

マルチベンダーDRA統合の構成ガイドの使用

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定手順とベストプラクティス](#)

[ステップ1:DRA接続モードの決定（着信ピアと発信ピア）](#)

[ステップ2:Policy Builderで着信ピアを設定します。](#)

[ステップ3:Host-IP-Address AVPを設定します。](#)

[ステップ4：ピア機能交換の検証](#)

[ステップ5:Diameterの一意のソースホスト名が各Diameterピアノードで定義されていることを確認します。](#)

[手順6:DRAピアのネクストホップルーティングテーブルを設定します。](#)

はじめに

このドキュメントでは、Cisco Policy Suite(CPS)のPCRFクラスタとマルチベンダーDRAを統合するためのベストプラクティスとともに、設定手順について説明します。

前提条件

要件

シスコでは、このソリューションを扱うエンジニアが次の項目に関する知識を持っていることを推奨します。

- Linuxオペレーティングシステム
- Cisco Policy Suite(CPS)プラットフォームおよびクラスタアーキテクチャ
- ポリシー/課金ルール機能(PCRF)
- Viエディタの使用
- Wiresharkネットワーク分析ツール

使用するコンポーネント

このドキュメントの情報は、CPS 25.1バージョンとAlmaLinuxリリース8.10に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定手順とベストプラクティス

ステップ1:DRA接続モードの決定（着信ピアと発信ピア）

- 着信ピア：PCRFは、指定されたDiameterピアからの接続要求を受け入れるように設定されます。ピアノードがPCRFに対してDiameter Capabilities-Exchange-Request(CER)を開始します。
- 発信ピア：PCRFは、ピアに対してCERを開始するように設定されます。

ベスト プラクティス:
ほとんどのマルチベンダーDRA統合では、DRAを着信ピアとして設定し、DRAがPCRFに対してCERを開始します。

ステップ2:Policy Builderで着信ピアを設定します。

Policy BuilderのGUIで、Inbound PeersテーブルとRealmsテーブルを参照して、着信ピア名とピアレルムを設定します。



注：パラメータの詳細な説明については、『CPS Mobile Configuration Guide, Release 25.1.0』の「Diameter Stack Configuration」セクションを参照してください。

次のパラメータは、着信ピアの下で設定できます。

ピアテーブル

項目	説明
----	----

Peers	PCRFへの接続を開始できるピア名を定義します。
ローカルホスト名	ポリシー・ダイレクタ (ロード・バランサ) のローカル・ホスト名が ピアからの着信接続を識別し、許可します。
インスタンス番号	ポリシーサーバー(QNS)プロセスの割り当て済み番号を示します。 発信ピアとの接続を開始します。  注:Policy Builder (ロードバランサ) 上で単一の Policy Server(QNS)プロセスだけが当該ピアの他のインスタンスとの接続を許可/開始する場合は、ローカルホスト名(LCN)とインスタンス番号を指定する必要があります。インスタンス番号は0のままにすることができます。この場合、Policy Director (ロードバランサ) 上のすべてのポリシーサーバ(QNS)プロセスは、ピアとの接続を試行し、許可します。デフォルト値は 0 です。
評価	PCRFが開始した要求を配信するために、このピアに割り当てられたプライオリティ。その レーティング値が高いほど、ピアに割り当てられるプライオリティが高くなります。 デフォルト値は 1 です。
ポート範囲	基礎となるトランスポート接続がSCTPの場合にのみ指定する必要があります TCPの場合は必要ありません。
応答タイムアウト	このパラメータは使用しないことをお勧めします。
名前パターン	CER内のOrigin-Host A VP値を、内のこのパターンに照らして検証する必要があります。 接続が確立される順序。この条件が満たされない場合、

	CER は通知なしに破棄され、TCP接続はPCRFによってリセットされます。 Accept Undefined Peerオプションの場合、名前パターンチェックが行われない diameterスタックの設定で説明します。 Name Patternは、標準のJava正規表現である必要があります 構文を説明します。
--	--

「レルム」表

項目	説明
レルム	どのピアレルムに対して接続を開始できるかを定義する PCRFを使用します。
ピアタイプ	インバウンド・レルムでは使用されません。
処理プロトコル	レルム名と特定のPCRFロジックとのマッピング をメッセージに適用すると、処理プロトコルの詳細が表示されます。 直径レルムを持つ直径スタックがプロトコルなしでインポートされた場合 割り当てられている場合、デフォルト値はGX_TGPPである。
評価	PCRFが開始した要求を配信するために、このレルムに割り当てられた優先順位。これは はSY_PRIME処理プロトコルでのみ使用されます。 デフォルト値は 0 です。 レーティング値が小さいほど、レルムに割り当てられる優先度が高くなります。 例えば、Rating=10のレルムは、Rating=10のレルムの後に使用されます 評価= 1。

統計エイリアス	各レルムに対して生成される統計情報が何であれ、 これらの統計情報に付加されたStats Aliasで設定される名前。 これは、com.broadhop.message mbean統計情報にのみ適用されます。
名前パターン	Origin-Realm CERのVP値は、このパターンに対して 処理される着信メッセージの順序。これが発生しない場合、 メッセージは通知なしに廃棄され、TCP接続はPCRFによってリセットされます。 Name Patternは、標準のJava正規表現である必要があります 構文を説明します。

ベスト プラクティス:

より詳細な制御が必要な場合は、要件に従って特定のピアとレルムのエントリを設定します。また、特定のピアからのピア作成だけを許可するには、Accept Undefined Peerのチェックマークを外します。

例：

図1：着信ピアテーブル

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.3gppnetwoi

☐ 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		.*

図1：着信ピアテーブル

ステップ3:Host-IP-Address AVPを設定します。

Diameter Host-IP-Address AVPは、SCTPベースの接続に対するCER/CEA交換中(RFC 3588)にノードのIPアドレスを伝達します。Cisco CPS PCRFでは、このアドレスはデフォルトで内部インターフェイスIPになります。これは、特定のDRAベンダーで想定されるDiameterサービスIPとは異なります。

Cisco CPS PCRFでは、ロードバランサ仮想IP(LbVIP)またはロードバランサVMの物理IPをdiameter-source-endpoint IPとして使用できます。

デフォルトでは、内部インターフェイスIPは図に示すようにDiameter CER/CEAメッセージのホストIPアドレスとして通信されます。キャプチャの送信元IPは、ホストIPアドレスAVPのIPとは異なります。

図2：内部IPアドレスがホストIPアドレスであるCEAメッセージ

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.mnc046.mcc044.3gppnetwork.org						
AVP: Origin-Realm(296) l=42 f=M- val=pcrf.mnc046.mcc044.3gppnetwork.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)						

図2：内部IPアドレスがホストIPアドレスであるCEAメッセージ

トランスポートプロトコルとしてTCP (RFC 3588を参照) を使用する場合、このAVPは必須ではありませんが、一部のDRAベンダーはDiameter接続の確立中にこのAVPを参照し、内部IPではなくPCRFのDiameterサービスIPを予期します。この期待値が満たされない場合、ピアの確立は失敗します。

ベスト プラクティス:

PCRFからHost-IP-Address AVPでDiameterサービスIPをアドバタイズするには、(Diameterスタックローカルエンドポイントで定義された) PCRF送信元FQDNを目的のIPアドレスにマッピングするエントリで/etc/hostsファイルを更新します。



注：詳細については、『CPS Mobile Configuration Guide, Release 25.1.0』の「Diameter Stack Configuration」セクションにある「Local End Points」の表を参照してください。

OpenstackベースのCPS PCRFで追加ホストエントリを更新するには、次の手順を実行します。

- CPSクラスタが導入済み状態であることを確認します。

curl -X [インストーラAPIシステム](#)を取得します。

- REST APIを介してadditional-hosts.yamlを取得および更新します。

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

- 製品ドキュメントの説明に従って、curlコマンドで変更を適用します。

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

このAPIコールが完了すると、Cluster Managerは新しい/etc/hostsfileを使用して設定され、その他の導入済みVMはすべて非同期で更新されます。



注：詳細な手順については、「Orchestration API」の「OpenStack用CPSインストールガイド」を参照してください。

VmwareベースのCPS PCRfで追加ホストエントリを更新するには、次の手順を実行します。

- パス/var/qps/config/deploy/csv/にあるAdditionalHosts.csvファイルにエントリを追加します
- Cluster Manager VMに変更をインポートするには、次の手順を実行します。

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

- Cluster Managerからの変更の適用:

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

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



注：詳細な手順については、「CPS Installation Guide for VMware」の「Additional Hosts Configuration」の項を参照してください。

例：

図3:GUIの直径スタックのローカルエンドポイント

*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 👆 👇

図3:GUIの直径スタックのローカルエンドポイント

/etc/hostsエントリの例：

<#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 ~]#

ステップ4：ピア機能交換の検証

DRAは、Capabilities-Exchange-Request(CER)メッセージおよびCapabilities-Exchange-Answer(CEA)メッセージで、Gx(16777238)およびRx(16777236)などのDiameterアプリケーションのサポートを明示的にアドバタイズする必要があります。

Application Identifier 0xffffffffのリレーアプリケーションは、Cisco PCRFではサポートされていません。リレーアプリケーション(4294967295)だけが交換され、Gx/Rxが交換されない場合、ピア接続はリレー専用モードとして確立され、PCRFはCCR-Iメッセージに応答しません。

詳細については、『CPS Mobile構成ガイド』の「ネクストホップルーティング」セクションを参照してください。

ベストプラクティス:

ピア接続の確立フェーズの間、PCRFのpcapを常にキャプチャして、DRAがAVP Auth-Application-ID 値セットDiameterアプリケーション(Gx(16777238)またはRx(16777236)またはその両方)とともにdiameter Capabilities-Exchange-Request(CER)メッセージを送信していること、およびPCRFがCapabilities-Exchange-Answer(CEA)メッセージで同様のの値で応答していることを確認します。

図4：リレーとしてのAuth-Application-Idの値が間違っているCERメッセージ

```

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=01ors.mnc.mcc.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..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
```

図4：リレーとしてのAuth-Application-Idの値が間違っているCERメッセージ

図5:Auth-Application-Idが正しい値のCERメッセージ：Gxおよび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
```

図5:Auth-Application-Idが正しい値のCERメッセージ：GxおよびRx

ステップ5:Diameterの一意のソースホスト名が各Diameterピアノードで定義されていることを確認します。

Cisco CPS PCRFは、接続された各ピアノードが固有のdiameterソースホスト名を必要とする環境をサポートします。

既存のdirect GxまたはRx接続からDRA仲介リンクへのdiameterピア接続に移行する場合、PCEFまたはP-CSCFとDRA間の各Diameterインターフェイス（GxまたはRx）のDRAリンクでは、diameterアプリケーションに対して、同じピアノードでのdirect PCRF接続に使用されるものとは異なる一意の送信元ホスト名を使用するのが理想的です。

これにより、ピアノードからの要求が正しいDRAピアリンク経由でルーティングされ、古いダイレクトリンクダウンエントリがPCRF show_peers.pyリストに存在する場合にドロップされないことが保証されます。

ベスト プラクティス:

ピア上のDRAリンクのホスト名を変更できない場合は、直接ピアリンクを削除した後、各ロードバランサVM上で4つすべてのQNSサービスの完全な再起動を順番に実行します。

これにより、PCEF/P-CSCFとPCRF間のdirect diameter interface(Gx/Rx)に以前に使用されたピアの古い廃止(Origin host:)エントリがPCRFのdiameterピア接続リストに存在しなくなります。また、show_peers.py出力にはDRAピア接続のみが含まれるため、DRAとPCRF間に新しく作成されたdiameterリンクからdiameterアプリケーションメッセージ (例 : Gx_CCA I、Gx_CCA I、I、T) がルーティングされます。



注:LB VMでQNSサービスを再起動すると、トラフィックに影響し、これらのQNSインスタンスのすべてのDiameterピア接続がリセットされます。この手順は、予定されたメンテナンスの時間帯に実行してください。

手順6: DRAピアのネクストホップルーティングテーブルを設定します。

この機能により、トポロジ非表示モードでないDRAとのインターワーキングが可能になります。DRAは接続を確立すると、自身のOrigin-HostとRealmの値をアドバタイズします。ただし、Diameterアプリケーションメッセージは、実際のアプリケーションホストのOrigin-HostおよびRealm (PCEF、TDF、AFなど) を使用するため、PCRFは、正しいホストにメッセージを配信するために使用するDRA接続を決定する必要があります。



注 : ネクストホップルートテーブルは、PCRFが開始した要求に対してのみ使用されます。着信要求に対する応答は、非対称ルーティングを防ぐために、常に受信したのと同じ接続で送信されます。

次のパラメータは、ネクストホップルーティングテーブルで設定できます。

項目	説明
ネクストホップレルム	CERまたはCEAのOrigin-Realm AVPで受信したDRAレルム名 メッセージに応答します。
	 注 : すべてのネクストホップレルム (ネクストホップレルム) は、着信

	CER/CEAメッセージのOrigin-Realm A VPの値と一致している必要があります。
ネクストホップホスト	CERまたはCEAのOrigin-Host AVPで受信したDRAホスト名リストメッセージに応答します。  注：すべてのネクストホップホスト名（ネクストホップホスト）は、着信CER/CEAメッセージのOrigin-Host A VP値と一致している必要があります。
アプリケーションId	DiameterアプリケーションIDは、DRAによってサポートされているとアドバタイズされます。これは、 サービスが特定のサービスを識別する情報が含まれるセッションが属しています。
宛先レルムのパターン	Origin-Realm AVPで受信した実際の宛先レルム名パターンをAARメッセージに追加します。パターンは、標準のJavaの正規パターンである必要があります 式の構文
宛先ホストパターン	Origin-Host AVP inで受信された実際の宛先ホスト名パターンAARメッセージ。パターンは標準のJavaパターンである必要があります パターンは標準のJavaの正規パターンである必要があります 式の構文

ベスト プラクティス:

の宛先レルムのパターンと宛先ホストパターンの列にエントリを作成する際は、常に正しい正規表現パターン（ワイルドカード照合）を使用するようにしてください

GxおよびRxピアの複数の接続の設定エントリを最小限に抑え、設定エラーを防ぐネクストホップルーティングテーブル。



注：詳細な設定ガイドンスについては、『CPS Mobile Configuration Guide, Release 25.1.0』の「Next Hop Routing」セクションを参照してください。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。