modello deve essere un modello Java standard convenzioni. Il pattern deve essere il normale standard Java sintassi dell'espressione.

Procedure ottimali:

Cercare sempre di utilizzare il modello regex corretto (corrispondenza con caratteri jolly) durante la creazione di voci nelle colonne Modello realm di destinazione e Modello host di destinazione in

Tabella Next Hop Routing per ridurre al minimo le voci di configurazione per più connessioni peer Gx e Rx e prevenire errori di configurazione.



Nota: Per ulteriori informazioni sulla configurazione, consultare la guida alla configurazione di CPS Mobile, versione 25.1.0, nella sezione Next Hop Routing.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).