

Utilice la guía de configuración para la integración de DRA de varios proveedores

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Pasos de configuración y prácticas recomendadas](#)

[Paso 1: Determinación del modo de conectividad DRA \(pares entrantes frente a salientes\)](#)

[Paso 2: Configuración de Peer Entrante en Policy Builder](#)

[Paso 3: Configurar AVP de dirección IP de host](#)

[Paso 4: Validar intercambio de capacidades entre pares](#)

[Paso 5: Asegúrese de que el nombre de host de origen único de diámetro esté definido en cada nodo de par de diámetro](#)

[Paso 6: Configuración de la Tabla de Ruteo de Siguiente Salto para Peers DRA](#)

Introducción

Este documento describe los pasos de configuración junto con las prácticas recomendadas para la integración de DRA de varios proveedores con el clúster PCRF de Cisco Policy Suite (CPS).

Prerequisites

Requirements

Cisco recomienda que los ingenieros que trabajen con esta solución se familiaricen con los siguientes temas:

- Sistema operativo Linux
- Arquitectura de clúster y plataforma Cisco Policy Suite (CPS)
- Función de reglas de cobro y políticas (PCRF)
- Uso del editor Vi
- Herramienta de análisis de red Wireshark

Componentes Utilizados

La información de este documento se basa en la versión 25.1 de CPS y en la versión 8.10 de AlmaLinux.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Pasos de configuración y prácticas recomendadas

Paso 1: Determinación del modo de conectividad DRA (pares entrantes frente a salientes)

- Peers entrantes: PCRF está configurado para aceptar solicitudes de conexión de pares Diámetro designados. El nodo de peer inicia la solicitud de intercambio de capacidades de diámetro (CER) a PCRF.
- Peers salientes: La PCRF se configura para iniciar la CER hacia sus pares.

Práctica recomendada:

Para la mayoría de las integraciones DRA de múltiples proveedores, configure el DRA como un Peer entrante, donde el DRA inicia la CER a la PCRF.

Paso 2: Configuración de Peer Entrante en Policy Builder

Dentro de la GUI del Policy Builder, configure el nombre de peer entrante y el rango de peer, haciendo referencia a las tablas de Peers y rangos entrantes.



Nota: Para obtener descripciones detalladas de los parámetros, consulte la Guía de configuración móvil de CPS, versión 25.1.0, en la sección Configuración de pila de diámetro.

Estos parámetros se pueden configurar en Peers entrantes:

Tabla Peers

Parámetro	Descripción
Pares	Define qué nombres de peer están permitidos para iniciar conexiones hacia PCRF.
Nombre de host local	Identifica el nombre de host local del director de políticas (equilibrador de carga) que identifica y permite una conexión entrante del par.
Número de instancia	Indica el número asignado del proceso de Policy Server (QNS) que inicia una conexión con el par de salida.  Nota: Se deben especificar el nombre de host local y el número de instancia si la intención es que solo un proceso de Policy Server (QNS) en el Policy Builder (equilibrador de carga) permita o inicie una conexión con dicho par. El número de instancia se puede mantener como 0. En este caso, todos los procesos de Policy Server (QNS) en el Policy Director (equilibrador de carga) intentarán/permitirán la conexión con el par. El valor predeterminado es 0.
Calificación	Prioridad asignada a este par para entregar una solicitud iniciada mediante PCRF. cuanto mayor sea el valor de clasificación, mayor será la prioridad asignada al par. El valor predeterminado es 1.
Intervalo de puertos	Sólo se debe especificar cuando la conexión de transporte subyacente es SCTP y no es necesario cuando el mismo es TCP .

Tiempo de respuesta	Cisco recomienda no utilizar este parámetro.
Patrón de nombre	El valor de VP de Host de origen en CER debe validarse con este patrón en orden para establecer la conexión. Si eso no sucede, la RCE se descarta silenciosamente y PCRF restablece la conexión TCP. La verificación del patrón de nombre no se realiza si la opción Aceptar par no definido se describe en Configuración de pila de diámetro. El patrón de nombres debe ser la expresión regular estándar de Java sintaxis aquí descrita.

Tabla de rangos

Parámetro	Descripción
Dominios	Define a qué rangos de peer se les permite iniciar conexiones hacia PCRF.
Tipo de peer	No se utiliza con reinos entrantes.
Protocolo de procesamiento	Asignación entre el nombre de rango y la lógica PCRF específica que puede para el mensaje, para obtener más información sobre el procesamiento del protocolo. Cuando se importa una pila de diámetro con un rango de diámetro sin protocolo asignado, toma el valor predeterminado como GX_TGPP .
Calificación	Prioridad asignada a este rango para entregar una solicitud iniciada por

	PCRF. Esto sólo se utiliza con el protocolo de procesamiento SY_PRIME. El valor predeterminado es 0. Cuanto más bajo sea el valor de clasificación, más alta será la prioridad asignada al rango. Por ejemplo, un rango con Rating=10 se utiliza después de que un rango tenga Valoración=1.
Alias de estadísticas	Cualesquiera que sean las estadísticas que se generen para el respectivo rango, se obtiene el nombre configurado en el alias de estadísticas anexo a esas estadísticas. Esto es aplicable solamente para las estadísticas de mbean de com.broadhop.message.
Patrón de nombre	Origen-Rango Un valor VP en CER debe validarse con este patrón en orden para que se procese el mensaje entrante. Si eso no sucede, el mensaje se descarta silenciosamente y PCRF reinicia la conexión TCP. El patrón de nombres debe ser la expresión regular estándar de Java sintaxis aquí descrita.

Práctica recomendada:

Para un control más granular, configure las entradas specific peer y realm según los requisitos, también para permitir la creación de peer solamente de peers específicos y desmarque la opción Accept Undefined Peer.

Ejemplo:

Figura 1: Tabla de Peers entrantes

*Name

Lab-PCRf

***Realm**

pcrf.mnc[REDACTED].mcc[REDACTED].3gppnetwoi

☐ Accept Undefined Peer

Settings

Inbound Peers

Peers

Local Host Name	Instance Number	*Rating	Port Range	*Response Timeout	*Name Pattern
	<u>0</u>	<u>1</u>		<u>■</u>	<u>. * ■ *</u>

Add Remove ↑ ↓

Realms

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

Figura 2: Mensaje CEA con IP interna como dirección IP de 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 (10.1.1.130), Dst: DRA IP (10.1.1.18)						
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=192.168.1.12 (192.168.1.12)						
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: Mensaje CEA con IP interna como dirección IP de host

Aunque este AVP no es obligatorio cuando se utiliza TCP como protocolo de transporte (consulte RFC 3588), algunos proveedores de DRA hacen referencia a este AVP al establecer la conexión Diameter y esperan la IP de servicio Diameter de PCRF en lugar de la IP interna. Si no se cumple esta expectativa, los pares no podrán establecer.

Práctica recomendada:

Para anunciar la IP del servicio Diameter en el AVP de dirección IP de host desde PCRF, actualice el archivo /etc/hosts con una entrada que asigne el FQDN de origen de PCRF (como se define en los puntos finales locales de pila de diámetro) a la dirección IP deseada.



Nota: Consulte las tablas Terminales Locales en la Guía de Configuración Móvil de CPS, Versión 25.1.0, en la sección Configuración de Pila de Diámetro para obtener más detalles.

Para actualizar entradas de hosts adicionales en PCRF de CPS basado en Openstack:

- Compruebe que el clúster de CPS está en un estado implementado.

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

- Recupere y actualice additional-hosts.yaml a través de la API REST.

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

- Aplique los cambios con comandos curl como se describe en la documentación del producto.

```
curl -X PUT API system additional hosts -H "Content-Type: application/yaml" --data-binary @additional-hosts.yaml
```

Cuando se completa esta llamada API, el Cluster Manager se configura con el nuevo archivo /etc/hosts y todas las demás VM implementadas se actualizan de forma asíncrona.



Nota: Para obtener instrucciones detalladas, consulte la Guía de instalación de CPS para OpenStack, sección Orquestación API.

Para actualizar entradas de hosts adicionales en PCRFS CPS basado en VMware:

- Agregue la entrada en el archivo AdditionalHosts.csv que se encuentra en la ruta /var/qps/config/deploy/csv/
- Para importar cambios en la máquina virtual del Administrador de clústeres:

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

- Aplicar cambios desde el Administrador de clústeres:

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

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



Nota: Para obtener instrucciones detalladas, consulte la Guía de instalación de CPS para VMware, sección Configuración de hosts adicionales.

Ejemplo:

Figura 3: GUI Diámetro Pila Terminales Locales

*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: GUI Diámetro Pila Terminales Locales

Ejemplo 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 ~]#
```

Paso 4: Validar intercambio de capacidades entre pares

El DRA debe anunciar explícitamente la compatibilidad con aplicaciones Diameter como Gx (16777238) y Rx (16777236) en mensajes Capabilities-Exchange-Request (CER) y Capabilities-Exchange-Answer (CEA).

Cisco PCRF no admite la aplicación de retransmisión, con el identificador de aplicación 0xffffffff. Si sólo se intercambia la aplicación de retransmisión (4294967295) y no Gx/Rx, la conexión de par se establecerá como modo de solo retransmisión y PCRF no responderá a los mensajes CCR-I.

Consulte la sección Ruteo de Salto Siguiendo en la Guía de Configuración Móvil de CPS para obtener más detalles.

Práctica recomendada:
Durante la fase de establecimiento de conexión entre pares, capture siempre el pcap en PCRF para asegurarse de que DRA está enviando el mensaje de diámetro Capabilities-Exchange-Request (CER) con el conjunto de valores Auth-Application-ID de AVP Diameter de aplicaciones

como Gx (16777238) o Rx (16777236) o ambos y PCRF está respondiendo con valores similares en el mensaje Capabilities-Exchange-Answer (CEA).

Figura 4: Mensaje CER con valor incorrecto en Auth-Application-Id as 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
```

Figura 4: Mensaje CER con valor incorrecto en Auth-Application-Id as Relay

Figura 5: Mensaje CER con valores correctos en Auth-Application-Id: Gx y 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: Mensaje CER con valores correctos en Auth-Application-Id: Gx y Rx

Paso 5: Asegúrese de que el nombre de host de origen único de diámetro esté definido en cada nodo de par de diámetro

Cisco CPS PCRF admite un entorno en el que cada nodo de par conectado requiere un nombre de host de origen de diámetro único.

Si la migración se va a realizar para las conexiones de pares de diámetro de la conectividad Gx o Rx directa existente a los links mediados por DRA, el link DRA para cada interfaz Diameter (Gx o Rx) entre PCEF o P-CSCF y DRA idealmente debe utilizar un nombre de host de origen único para la aplicación de diámetro (el valor de AVP Origin-Host) que sería diferente del utilizado para la conectividad PCRF directa con el mismo nodo de peer.

Esto garantiza que las solicitudes de los nodos de peer se enruten a través del link de peer DRA correcto y no se descarten si las entradas de link directo descendente antiguas están presentes en la lista PCRF show_peers.py.

Práctica recomendada:

Si no es factible cambiar el nombre de host para los links DRA en el peer, realice un reinicio completo de los cuatro servicios QNS secuencialmente en cada VM de balanceador de carga después de eliminar los links de peer directos.

Esto aseguraría que las antiguas entradas obsoletas (Origin host:) de peers utilizadas anteriormente para la interfaz de diámetro directo (Gx/Rx) entre PCEF/P-CSCF y PCRF ya no estén presentes en la lista de conexiones de peer de diámetro PCRF, y que la salida show_peers.py tenga solamente conexiones de peer DRA y por lo tanto el ruteo adecuado de los mensajes de aplicación de diámetro (por ejemplo: Gx_CCA-I, Gx_CCA-T) a partir de los enlaces de diámetro recién creados entre DRA y PCRF.



Nota: El reinicio de los servicios QNS en las VM de LB afecta al tráfico y restablece todas las conexiones de peer Diameter en esas instancias de QNS. Realice este paso durante una ventana de mantenimiento planificado.

Paso 6: Configuración de la Tabla de Ruteo de Siguiente Salto para Peers DRA

Esta función permite la interacción con un DRA que no está en modo de ocultación de topología. Cuando un DRA establece una conexión, anuncia sus propios valores Origin-Host y Realm. Sin embargo, los mensajes de aplicación Diameter utilizan Origin-Host y Realm (por ejemplo, PCEF, TDF, AF) del host de aplicación real, por lo que PCRF necesita determinar qué conexión DRA utilizar para entregar mensajes al host correcto.



Nota: La tabla Rutas de próximo salto sólo se utiliza para solicitudes iniciadas por PCRF. Las respuestas a las solicitudes entrantes siempre se envían a través de la misma conexión en la que se recibieron, para evitar el ruteo asimétrico.

Estos parámetros se pueden configurar en la tabla de ruteo de próximo salto:

Parámetro	Descripción
Rango de salto siguiente	Nombre de rango DRA tal como se recibe en el AVP de rango de origen en CER o CEA mensaje.

	 Nota: Todos los rangos de salto siguiente (rango de salto siguiente) deben coincidir con el valor de VP Origin-Realm A en el mensaje CER/CEA entrante.
Hosts de próximo salto	Lista de nombres de hosts DRA tal como se recibe en el AVP de host de origen en CER o CEA mensaje.  Nota: Todos los nombres de host de salto siguiente (hosts de salto siguiente) deben coincidir con el valor de VP Origin-Host A en el mensaje CER/CEA entrante.
ID de aplicación	Id. de aplicación de diámetro anunciado como admitido por el DRA. Es contiene información que identifica el servicio concreto que el servicio la sesión pertenece a.
Patrón de rangos de destino	Patrón de nombre de territorio de destino real tal como se recibió en AVP de dominio de origen en el mensaje AAR. El patrón debe ser el estándar de Java regular sintaxis de expresión.
Patrón de host de destino	Patrón de nombre de host de destino real tal y como se recibió en Origen-Host AVP en mensaje AAR. El patrón debe ser un patrón estándar de Java convenciones. El patrón debe ser el estándar de Java regular sintaxis de expresión.

Práctica recomendada:

Siempre intente utilizar el patrón regex correcto (coincidencia de comodín) mientras realiza entradas en las columnas Patrón de rangos de destino y Patrón de host de destino en

Tabla de ruteo de próximo salto para minimizar las entradas de configuración para los pares Gx y Rx con conexiones múltiples y evitar errores de configuración.



Nota: Consulte la Guía de configuración de CPS Mobile, versión 25.1.0, en la sección Routing de próximo salto para obtener información detallada sobre la configuración.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).