

Use o Guia de configuração para integração de DRA de vários fornecedores

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Etapas de configuração e práticas recomendadas](#)

[Passo 1: Determine o modo de conectividade DRA \(pares de entrada versus de saída\)](#)

[Passo 2: Configurar Par de Entrada no Construtor de Políticas](#)

[Passo 3: Configurar Host-IP-Address AVP](#)

[Passo 4: Validar Intercâmbio de Recursos de Par](#)

[Passo 5: Verifique se o nome de host de origem exclusivo do diâmetro está definido em cada nó de par de diâmetro](#)

[Etapa 6: Configure a tabela de roteamento de próximo salto para pares DRA](#)

Introdução

Este documento descreve as etapas de configuração juntamente com as práticas recomendadas para integração de DRA de vários fornecedores com o cluster PCRF do Cisco Policy Suite (CPS).

Pré-requisitos

Requisitos

A Cisco recomenda que os engenheiros que trabalham com esta solução tenham familiaridade com estes tópicos:

- sistema operacional Linux
- Plataforma e arquitetura de cluster do Cisco Policy Suite (CPS)
- Policy and Charging Rules Function (PCRF) (Função de política e regras de tarifação)
- Uso do editor Vi
- Ferramenta de análise de rede Wireshark

Componentes Utilizados

As informações neste documento são baseadas no CPS 25.1 e no AlmaLinux versão 8.10.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Etapas de configuração e práticas recomendadas

Passo 1: Determine o modo de conectividade DRA (pares de entrada versus de saída)

- Pares de Entrada: O PCRF é configurado para aceitar solicitações de conexão de pares de Diâmetro designados. O nó par inicia os recursos de diâmetro - solicitação de troca (CER) para o PCRF.
- Pares de Saída: O PCRF é configurado para iniciar o CER em relação aos seus pares.

Prática recomendada:

Para a maioria das integrações DRA de vários fornecedores, configure o DRA como um ponto de entrada, onde o DRA inicia o CER para o PCRF.

Passo 2: Configurar Par de Entrada no Construtor de Políticas

Na GUI do Policy Builder, configure o nome do peer de entrada e o realm do peer, fazendo referência às tabelas de Peers de Entrada e Realms.



Note: Para obter descrições detalhadas dos parâmetros, consulte o Guia de configuração do CPS Mobile, versão 25.1.0, na seção Configuração da pilha de diâmetro.

Esses parâmetros podem ser configurados em Inbound Peers:

Tabela de Pares

Parâmetro	Descrição
Pares	Define quais nomes de peer podem iniciar conexões para PCRF.
Nome do host local	Identifica o nome do host local do Diretor de Políticas (balanceador de carga) que identifica e permite uma conexão de entrada do Peer.
Número da instância	Indica o número atribuído do processo do Servidor de Políticas (QNS) que inicia uma conexão com o Par de Saída.  Note: O Nome do Host Local e o Número da Instância devem ser especificados se a intenção for apenas um único processo do Servidor de Políticas (QNS) no Construtor de Políticas (balanceador de carga) para permitir/iniciar uma conexão com o correspondente. Caso contrário, o número da Instância pode ser mantido como 0. Nesse caso, todos os processos do Servidor de Políticas (QNS) no Diretor de Políticas (balanceador de carga) devem tentar/permitir a conexão com o correspondente. O valor padrão é 0.
Classificação	Prioridade atribuída a este peer para entrega de uma solicitação iniciada por PCRF. O maior o valor de classificação, maior é a prioridade atribuída ao peer. O valor padrão é 1.
Intervalo de portas	Deve ser especificado somente quando a conexão de transporte subjacente é SCTP e não é necessário quando o mesmo é o TCP .

Tempo Limite de Resposta	A Cisco recomenda não usar esse parâmetro.
Padrão de nome	O valor de VP do Host de Origem A no CER precisa ser validado em relação a esse padrão no para que a conexão seja estabelecida. Se isso não acontecer, o CER é descartado silenciosamente e a conexão TCP é redefinida por PCRF. A verificação do padrão de nome não ocorrerá se a opção Aceitar Par Indefinido descrito em Configuração da pilha de diâmetro. O padrão de nome precisa ser a expressão regular Java padrão a sintaxe descrita aqui.

Tabela Realms

Parâmetro	Descrição
Territórios	Define em quais territórios de peer é permitido iniciar conexões PCRF.
Tipo de Par	Não usado com realms de entrada.
Protocolo de processamento	O mapeamento entre o nome do território e a lógica de PCRF especifica que pode ser aplicado à mensagem, para obter mais informações sobre o protocolo de processamento. Quando uma Pilha de diâmetro com um domínio de diâmetro é importada sem protocolo atribuído, ele assume o valor padrão como GX_TGPP .
Classificação	Prioridade atribuída a este território para entrega de uma solicitação

	iniciada por PCRF. Este é usado somente com o protocolo de processamento SY_PRIME. O valor padrão é 0. Quanto menor o valor da classificação, maior será a prioridade atribuída ao território. Por exemplo, um território com Classificação=10 é usado depois de um território com Classificação=1.
Alias de Estatísticas	Quaisquer que sejam as estatísticas geradas para o respectivo território, nome configurado em Alias de estatísticas anexado a essas estatísticas. Aplicável somente para estatísticas mbean com.broadhop.message.
Padrão de nome	Território de origem Um valor VP no CER precisa ser validado em relação a esse padrão no para que a mensagem recebida seja processada. Se isso não acontecer, a mensagem é descartada silenciosamente e a conexão TCP é redefinida por PCRF. O padrão de nome precisa ser a expressão regular Java padrão a sintaxe descrita aqui.

Prática recomendada:

Para um controle mais granular, configure as entradas específicas de peer e realm conforme o requisito, também para permitir a criação de peer somente de peers específicos desmarque a opção Accept Undefined Peer.

Exemplo:

Figura 1: Tabela de Correspondentes de Entrada

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[REDACTED].mcc[REDACTED].3gppnetwork

☐ Accept Undefined Peer

Settings

Inbound Peers

Peers

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

Add
Remove
↑
↓

Realms

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

Figura 1: Tabela de Correspondentes de Entrada

Passo 3: Configurar Host-IP-Address AVP

O Diameter Host-IP-Address AVP comunica o endereço IP do nó durante trocas de CER/CEA (RFC 3588) para conexões baseadas em SCTP. No Cisco CPS PCRF, esse endereço é, por padrão, o IP da interface interna, que é diferente do IP do serviço Diameter esperado para determinados fornecedores de DRA.

No Cisco CPS PCRF, você pode usar o IP Virtual do Balanceador de Carga (LbVIP) ou o IP físico das VMs do balanceador de carga como o IP do ponto final da origem do diâmetro.

Por padrão, o IP da interface interna é comunicado como o Host-IP-Address em mensagens de Diâmetro CER/CEA como mostrado na figura, onde é possível ver que o IP de origem na captura é diferente do IP visto no Host-IP-Address AVP.

Figura 2: Mensagem CEA com IP interno como endereço IP do 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 (10.10.10.130), Dst: DRA IP (10.10.10.18)						
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.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=192.168.12 (192.168.12)						
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: Mensagem CEA com IP interno como endereço IP do host

Embora este AVP não seja obrigatório quando o TCP é usado como protocolo de transporte (consulte RFC 3588), alguns fornecedores de DRA referem-se a este AVP ao estabelecer a conexão de Diâmetro e esperam o IP de serviço de Diâmetro de PCRF em vez do IP interno. Se essa expectativa não for atendida, os correspondentes não conseguirão estabelecer.

Prática recomendada:

Para anunciar o IP do serviço Diameter no Host-IP-Address AVP do PCRF, atualize o arquivo /etc/hosts com uma entrada que mapeia o FQDN de origem do PCRF (conforme definido nos Pontos de Extremidade Locais da Pilha de Diâmetro) para o endereço IP desejado.



Note: Consulte as tabelas de endpoints locais no Guia de configuração do CPS Mobile, versão 25.1.0, na seção Configuração da pilha de diâmetro para obter mais detalhes.

Para atualizar entradas de hosts adicionais no CPS PCRF baseado em Openstack:

- Verifique se o cluster do CPS está em um estado implantado.

curl -X [sistema de API do instalador](#) GET.

- Recupere e atualize o arquivo `additional-hosts.yaml` via API REST.

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

- Aplique alterações com comandos `curl`, conforme descrito na documentação do produto.

```
curl -X PUT sistema de API hosts adicionais -H "Tipo de conteúdo: application/yaml" — data-  
binary @additional-hosts.yaml
```

Quando essa chamada de API é concluída, o Cluster Manager é configurado com o novo arquivo de host `/etc/e` e todas as outras VMs implantadas são atualizadas de forma assíncrona.



Note: Para obter instruções detalhadas, consulte o Guia de instalação do CPS para OpenStack, seção *Orchestration API*.

Para atualizar entradas de hosts adicionais no CPS PCRF baseado em Vmware:

- Adicione a entrada no arquivo `AdditionalHosts.csv` localizado no caminho `/var/qps/config/deploy/csv/`
- Para importar alterações para a VM do Cluster Manager:

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

- Aplicar alterações do Gerenciador de Cluster:

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

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



Note: Para obter instruções detalhadas, consulte o Guia de instalação do CPS para VMware, seção *Configuração adicional de hosts*.

Exemplo:

Figura 3: Pontos finais locais da pilha de diâmetro da 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: Pontos finais locais da pilha de diâmetro da GUI

Exemplo de entrada /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 ~]#
```

Passo 4: Validar Intercâmbio de Recursos de Par

O DRA deve anunciar explicitamente o suporte para aplicações de Diâmetro como Gx (16777238) e Rx (16777236) em mensagens Capabilities-Exchange-Request (CER) e Capabilities-Exchange-Answer (CEA).

O aplicativo Relay, com Identificador de Aplicativo 0xffffffff, não é suportado pelo Cisco PCRF. Se apenas o aplicativo Relay (4294967295) for trocado e não Gx/Rx, a conexão de peer será estabelecida como modo somente relay e o PCRF não responderá às mensagens CCR-I.

Consulte a seção Roteamento do próximo salto no Guia de configuração do CPS Mobile para obter mais detalhes.

Prática recomendada:

Durante a fase de estabelecimento da conexão de peer, sempre capture o pcap no PCRF para garantir que o DRA esteja enviando a mensagem Capabilities-Exchange-Request (CER) de diâmetro com o conjunto de valores AVP Auth-Application-ID Aplicativos de diâmetro como Gx (16777238) ou Rx (16777236) ou ambos e o PCRF esteja respondendo com valores semelhantes na mensagem Capabilities-Exchange-Answer (CEA).

Figura 4: Mensagem CER com valor incorreto em Auth-Application-Id como retransmissão

```

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: Mensagem CER com valor incorreto em Auth-Application-Id como Relay

Figura 5: Mensagem CER com valores corretos em 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]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
```

Figura 5: Mensagem CER com valores corretos em Auth-Application-Id: Gx e Rx

Passo 5: Verifique se o nome de host de origem exclusivo do diâmetro está definido em cada nó de par de diâmetro

O Cisco CPS PCRF é compatível com um ambiente em que cada nó de peer conectado requer um nome de host de origem de diâmetro exclusivo.

Se a migração tiver que ser feita para conexões de pares de diâmetro da conectividade direta Gx ou Rx existente para links mediados por DRA, o link DRA para cada interface de Diâmetro (Gx ou Rx) entre PCEF ou P-CSCF e DRA idealmente deve usar um nome de host de origem exclusivo para aplicação de diâmetro (o valor do AVP Origin-Host) que seria diferente do usado para conectividade direta PCRF com o mesmo nó de pares.

Isso garante que as solicitações dos nós de peer sejam roteadas através do link de peer correto do DRA e não sejam descartadas se entradas de link direto antigas estiverem presentes na lista show_peers.py do PCRF.

Práticas recomendadas:

Se não for viável alterar o nome de host para links DRA no peer, execute uma reinicialização completa de todos os quatro serviços QNS sequencialmente em cada VM do balanceador de carga após remover os links diretos do peer.

Isso garantiria que as entradas obsoletas antigas (Origin host:) de pares usados anteriormente para a interface de diâmetro direto (Gx/Rx) entre PCEF/P-CSCF e PCRF não estivessem mais presentes na lista de conexão de pares de diâmetro PCRF, e a saída show_peers.py teria apenas conexões de pares DRA e, portanto, o roteamento adequado de mensagens de aplicação de diâmetro (por exemplo: Gx_CCA-I, Gx_CCA-T) a partir de links de diâmetro recém-criados entre DRA e PCRF.



Note: A reinicialização de serviços QNS em VMs LB está afetando o tráfego e redefine todas as conexões do par de Diâmetro nessas instâncias QNS. Execute esta etapa durante uma janela de manutenção planejada.

Etapa 6: Configure a tabela de roteamento de próximo salto para pares DRA

Este recurso permite o interfuncionamento com um DRA que não esteja no modo de ocultação de topologia. Quando um DRA estabelece uma conexão, ele anuncia seus próprios valores de Origin-Host e Realm. No entanto, as mensagens do aplicativo Diâmetro usam o Origin-Host e o Realm (por exemplo, PCEF, TDF, AF) do host real do aplicativo, portanto o PCRF precisa determinar qual conexão DRA usar para enviar mensagens ao host correto.



Note: A tabela Rotas de próximo salto é usada apenas para solicitações iniciadas por PCRF. As respostas às solicitações de entrada são sempre enviadas pela mesma conexão em que foram recebidas, para evitar o roteamento assimétrico.

Esses parâmetros podem ser configurados na tabela de roteamento de próximo salto:

Parâmetro	Descrição
Território do Próximo Salto	Nome de território DRA como recebido no AVP de território de origem no CER ou CEA mensagem.

	 Note: Todos os territórios do próximo salto (Território do próximo salto) devem corresponder ao valor de VP do Território de Origem A na mensagem CER/CEA recebida.
Hosts do Próximo Salto	Lista de nomes de hosts de DRA como recebido no AVP de origem-host no CER ou CEA mensagem.  Note: Todos os nomes de host do próximo salto (Hosts do próximo salto) devem corresponder ao valor de VP do host de origem A na mensagem CER/CEA recebida.
ID do aplicativo	ID do aplicativo de diâmetro anunciado como sendo suportado pelo DRA. Ela contém informações que identificam o serviço específico que o serviço à qual a sessão pertence.
Padrão de territórios de destino	Padrão de nome do território de destino real conforme recebido no AVP do Território de Origem na mensagem AAR. O padrão precisa ser o padrão Java regular sintaxe de expressão.
Padrão de host de destino	O padrão do nome do host de destino real conforme recebido no AVP do Host de Origem em mensagem AAR. O padrão precisa ser padrão Java convenções. O padrão precisa ser o padrão Java regular sintaxe de expressão.

Prática recomendada:

Sempre tente usar o padrão regex correto (correspondência de curingas) ao criar entradas nas colunas Destination Realms Pattern e Destination Host Pattern no

Tabela de roteamento de próximo salto para minimizar entradas de configuração para pares Gx e Rx várias conexões e evitar erros de configuração.



Note: Consulte o Guia de configuração do CPS Mobile, versão 25.1.0, na seção Roteamento do próximo salto, para obter orientações detalhadas sobre a configuração.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.