Guia de Operações do OmniHSS

Introdução

OmniHSS é uma implementação de Home Subscriber Server (HSS) projetada para redes 4G LTE (EPC) e IMS (IP Multimedia Subsystem). Como o banco de dados central e centro de autenticação para redes móveis, o OmniHSS gerencia credenciais de assinantes, dados de perfil e fornece serviços de autenticação e autorização para serviços de dados e voz.

Construído em Elixir e na VM Erlang, o OmniHSS oferece alta disponibilidade, tolerância a falhas e escalabilidade necessárias para a infraestrutura moderna de telecomunicações.

O que é um Home Subscriber Server?

O HSS é um componente crítico nas redes LTE e IMS que:

- **Armazena dados do assinante** - Credenciais, informações de perfil e assinaturas de serviço
- **Realiza autenticação** - Valida assinantes que tentam acessar a rede
- **Gerencia autorização** - Controla quais serviços os assinantes podem acessar
- **Rastreia localização** - Mantém informações de localização atual para roteamento
- **Controla roaming** - Impõe políticas de roaming com base nas redes visitadas
- **Gerencia equipamentos** - Funciona como Equipment Identity Register (EIR) para controle de dispositivos

Principais Recursos

Recursos Operacionais

- **Interface S6a** - Autenticação e gerenciamento de localização para redes LTE/EPC
- **Interface Cx** - Registro e autenticação IMS
- **Interface Sh** - Acesso a dados de perfil IMS e notificações de assinatura
- **Interface S13** - Verificação de Identidade de Equipamento (OmniHSS funciona como EIR)
- **Interface Gx** - Controle de Políticas e Cobrança (OmniHSS funciona como

PCRF)
- **Interface Rx** - Controle de políticas de mídia IMS (OmniHSS funciona como PCRF)
- **Controle de Roaming** - Controle granular sobre roaming de dados e IMS por PLMN
- **Múltiplos MSISDNs** - Suporte para múltiplos números de telefone por assinante
- **API RESTful** - API completa de provisionamento para integração (também usada pelo OmniHLR)
- **Painel de Controle Web** - Monitoramento em tempo real e status do sistema

Integração de Elementos de Rede

OmniHSS se conecta com os seguintes elementos de rede:

- **MME** (Mobility Management Entity) - Gerenciamento de mobilidade e sessão LTE
- **P-GW** (PDN Gateway) - Recebe políticas do OmniHSS (função PCRF)
- **P-CSCF** (Proxy Call Session Control Function) - Autorização de mídia IMS
- **I-CSCF** (Interrogating CSCF) - Consultas de roteamento IMS
- **S-CSCF** (Serving CSCF) - Registro e autenticação IMS
- **AS** (Application Server) - Acesso a dados de assinantes IMS
- **OmniHLR** - HLR legado que se comunica com o OmniHSS via API

Estrutura da Documentação

Este guia de operações está organizado nos seguintes documentos:

Documentação Principal

- **Visão Geral da Arquitetura** - Arquitetura do sistema, componentes e pilha Diameter
- **Guia de Configuração** - Referência completa de configuração com exemplos
- **Relações de Entidade** - Modelo de dados e relações de entidade

Guias Operacionais

- **Painel de Controle** - Usando a interface de monitoramento baseada na web
- **Métricas & Monitoramento** - Monitoramento do sistema e verificações de saúde
- **Guia de Solução de Problemas** - Diagnóstico e resolução de problemas comuns
- **Referência da API** - Documentação completa dos endpoints da API
- **Webhooks** - Notificações de eventos em tempo real e integração

Documentação de Recursos

- **Gerenciamento de Perfis** - Perfis EPC, IMS, APN e de roaming
- **Controle de Roaming** - Configurando políticas de roaming
- **Fluxos de Protocolo** - Procedimentos e fluxos de mensagens do protocolo Diameter
- **PCRF** - Função de Políticas e Regras de Cobrança (interfaces Gx/Rx, QoS, VoLTE)
- **EIR** - Registro de Identidade de Equipamento (interface S13, validação de IMEI)
- **Recursos Multi-MSISDN e Multi-IMSI** - Suporte a múltiplos números de telefone e múltiplos IMSI

Início Rápido para Operações

Acessando o Sistema

Painel de Controle (Interface Web)

```
URL: https://[hostname]:7443
```

O Painel de Controle fornece monitoramento em tempo real de assinantes e pares Diameter.

Endpoint da API

```
URL: https://[hostname]:8443
```

A API RESTful permite provisionamento e gerenciamento de assinantes.

Principais Arquivos de Configuração

- `config/runtime.exs` - Configuração em tempo de execução (banco de dados, Diameter, configurações de rede)
- `priv/cert/` - Certificados TLS para HTTPS e Diameter

Operações Essenciais

1. **Verificar Status do Sistema** - Acessar a página de Visão Geral do Painel de Controle
2. **Monitorar Pares Diameter** - Acessar a página Diameter do Painel de Controle
3. **Consultar Assinante** - Usar o endpoint da API `/api/subscriber/imsi/:imsi`
4. **Visualizar Banco de Dados** - Conectar ao Banco de Dados SQL no hostname configurado

Suporte e Solução de Problemas

Arquivos de Log

Os logs do sistema são enviados para stdout/stderr e podem ser capturados pelo seu gerenciador de processos (systemd, supervisord, etc.).

Verificações Comuns

- **Conectividade Diameter** - Verifique a página Diameter para o status dos pares
- **Conectividade do Banco de Dados** - Verifique a configuração do banco de dados em runtime.exs
- **Falhas de autenticação de assinantes** - Verifique o estado do assinante para contagem de falhas

Monitoramento de Saúde

- **Verificação de Saúde da API** - `GET /api/status`
- **Painel de Controle** - Acesse qualquer página do Painel de Controle
- **Banco de Dados** - Conecte-se ao Banco de Dados SQL e verifique o acesso à tabela

Considerações de Segurança

- **TLS Necessário** - Tanto a API quanto o Painel de Controle usam HTTPS
- **Gerenciamento de Certificados** - Certificados em `priv/cert/` devem ser válidos
- **Segurança do Banco de Dados** - Proteja as credenciais do banco de dados em runtime.exs
- **Isolamento de Rede** - A interface Diameter deve estar na rede de gerenciamento
- **Autenticação da API** - Considere implementar autenticação para uso em produção

Arquitetura em um Relance

Próximos Passos

Para procedimentos operacionais detalhados, consulte as seções específicas da documentação:

- Comece com **Visão Geral da Arquitetura** para entender os componentes do sistema
- Revise **Guia de Configuração** para personalizar sua implantação

- Explore **Painel de Controle** para monitoramento diário
- Consulte **Referência da API** para automação de provisionamento

---

Versão do Documento: 1.0
Mantido Por: Equipe de Operações da Omnitouch

EIR (Registro de Identidade de Equipamento)

Visão Geral

O HSS inclui um EIR (Registro de Identidade de Equipamento) embutido que fornece verificação de identidade de equipamento para dispositivos móveis. O EIR valida números IMEI (Identidade Internacional de Equipamento Móvel) para determinar se o equipamento móvel está autorizado, foi roubado ou está sob observação antes de permitir o acesso à rede.

Principais Capacidades

- **Interface S13**: Verificação de identidade de equipamento via protocolo Diameter
- **Validação de IMEI**: Verificar a identidade do equipamento usando IMEI/IMEISV
- **Correspondência Flexível**: Correspondência de padrões baseada em Regex para IMEI, IMEISV e IMSI
- **Classificação em Três Níveis**: Suporte a lista branca, lista negra e lista cinza
- **Políticas Configuráveis**: Comportamento personalizável para equipamentos desconhecidos
- **REST API**: Operações completas de CRUD para gerenciamento de regras do EIR

Arquitetura

Interface Diameter

Interface	ID da Aplicação	Par	Propósito
S13	16.777.252	MME/SGSN	Verificação de identidade de equipamento

Banco de Dados de Regras de Equipamento

O EIR utiliza um sistema de correspondência baseado em regras flexíveis:

Ações de Regra:

- `whitelist` - Permitir equipamento
- `blacklist` - Bloquear equipamento
- `greylist` - Monitorar equipamento

Padrões Regex: Correspondência contra IMEI, IMEISV ou IMSI

Valores de Status de Equipamento

Status	Código	Significado	Ação na Rede
Whitelist	0	Equipamento aprovado	Permitir acesso à rede
Blacklist	1	Equipamento roubado/bloqueado	Negar acesso à rede
Greylist	2	Equipamento sob observação	Permitir com monitoramento

Interface S13

Operações Suportadas

Solicitação de Verificação de Identidade de Equipamento (ECR) / Resposta de Verificação de Identidade de Equipamento (ECA)

Direção: MME/SGSN → HSS (EIR)

Gatilho: MME verifica a identidade do equipamento durante o anexo ou atualização da área de rastreamento

AVPs de Solicitação:

- Session-Id
- Origin-Host, Origin-Realm
- Destination-Realm
- Auth-Session-State
- Terminal-Information
    - IMEI (15 dígitos)
    - Software-Version (2 dígitos, opcional)
- User-Name (IMSI, opcional)
- Vendor-Specific-Application-Id

Ações do EIR:

1. Extrair IMEI, Software-Version (se presente) e IMSI (se presente)
2. Se IMSI fornecido:
    - Validar se o assinante existe e está habilitado
    - Atualizar o estado do assinante com informações do último visto
3. Tentar busca de equipamento em ordem de prioridade:
    - **Correspondência IMEISV** (IMEI + Software-Version concatenados)
    - **Correspondência IMEI** (somente IMEI)
    - **Correspondência IMSI** (se fornecido na solicitação)
    - **Política de equipamento desconhecido** (comportamento padrão configurado)
4. Retornar status do equipamento

AVPs de Resposta:

- Session-Id (ecoado da solicitação)
- Result-Code: 2001 (sucesso)
- Equipment-Status: 0 (whitelist) / 1 (blacklist) / 2 (greylist)

Respostas de Erro:

- Experimental-Result: 5422 (equipamento/assinante não encontrado)
- Experimental-Result: 5012 (erro geral)

Lógica de Correspondência de Equipamento

Ordem de Prioridade

O EIR utiliza uma estratégia de busca em cascata para maximizar a flexibilidade de correspondência:

```
1. IMEISV (IMEI + Software-Version)
   ↓ (se não houver correspondência)
2. IMEI somente
   ↓ (se não houver correspondência)
3. IMSI (se fornecido na solicitação)
   ↓ (se não houver correspondência)
4. Política de Equipamento Desconhecido
```

Algoritmo de Correspondência

Passo 1: Correspondência IMEISV

- Concatenar IMEI + Software-Version: `"35979139461611" + "08" = "3597913946161108"`
- Testar contra todos os padrões regex de regras do EIR
- Retornar ação ("whitelist", "blacklist", "greylist") da primeira regra correspondente

Passo 2: Correspondência IMEI (fallback)

- Usar somente IMEI: `"35979139461611"`
- Testar contra todos os padrões regex de regras do EIR
- Retornar ação da primeira regra correspondente

Passo 3: Correspondência IMSI (fallback se IMSI fornecido)

- Usar IMSI da solicitação: `"999999876543210"`
- Testar contra todos os padrões regex de regras do EIR
- Retornar ação da primeira regra correspondente
- **Caso de uso**: Bloquear todos os equipamentos para um assinante específico

Passo 4: Política de Equipamento Desconhecido (fallback final)

- Configuração: `eir_unknown_equipment_behaviour`
- Opções:
  - `:whitelist` - Permitir equipamentos desconhecidos (permissivo)
  - `:blacklist` - Bloquear equipamentos desconhecidos (restritivo)
  - `:greylist` - Observar equipamentos desconhecidos (moderado)
  - `:reject_unknown_equipment` - Retornar erro 5422 (estrito)

Exemplos de Padrões Regex

Padrão	Correspondências	Caso de Uso
`"35979139461650"`	IMEI exato	Lista branca/lista negra de dispositivo único
`"3597913946165.*"`	Coringa de prefixo IMEI	Faixa de fabricante/modelo
`"3597913946161108"`	IMEISV exato	Dispositivo específico com versão de software
`"999999876543210"`	IMSI	Bloquear todos os equipamentos para assinante
`"359791.*"`	Coringa TAC	Atribuição de todo tipo de dispositivo

Fluxos de Mensagem Comuns

Fluxo 1: Verificação de Equipamento - IMEI Conhecido na Lista Branca

Fluxo 2: Verificação de Equipamento - IMEI na Lista Negra (Dispositivo Roubado)

Fluxo 3: Verificação de Equipamento - Equipamento Desconhecido (Política de Lista Branca)

Fluxo 4: Verificação de Equipamento - Equipamento Desconhecido (Política de Rejeição)

Fluxo 5: Verificação de Equipamento - Assinante Desconhecido

Fluxo 6: Verificação de Equipamento - Correspondência IMEISV

Fluxo 7: Verificação de Equipamento - Bloqueio de IMSI

REST API

Gerenciamento de Regras do EIR

Caminho base: `/api/eir/rule`

Listar Todas as Regras do EIR

Solicitação:

```
GET /api/eir/rule
```

Resposta (HTTP 200):

```
{
  "data": [
    {
      "id": 1,
      "action": "whitelist",
      "regex": "3597913946165.*",
      "inserted_at": "2025-01-15T10:30:00Z",
      "updated_at": "2025-01-15T10:30:00Z"
    },
    {
      "id": 2,
      "action": "blacklist",
      "regex": "35979139461640",
      "inserted_at": "2025-01-16T14:20:00Z",
      "updated_at": "2025-01-16T14:20:00Z"
    }
  ]
}
```


Obter Regra Específica do EIR

Solicitação:

```
GET /api/eir/rule/{id}
```

Resposta (HTTP 200):


```
{
  "data": {
    "id": 1,
    "action": "whitelist",
    "regex": "3597913946165.*"
  }
}
```


Criar Regra do EIR

Solicitação:

```
POST /api/eir/rule
Content-Type: application/json

{
  "action": "blacklist",
  "regex": "35979139461640"
}
```

Validação:

- `action`: Obrigatório, deve ser "whitelist", "blacklist" ou "greylist"
- `regex`: Obrigatório, deve ser um padrão regex válido, único entre todas as regras

Resposta (HTTP 201):

```
{
  "data": {
    "id": 3,
    "action": "blacklist",
    "regex": "35979139461640"
  }
}
```

Resposta de Erro (HTTP 400):

```
{
  "errors": {
    "regex": ["já foi utilizado"]
  }
}
```

Atualizar Regra do EIR (Parcial)

Solicitação:

```
PATCH /api/eir/rule/{id}
Content-Type: application/json

{
  "action": "greylist"
}
```

Resposta (HTTP 200):

```
{
  "data": {
    "id": 3,
    "action": "greylist",
    "regex": "35979139461640"
  }
}
```

Substituir Regra do EIR

Solicitação:

```
PUT /api/eir/rule/{id}
Content-Type: application/json

{
  "action": "whitelist",
  "regex": "359791394616.*"
}
```

Resposta (HTTP 200):

```
{
  "data": {
    "id": 3,
    "action": "whitelist",
    "regex": "359791394616.*"
  }
}
```

Deletar Regra do EIR

Solicitação:

```
DELETE /api/eir/rule/{id}
```

Resposta (HTTP 204 Sem Conteúdo)

Configuração

Configuração do Serviço Diameter

Aplicação S13 (`config/runtime.exs`):

```
%{
  application_name: :hss_s13,
  application_dictionary: :diameter_gen_3gpp_s13,
  vendor_specific_application_ids: [
    %{vendor_id: 10415, auth_application_id: 16_777_252}
  ]
}
```

Comportamento de Equipamento Desconhecido

Configure o comportamento padrão para equipamentos que não correspondem a nenhuma regra em `config/runtime.exs`:

Exemplo:

```
config :hss, :eir,
  unknown_equipment_behaviour: :whitelist
```

Valores Válidos:

- `:whitelist` - Permitir equipamentos desconhecidos (padrão, permissivo)
- `:blacklist` - Bloquear equipamentos desconhecidos (restritivo)
- `:greylist` - Monitorar equipamentos desconhecidos (moderado)
- `:reject_unknown_equipment` - Retornar erro Diameter 5422 (estrito)

Casos de Uso:

- **Desenvolvimento/Teste**: `:whitelist` - Permitir todos os dispositivos
- **Produção (permissivo)**: `:whitelist` - Apenas bloquear dispositivos conhecidos como ruins
- **Produção (moderado)**: `:greylist` - Registrar dispositivos desconhecidos para revisão
- **Produção (estrito)**: `:reject_unknown_equipment` - Apenas permitir dispositivos registrados

Tratamento de Erros

Código de Resultado	Tipo	Significado	Causa
2001	Sucesso	DIAMETER_SUCCESS	Verificação de equipamento concluída
5422	Experimental	DIAMETER_ERROR_EQUIPMENT_UNKNOWN	Assinante não encontrado ou equipamento desconhecido rejeitado
5012	Experimental	DIAMETER_ERROR_UNKNOWN	Erro de processamento

Casos de Uso

1. Gerenciamento de Dispositivo Roubado

Cenário: Dispositivo reportado como roubado

Ação:

```
POST /api/eir/rule
{
  "action": "blacklist",
  "regex": "35979139461640"  # IMEI exato
}
```

Resultado: Dispositivo negado acesso à rede na próxima conexão

2. Lista Branca de Fabricante

Cenário: Pré-aprovar toda a faixa de modelos de dispositivos

Ação:

```
POST /api/eir/rule
{
  "action": "whitelist",
  "regex": "359791394.*"  # TAC para fabricante/modelo
```

```
}
```

Resultado: Todos os dispositivos na faixa TAC aprovados

3. Bloqueio de Equipamento do Assinante

Cenário: Bloquear todos os equipamentos para um assinante específico (bloqueio de SIM)

Ação:

```
POST /api/eir/rule
{
  "action": "blacklist",
  "regex": "999999876543210"  # IMSI
}
```

Resultado: Qualquer equipamento usado com este SIM é bloqueado

4. Lista Cinza de Equipamento de Teste

Cenário: Monitorar equipamentos de teste em produção

Ação:

```
POST /api/eir/rule
{
  "action": "greylist",
  "regex": "35979139.*"  # Faixa TAC de equipamentos de teste
}
```

Resultado: Equipamento permitido, mas sinalizado para monitoramento

5. Controle de Versão de Software

Cenário: Bloquear versão de firmware vulnerável específica

Ação:

```
POST /api/eir/rule
{
  "action": "blacklist",
  "regex": "359791394616.*05"  # Faixa IMEI + Versão de Software 05
}
```

Resultado: Apenas dispositivos com Versão de Software "05" na faixa IMEI bloqueados

Detalhes da Implementação

Componentes Internos

A funcionalidade do EIR é implementada usando vários módulos internos:

- **Manipulador de Protocolo S13** - Processamento de mensagens ECR/ECA
- **Motor de Correspondência de Equipamento** - Correspondência baseada em regex para IMEI/IMEISV/IMSI
- **Banco de Dados de Regras do EIR** - Armazenamento e busca de padrões
- **Controlador de REST API** - Endpoints de gerenciamento de regras

Função de Busca de Status de Equipamento

A busca de status de equipamento segue esta lógica em cascata:

1. **Correspondência IMEISV**: Verificar IMEI + Software-Version concatenados
2. **Correspondência IMEI**: Verificar somente IMEI
3. **Correspondência IMSI**: Verificar IMSI (se fornecido)
4. **Equipamento Desconhecido**: Aplicar política padrão configurada

Resultados Possíveis:

- `whitelist` - Equipamento permitido
- `blacklist` - Equipamento bloqueado
- `greylist` - Equipamento sob observação
- `reject_unknown_equipment` - Rejeição estrita

Considerações de Segurança

Privacidade do IMEI

Números IMEI são identificadores sensíveis. O EIR:

- Não registra valores IMEI em texto simples por padrão
- Usa buscas em banco de dados com hash (se configurado)
- Restringe o acesso à API a administradores autenticados

Ordenação de Regras

As regras do EIR são avaliadas na ordem do banco de dados (por ID). Para padrões conflitantes:

```
Regra 1: regex "359791.*" ação "whitelist"  (ampla)
Regra 2: regex "35979139461640" ação "blacklist"  (específica)
```

Recomendação: Crie regras específicas antes de curingas amplos para garantir que a lista negra tenha precedência.

Limitação de Taxa

Considere implementar limitação de taxa em:

- Solicitações S13 ECR de pares não confiáveis
- Modificações de regras da REST API do EIR
- Consultas de busca de IMEI para prevenir ataques de enumeração

Documentação Relacionada

- Protocolos Diameter - Especificação do protocolo S13
- Referência da API - Documentação completa da API
- Arquitetura - Arquitetura geral do HSS
- Guia de Operações - Procedimentos operacionais

Apêndice: Estrutura do IMEI

Formato do IMEI (15 dígitos)

```
35 9791 394616 1
│  │    │      └─ Dígito de verificação (algoritmo de Luhn)
│  │    └─ Número de série (6 dígitos)
│  └─ FAC (Código de Montagem Final, 4 dígitos)
└─ TAC (Código de Atribuição de Tipo, 8 dígitos no total incluindo RBI)
   │  └─ RBI (Identificador do Corpo de Relato, 2 dígitos)
   └─ Fabricante/Modelo (6 dígitos)
```

Formato do IMEISV (16 dígitos)

```
35 9791 394616 1 08
│  │    │      │ └─ Versão do Software (2 dígitos)
└─ IMEI (15 dígitos)
```

Exemplos de Padrões

IMEI/IMEISV	Padrão	Correspondências
359791394616108	`3597913946161.*`	Todos os dispositivos com TAC+FAC+Serial 359791394616*
359791394616140	`35979139461614.`	Todos os dígitos de verificação para Serial 359791394616141-9
35979139461640	`35979139461640`	Correspondência exata de IMEI
3597913946163008	`3597913946163008`	Correspondência exata de IMEISV (IMEI + SV)

PCRF (Função de Regras de Política e Cobrança)

Visão Geral

O HSS inclui um PCRF (Função de Regras de Política e Cobrança) embutido que fornece controle de política e regras de cobrança para sessões de dados móveis. O PCRF controla políticas de Qualidade de Serviço (QoS), alocação de largura de banda e regras de cobrança para portadoras padrão e dedicadas em redes LTE.

Principais Capacidades

- **Interface Gx**: Controle de política para PGW/PCEF (Gateway de Rede de Dados por Pacote / Função de Aplicação e Cobrança de Política)
- **Interface Rx**: Autorização e QoS para fluxos de mídia IMS (Subsistema Multimídia IP)
- **Gerenciamento Dinâmico de Políticas**: Atualizações de políticas em tempo real via Re-Auth Requests (RAR)
- **Suporte a VoLTE**: Criação de portadora dedicada para chamadas de voz com QoS garantido
- **Regras de Cobrança**: Definir comportamento de cobrança e perfis de velocidade usando Traffic Flow Templates (TFTs)
- **REST API**: Controle programático da aplicação de políticas e gerenciamento de regras

Arquitetura

Interfaces Diameter

Interface	ID da Aplicação	Par	Propósito
Gx	16.777.238	PGW (PCEF)	Gerenciamento de sessão PDN, aplicação de QoS, regras de cobrança
Rx	16.777.236	P-CSCF (AF)	Autorização de mídia IMS, reserva de largura de banda

Gerenciamento de Estado da Sessão

O PCRF mantém o estado da sessão para conexões PDN ativas e chamadas VoLTE:

Interface Gx

Operações Suportadas

1. Solicitação de Controle de Crédito - Inicial (CCR-I)

Gatilho: PGW cria nova conexão PDN para o assinante

AVPs de Solicitação:

- Session-Id
- Origin-Host, Origin-Realm
- Subscription-Id (contém IMSI)
- Called-Station-Id (nome do APN)
- IP-CAN-Type (tipo de Rede de Acesso à Conectividade IP)
- RAT-Type (Tecnologia de Acesso Rádio)
- Framed-IP-Address (endereço IP do UE)

Ações do PCRF:

1. Buscar assinante pelo IMSI
2. Recuperar perfil APN e configuração de QoS
3. Criar entrada de rastreamento de sessão
4. Construir políticas de QoS a partir do perfil APN

AVPs de Resposta:

- Result-Code: 2001 (DIAMETER_SUCCESS)
- QoS-Information (limites de largura de banda agregada do APN)
- Default-EPS-Bearer-QoS (QCI, ARP, prioridade)
- Bearer-Control-Mode

2. Solicitação de Controle de Crédito - Atualização (CCR-U)

Gatilho: PGW relata mudanças na sessão (atualização de localização, mudança de RAT, etc.)

Ações do PCRF:

1. Localizar sessão existente pelo ID da sessão
2. Atualizar parâmetros da sessão (tipo de RAT, localização, etc.)
3. Retornar políticas atualizadas, se necessário

Resposta: Result-Code 2001 com atualizações de política opcionais

3. Solicitação de Controle de Crédito - Terminar (CCR-T)

Gatilho: PGW termina a conexão PDN

Ações do PCRF:

1. Localizar sessão pelo ID da sessão
2. Excluir sessão e registros de chamada associados
3. Confirmar a terminação

Resposta: Result-Code 2001

4. Solicitação de Re-Auth (RAR)

Direção: PCRF → PGW (HSS inicia)

Gatilho:

- Configuração de chamada IMS (Rx AAR aciona Gx RAR)
- Desconexão de chamada IMS (Rx STR aciona Gx RAR)
- Re-autenticação manual via REST API

AVPs RAR:

- Session-Id (ID da sessão PGW)
- Auth-Application-Id: 16.777.238
- Re-Auth-Request-Type (0 = Apenas Autorizar)
- Charging-Rule-Install/Remove
- QoS-Information (para portadoras dedicadas)

Ações do PGW: Criar/modificar/excluir portadoras dedicadas com base nas regras de cobrança

Regras de Cobrança e Traffic Flow Templates

O PCRF suporta a definição de regras de cobrança com Traffic Flow Templates (TFTs) para controlar:

- **Cobrança específica de serviço** - Tarifas diferentes para vídeo, jogos, redes sociais, etc.
- **Perfis de velocidade** - Limitar ou priorizar tráfego que corresponda a padrões específicos
- **Políticas baseadas em uso** - Aplicar diferentes QoS com base no tipo de tráfego ou destino

As regras de cobrança podem ser:

- Instaladas dinamicamente via Gx RAR com base na detecção de aplicativos

- Pré-definidas e acionadas por condições específicas (hora do dia, localização, cota)
- Associadas a TFTs usando regras de filtro de pacotes (5-tuple: protocolo, IP de origem/destino, porta de origem/destino)

Casos de Uso Comuns:

- **Zero-rating** - Acesso ilimitado a serviços específicos (Spotify, WhatsApp, Facebook) sem consumir cota de dados
- **Acesso pós-cota** - Permitir portal de autoatendimento e sites de suporte mesmo após o assinante esgotar a cota de dados
- **Velocidade em camadas** - Alta velocidade para serviços premium, limitada para conteúdo padrão
- **Políticas baseadas em tempo** - Streaming ilimitado fora do pico, priorização em horários de pico
- **Políticas de roaming** - Cobrança diferente para uso de dados internacional vs nacional
- **SLAs empresariais** - QoS garantido para aplicativos críticos para os negócios

Estrutura da Política de QoS

QoS da Portadora Padrão (do perfil APN):

```
{
  "QoS-Class-Identifier": 9,          // QCI (9 = portadora padrão)
  "APN-Aggregate-Max-Bitrate-UL": 50000,  // kbps
  "APN-Aggregate-Max-Bitrate-DL": 100000, // kbps
  "Allocation-Retention-Priority": {
    "Priority-Level": 8,
    "Pre-emption-Capability": 1,      // Pode preemptar
    "Pre-emption-Vulnerability": 1    // Pode ser preemptado
  }
}
```

QoS da Portadora Dedicada (para VoLTE):

```
{
  "QoS-Class-Identifier": 1,          // QCI 1 = Voz Conversacional
  "Max-Requested-Bandwidth-UL": 128000,   // bps
  "Max-Requested-Bandwidth-DL": 128000,   // bps
  "Guaranteed-Bitrate-UL": 128000,
  "Guaranteed-Bitrate-DL": 128000
}
```

Interface Rx

Operações Suportadas

1. Solicitação AA (AAR) / Resposta AA (AAA)

Gatilho: P-CSCF solicita autorização para sessão de mídia IMS (configuração de chamada VoLTE)

AVPs de Solicitação:

- Session-Id (identificador da sessão P-CSCF)
- Subscription-Id (IMSI ou SIP URI)
- Media-Component-Description
    - Media-Type (áudio, vídeo)
    - Max-Requested-Bandwidth-UL/DL
    - Codec-Data
    - Flow-Description (filtros de pacotes 5-tuple)
- AF-Application-Identifier

Ações do PCRF:

1. Buscar assinante pelo IMSI ou SIP URI
2. Encontrar sessão IMS ativa
3. Extrair parâmetros de mídia (codec, largura de banda, regras de fluxo)
4. Criar entrada de rastreamento de chamada
5. **Acionar Gx RAR para PGW** para criar portadora dedicada
6. Aguardar resposta Gx RAA
7. Retornar Rx AAA com resultado da autorização

AVPs de Resposta:

- Result-Code: 2001 (sucesso) ou 5063 (serviço não autorizado)

2. Solicitação de Término de Sessão (STR) / Resposta de Término de Sessão (STA)

Gatilho: P-CSCF termina sessão IMS (desconexão da chamada)

Ações do PCRF:

1. Localizar sessão de chamada pelo ID da sessão P-CSCF
2. **Acionar Gx RAR para PGW** para remover portadora dedicada
3. Excluir entrada de rastreamento de chamada
4. Retornar confirmação STA

Resposta: Result-Code 2001

Fluxos de Mensagens Comuns

Fluxo 1: Estabelecimento de Sessão PDN

Fluxo 2: Configuração de Chamada VoLTE (Rx AAR → Gx RAR)

Fluxo 3: Desconexão de Chamada VoLTE (Rx STR → Gx RAR)

Fluxo 4: Atualização da Sessão PDN

Fluxo 5: Término da Sessão PDN

Fluxo 6: Re-Auth Manual via REST API

REST API

Endpoint de Re-Auth do PCRF

Endpoint: `POST /api/operation/pcrf_re_auth`

Propósito: Acionar manualmente a Solicitação de Re-Auth Gx para atualizar políticas

Quando Usar: Este endpoint manual é tipicamente usado para solucionar problemas ou forçar a atualização de políticas em assinantes específicos. Para atualizações de políticas de rotina (mudança de perfis de QoS do APN), o sistema aciona automaticamente re-autenticações para todas as sessões afetadas - nenhuma ação manual é necessária.

Corpo da Solicitação:

```
{
  "imsi": "999999876543210",
  "apn": "ims"
}
```

Resposta de Sucesso (HTTP 200):

```
{
  "data": "Gx Re-Auth Request para 999999876543210 enviado para
pgw.epc.mnc999.mcc999.3gppnetwork.org, Result-Code: 2001"
}
```

Resposta de Erro (HTTP 400):

```
{
```

```
  "error": "Não foi possível enviar Re-Auth Request para
999999876543210 no APN ims, nenhuma sessão PDN ativa encontrada"
}
```

API de Configuração de Políticas

O PCRF recupera políticas de QoS das configurações de APN armazenadas no banco de dados. Essas políticas podem ser criadas e gerenciadas via REST API.

Aplicação Automática de Políticas: Quando você atualiza um perfil de QoS do APN (por exemplo, altera limites de largura de banda ou QCI), o sistema envia automaticamente Solicitações de Re-Auth Gx (RAR) para todos os PGWs com sessões PDN ativas usando esse APN. Isso garante que as mudanças de política sejam aplicadas imediatamente a todos os assinantes conectados sem intervenção manual.

Arquitetura da Política

As políticas são definidas através de uma estrutura de três camadas:

```
Identificador do APN → Perfil de QoS do APN → Perfil APN
     ↓                      ↓                    ↓
  "internet"       QCI, AMBR, ARP     Liga ambos
```

1. Criar Identificador do APN

Defina o nome do APN e o suporte à versão IP.

Endpoint: `POST /api/apn/identifier`

Corpo da Solicitação:

```
{
  "apn_identifier": {
    "apn": "internet",
    "ip_version": "ipv4v6"
  }
}
```

Opções de Versão IP:

- `"ipv4"` - Apenas IPv4
- `"ipv6"` - Apenas IPv6
- `"ipv4v6"` - Pilha dupla (tanto IPv4 quanto IPv6)
- `"ipv4_or_ipv6"` - A rede decide (ou IPv4 ou IPv6)

Resposta (HTTP 201):

```
{
  "data": {
    "id": 1,
    "apn": "internet",
    "ip_version": "ipv4v6"
  }
}
```

Validação:

- `apn`: Obrigatório, 1-254 caracteres, único
- `ip_version`: Obrigatório, deve ser uma das quatro opções acima

Listar Identificadores de APN: `GET /api/apn/identifier`

2. Criar Perfil de QoS do APN

Defina os parâmetros de QoS (largura de banda, QCI, prioridade).

Endpoint: `POST /api/apn/qos_profile`

Corpo da Solicitação:

```
{
  "apn_qos_profile": {
    "name": "Internet de Melhor Esforço",
    "qci": 9,
    "allocation_retention_priority": 8,
    "apn_ambr_dl_kbps": 100000,
    "apn_ambr_ul_kbps": 50000,
    "pre_emption_capability": false,
    "pre_emption_vulnerability": true
  }
}
```

Parâmetros de QoS:

Campo	Tipo	Faixa	Descrição
`name`	string	1-254 chars	Nome do perfil (único)
`qci`	integer	1-254	Identificador de Classe de QoS (1-4 = GBR, 5-9 = Non-GBR)
`allocation_retention_priority`	integer	1-15	Nível de ARP (1 = maior prioridade)
`apn_ambr_dl_kbps`	integer	1-4.294.967.293	Taxa Máxima de Bit Agregada do APN Downlink (kbps)
`apn_ambr_ul_kbps`	integer	1-4.294.967.293	Taxa Máxima de Bit

Campo	Tipo	Faixa	Descrição
			Agregada do APN Uplink (kbps)
`pre_emption_capability`	boolean	true/false	Pode preemptar portadoras de prioridade inferior
`pre_emption_vulnerability`	boolean	true/false	Pode ser preemptado por portadoras de prioridade superior

Valores Comuns de QCI:

- 1 - Voz Conversacional (VoLTE) - GBR, 100ms de orçamento de atraso
- 2 - Vídeo Conversacional - GBR, 150ms de orçamento de atraso
- 5 - Sinalização IMS - Non-GBR, 100ms de orçamento de atraso
- 9 - Portadora Padrão (Internet) - Non-GBR, 300ms de orçamento de atraso

Resposta (HTTP 201):

```
{
  "data": {
    "id": 1,
    "name": "Internet de Melhor Esforço",
    "qci": 9,
    "allocation_retention_priority": 8,
    "apn_ambr_dl_kbps": 100000,
    "apn_ambr_ul_kbps": 50000,
    "pre_emption_capability": false,
    "pre_emption_vulnerability": true
  }
}
```

Listar Perfis de QoS: `GET /api/apn/qos_profile`

3. Criar Perfil APN

Vincule o identificador do APN a um perfil de QoS.

Endpoint: `POST /api/apn/profile`

Corpo da Solicitação:

```
{
  "apn_profile": {
    "name": "Perfil APN Internet",
    "apn_identifier_id": 1,
    "apn_qos_profile_id": 1
  }
```

```
}
```

Campos:

- `name`: Nome do perfil (único), usado para referência
- `apn_identifier_id`: ID do Criar Identificador do APN
- `apn_qos_profile_id`: ID do Criar Perfil de QoS do APN

Resposta (HTTP 201):

```
{
  "data": {
    "id": 1,
    "name": "Perfil APN Internet",
    "apn_identifier_id": 1,
    "apn_qos_profile_id": 1
  }
}
```

Restrições:

- `apn_identifier_id` e `apn_qos_profile_id` devem referenciar registros existentes
- Cada combinação de identificador do APN e perfil de QoS deve ser única

Listar Perfis APN: `GET /api/apn/profile`

Exemplo Completo de Configuração de Políticas

Passo 1: Criar Política APN IMS (VoLTE)

```
# 1. Criar Identificador do APN
curl -X POST https://hss.example.com:8443/api/apn/identifier \
  -H "Content-Type: application/json" \
  -d '{
    "apn_identifier": {
      "apn": "ims",
      "ip_version": "ipv4v6"
    }
  }'
# Resposta: {"data": {"id": 2, ...}}

# 2. Criar Perfil de QoS (Sinalização IMS)
curl -X POST https://hss.example.com:8443/api/apn/qos_profile \
  -H "Content-Type: application/json" \
  -d '{
    "apn_qos_profile": {
      "name": "QoS de Sinalização IMS",
```

```
      "qci": 5,
      "allocation_retention_priority": 2,
      "apn_ambr_dl_kbps": 5000,
      "apn_ambr_ul_kbps": 5000,
      "pre_emption_capability": true,
      "pre_emption_vulnerability": false
    }
  }'
# Resposta: {"data": {"id": 2, ...}}

# 3. Criar Perfil APN
curl -X POST https://hss.example.com:8443/api/apn/profile \
  -H "Content-Type: application/json" \
  -d '{
    "apn_profile": {
      "name": "Perfil APN IMS",
      "apn_identifier_id": 2,
      "apn_qos_profile_id": 2
    }
  }'
# Resposta: {"data": {"id": 2, ...}}
```

Passo 2: Atribuir ao Assinante

Uma vez criado, o perfil APN é atribuído a assinantes via perfis EPC. Veja Referência da API para vincular perfis APN a assinantes.

Atualização e Exclusão de Políticas

Atualizar Perfil de QoS:

```
PATCH /api/apn/qos_profile/{id}
PUT /api/apn/qos_profile/{id}
```

Exemplo - Aumentar Largura de Banda para Todos os Usuários:

```
# Atualizar perfil de QoS ID 1 para aumentar largura de banda
curl -X PATCH https://hss.example.com:8443/api/apn/qos_profile/1 \
  -H "Content-Type: application/json" \
  -d '{
    "apn_qos_profile": {
      "apn_ambr_dl_kbps": 150000,
      "apn_ambr_ul_kbps": 75000
    }
  }'
```

O que Acontece Automaticamente:

1. O perfil de QoS é atualizado no banco de dados
2. O sistema identifica todas as sessões PDN ativas usando APNs vinculados a este perfil de QoS
3. Para cada sessão ativa, um Gx RAR é enviado ao PGW correspondente
4. Os PGWs atualizam a QoS da portadora para refletir os novos limites de largura de banda
5. Todos os assinantes conectados recebem imediatamente a política atualizada

Exemplo de Cenário: Se 100 assinantes estão atualmente conectados no APN "internet" usando o perfil de QoS ID 1, todos os 100 terão seus limites de largura de banda atualizados para 150 Mbps de download / 75 Mbps de upload dentro de segundos após a conclusão da chamada da API.

Nota: Quando você atualiza um perfil de QoS do APN, o sistema **aciona automaticamente a re-autenticação** para todas as sessões PDN ativas usando esse APN, aplicando as novas políticas imediatamente aos assinantes conectados. Nenhuma re-autenticação manual é necessária.

Excluir Recursos:

```
DELETE /api/apn/identifier/{id}
DELETE /api/apn/qos_profile/{id}
DELETE /api/apn/profile/{id}
```

Restrições de Exclusão:

- Não é possível excluir identificadores de APN ou perfis de QoS referenciados por perfis APN
- Não é possível excluir perfis APN atribuídos a assinantes ativos

Modelos de Políticas

Internet de Alta Velocidade (100 Mbps de download / 50 Mbps de upload):

```
{
  "apn_qos_profile": {
    "name": "Internet de Alta Velocidade",
    "qci": 9,
    "allocation_retention_priority": 8,
    "apn_ambr_dl_kbps": 100000,
    "apn_ambr_ul_kbps": 50000,
    "pre_emption_capability": false,
    "pre_emption_vulnerability": true
  }
}
```

Internet Premium (500 Mbps de download / 100 Mbps de upload):

```
{
  "apn_qos_profile": {
    "name": "Internet Premium",
    "qci": 8,
    "allocation_retention_priority": 5,
    "apn_ambr_dl_kbps": 500000,
    "apn_ambr_ul_kbps": 100000,
    "pre_emption_capability": true,
    "pre_emption_vulnerability": false
  }
}
```

IoT/M2M (Baixa Largura de Banda):

```
{
  "apn_qos_profile": {
    "name": "IoT M2M",
    "qci": 9,
    "allocation_retention_priority": 10,
    "apn_ambr_dl_kbps": 1024,
    "apn_ambr_ul_kbps": 512,
    "pre_emption_capability": false,
    "pre_emption_vulnerability": true
  }
}
```

Serviços de Emergência (Maior Prioridade):

```
{
  "apn_qos_profile": {
    "name": "APN de Emergência",
    "qci": 5,
    "allocation_retention_priority": 1,
    "apn_ambr_dl_kbps": 10000,
    "apn_ambr_ul_kbps": 10000,
    "pre_emption_capability": true,
    "pre_emption_vulnerability": false
  }
}
```

Configuração

Configuração do Serviço Diameter

Aplicativo Gx (`config/runtime.exs`):

```
%{
  application_name: :hss_gx,
```

```
  application_dictionary: :diameter_gen_3gpp_gx,
  vendor_specific_application_ids: [
    %{vendor_id: 10415, auth_application_id: 16_777_238}
  ]
}
```

Aplicativo Rx (`config/runtime.exs`):

```
%{
  application_name: :hss_rx,
  application_dictionary: :diameter_gen_3gpp_rx,
  vendor_specific_application_ids: [
    %{vendor_id: 10415, auth_application_id: 16_777_236}
  ]
}
```

Parâmetros de QoS

Os parâmetros de QoS são obtidos de:

- **Portadora Padrão**: Configuração do perfil APN no banco de dados
    - `apn_qos_profile.qci` (Identificador de Classe de QoS)
    - `apn_qos_profile.apn_ambr_ul_kbps` (Taxa Máxima de Bit Agregada Uplink)
    - `apn_qos_profile.apn_ambr_dl_kbps` (Taxa Máxima de Bit Agregada Downlink)
    - `apn_qos_profile.priority_level` (Prioridade de Retenção de Alocação)
- **Portadora Dedicada**: Extraída da Descrição do Componente de Mídia AAR Rx
    - QCI: 1 (Voz Conversacional)
    - Bitrate Garantido: Dos AVPs de Max-Requested-Bandwidth
    - Filtros de fluxo: Dos AVPs de Flow-Description

Tratamento de Erros

Código de Resultado	Tipo	Significado	Causa
2001	Sucesso	DIAMETER_SUCCESS	Solicitação processada com sucesso
5001	Experimental	Usuário não encontrado	IMSI não está no banco de dados de assinantes
5002	Experimental	Sessão não encontrada	A sessão PDN não existe para atualização/terminação

Código de Resultado	Tipo	Significado	Causa
5063	Experimental	Serviço não autorizado	Autorização de mídia IMS negada

Detalhes de Implementação

Gerenciamento de Sessão

O PCRF rastreia:

- **Sessões PDN Ativas** - Uma por APN, por assinante
- **Chamadas VoLTE** - Múltiplas chamadas por sessão IMS (suporta chamadas em conferência)
- **Políticas de QoS** - Aplicadas dinamicamente com base na configuração do APN
- **Regras de Cobrança** - Templates de fluxo de tráfego e políticas específicas de serviço

Recursos Avançados de Política

O PCRF suporta controle avançado de políticas, incluindo:

- **Instalação/remoção de regras de cobrança** via interface Gx
- **Correspondência de Traffic Flow Template (TFT)** para diferenciação de serviços
- **Perfis de velocidade dinâmicos** com base em aplicativo ou tipo de tráfego
- **Políticas conscientes de serviço** acionadas por condições de rede ou comportamento do assinante

Entre em contato com seu administrador de sistema para obter informações sobre como configurar regras de cobrança avançadas e políticas baseadas em TFT.

Documentação Relacionada

- Protocolos Diameter - Especificações detalhadas do protocolo
- Referência da API - Documentação completa da API
- Arquitetura - Arquitetura geral do HSS
- Mapeamento de Dados - Mapeamentos de banco de dados para AVPs Diameter

Tratamento de Erros da API

← Voltar para a Referência da API

Índice

Respostas de Erro Comuns

400 Solicitação Inválida

```
{
  "error": "Formato JSON inválido"
}
```

Causas:

- JSON malformado
- Campos obrigatórios ausentes
- Tipos de dados inválidos

404 Não Encontrado

```
{
  "error": "Recurso não encontrado"
}
```

Causas:

- Assinante/perfil/entidade não existe
- ID incorreto na URL

422 Entidade Não Processável

```
{
  "errors": {
    "imsi": ["já foi utilizado"],
    "key_set_id": ["não existe"]
  }
```

```
}
```

Causas:

- Falhas de validação
- Restrições do banco de dados violadas
- Referências de chave estrangeira não existem

500 Erro Interno do Servidor

```
{
  "error": "Erro interno do servidor"
}
```

Causas:

- Problemas de conectividade com o banco de dados
- Erros inesperados da aplicação

Fluxo de Tratamento de Erros

← Voltar para a Referência da API

Exemplos de Uso da API

← Voltar para a Referência da API

Índice

Provisionamento Completo de Assinante

Este exemplo demonstra o fluxo de trabalho completo para provisionar um novo assinante do zero. O processo envolve a criação de todos os perfis e componentes necessários antes de criar o assinante.

Pré-requisitos: Este exemplo usa `jq` para análise de JSON. Instale com `apt-get install jq` ou `brew install jq`.

Seções Relacionadas:

- Gerenciamento de Conjunto de Chaves
- Perfis APN
- Perfis EPC
- Gerenciamento de Assinantes

```
# 1. Criar Conjunto de Chaves
KEY_SET_ID=$(curl -k -X POST https://hss.example.com:8443/api/key_set
\
  -H "Content-Type: application/json" \
  -d '{
    "key_set": {
      "ki": "0123456789ABCDEF0123456789ABCDEF",
      "opc": "FEDCBA9876543210FEDCBA9876543210",
      "authentication_algorithm": "milenage"
    }
  }' | jq -r '.data.id')

# 2. Criar Perfil de QoS APN
APN_QOS_ID=$(curl -k -X POST https://hss.example.com:8443/api/apn/
qos_profile \
  -H "Content-Type: application/json" \
```

```
  -d '{
    "apn_qos_profile": {
      "name": "Default Internet QoS",
      "qci": 9,
      "allocation_retention_priority": 8,
      "apn_ambr_dl_kbps": 50000,
      "apn_ambr_ul_kbps": 25000
    }
  }' | jq -r '.data.id')

# 3. Criar Identificador APN
APN_ID=$(curl -k -X POST https://hss.example.com:8443/api/apn/
identifier \
  -H "Content-Type: application/json" \
  -d '{
    "apn_identifier": {
      "apn": "internet",
      "ip_version": 2
    }
  }' | jq -r '.data.id')

# 4. Criar Perfil APN
APN_PROFILE_ID=$(curl -k -X POST https://hss.example.com:8443/api/
apn/profile \
  -H "Content-Type: application/json" \
  -d "{
    \"apn_profile\": {
      \"name\": \"Internet APN\",
      \"apn_identifier_id\": $APN_ID,
      \"apn_qos_profile_id\": $APN_QOS_ID
    }
  }" | jq -r '.data.id')

# 5. Criar Perfil EPC
EPC_PROFILE_ID=$(curl -k -X POST https://hss.example.com:8443/api/
epc/profile \
  -H "Content-Type: application/json" \
  -d '{
    "epc_profile": {
      "name": "Standard Data Plan",
      "ue_ambr_dl_kbps": 100000,
      "ue_ambr_ul_kbps": 50000
    }
  }' | jq -r '.data.id')

# 6. Criar Assinante
SUBSCRIBER_ID=$(curl -k -X POST https://hss.example.com:8443/api/
subscriber \
```

```
  -H "Content-Type: application/json" \
  -d "{
    \"subscriber\": {
      \"imsi\": \"001001123456789\",
      \"key_set_id\": $KEY_SET_ID,
      \"epc_profile_id\": $EPC_PROFILE_ID
    }
  }" | jq -r '.data.id')

echo "Assinante provisionado com sucesso com ID: $SUBSCRIBER_ID"
```

O que isso cria:

Este fluxo de trabalho de provisionamento cria um assinante completo com:

1. **Chaves criptográficas** (Conjunto de Chaves) - Para autenticação
2. **Perfil de serviço de dados** (Perfil EPC) - Configurações de largura de banda e acesso à rede
3. **Configuração APN** (Perfil APN) - Ponto de acesso com QoS
4. **Registro de assinante** (Assinante) - A entidade de assinante real

Próximos Passos:

- Adicionar números de telefone: Veja Gerenciamento de MSISDN
- Habilitar serviços de voz: Criar e atribuir Perfil IMS
- Configurar roaming: Criar e atribuir Perfil de Roaming
- Vincular SIM físico: Criar e atribuir SIM

Veja Também:

- Documentação Multi-MSISDN - Atribuindo múltiplos números de telefone
- Documentação de Perfis - Configuração avançada de perfis

Provisionamento Completo de IP Estático

Este exemplo demonstra o provisionamento de um assinante com um endereço IP estático do zero.

Cenário: Provisionar um assinante de dispositivo IoT que precisa de um endereço IPv4 estático no APN "internet".

```
# Pré-requisitos: jq deve estar instalado (apt-get install jq ou brew
install jq)

# 1. Criar Conjunto de Chaves
KEY_SET_ID=$(curl -k -X POST https://hss.example.com:8443/api/key_set
\
```

```
  -H "Content-Type: application/json" \
  -d '{
    "key_set": {
      "ki": "0123456789ABCDEF0123456789ABCDEF",
      "opc": "FEDCBA9876543210FEDCBA9876543210",
      "authentication_algorithm": "milenage"
    }
  }' | jq -r '.data.id')

# 2. Criar Perfil de QoS APN
APN_QOS_ID=$(curl -k -X POST https://hss.example.com:8443/api/apn/
qos_profile \
  -H "Content-Type: application/json" \
  -d '{
    "apn_qos_profile": {
      "name": "IoT Best Effort",
      "qci": 9,
      "allocation_retention_priority": 8,
      "apn_ambr_dl_kbps": 10000,
      "apn_ambr_ul_kbps": 5000
    }
  }' | jq -r '.data.id')

# 3. Criar Identificador APN
APN_ID=$(curl -k -X POST https://hss.example.com:8443/api/apn/
identifier \
  -H "Content-Type: application/json" \
  -d '{
    "apn_identifier": {
      "apn": "internet",
      "ip_version": 0
    }
  }' | jq -r '.data.id')

# 4. Criar Perfil APN
APN_PROFILE_ID=$(curl -k -X POST https://hss.example.com:8443/api/
apn/profile \
  -H "Content-Type: application/json" \
  -d "{
    \"apn_profile\": {
      \"name\": \"IoT Internet APN\",
      \"apn_identifier_id\": $APN_ID,
      \"apn_qos_profile_id\": $APN_QOS_ID
    }
  }" | jq -r '.data.id')

# 5. Criar IP Estático para o APN
STATIC_IP_ID=$(curl -k -X POST https://hss.example.com:8443/api/epc/
```

```
static_ip \
  -H "Content-Type: application/json" \
  -d "{
    \"static_ip\": {
      \"apn_profile_id\": $APN_PROFILE_ID,
      \"ipv4_static_ip\": \"100.64.1.100\"
    }
  }" | jq -r '.data.id')

# 6. Criar Perfil EPC
EPC_PROFILE_ID=$(curl -k -X POST https://hss.example.com:8443/api/
epc/profile \
  -H "Content-Type: application/json" \
  -d '{
    "epc_profile": {
      "name": "IoT Data Plan",
      "ue_ambr_dl_kbps": 10000,
      "ue_ambr_ul_kbps": 5000
    }
  }' | jq -r '.data.id')

# 7. Criar MSISDN (número de telefone)
MSISDN_ID=$(curl -k -X POST https://hss.example.com:8443/api/msisdn \
  -H "Content-Type: application/json" \
  -d '{
    "msisdn": {
      "msisdn": "14155551000"
    }
  }' | jq -r '.data.id')

# 8. Criar Assinante com IP Estático
SUBSCRIBER_ID=$(curl -k -X POST https://hss.example.com:8443/api/
subscriber \
  -H "Content-Type: application/json" \
  -d "{
    \"subscriber\": {
      \"imsi\": \"001001999999999\",
      \"key_set_id\": $KEY_SET_ID,
      \"epc_profile_id\": $EPC_PROFILE_ID,
      \"msisdns\": [$MSISDN_ID],
      \"static_ips\": [$STATIC_IP_ID]
    }
  }" | jq -r '.data.id')

echo "Assinante IoT provisionado com sucesso!"
echo "  ID do Assinante: $SUBSCRIBER_ID"
echo "  IMSI: 001001999999999"
echo "  MSISDN: 14155551000"
```

```
echo "  IPv4 Estático: 100.64.1.100 (no APN 'internet')"
```

O que isso cria:

Este fluxo de trabalho de provisionamento cria um assinante IoT completo com:

1. **Chaves criptográficas** (Conjunto de Chaves) - Para autenticação
2. **Configuração APN** (Perfil APN) - Ponto de acesso "internet"
3. **Atribuição de IP Est��tico** (IP Estático) - Endereço IPv4 fixo 100.64.1.100
4. **Perfil de serviço de dados** (Perfil EPC) - Limites de largura de banda otimizados para IoT
5. **Número de telefone** (MSISDN) - Para identificação do dispositivo
6. **Registro de assinante** (Assinante) - A entidade de assinante completa

Resultado:

Quando este assinante se conecta à rede e se conecta ao APN "internet", ele receberá o endereço IP estático `100.64.1.100` em vez de um endereço DHCP dinâmico.

Próximos Passos:

- Adicionar APNs adicionais com IPs estáticos: Repita os passos 2-5 para cada APN
- Habilitar serviços de voz: Criar e atribuir Perfil IMS
- Configurar roaming: Criar e atribuir Perfil de Roaming
- Vincular SIM físico: Criar e atribuir SIM

Veja Também:

- Gerenciamento de IP Estático - Documentação detalhada sobre IP estático
- Provisionamento Completo de Assinante - Provisionamento básico sem IP estático
- Documentação Multi-MSISDN - Atribuindo múltiplos números de telefone

---

← Voltar para a Referência da API

Referência da API OmniHSS

← Voltar ao Guia de Operações

Índice

Visão Geral da API

URL Base

```
https://[hostname]:8443/api
```

Formato da Solicitação

- **Content-Type:** `application/json`
- **Protocolo:** Somente HTTPS
- **Porta:** 8443 (configurável)

Formato da Resposta

Todas as respostas são em JSON com a seguinte estrutura:

Resposta de Sucesso:

```
{
  "data": { ... }
}
```

Resposta de Erro:

```
{
```

```
  "error": "Descrição da mensagem de erro"
}
```

Códigos de Status HTTP

Código	Significado	Caso de Uso
200	OK	GET, PUT, DELETE bem-sucedidos
201	Criado	POST bem-sucedido
400	Solicitação Inválida	Dados de entrada inválidos
404	Não Encontrado	O recurso não existe
422	Entidade Não Processável	Erro de validação
500	Erro Interno do Servidor	Erro do lado do servidor

Fluxo de Solicitação da API

Gerenciamento de Assinantes

Listar Assinantes

Recuperar todos os assinantes ou filtrar por critérios.

Endpoint: `GET /api/subscriber`

Parâmetros de Consulta:

Parâmetro	Tipo	Descrição
`enabled`	boolean	Filtrar por status habilitado
`ims_enabled`	boolean	Filtrar por status habilitado IMS

Exemplo de Solicitação:

```
curl -k https://hss.example.com:8443/api/subscriber
```

Exemplo de Resposta:

```
{
  "data": [
    {
      "id": 1,
      "imsi": "001001123456789",
      "enabled": true,
      "ims_enabled": true,
      "sim_id": 1,
      "key_set_id": 1,
      "epc_profile_id": 1,
      "ims_profile_id": 1,
      "roaming_profile_id": 1,
      "custom_attributes": {},
      "inserted_at": "2025-10-15T10:30:00Z",
      "updated_at": "2025-10-15T10:30:00Z"
```

```
    }
  ]
}
```

Obter Assinante por ID

Recuperar um assinante específico pelo ID do banco de dados.

Endpoint: `GET /api/subscriber/:id`

Parâmetros de Caminho:

Parâmetro	Tipo	Descrição
`id`	integer	ID do assinante no banco de dados

Exemplo de Solicitação:

```
curl -k https://hss.example.com:8443/api/subscriber/1
```

Obter Assinante por IMSI

Recuperar um assinante pelo seu IMSI.

Endpoint: `GET /api/subscriber/imsi/:imsi`

Parâmetros de Caminho:

Parâmetro	Tipo	Descrição	Formato
`imsi`	string	Identidade Internacional do Assinante Móvel	14-15 dígitos

Exemplo de Solicitação:

```
curl -k https://hss.example.com:8443/api/subscriber/imsi/001001123456789
```

Caso de Uso: Solucionar problemas de um assinante específico pelo seu IMSI.

Obter Assinante por MSISDN

Recuperar um assinante pelo seu número de telefone.

Endpoint: `GET /api/subscriber/msisdn/:msisdn`

Parâmetros de Caminho:

Parâmetro	Tipo	Descrição	Formato
`msisdn`	string	Número ISDN da Estação Móvel	1-15 dígitos (E.164)

Exemplo de Solicitação:

```
curl -k https://hss.example.com:8443/api/subscriber/msisdn/14155551234
```

Caso de Uso: Consultar informações do assinante quando você só tem o número de

telefone.

Criar Assinante

Provisionar um novo assinante.

Endpoint: `POST /api/subscriber`

Corpo da Solicitação:

```
{
  "subscriber": {
    "imsi": "001001123456789",
    "enabled": true,
    "ims_enabled": true,
    "sim_id": 1,
    "key_set_id": 1,
    "epc_profile_id": 1,
    "ims_profile_id": 1,
    "roaming_profile_id": 1,
    "custom_attributes": {
      "note": "Assinante de teste"
    }
  }
}
```

Campos Obrigatórios:

- `imsi` - Deve ter 14-15 dígitos, único
- `key_set_id` - Deve referenciar um Conjunto de Chaves existente
- `epc_profile_id` - Deve referenciar um Perfil EPC existente

Campos Opcionais:

- `enabled` - Padrão: true
- `ims_enabled` - Padrão: true
- `sim_id` - Referência ao cartão SIM
- `ims_profile_id` - Referência ao Perfil IMS (necessário para serviços IMS)
- `roaming_profile_id` - Referência ao Perfil de Roaming (necessário para controle de roaming)
- `msisdns` - Array de IDs de MSISDN (números de telefone)
- `static_ips` - Array de IDs de IP Estático para atribuições de APN
- `custom_attributes` - Pares chave-valor personalizados

Veja Também:

- Exemplo Completo de Provisionamento de Assinante - Fluxo de trabalho de ponta a ponta
- Documentação Multi-MSISDN - Atribuindo números de telefone a assinantes
- Gerenciamento de IP Estático - Atribuindo IPs estáticos a APNs

Exemplo de Solicitação:

```
curl -k -X POST https://hss.example.com:8443/api/subscriber \
  -H "Content-Type: application/json" \
  -d '{
    "subscriber": {
      "imsi": "001001123456789",
      "key_set_id": 1,
      "epc_profile_id": 1
    }
  }'
```

Fluxo de Provisionamento:

Atualizar Assinante

Modificar um assinante existente.

Endpoint: `PUT /api/subscriber/:id`

Parâmetros de Caminho:

Parâmetro	Tipo	Descrição
`id`	integer	ID do assinante no banco de dados

Corpo da Solicitação:

```
{
  "subscriber": {
    "enabled": false,
    "ims_enabled": false,
    "epc_profile_id": 2,
    "custom_attributes": {
      "note": "Desativado temporariamente"
    }
  }
}
```

Campos Atualizáveis:

- `enabled` - Habilitar/desabilitar todos os serviços
- `ims_enabled` - Habilitar/desabilitar serviços IMS
- `sim_id` - Alterar atribuição de cartão SIM
- `key_set_id` - Alterar chaves criptográficas (cuidado!)
- `epc_profile_id` - Alterar perfil de serviço de dados
- `ims_profile_id` - Alterar perfil de serviço de voz
- `roaming_profile_id` - Alterar política de roaming
- `msisdns` - Atualizar números de telefone atribuídos ao assinante
- `static_ips` - Atualizar atribuições de IP estático para APNs
- `custom_attributes` - Atualizar dados personalizados

Não Atualizável:

- `imsi` - Não pode alterar IMSI (excluir e recriar em vez disso)

Veja Também:

- Gerenciamento de Perfis - Gerenciando perfis de serviço

Exemplo de Solicitação:

```
curl -k -X PUT https://hss.example.com:8443/api/subscriber/1 \
  -H "Content-Type: application/json" \
  -d '{
    "subscriber": {
      "enabled": false
    }
  }'
```

Casos de Uso:

- Desativar temporariamente o assinante: `{"enabled": false}`
- Desativar apenas os serviços de voz: `{"ims_enabled": false}`
- Alterar perfil de serviço: `{"epc_profile_id": 2}` (veja Perfis EPC)
- Atualizar política de roaming: `{"roaming_profile_id": 3}` (veja Gerenciamento de Roaming)

Excluir Assinante

Remover um assinante do sistema.

Endpoint: `DELETE /api/subscriber/:id`

Parâmetros de Caminho:

Parâmetro	Tipo	Descrição
`id`	integer	ID do assinante no banco de dados

Exemplo de Solicitação:

```
curl -k -X DELETE https://hss.example.com:8443/api/subscriber/1
```

Aviso: Isso exclui permanentemente o assinante e todos os dados de estado associados (sessões PDN, chamadas, etc.). O IMSI pode ser reutilizado após a exclusão.

Nota: Excluir um assinante NÃO exclui os associados:

- Conjunto de Chaves - Pode ser reutilizado para outros assinantes
- SIM - Pode ser reatribuído a um novo assinante
- Perfis - Recursos compartilhados usados por vários assinantes
- MSISDNs - Devem ser excluídos separadamente, se desejado

Cancelar Solicitação de Localização (Desconexão Forçada)

Enviar uma Solicitação de Cancelamento de Localização (CLR) para forçar a desconexão de um assinante do seu MME atualmente registrado.

Endpoint: `POST /api/subscriber/cancel_location`

Corpo da Solicitação:

```
{
  "imsi": "001001123456789"
}
```

Parâmetros:

Parâmetro	Tipo	Obrigatório	Descrição
`imsi`	string	Sim	IMSI do assinante a ser desconectado (14-15 dígitos)

Exemplo de Solicitação:

```
curl -k -X POST https://hss.example.com:8443/api/subscriber/cancel_location
\
  -H "Content-Type: application/json" \
  -d '{"imsi": "001001123456789"}'
```

Resposta de Sucesso (200 OK):

```
{
  "data": {
    "message": "Solicitação de Cancelamento de Localização enviada com
sucesso",
    "imsi": "001001123456789",
    "destination_host": "mme01.operator.com",
    "destination_realm": "epc.operator.com"
  }
}
```

Resposta de Erro (404 Não Encontrado):

```
{
  "error": "Assinante não encontrado ou não registrado atualmente em nenhum
MME"
}
```

Comportamento:

- Envia S6a CLR para o MME onde o assinante está atualmente registrado (`subscriber_state.last_seen_mme`)
- Usa `Cancellation-Type: subscription_withdrawal` (força desconexão total)
- Define `CLR-Flags: {s6a_indicator: 1, reattach_required: 1}` (UE deve reautenticar)
- Retorna 404 se o assinante nunca se registrou ou `last_seen_mme` é nulo
- **Afeta todos os MSISDNs** associados ao IMSI (mesmo dispositivo/SIM físico)

Casos de Uso:

- **Prevenção de Fraude:** Desconectar imediatamente assinante suspeito
- **Rescisão de Assinatura:** Forçar logout quando a conta é desativada
- **Solução de Problemas:** Limpar registro MME obsoleto para depuração
- **Migração:** Forçar reautenticação para aplicar novas configurações de perfil

- **Segurança:** Desconectar imediatamente assinante comprometido

Considerações Multi-IMSI:

Ao usar CLR com cenários multi-MSISDN:

1. **Múltiplos MSISDNs, Um Único IMSI:**

   ```
   // Assinante com IMSI 001001123456789 com MSISDNs ["+1234567890",
   "+9876543210"]
   POST /api/subscriber/cancel_location
   {"imsi": "001001123456789"}

   // Resultado: Um CLR enviado, ambos os MSISDNs afetados (mesmo
   dispositivo)
   ```

2. **IMSI Diferentes (Dispositivos Diferentes):**

   ```
   // Dois assinantes com o mesmo MSISDN, mas IMSIs diferentes (cenário de
   portabilidade de número)
   // Assinante A: IMSI 001001111111111, MSISDN "+1234567890"
   // Assinante B: IMSI 001001222222222, MSISDN "+1234567890"

   POST /api/subscriber/cancel_location
   {"imsi": "001001111111111"}

   // Resultado: Apenas Assinante A desconectado, Assinante B não afetado
   ```

Notas Importantes:

- **Baseado em IMSI:** CLR é sempre enviado por IMSI, não por MSISDN
- **Assíncrono:** CLR é enviado de forma assíncrona; a resposta de sucesso significa que o CLR foi enviado, não que o MME o processou
- **Sem validação do status do MME:** CLR é enviado mesmo que o MME esteja inacessível (comportamento padrão do HSS)
- **Idempotente:** Seguro chamar várias vezes para o mesmo IMSI

Documentação Relacionada:

- Fluxo de Protocolo de Solicitação de Cancelamento de Localização
- Cenários Multi-IMSI
- Arquitetura da Interface S6a

Gerenciamento de MSISDN

MSISDNs (números de telefone) podem ser atribuídos a assinantes para habilitar serviços de voz. Veja Documentação Multi-MSISDN para detalhes sobre a atribuição de vários números a um único assinante.

Listar MSISDNs

Recuperar todos os números de telefone.

Endpoint: `GET /api/msisdn`

Exemplo de Solicitação:

```
curl -k https://hss.example.com:8443/api/msisdn
```

Obter MSISDN

Recuperar um número de telefone específico.

Endpoint: `GET /api/msisdn/:id`

Exemplo de Solicitação:

```
curl -k https://hss.example.com:8443/api/msisdn/1
```

Criar MSISDN

Criar um novo número de telefone.

Endpoint: `POST /api/msisdn`

Corpo da Solicitação:

```
{
  "msisdn": {
    "msisdn": "14155551234"
  }
}
```

Validação:

- Deve ter 1-15 dígitos
- Deve ser único
- Deve seguir o formato E.164 (formato internacional sem sinal de +)

Exemplo de Solicitação:

```
curl -k -X POST https://hss.example.com:8443/api/msisdn \
  -H "Content-Type: application/json" \
  -d '{
    "msisdn": {
      "msisdn": "14155551234"
    }
  }'
```

Atribuir MSISDN a Assinante

Para atribuir um número de telefone a um assinante, você precisa criar um registro de junção. Isso é tipicamente feito através do endpoint de atualização do assinante ou via manipulação direta do banco de dados.

Padrão Multi-MSISDN:

Veja Recursos Multi-MSISDN e Multi-IMSI para uso detalhado.

Excluir MSISDN

Remover um número de telefone.

Endpoint: `DELETE /api/msisdn/:id`

Exemplo de Solicitação:

```
curl -k -X DELETE https://hss.example.com:8443/api/msisdn/1
```

Gerenciamento de SIM

Os registros de cartão SIM armazenam informações físicas do cartão SIM, incluindo ICCID, detalhes do fornecedor, códigos PIN/PUK e chaves OTA. Os registros de SIM podem ser opcionalmente vinculados a assinantes.

Veja Também:

- Documentação Multi-IMSI - Vários assinantes em um único SIM físico

Listar SIMs

Recuperar todos os cartões SIM.

Endpoint: `GET /api/sim`

Exemplo de Solicitação:

```
curl -k https://hss.example.com:8443/api/sim
```

Obter SIM

Recuperar um cartão SIM específico.

Endpoint: `GET /api/sim/:id`

Exemplo de Solicitação:

```
curl -k https://hss.example.com:8443/api/sim/1
```

Criar SIM

Criar um novo registro de cartão SIM.

Endpoint: `POST /api/sim`

Corpo da Solicitação:

```
{
```

```
  "sim": {
    "iccid": "8991101200003204510",
    "sim_vendor": "Gemalto",
    "batch_name": "2025-Q1-Batch-01",
    "is_esim": false,
    "pin1": "1234",
    "pin2": "5678",
    "puk1": "12345678",
    "puk2": "87654321",
    "adm1": "admin-code-1",
    "kic": "0123456789ABCDEF0123456789ABCDEF",
    "kid": "FEDCBA9876543210FEDCBA9876543210"
  }
}
```

Campos Obrigatórios:

- `iccid` - 19-20 dígitos, único

Campos Opcionais, mas Importantes:

- `sim_vendor` - Nome do fabricante
- `batch_name` - Para rastreamento
- `is_esim` - Flag booleana para eSIM
- `pin1`, `pin2` - Códigos PIN do usuário final
- `puk1`, `puk2` - Códigos de desbloqueio PIN
- `adm1-adm10` - Códigos administrativos
- `kic`, `kid` - Chaves de segurança OTA (string hexadecimal)

Exemplo de Solicitação:

```
curl -k -X POST https://hss.example.com:8443/api/sim \
  -H "Content-Type: application/json" \
  -d '{
    "sim": {
      "iccid": "8991101200003204510",
      "sim_vendor": "Gemalto"
    }
  }'
```

Atualizar SIM

Modificar os dados do cartão SIM.

Endpoint: `PUT /api/sim/:id`

Exemplo de Solicitação:

```
curl -k -X PUT https://hss.example.com:8443/api/sim/1 \
  -H "Content-Type: application/json" \
  -d '{
    "sim": {
      "batch_name": "Nome do Lote Atualizado"
```

```
    }
  }'
```

Excluir SIM

Remover um registro de cartão SIM.

Endpoint: `DELETE /api/sim/:id`

Aviso: Certifique-se de que nenhum assinante faça referência a este SIM antes de excluí-lo.

Gerenciamento de Conjunto de Chaves

Os conjuntos de chaves contêm o material criptográfico (Ki, OPC/OP, AMF, SQN) usado para autenticação de assinantes via o algoritmo Milenage. Cada assinante deve referenciar um conjunto de chaves.

Veja Também:

- Fluxos de Protocolo - Procedimentos de autenticação usando conjuntos de chaves

Listar Conjuntos de Chaves

Recuperar todos os conjuntos de chaves criptográficas.

Endpoint: `GET /api/key_set`

Exemplo de Solicitação:

```
curl -k https://hss.example.com:8443/api/key_set
```

Obter Conjunto de Chaves

Recuperar um conjunto de chaves específico.

Endpoint: `GET /api/key_set/:id`

Exemplo de Solicitação:

```
curl -k https://hss.example.com:8443/api/key_set/1
```

Exemplo de Resposta:

```
{
  "data": {
    "id": 1,
    "ki": "0123456789ABCDEF0123456789ABCDEF",
    "opc": "FEDCBA9876543210FEDCBA9876543210",
    "op": null,
    "amf": "8000",
```

```
    "sqn": 0,
    "authentication_algorithm": "milenage",
    "ota_counter": 0
  }
}
```

Criar Conjunto de Chaves

Criar um novo conjunto de chaves criptográficas.

Endpoint: `POST /api/key_set`

Corpo da Solicitação:

```
{
  "key_set": {
    "ki": "0123456789ABCDEF0123456789ABCDEF",
    "opc": "FEDCBA9876543210FEDCBA9876543210",
    "amf": "8000",
    "sqn": 0,
    "authentication_algorithm": "milenage"
  }
}
```

Campos Obrigatórios:

- `ki` - Chave de 128 bits (32 caracteres hexadecimais)
- Ou `opc` OU `op` (OPC pode ser derivado de OP)
- `authentication_algorithm` - Atualmente apenas "milenage"

Campos Opcionais:

- `amf` - Padrão: "8000"
- `sqn` - Padrão: 0
- `ota_counter` - Padrão: 0

Formato da Chave:

- Todas as chaves são strings hexadecimais
- Ki, OPC, OP: 32 caracteres hexadecimais (128 bits)
- AMF: 4 caracteres hexadecimais (16 bits)

Exemplo de Solicitação:

```
curl -k -X POST https://hss.example.com:8443/api/key_set \
  -H "Content-Type: application/json" \
  -d '{
    "key_set": {
      "ki": "0123456789ABCDEF0123456789ABCDEF",
      "opc": "FEDCBA9876543210FEDCBA9876543210",
      "authentication_algorithm": "milenage"
    }
  }'
```

Aviso de Segurança: Conjuntos de chaves contêm material criptográfico altamente sensível. Proteja o acesso à API de acordo.

Atualizar Conjunto de Chaves

Modificar um conjunto de chaves existente.

Endpoint: `PUT /api/key_set/:id`

Aviso: Alterar chaves para um assinante ativo causará falhas de autenticação. Atualize as chaves apenas durante janelas de manutenção ou para novos assinantes.

Impacto: Atualizações afetam todos os assinantes que usam este conjunto de chaves imediatamente. Assinantes ativos falharão na autenticação na próxima tentativa de conexão.

Excluir Conjunto de Chaves

Remover um conjunto de chaves.

Endpoint: `DELETE /api/key_set/:id`

Aviso: Certifique-se de que nenhum assinante faça referência a este conjunto de chaves antes de excluí-lo. Consulte os assinantes primeiro para verificar referências.

Gerenciamento de Perfis

Perfis EPC

Os perfis EPC (Evolved Packet Core) definem parâmetros de serviço de dados para assinantes. Esses perfis são referenciados ao criar assinantes.

Listar Perfis EPC

Endpoint: `GET /api/epc/profile`

Obter Perfil EPC

Endpoint: `GET /api/epc/profile/:id`

Criar Perfil EPC

Endpoint: `POST /api/epc/profile`

Corpo da Solicitação:

```
{
  "epc_profile": {
    "name": "Plano de Dados Padrão",
    "ue_ambr_dl_kbps": 100000,
```

```
    "ue_ambr_ul_kbps": 50000,
    "network_access_mode": 0,
    "tracking_area_update_interval_seconds": 54
  }
}
```

Campos:

Campo	Descrição	Unidades	Valores Típicos
`name`	Nome do perfil	Texto	Identificador único
`ue_ambr_dl_kbps`	Limite de largura de banda de download	Kbps	10000-1000000
`ue_ambr_ul_kbps`	Limite de largura de banda de upload	Kbps	5000-500000
`network_access_mode`	Tipo de acesso	Enum	0=Somente Pacote, 2=Pacote+Reservado
`tracking_area_update_interval_seconds`	Temporizador TAU	Segundos	54 (típico)

Exemplo de Solicitação:

```
curl -k -X POST https://hss.example.com:8443/api/epc/profile \
  -H "Content-Type: application/json" \
  -d '{
    "epc_profile": {
      "name": "Premium 100Mbps",
      "ue_ambr_dl_kbps": 100000,
      "ue_ambr_ul_kbps": 50000
    }
  }'
```

Veja Também:

- Documentação de Perfis - Guia de configuração de perfil detalhado
- Provisionamento Completo de Assinante - Usando perfis EPC no provisionamento

Atualizar Perfil EPC

Endpoint: `PUT /api/epc/profile/:id`

Nota: Alterações nos perfis EPC afetam todos os assinantes que usam este perfil. Sessões ativas podem precisar ser restabelecidas.

Excluir Perfil EPC

Endpoint: `DELETE /api/epc/profile/:id`

Aviso: Certifique-se de que nenhum assinante faça referência a este perfil antes de excluí-lo.

Perfis IMS

Os perfis IMS (IP Multimedia Subsystem) definem parâmetros de serviço de voz e Critérios de Filtro Iniciais (IFC) para assinantes. Esses perfis são referenciados ao criar assinantes com serviços IMS habilitados.

Listar Perfis IMS

Endpoint: `GET /api/ims/profile`

Criar Perfil IMS

Endpoint: `POST /api/ims/profile`

Corpo da Solicitação:

```
{
  "ims_profile": {
    "name": "VoLTE Padrão",
    "ifc_template": "<IMS-XML-Template-Here>"
  }
}
```

Veja Também:

- Documentação de Perfis - Detalhes e exemplos do template IFC
- Fluxos de Protocolo - Fluxos de registro IMS e chamadas

Perfis APN

Os perfis APN (Access Point Name) consistem em três componentes que trabalham juntos:

1. **Identificador APN** - Define o nome do APN e a versão IP
2. **Perfil QoS APN** - Define parâmetros de Qualidade de Serviço
3. **Perfil APN** - Combina identificador e QoS, vinculado a Perfis EPC

Veja Documentação PCRF para configuração detalhada de políticas, gerenciamento de QoS e reautenticação automática. Veja também Documentação de Perfis para exemplos de configuração de APN.

Listar Identificadores APN

Endpoint: `GET /api/apn/identifier`

Criar Identificador APN

Endpoint: `POST /api/apn/identifier`

Corpo da Solicitação:

```
{
  "apn_identifier": {
    "apn": "internet",
    "ip_version": 2
  }
}
```

Valores da Versão IP:

- `0` - Apenas IPv4
- `1` - Apenas IPv6
- `2` - IPv4v6 (dual stack)
- `3` - IPv4 ou IPv6 (escolha da rede)

Listar Perfis QoS APN

Endpoint: `GET /api/apn/qos_profile`

Criar Perfil QoS APN

Endpoint: `POST /api/apn/qos_profile`

Corpo da Solicitação:

```
{
  "apn_qos_profile": {
    "name": "Internet de Melhor Esforço",
    "qci": 9,
    "allocation_retention_priority": 8,
    "apn_ambr_dl_kbps": 50000,
    "apn_ambr_ul_kbps": 25000,
    "pre_emption_capability": false,
    "pre_emption_vulnerability": true
  }
}
```

Listar Perfis APN

Endpoint: `GET /api/apn/profile`

Criar Perfil APN

Endpoint: `POST /api/apn/profile`

Corpo da Solicitação:

```
{
  "apn_profile": {
    "name": "APN de Internet",
    "apn_identifier_id": 1,
    "apn_qos_profile_id": 1
  }
```

```
}
```

Campos Obrigatórios:

- `apn_identifier_id` - Deve referenciar um Identificador APN existente
- `apn_qos_profile_id` - Deve referenciar um Perfil QoS APN existente

Veja Também:

- Provisionamento Completo de Assinante - Exemplo completo incluindo configuração de APN
- Perfis EPC - Perfis APN estão vinculados a perfis EPC

Gerenciamento de IP Estático

Endereços IP estáticos podem ser atribuídos a APNs específicos para assinantes individuais. Isso permite que os assinantes recebam um endereço IPv4 e/ou IPv6 predeterminado ao se conectar a um APN específico, em vez de receber um endereço dinâmico de um pool DHCP.

Arquitetura:

Fluxo de Dados Quando o Assinante Conecta:

Resposta de Atualização de Localização - Mapeamento de Dados de Configuração do APN:

Este diagrama mostra exatamente de onde cada campo no AVP de Configuração do APN da Resposta de Atualização de Localização S6a vem no banco de dados:

Observações Chave:

1. **Identificador de Contexto**: Índice sequencial (0, 1, 2...) para cada APN no perfil
2. **Seleção de Serviço**: Vem diretamente de `apn_identifier.apn` (ex: "internet", "ims")
3. **Tipo de PDN**: Codificado a partir de `apn_identifier.ip_version` (ipv4=0, ipv6=1, ipv4v6=2, ipv4_ou_ipv6=3)
4. **Parâmetros QoS**: Todos da tabela `apn_qos_profile`
5. **Largura de Banda AMBR**: Valores são multiplicados por 1000 (kbps → bps)
6. **Endereço IP do Parte Servida**: Incluído apenas se um IP estático existir para esta combinação assinante+APN
    - Processo de busca: `subscriber.static_ips` → filtrar por `apn_profile_id` → extrair IPs
    - Compatibilidade da versão IP verificada em relação a `apn_identifier.ip_version`
7. **VPLMN-Dynamic-Address-Allowed**: Codificado como 0 (não permitido) - força o uso de IP estático se fornecido

Hierarquia de Relacionamento:

Conceitos Chave:

- **Atribuição por APN**: Cada IP Estático está vinculado a um Perfil APN específico
- **Um IP por APN por Assinante**: Um assinante pode ter apenas uma atribuição de IP estático por APN
- **Suporte IPv4 e IPv6**: IPs estáticos podem ser apenas IPv4, apenas IPv6 ou dual-stack
- **Unicidade Global do IP**: Cada endereço IP deve ser globalmente único em **todos** os registros de IP estático no sistema
  - O mesmo endereço IPv4 ou IPv6 não pode ser atribuído a vários assinantes (mesmo em APNs diferentes)
  - Isso previne conflitos de roteamento e ambiguidade de endereço IP
  - Imposto por índices únicos no banco de dados nos campos `ipv4_static_ip` e `ipv6_static_ip`
- **Relacionamento Muitos-para-Muitos**: Assinantes e IPs Estáticos estão vinculados através de uma tabela de junção

Casos de Uso:

- Endereços IP fixos para dispositivos IoT
- Hospedagem de servidores em dispositivos móveis (requer IP estático para conexões de entrada)
- Aplicações legadas que requerem endereços IP específicos
- Roteamento de políticas de rede baseado em IP de origem
- Conformidade regulatória que requer rastreamento de endereços IP

Listar IPs Estáticos

Recuperar todas as atribuições de IP estático.

Endpoint: `GET /api/epc/static_ip`

Exemplo de Solicitação:

```
curl -k https://hss.example.com:8443/api/epc/static_ip
```

Exemplo de Resposta:


```
{
  "data": [
    {
      "id": 1,
      "apn_profile_id": 5,
      "ipv4_static_ip": "100.64.1.1",
      "ipv6_static_ip": "2606:4700:4700::1111",
      "apn_profile": {
        "id": 5,
        "name": "APN de Internet",
        "apn_identifier": {
          "apn": "internet",
          "ip_version": "ipv4v6"
        }
      },
      "inserted_at": "2025-11-15T10:30:00Z",
      "updated_at": "2025-11-15T10:30:00Z"
```

```
    }
  ]
}
```

Obter IP Estático

Recuperar uma atribuição de IP estático específica.

Endpoint: `GET /api/epc/static_ip/:id`

Parâmetros de Caminho:

Parâmetro	Tipo	Descrição
`id`	integer	ID do IP estático no banco de dados

Exemplo de Solicitação:

```
curl -k https://hss.example.com:8443/api/epc/static_ip/1
```

Criar IP Estático

Criar uma nova atribuição de IP estático para um APN.

Endpoint: `POST /api/epc/static_ip`

Corpo da Solicitação:

```
{
  "static_ip": {
    "apn_profile_id": 5,
    "ipv4_static_ip": "100.64.1.1",
    "ipv6_static_ip": "2606:4700:4700::1111"
  }
}
```

Campos Obrigatórios:

- `apn_profile_id` - Deve referenciar um Perfil APN existente
- Pelo menos um dos `ipv4_static_ip` OU `ipv6_static_ip` deve ser especificado

Campos Opcionais:

- `ipv4_static_ip` - Endereço IPv4 (notação decimal pontuada)
- `ipv6_static_ip` - Endereço IPv6 (notação padrão)

Validação do Formato do IP:

- IPv4: Formato decimal pontuado padrão (ex: `100.64.1.1`)
- IPv6: Formato hexadecimal separado por dois pontos padrão (ex: `2606:4700:4700::1111`)
- Ambos os endereços IPv4 e IPv6 devem ser **globalmente únicos em todos os registros de IP estático**
  - Isso previne conflitos de endereço IP na rede

- O mesmo IP não pode ser atribuído a vários assinantes, mesmo em APNs diferentes
- Esta é uma restrição de nível de banco de dados imposta por índices únicos

Opções de Configuração:

Configuração	IPv4	IPv6	Exemplo
Apenas IPv4	✓	-	`{"ipv4_static_ip": "100.64.1.1"}`
Apenas IPv6	-	✓	`{"ipv6_static_ip": "2606:4700:4700::1111"}`
Dual Stack	✓	✓	Ambos os campos especificados

Exemplos de Solicitações:

IP Estático apenas IPv4:

```
curl -k -X POST https://hss.example.com:8443/api/epc/static_ip \
  -H "Content-Type: application/json" \
  -d '{
    "static_ip": {
      "apn_profile_id": 5,
      "ipv4_static_ip": "100.64.1.1"
    }
  }'
```

IP Estático apenas IPv6:

```
curl -k -X POST https://hss.example.com:8443/api/epc/static_ip \
  -H "Content-Type: application/json" \
  -d '{
    "static_ip": {
      "apn_profile_id": 6,
      "ipv6_static_ip": "2606:4700:4700::1111"
    }
  }'
```

IP Estático Dual-stack:

```
curl -k -X POST https://hss.example.com:8443/api/epc/static_ip \
  -H "Content-Type: application/json" \
  -d '{
    "static_ip": {
      "apn_profile_id": 5,
      "ipv4_static_ip": "100.64.1.1",
      "ipv6_static_ip": "2606:4700:4700::1111"
    }
  }'
```

Resposta de Sucesso (201 Criado):

```
{
  "data": {
    "id": 1,
    "apn_profile_id": 5,
```

```
    "ipv4_static_ip": "100.64.1.1",
    "ipv6_static_ip": "2606:4700:4700::1111",
    "inserted_at": "2025-11-15T10:30:00Z",
    "updated_at": "2025-11-15T10:30:00Z"
  }
}
```

Veja Também:

- Atribuir IP Estático a Assinante - Como vincular isso a um assinante
- Perfis APN - Gerenciando configurações de APN

Atualizar IP Estático

Modificar uma atribuição de IP estático existente.

Endpoint: `PUT /api/epc/static_ip/:id`

Parâmetros de Caminho:

Parâmetro	Tipo	Descrição
`id`	integer	ID do IP estático no banco de dados

Corpo da Solicitação:

```
{
  "static_ip": {
    "ipv4_static_ip": "100.64.1.2",
    "ipv6_static_ip": "2606:4700:4700::1112"
  }
}
```

Campos Atualizáveis:

- `ipv4_static_ip` - Alterar endereço IPv4
- `ipv6_static_ip` - Alterar endereço IPv6
- `apn_profile_id` - Alterar atribuição de APN

Não Atualizável:

- `id` - Chave primária (somente leitura)

Aviso: Alterar o endereço IP para um assinante ativo afetará sua próxima conexão PDN. Sessões PDN ativas continuarão a usar o IP antigo até desconectar e reconectar.

Exemplo de Solicitação:

```
curl -k -X PUT https://hss.example.com:8443/api/epc/static_ip/1 \
  -H "Content-Type: application/json" \
  -d '{
    "static_ip": {
      "ipv4_static_ip": "100.64.1.2"
    }
```

```
  }'
```

Excluir IP Estático

Remover uma atribuição de IP estático.

Endpoint: `DELETE /api/epc/static_ip/:id`

Parâmetros de Caminho:

Parâmetro	Tipo	Descrição
`id`	integer	ID do IP estático no banco de dados

Exemplo de Solicitação:

```
curl -k -X DELETE https://hss.example.com:8443/api/epc/static_ip/1
```

Comportamento:

- Remove a atribuição de IP estático
- NÃO afeta o Perfil APN (APN continua disponível para outros assinantes)
- Assinantes usando este IP estático receberão IPs dinâmicos na próxima conexão
- O endereço IP se torna disponível para reutilização após a exclusão

Aviso: Se um assinante estiver usando ativamente este IP estático, excluí-lo fará com que ele receba um IP dinâmico na próxima conexão PDN. Certifique-se de que os assinantes estejam offline ou envie uma Solicitação de Cancelamento de Localização antes de excluir.

Atribuir IP Estático a Assinante

Para atribuir um IP estático a um assinante, você precisa associar o registro de IP Estático ao Assinante durante a criação ou atualização.

Padrão de Atribuição:

1. **Criar o IP Estático** (veja Criar IP Estático)
2. **Atribuir ao Assinante** usando o campo `static_ips`

Criar Assinante com IP Estático:

```
# Passo 1: Criar IP estático para APN "internet"
STATIC_IP_ID=$(curl -k -X POST https://hss.example.com:8443/api/epc/
static_ip \
  -H "Content-Type: application/json" \
  -d '{
    "static_ip": {
      "apn_profile_id": 5,
      "ipv4_static_ip": "100.64.1.1",
      "ipv6_static_ip": "2606:4700:4700::1111"
    }
  }' | jq -r '.data.id')

# Passo 2: Criar assinante com IP estático atribuído
```

```
curl -k -X POST https://hss.example.com:8443/api/subscriber \
  -H "Content-Type: application/json" \
  -d "{
    \"subscriber\": {
      \"imsi\": \"001001123456789\",
      \"key_set_id\": 1,
      \"epc_profile_id\": 1,
      \"static_ips\": [$STATIC_IP_ID]
    }
  }"
```

Atualizar Assinante Existente com IP Estático:

```
curl -k -X PUT https://hss.example.com:8443/api/subscriber/1 \
  -H "Content-Type: application/json" \
  -d '{
    "subscriber": {
      "static_ips": [1, 2]
    }
  }'
```

Múltiplos IPs Estáticos (APNs Diferentes):

Um assinante pode ter vários IPs estáticos, desde que cada um seja para um APN diferente:

```
# Criar IP estático para APN "internet"
INTERNET_IP=$(curl -k -X POST https://hss.example.com:8443/api/epc/static_ip
\
  -H "Content-Type: application/json" \
  -d '{
    "static_ip": {
      "apn_profile_id": 5,
      "ipv4_static_ip": "100.64.1.1"
    }
  }' | jq -r '.data.id')

# Criar IP estático para APN "ims"
IMS_IP=$(curl -k -X POST https://hss.example.com:8443/api/epc/static_ip \
  -H "Content-Type: application/json" \
  -d '{
    "static_ip": {
      "apn_profile_id": 6,
      "ipv4_static_ip": "100.64.2.1"
    }
  }' | jq -r '.data.id')

# Atribuir ambos ao assinante
curl -k -X POST https://hss.example.com:8443/api/subscriber \
  -H "Content-Type: application/json" \
  -d "{
    \"subscriber\": {
      \"imsi\": \"001001123456789\",
```

```
      \"key_set_id\": 1,
      \"epc_profile_id\": 1,
      \"static_ips\": [$INTERNET_IP, $IMS_IP]
    }
  }"
```

Regras de Validação:

- ✓ **Permitido**: Vários IPs estáticos para APNs diferentes
- ✗ **Rejeitado**: Vários IPs estáticos para o mesmo APN

Exemplo de Erro - APN Duplicada:

```
# Isso irá FALHAR se ambos os IPs estáticos referenciam o mesmo APN
curl -k -X POST https://hss.example.com:8443/api/subscriber \
  -H "Content-Type: application/json" \
  -d '{
    "subscriber": {
      "imsi": "001001123456789",
      "static_ips": [1, 2]
    }
  }'

# Resposta de Erro:
{
  "errors": {
    "static_ips": [
      "IPs estáticos por APN por assinante devem ser únicos. Ex: um
assinante não pode ser atribuído ao IP estático 100.64.1.1 para internet e
também 100.64.1.2 para internet"
    ]
  }
}
```

Veja Também:

- Criar Assinante - Provisionamento de assinante
- Atualizar Assinante - Modificando a configuração do assinante
- Exemplo Completo de Provisionamento de IP Estático - Fluxo de trabalho de ponta a ponta

---

Gerenciamento de Roaming

Os perfis de roaming controlam se os assinantes podem acessar serviços de dados e IMS em redes visitadas. Os perfis são atribuídos a assinantes e consistem em regras correspondentes a MCC/MNC.

Listar Perfis de Roaming

Endpoint: `GET /api/roaming/profile`

Criar Perfil de Roaming

Endpoint: `POST /api/roaming/profile`

Corpo da Solicitação:

```
{
  "roaming_profile": {
    "name": "Apenas Operadoras dos EUA",
    "data_action_if_no_rules_match": 1,
    "ims_action_if_no_rules_match": 1
  }
}
```

Valores de Ação:

- `0` - Permitir
- `1` - Negar

Ações Padrão:

- `data_action_if_no_rules_match` - Ação quando nenhuma regra de roaming corresponde
- `ims_action_if_no_rules_match` - Ação padrão específica do IMS

Listar Regras de Roaming

Endpoint: `GET /api/roaming/rule`

Criar Regra de Roaming

Endpoint: `POST /api/roaming/rule`

Corpo da Solicitação:

```
{
  "roaming_rule": {
    "name": "Permitir AT&T",
    "mcc": "310",
    "mnc": "410",
    "data_action": 0,
    "ims_action": 0
  }
}
```

Campos:

- `mcc` - Código do País Móvel (3 dígitos)
- `mnc` - Código da Rede Móvel (2-3 dígitos)
- `data_action` - Permitir (0) ou Negar (1) serviços de dados
- `ims_action` - Permitir (0) ou Negar (1) serviços IMS/voz

Veja Também:

- Documentação de Roaming - Configuração detalhada e exemplos
- Fluxos de Protocolo - Como o controle de roaming funciona em fluxos Diameter

---

Gerenciamento de EIR

OmniHSS funciona como um Registro de Identidade de Equipamento (EIR) via a interface Diameter S13. As regras de EIR controlam o acesso de dispositivos com base em padrões de IMEI.

Veja Documentação de EIR para verificação detalhada de identidade de equipamentos, fluxos de interface S13 e validação de IMEI.

Listar Regras de EIR

Endpoint: `GET /api/eir/rule`

Criar Regra de EIR

Endpoint: `POST /api/eir/rule`

Corpo da Solicitação:

```
{
  "eir_rule": {
    "name": "Bloquear iPhone 6",
    "imei_regex": "^35[0-9]{6}0[0-9]{7}$",
    "action": 1
  }
}
```

Campos:

- `name` - Nome descritivo para a regra
- `imei_regex` - Expressão regular para corresponder a números IMEI
- `action` - Lista branca (0), Lista negra (1) ou Lista cinza (2)

Valores de Ação:

- `0` - Lista branca (permitir)
- `1` - Lista negra (negar)
- `2` - Lista cinza (permitir, mas rastrear)

Casos de Uso:

- Bloquear dispositivos roubados (lista negra de IMEIs específicos)
- Restringir tipos de dispositivos (lista negra por padrão TAC)
- Permitir apenas dispositivos aprovados (padrão de lista branca com negação padrão)

Veja Também:

- Fluxos de Protocolo - Fluxo de verificação da interface S13 e EIR

- Visão Geral da Arquitetura - Função EIR do OmniHSS

Documentação Adicional

Para mais informações, consulte a seguinte documentação:

- **Status e Saúde** - Endpoints de verificação de saúde da API
- **Tratamento de Erros** - Erros comuns e solução de problemas
- **Exemplos de Uso da API** - Fluxos de trabalho completos de provisionamento

---

← Voltar ao Guia de Operações | Próximo: Painel de Controle →

Status e Saúde da API

← Voltar para a Referência da API

Status do Sistema

Verifique se a API está respondendo.

Endpoint: `GET /api/status`

Exemplo de Requisição:

```
curl -k https://hss.example.com:8443/api/status
```

Exemplo de Resposta:

```
{
  "status": "ok"
}
```

Caso de Uso: Verificação de saúde para balanceadores de carga e sistemas de monitoramento.

← Voltar para a Referência da API

Visão Geral da Arquitetura do OmniHSS

← Voltar ao Guia de Operações

Índice

Visão Geral do Sistema

OmniHSS é construído sobre Elixir e a plataforma Erlang/OTP, fornecendo um sistema altamente concorrente e tolerante a falhas, projetado para cargas de trabalho de telecomunicações. A arquitetura segue uma abordagem em camadas com clara separação de preocupações.

Arquitetura de Componentes

Componentes Principais

Manipuladores de Aplicação Diameter

Cada aplicação Diameter (S6a, Cx, Sh, S13, Gx, Rx) é implementada como um módulo manipulador DiameterEx que:

1. **Registra-se no DiameterEx** - Inscreve-se em IDs de Aplicação Diameter específicos
2. **Valida Solicitações** - Extrai AVPs, valida o estado do assinante
3. **Processa Lógica de Negócios** - Chama os módulos de lógica de negócios apropriados
4. **Constrói Respostas** - Monta mensagens de resposta Diameter com AVPs
5. **Lida com Erros** - Retorna códigos de resultado Diameter apropriados

---

Pilha Diameter

Configuração do Serviço Diameter

OmniHSS configura um único serviço Diameter com várias aplicações suportadas:

Gerenciamento de Conexão de Pares

Fluxo de Mensagens Diameter

Camada de Aplicação

Interface S6a (LTE/EPC)

Lida com autenticação e gerenciamento de mobilidade para redes LTE.

Interface Cx (IMS)

Lida com registro e autenticação IMS.

Interface Sh (Dados de Perfil IMS)

Fornece aos servidores de aplicação IMS acesso aos dados de perfil do assinante.

Interface Gx (Controle de Políticas)

Gerencia controle de políticas e cobrança para sessões de dados. **Veja Documentação PCRF para detalhes.**

Interface Rx (Mídia IMS)

Controla a política de mídia IMS e os bearers dedicados para VoLTE. **Veja Documentação PCRF para detalhes.**

Interface S13 (EIR)

Valida o IMEI do dispositivo em relação às regras de identidade de equipamentos. **Veja Documentação EIR para detalhes.**

Camada de Dados

Visão Geral do Esquema do Banco de Dados

Padrão de Repositório Ecto

Estratégia de Consulta Otimizada

Cada procedimento Diameter utiliza consultas otimizadas que pré-carregam apenas associações necessárias:

Interfaces Externas

Arquitetura da API

Arquitetura do Painel de Controle

Arquitetura de Implantação

Implantação em Um Único Nó

Exemplo de Fluxo de Processo: Autenticação

Este exemplo mostra o fluxo completo para uma solicitação de autenticação:

Princípios Arquitetônicos Chave

1. Tolerância a Falhas

- Árvores de supervisão Erlang/OTP reiniciam automaticamente processos com falha
- Manipuladores Diameter isolados evitam falhas em cascata
- Pooling de conexões de banco de dados com reconexão automática

2. Concorrência

- Cada solicitação Diameter é tratada em seu próprio processo
- Sem estado compartilhado entre manipuladores de solicitação
- Pooling de conexões de banco de dados para consultas paralelas

3. Modularidade

- Cada aplicação Diameter em módulo separado
- Clara separação entre interface, lógica de negócios e camadas de dados
- Algoritmos de autenticação plugáveis

4. Desempenho

- Consultas de banco de dados otimizadas com pré-carregamento seletivo
- Transfer��ncia mínima de dados para cada tipo de procedimento
- Pooling de conexões e keepalive

5. Observabilidade

- Monitoramento em tempo real via Painel de Controle
- Registro estruturado em toda a aplicação
- Rastreamento de status de pares Diameter
- Rastreamento de estado do assinante com timestamps

← Voltar ao Guia de Operações | Próximo: Configuração →

Guia de Configuração do OmniHSS

← Voltar ao Guia de Operações

Índice

Visão Geral do Arquivo de Configuração

OmniHSS usa dois arquivos de configuração principais:

config/config.exs (Tempo de Compilação)

Contém configuração estática que não muda entre ambientes:

- Configuração da página do Painel de Controle
- Configuração do endpoint da API
- Configurações de telemetria

config/runtime.exs (Tempo de Execução)

Contém configuração específica do ambiente que muda por implantação:

- Parâmetros de conexão do banco de dados
- Configuração de pares Diameter
- Configurações do PLMN de origem
- Seleção do S-CSCF do IMS
- Vínculos de interface de rede

Configuração em Tempo de Execução

Prioridade de Configuração

Padrão de Variável de Ambiente

OmniHSS segue este padrão para configuração:

- Nomes de variáveis de ambiente são MAIÚSCULAS com sublinhados
- Valores padrão são fornecidos em runtime.exs
- Credenciais do banco de dados devem usar variáveis de ambiente em produção

---

Configuração do Banco de Dados

Configuração Básica do Banco de Dados

```
# config/runtime.exs

config :hss, Hss.Repo,
  # Parâmetros de conexão do banco de dados
  username: System.get_env("DATABASE_USERNAME", "root"),
  password: System.get_env("DATABASE_PASSWORD", "password"),
  hostname: System.get_env("DATABASE_HOSTNAME", "localhost"),
  database: System.get_env("DATABASE_NAME", "omnihss"),

  # Configurações do pool de conexão
  pool_size: String.to_integer(System.get_env("DATABASE_POOL_SIZE", "20")),

  # Timeouts (em milissegundos)
  timeout: 15_000,
  connect_timeout: 15_000,

  # Opções adicionais
  show_sensitive_data_on_connection_error: false
```

Parâmetros de Configuração do Banco de Dados

Parâmetro	Descrição	Padrão	Recomendação
`username`	Nome de usuário do Banco de Dados SQL	`"root"`	Use um usuário dedicado em produção
`password`	Senha do Banco de Dados SQL	`"password"`	Use uma senha forte, armazene em var env
`hostname`	Nome do servidor do Banco de Dados SQL	`"localhost"`	Use FQDN ou IP em produção
`database`	Nome do banco de dados	`"omnihss"`	Mantenha o padrão, a menos que múltiplas instâncias
`pool_size`	Tamanho do pool de conexão	`20`	Ajuste com base na carga (10-50 típico)

Ajuste do Tamanho do Pool

Diretrizes:

- Comece com 20 conexões
- Monitore por erros de "timeout do pool de conexão"
- Aumente em 10 se ocorrerem timeouts sob carga normal
- Cada conexão usa ~4MB de memória
- Muitas conexões podem degradar o desempenho do Banco de Dados SQL

Exemplo: Configuração do Banco de Dados em Produção

```
# config/runtime.exs - Exemplo de produção

config :hss, Hss.Repo,
  username: System.fetch_env!("DATABASE_USERNAME"),      # Necessário em
produção
  password: System.fetch_env!("DATABASE_PASSWORD"),      # Necessário em
produção
  hostname: System.get_env("DATABASE_HOSTNAME", "db.internal.example.com"),
  database: System.get_env("DATABASE_NAME", "omnihss"),
  port: String.to_integer(System.get_env("DATABASE_PORT", "3306")),
  pool_size: String.to_integer(System.get_env("DATABASE_POOL_SIZE", "30")),
  ssl: true,
  ssl_opts: [
    cacertfile: "/etc/ssl/certs/mysql-ca.pem",
    verify: :verify_peer
  ]
```

Configuração do Diameter

Configuração do Serviço Diameter

```
# config/runtime.exs

diameter_config = %{
  service_name: :omnitouch_hss,

  # Vínculo de rede
  listen_ip: System.get_env("DIAMETER_LISTEN_IP", "10.7.25.186"),
  listen_port: String.to_integer(System.get_env("DIAMETER_LISTEN_PORT",
"3868")),

  # Identidade Diameter
  host: System.get_env("DIAMETER_HOST", "omnihss"),
  realm: System.get_env("DIAMETER_REALM",
"epc.mnc001.mcc001.3gppnetwork.org"),

  # Identificação do produto
  product_name: "OmniHSS",
  vendor_id: 10415,  # 3GPP
```

```
  supported_vendor_ids: [5535, 10415],

  # Configurações de protocolo
  request_timeout: 5000,

  # Configuração de pares
  peers: [
    # Adicione configurações de pares aqui
  ]
}

config :hss, :diameter, diameter_config
```

Configuração de Identidade Diameter

Diretrizes:

- **Host:** Nome curto do HSS (ex: "omnihss", "hss01")
- **Realm:** Realm Diameter que corresponde ao seu PLMN (ex: "epc.mnc001.mcc001.3gppnetwork.org")
- **Identidade Completa:** Construído como `{host}.{realm}`

Adicionando Pares Diameter

Configuração de Par Estático (Modo de Conexão)

```
# config/runtime.exs

peers: [
  # Exemplo de Par MME
  %{
    host: "mme01.epc.mnc001.mcc001.3gppnetwork.org",
    realm: "epc.mnc001.mcc001.3gppnetwork.org",
    ip: "10.7.25.100",
    port: 3868,
    transport: :sctp,  # ou :tcp
    applications: [:s6a]
  },

  # Exemplo de Par P-GW
  %{
    host: "pgw01.epc.mnc001.mcc001.3gppnetwork.org",
    realm: "epc.mnc001.mcc001.3gppnetwork.org",
    ip: "10.7.25.101",
    port: 3868,
    transport: :sctp,
    applications: [:gx]
  },

  # Exemplo de Par I-CSCF
  %{
    host: "icscf01.ims.mnc001.mcc001.3gppnetwork.org",
```

```
    realm: "ims.mnc001.mcc001.3gppnetwork.org",
    ip: "10.7.25.102",
    port: 3868,
    transport: :tcp,
    applications: [:cx]
  }
]
```

Modo Apenas de Escuta

Para ambientes onde os pares iniciam conexões com o HSS:

```
# config/runtime.exs

diameter_config = %{
  # ... outras configurações ...
  peers: []  # Vazio - aceitar apenas conexões de entrada
}
```

Modos de Conexão de Par Diameter

Seleção do Protocolo de Transporte

Transporte	Vantagens	Desvantagens	Recomendação
SCTP	Multi-streaming, melhor detecção de falhas	Requer suporte do kernel, configuração de firewall	Preferido para Diameter
TCP	Suporte universal, regras de firewall mais simples	Fluxo único, detecção de falhas mais lenta	Use se SCTP não estiver disponível

Configuração de Rede

Configuração do PLMN de Origem

O PLMN de origem identifica seu operador de rede:

```
# config/runtime.exs

config :hss, :home_plmn, %{
  mcc: System.get_env("HOME_PLMN_MCC", "001"),  # Código do País Móvel
  mnc: System.get_env("HOME_PLMN_MNC", "001")   # Código da Rede Móvel
}
```

Formato do Código PLMN

Exemplos:

- AT&T (EUA): MCC=310, MNC=410
- Verizon (EUA): MCC=311, MNC=480
- Vodafone (Reino Unido): MCC=234, MNC=15
- Rede de Teste: MCC=001, MNC=01

Vínculo de Interface de Rede

```
# config/runtime.exs

# Interface Diameter
listen_ip: System.get_env("DIAMETER_LISTEN_IP", "0.0.0.0"),  # Todas as
interfaces
# Ou interface específica:
# listen_ip: "10.7.25.186",

# Interface da API
config :hss, HssWeb.Api.Endpoint,
  http: [
    ip: {0, 0, 0, 0},  # Todas as interfaces
    port: 8443
  ]

# Interface do Painel de Controle
config :hss, HssWeb.ControlPanel.Endpoint,
  http: [
    ip: {0, 0, 0, 0},  # Todas as interfaces
    port: 7443
  ]
```

Opções de Vínculo de Interface:

Configuração do IMS

Configuração de Seleção do S-CSCF

```
# config/runtime.exs

config :hss, :ims, %{
  scscf: %{
    # Método de seleção: :random_peer ou :round_robin
    selection_method: :random_peer,

    # Lista de pares S-CSCF disponíveis
    peers: [
      %{
        host: "sip:scscf01.ims.mnc001.mcc001.3gppnetwork.org:5060",
        capabilities: []  # Opcional: correspondência de capacidade
      },
      %{
        host: "sip:scscf02.ims.mnc001.mcc001.3gppnetwork.org:5060",
        capabilities: []
      }
    ]
  }
}
```

Métodos de Seleção do S-CSCF

Métodos de Seleção:

Método	Descrição	Caso de Uso
`:random_peer`	Seleciona aleatoriamente um S-CSCF	Distribuição de carga uniforme
`:round_robin`	Atribui S-CSCFs sequencialmente	Distribuição previsível

Configuração do Realm IMS

Normalmente, o IMS usa um realm separado do EPC:

```
# Realm EPC
"epc.mnc001.mcc001.3gppnetwork.org"

# Realm IMS
"ims.mnc001.mcc001.3gppnetwork.org"
```

Configuração do EIR

Veja [Documentação do EIR] para detalhes completos sobre verificação de identidade de equipamentos.

Configurações do Registro de Identidade de Equipamentos

```
# config/runtime.exs

config :hss, :eir, %{
  # Comportamento para equipamentos desconhecidos (sem regra correspondente)
  unknown_equipment_behaviour: :whitelist
  # Opções:
  #   :whitelist - Permitir equipamentos desconhecidos
  #   :blacklist - Bloquear equipamentos desconhecidos
  #   :greylist - Rastrear, mas permitir equipamentos desconhecidos
  #   :reject_unknown_equipment - Rejeitar com código de resultado
específico
}
```

Comportamento de Equipamentos Desconhecidos

Opções de Comportamento:

Opção	Resultado	Caso de Uso
`:whitelist`	Permitir todos os IMEIs desconhecidos	Rede aberta, testes
`:blacklist`	Bloquear todos os IMEIs desconhecidos	Segurança moderada
`:greylist`	Permitir, mas rastrear IMEIs desconhecidos	Modo de monitoramento

Opção	Resultado	Caso de Uso
`:reject_unknown_equipment`	Rejeitar com código específico	Alta segurança

Recomendação: Comece com `:whitelist` durante os testes, passe para `:greylist` para monitoramento em produção e, em seguida, `:blacklist` para segurança rigorosa.

Configuração da API e do Painel de Controle

Configuração do Endpoint da API

```
# config/config.exs

config :hss, HssWeb.Api.Endpoint,
  url: [host: "localhost"],
  render_errors: [view: HssWeb.ErrorView, accepts: ~w(json)],
  pubsub_server: Hss.PubSub,

  # Configuração HTTPS
  https: [
    port: 8443,
    cipher_suite: :strong,
    certfile: "priv/cert/omnitouch.crt",
    keyfile: "priv/cert/omnitouch.pem"
  ]
```

Configuração do Painel de Controle

```
# config/config.exs

config :hss, HssWeb.ControlPanel.Endpoint,
  url: [host: "localhost"],
  render_errors: [view: HssWeb.ErrorView, accepts: ~w(html json)],
  pubsub_server: Hss.PubSub,
  live_view: [signing_salt: "some-secret"],

  # Configuração HTTPS
  https: [
    port: 7443,
    cipher_suite: :strong,
    certfile: "priv/cert/omnitouch.crt",
    keyfile: "priv/cert/omnitouch.pem"
  ]
```

Configuração do Certificado TLS

Requisitos do Certificado:

- Certificado X.509 válido
- Chave privada correspondente
- Incluir certificados intermediários, se necessário

- CN ou SAN deve corresponder ao nome do host

Para Produção:

```
https: [
  port: 8443,
  cipher_suite: :strong,
  certfile: System.get_env("TLS_CERT_FILE", "/etc/ssl/certs/omnihss.crt"),
  keyfile: System.get_env("TLS_KEY_FILE", "/etc/ssl/private/omnihss.key"),
  cacertfile: System.get_env("TLS_CA_FILE", "/etc/ssl/certs/ca-bundle.crt")
]
```

Fluxo de Trabalho de Configuração

Configuração Inicial de Implantação

Lista de Verificação de Configuração

Configuração Essencial

- ☐ Conexão do banco de dados (hostname, credenciais)
- ☐ PLMN de origem (MCC, MNC)
- ☐ Host e realm Diameter
- ☐ IP e porta de escuta Diameter
- ☐ Certificados TLS para API e Painel de Controle

Integração de Elementos de Rede

- ☐ Pares Diameter configurados (se usando modo de conexão)
- ☐ Regras de firewall permitem tráfego Diameter (porta 3868)
- ☐ Regras de firewall permitem tráfego HTTPS (portas 7443, 8443)
- ☐ Resolução DNS para identidades Diameter

Configuração do IMS (se usando recursos do IMS)

- ☐ Lista de pares S-CSCF configurada
- ☐ Método de seleção do S-CSCF escolhido
- ☐ Realm IMS configurado

Configuração Opcional

- ☐ Comportamento do EIR configurado
- ☐ Tamanho do pool do banco de dados ajustado
- ☐ Vínculo da interface de rede restrito

Verificando a Configuração

Após modificar a configuração:

1. **Verificação de Sintaxe:**

   ```
   Verifique os logs em busca de erros de carregamento de configuração
   ```

2. **Acesso ao Painel de Controle:**

   ```
   Acesse https://[hostname]:7443
   Verifique se a página de Visão Geral carrega
   ```

3. **Acesso à API:**

   ```
   curl -k https://[hostname]:8443/api/status
   ```

4. **Status do Diameter:**

   ```
   Verifique a página Diameter do Painel de Controle
   Verifique as conexões de pares
   ```

5. **Conectividade do Banco de Dados:**

   ```
   Verifique o Painel de Controle para dados de assinantes
   Ou conecte-se diretamente ao Banco de Dados SQL
   ```

Exemplo Completo de Configuração em Tempo de Execução

```
# config/runtime.exs - Exemplo completo de produção

import Config

#
================================================================================
# CONFIGURAÇÃO DO BANCO DE DADOS
#
================================================================================
config :hss, Hss.Repo,
  username: System.fetch_env!("DATABASE_USERNAME"),
  password: System.fetch_env!("DATABASE_PASSWORD"),
  hostname: System.get_env("DATABASE_HOSTNAME", "db.omnihss.internal"),
  database: System.get_env("DATABASE_NAME", "omnihss"),
  port: String.to_integer(System.get_env("DATABASE_PORT", "3306")),
  pool_size: String.to_integer(System.get_env("DATABASE_POOL_SIZE", "30")),
  timeout: 15_000,
  connect_timeout: 15_000,
  ssl: true,
  ssl_opts: [
    cacertfile: "/etc/ssl/certs/mysql-ca.pem",
```

```
    verify: :verify_peer
  ]

#
================================================================================
# CONFIGURAÇÃO DO PLMN DE ORIGEM
#
================================================================================
config :hss, :home_plmn, %{
  mcc: System.get_env("HOME_PLMN_MCC", "001"),
  mnc: System.get_env("HOME_PLMN_MNC", "001")
}

#
================================================================================
# CONFIGURAÇÃO DO DIAMETER
#
================================================================================
diameter_config = %{
  service_name: :omnitouch_hss,
  listen_ip: System.get_env("DIAMETER_LISTEN_IP", "10.7.25.186"),
  listen_port: String.to_integer(System.get_env("DIAMETER_LISTEN_PORT",
"3868")),
  host: System.get_env("DIAMETER_HOST", "omnihss01"),
  realm: System.get_env("DIAMETER_REALM",
"epc.mnc001.mcc001.3gppnetwork.org"),
  product_name: "OmniHSS",
  vendor_id: 10415,
  supported_vendor_ids: [5535, 10415],
  request_timeout: 5000,
  peers: [
    %{
      host: "mme01.epc.mnc001.mcc001.3gppnetwork.org",
      realm: "epc.mnc001.mcc001.3gppnetwork.org",
      ip: "10.7.25.100",
      port: 3868,
      transport: :sctp,
      applications: [:s6a]
    }
  ]
}

config :hss, :diameter, diameter_config

#
================================================================================
# CONFIGURAÇÃO DO IMS
#
================================================================================
config :hss, :ims, %{
  scscf: %{
    selection_method: :random_peer,
    peers: [
```

```
      %{host: "sip:scscf01.ims.mnc001.mcc001.3gppnetwork.org:5060"},
      %{host: "sip:scscf02.ims.mnc001.mcc001.3gppnetwork.org:5060"}
    ]
  }
}

#
============================================================================
# CONFIGURAÇÃO DO EIR
#
============================================================================
config :hss, :eir, %{
  unknown_equipment_behaviour: :whitelist
}

#
============================================================================
# CONFIGURAÇÃO DO ENDPOINT DA API
#
============================================================================
config :hss, HssWeb.Api.Endpoint,
  http: [ip: {0, 0, 0, 0}, port: 8443],
  https: [
    port: 8443,
    cipher_suite: :strong,
    certfile: System.get_env("TLS_CERT_FILE", "/etc/ssl/certs/omnihss.crt"),
    keyfile: System.get_env("TLS_KEY_FILE", "/etc/ssl/private/omnihss.key")
  ],
  url: [host: System.get_env("API_HOST", "api.omnihss.internal"), port:
8443]

#
============================================================================
# CONFIGURAÇÃO DO ENDPOINT DO PAINEL DE CONTROLE
#
============================================================================
config :hss, HssWeb.ControlPanel.Endpoint,
  http: [ip: {0, 0, 0, 0}, port: 7443],
  https: [
    port: 7443,
    cipher_suite: :strong,
    certfile: System.get_env("TLS_CERT_FILE", "/etc/ssl/certs/omnihss.crt"),
    keyfile: System.get_env("TLS_KEY_FILE", "/etc/ssl/private/omnihss.key")
  ],
  url: [host: System.get_env("CP_HOST", "hss.omnihss.internal"), port: 7443]
```

← Voltar ao Guia de Operações | Próximo: Relacionamentos de Entidade →

Guia do Painel de Controle do OmniHSS

← Voltar ao Guia de Operações

Índice

Visão Geral do Painel de Controle

O Painel de Controle do OmniHSS é uma interface de monitoramento baseada na web que fornece visibilidade em tempo real sobre o status do sistema, atividade dos assinantes e conectividade de Diâmetro. Construído com Phoenix LiveView, ele se atualiza automaticamente sem a necessidade de atualizações de página.

Principais Recursos

- **Atualizações em Tempo Real** - Atualiza automaticamente a cada segundo
- **Monitoramento de Assinantes** - Visualize assinantes ativos e seu estado atual
- **Status do Diâmetro** - Monitore conexões de pares em tempo real
- **Recursos do Sistema** - Acompanhe o desempenho da aplicação
- **Visualizador de Configuração** - Inspecione a configuração em tempo de execução

Informações de Acesso

```
URL: https://[hostname]:7443
Protocolo: Apenas HTTPS
Porta: 7443 (configurável)
Certificado: Configurado em config/config.exs
```

Acessando o Painel de Controle

Acesso Inicial

1. Abra um navegador web
2. Navegue até `https://[hostname]:7443`
3. Aceite o certificado TLS (se autoassinado)
4. Você será apresentado à página de Visão Geral por padrão

Avisos de Certificado TLS

Se estiver usando certificados autoassinados, os navegadores mostrarão avisos de segurança. Isso é esperado para implantações internas.

Para Produção: Use certificados assinados por uma Autoridade Certificadora confiável.

Requisitos de Rede

- **A Porta 7443** deve ser acessível a partir da sua rede de gerenciamento
- **HTTPS** é obrigatório - HTTP não é suportado
- **Regras de firewall** devem permitir tráfego para a porta 7443

Compatibilidade do Navegador

O Painel de Controle utiliza tecnologias web modernas (LiveView, WebSockets):

- Chrome/Chromium (recomendado)
- Firefox
- Safari
- Edge

Nota: Internet Explorer não é suportado.

Página de Visão Geral

URL: `https://[hostname]:7443/overview`

A página de Visão Geral exibe todos os assinantes e suas informações de estado em tempo real.

Layout da Página

Colunas da Tabela

Coluna	Descrição	Valores
ID	ID do banco de dados do assinante	Inteiro
Enabled	Status do serviço	✓ (habilitado) / ✗ (desabilitado)
IMSI	Identidade Internacional do Assinante Móvel	14-15 dígitos
ICCID	ID do cartão SIM	19-20 dígitos ou "N/A"
EPC Profile	Nome do perfil de serviço de dados	Nome ou ID do perfil
IMS Profile	Nome do perfil de serviço de voz	Nome do perfil, ID ou "N/A"
Roaming Profile	Nome da política de roaming	Nome do perfil, ID ou "N/A"

Detalhes da Linha Expansível

Clique em qualquer linha para expandir e visualizar o estado detalhado do assinante:

Informações de Localização

Campos:

- **MCC** - Código do País Móvel (3 dígitos)
- **MNC** - Código da Rede Móvel (2-3 dígitos)
- **TAC** - Código da Área de Rastreamento
- **Cell ID** - Identificador da célula de serviço
- **eNodeB ID** - Identificador da estação base
- **ECI** - Identificador da Célula E-UTRAN

Informações de Rede

Campos:

- **Último MME Visto** - Nome do host do MME de servi��o atual
- **Último Realm Visto** - Realm de Diâmetro do MME
- **Tipo de RAT** - Tecnologia de Acesso Rádio (por exemplo, "E-UTRAN" para LTE)
- **Último Visto Em** - Timestamp da última mensagem de Diâmetro

Informações de IMS

Campos:

- **S-CSCF Atribuído** - URI SIP S-CSCF atualmente atribuído
- **Identidade Pública IMS** - URI SIP (por exemplo, sip:+14155551234@ims.example.com)
- **Último P-CSCF Visto** - Último P-CSCF que contatou o HSS
- **Último I-CSCF Visto** - Último I-CSCF que contatou o HSS

Informações da Sessão

Campos:

- **Sessões PDN** - Número de conexões de dados ativas
- **Chamadas Ativas** - Número de chamadas VoLTE ativas

Indicadores de Estado

Como identificar o estado:

- **Idle:** Sem informações de localização, sem MME
- **Attached:** Último MME Visto presente, informações de localização disponíveis
- **PDN Active:** Contagem de sessões PDN > 0
- **IMS Registered:** S-CSCF Atribuído presente
- **In Call:** Contagem de chamadas ativas > 0

Auto-Atualização

A página de Visão Geral atualiza automaticamente **a cada 1 segundo** para mostrar atualizações em tempo real.

Indicadores visuais:

- Novos dados aparecem sem recarregar a página
- Timestamps atualizam em tempo real
- Nenhuma atualização manual necessária

Casos de Uso

1. **Monitorar Assinantes Ativos**
    - Veja quais assinantes estão atualmente anexados
    - Verifique a rede de serviço atual (para roaming)
    - Verifique o status de registro IMS
2. **Solução de Problemas**
    - Verifique se o assinante está habilitado
    - Verifique o timestamp do último visto (o assinante está responsivo?)
    - Confirme as atribuições de perfil

    - Veja as informações de localização atuais

3. **Monitoramento de Capacidade**
    - Conte o total de assinantes anexados
    - Monitore as contagens de sessões PDN
    - Acompanhe as chamadas VoLTE ativas

Página de Diâmetro

URL: `https://[hostname]:7443/diameter`

A página de Diâmetro mostra o status em tempo real de todas as conexões de pares de Diâmetro.

Layout da Página

Colunas da Tabela

Coluna	Descrição	Valores
Hostname	Nome do host do par de Diâmetro	FQDN
Realm	Realm de Diâmetro	Nome de domínio
IP:Port	Endereço de rede	Endereço IP e porta
Transport	Protocolo de transporte	TCP ou SCTP
Status	Status da conexão	Conectado / Desconectado

Status da Conexão

Detalhes da Linha Expansível

Clique em qualquer par para visualizar informações adicionais:

Informações de Conexão:

- **Tipo de Conexão** - Iniciada pelo HSS ou par
- **Nome do Produto** - Identificação do produto do par
- **IDs de Aplicação** - Aplicações de Diâmetro suportadas

Exemplos de ID de Aplicação:

- 16777251 - S6a (MME)
- 16777238 - Gx (P-GW)
- 16777216 - Cx (I-CSCF, S-CSCF)
- 16777217 - Sh (Servidor de Aplicação)
- 16777236 - Rx (P-CSCF)

- 16777252 - S13 (cliente EIR, se externo)

Fluxo de Conexão de Par

Auto-Atualização

A página de Diâmetro atualiza automaticamente **a cada 1 segundo**.

Casos de Uso

1. **Verificar Conectividade**
    - Garantir que todos os pares esperados estejam conectados
    - Identificar pares desconectados imediatamente
    - Monitorar conexões instáveis
2. **Solução de Problemas**
    - Verifique se o par é acessível
    - Verifique o protocolo de transporte (TCP vs SCTP)
    - Confirme se os IDs de aplicação correspondem às expectativas
    - Identifique qual lado iniciou a conexão
3. **Planejamento de Capacidade**
    - Conte o total de pares conectados
    - Monitore a estabilidade da conexão
    - Planeje capacidade adicional para pares

Problemas Comuns

Par Mostra Desconectado

Causas Possíveis:

1. Problema de conectividade de rede
2. Par está fora do ar ou reiniciando
3. Firewall bloqueando tráfego
4. Incompatibilidade de configuração de Diâmetro
5. Problema de certificado (se usando TLS)

Passos de Solução de Problemas:

1. Verifique a conectividade de rede: `ping [peer-ip]`
2. Verifique se a porta é acessível: `telnet [peer-ip] 3868`
3. Verifique as regras de firewall
4. Revise os logs do HSS para mensagens de erro
5. Verifique se a configuração de Diâmetro do par corresponde ao HSS

Par Conecta e Desconecta Repetidamente

Causas Possíveis:

1. Instabilidade na rede
2. Incompatibilidade de timeout de keepalive
3. Problemas de recursos do par
4. Incompatibilidade de aplicação de Diâmetro

Passos de Solução de Problemas:

1. Verifique a estabilidade da rede
2. Revise os temporizadores de keepalive em ambos os lados
3. Verifique os recursos do sistema do par
4. Verifique se os IDs de aplicação correspondem em ambos os lados

---

Página de Aplicação

URL: `https://[hostname]:7443/application`

A página de Aplicação fornece informações de monitoramento em nível de sistema e uso de recursos.

Recursos

- **Informações do Processo** - Contagem de processos da VM Erlang e memória
- **Memória do Sistema** - Memória total e usada
- **Tempo de Atividade da Aplicação** - Quanto tempo o OmniHSS está em execução
- **Versão da VM Erlang** - Informações da versão em execução

Principais Métricas

Casos de Uso

1. **Monitoramento de Saúde**
    - Verifique se a aplicação está em execução
    - Verifique se há vazamentos de memória (memória aumentando ao longo do tempo)
    - Monitore o crescimento da contagem de processos
2. **Planejamento de Capacidade**
    - Acompanhe as tendências de uso de memória

    - Planeje a escalabilidade com base na contagem de processos
    - Verifique se há recursos adequados do sistema

3. **Solução de Problemas**

    - Identifique a exaustão de recursos
    - Verifique se é necessário reiniciar
    - Verifique a versão da VM Erlang

Página de Configuração

URL: `https://[hostname]:7443/configuration`

A página de Configuração exibe a configuração atual em tempo de execução do OmniHSS.

Recursos

- **Visualizar Configuração** - Inspecione todos os parâmetros de configuração
- **Pesquisar Configuração** - Encontre configurações específicas
- **Variáveis de Ambiente** - Veja os valores resolvidos

Categorias de Configuração

Casos de Uso

1. **Verificação de Configuração**

    - Verifique se as configurações de runtime.exs estão aplicadas
    - Confirme os parâmetros de conexão do banco de dados
    - Verifique a configuração do par de Diâmetro

2. **Solução de Problemas**

    - Identifique configurações incorretas
    - Verifique se as variáveis de ambiente estão definidas corretamente
    - Compare a configuração esperada com a real

3. **Documentação**

    - Exporte a configuração atual para documentação
    - Compartilhe a configuração com a equipe de suporte

Nota de Segurança: A página de configuração pode exibir informações sensíveis (senhas de banco de dados, chaves). Restrinja o acesso adequadamente.

Navegação e Interface

Barra de Navegação Superior

A navegação está sempre visível na parte superior da página para acesso rápido.

Atalhos de Teclado

Embora o Painel de Controle não implemente atalhos de teclado personalizados, os atalhos padrão do navegador funcionam:

- **Ctrl+R / F5** - Atualização manual da página (embora a autoatualização torne isso desnecessário)
- **Ctrl+F** - Pesquisar na página
- **Ctrl+T** - Abrir nova aba (para várias páginas)

Monitoramento em Múltiplas Abas

Você pode abrir várias páginas do Painel de Controle em abas separadas do navegador para monitoramento simultâneo:

Configuração de Exemplo:

- Aba 1: Página de Visão Geral (monitorar assinantes)
- Aba 2: Página de Diâmetro (monitorar conectividade)
- Aba 3: Página de Aplicação (monitorar recursos)

Todas as abas serão atualizadas automaticamente de forma independente.

Design Responsivo

O Painel de Controle é otimizado para navegadores de desktop. Navegadores móveis são suportados, mas podem exigir rolagem horizontal para tabelas.

Resolução Recomendada: 1920x1080 ou superior para visualização confortável.

Melhores Práticas de Monitoramento

Operações Diárias

1. **Início do Turno**
    - Abra a página de Visão Geral do Painel de Controle

- Verifique se o número esperado de assinantes está anexado
- Verifique a página de Diâmetro - todos os pares conectados

2. **Durante o Turno**

   - Mantenha a página de Visão Geral aberta para monitoramento em tempo real
   - Fique atento a mudanças de estado incomuns
   - Monitore pares desconectados na página de Diâmetro

3. **Fim do Turno**

   - Verifique se o sistema está estável
   - Verifique a página de Aplicação para tendências de uso de recursos
   - Documente quaisquer anomalias

Fluxo de Trabalho de Solução de Problemas

Limites de Alerta

Estabeleça limites de monitoramento para alertas proativos:

Métrica	Aviso	Crítico
Pares de Diâmetro Desconectados	1 par	2+ pares ou par crítico
Uso de Memória	> 80%	> 90%
Falhas de Autenticação de Assinantes	> 5%	> 10%
Contagem de Processos	> 80% do limite	> 95% do limite

← Voltar ao Guia de Operações | Próximo: Métricas & Monitoramento →

OmniHSS Relacionamentos de Entidade

← Voltar para o Guia de Operações

Índice

Visão Geral da Entidade

OmniHSS organiza os dados dos assinantes em entidades lógicas com relacionamentos claros. Compreender essas entidades é crucial para tarefas operacionais como provisionamento, solução de problemas e planejamento de capacidade.

Categorias de Entidade

Entidades Principais

Assinante

O **Assinante** é a entidade central que representa um usuário móvel.

Campos:

Campo	Tipo	Descrição	Restrições
`id`	bigint	Chave primária	Auto-incremento
`enabled`	boolean	Sinalizador de serviço habilitado	Padrão: true
`ims_enabled`	boolean	Serviços IMS habilitados	Padrão: true
`imsi`	string	Identidade Internacional do	14-15 dígitos,

Campo	Tipo	Descrição	Restrições
		Assinante Móvel	único
`custom_attributes`	map	Dados personalizados de chave-valor	Opcional
`sim_id`	bigint	Chave estrangeira para SIM	Opcional
`key_set_id`	bigint	Chave estrangeira para Conjunto de Chaves	Obrigatório
`epc_profile_id`	bigint	Chave estrangeira para Perfil EPC	Obrigatório
`ims_profile_id`	bigint	Chave estrangeira para Perfil IMS	Opcional
`roaming_profile_id`	bigint	Chave estrangeira para Perfil de Roaming	Opcional
`subscriber_state_id`	bigint	Chave estrangeira para Estado do Assinante	Criado automaticamente

Pontos Chave:

- Cada assinante deve ter exatamente um IMSI
- IMSI deve ter 14-15 dígitos (sem letras ou caracteres especiais)
- Um assinante pode ter múltiplos MSISDNs (números de telefone)
- O estado do assinante é criado automaticamente quando o assinante é criado
- O sinalizador `enabled` controla todos os serviços (dados e IMS)
- O sinalizador `ims_enabled` controla apenas os serviços IMS

SIM

A **SIM** representa um cartão SIM físico ou embutido.

Campos:

Campo	Tipo	Descrição	Nível de Segurança
`iccid`	string	ID do Cartão de Circuito Integrado	Público
`sim_vendor`	string	Fabricante do SIM	Público
`batch_name`	string	Lote de fabricação	Público
`is_esim`	boolean	Sinalizador de SIM embutido	Público
`pin1`, `pin2`	string	Códigos PIN	Sensível
`puk1`, `puk2`	string	Códigos PUK	Sensível
`adm1` - `adm10`	string	Códigos administrativos	Altamente Sensível
`kic`, `kid`	binary	Chaves de segurança OTA	Altamente Sensível

Pontos Chave:

- ICCID identifica exclusivamente o cartão SIM
- Um SIM pode ser atribuído a um assinante por vez

- Códigos PIN/PUK são para bloqueio de SIM pelo usuário final
- Códigos ADM são para operações administrativas de SIM
- KIC/KID são para atualizações OTA (Over-The-Air) do SIM

Conjunto de Chaves

O **Conjunto de Chaves** contém chaves criptográficas para autenticação.

Campos:

Campo	Tipo	Descrição	Tamanho
`ki`	binary	Chave secreta	128 bits (16 bytes)
`opc`	binary	Chave variante do operador (derivada)	128 bits
`op`	binary	Chave do operador (para derivar OPC)	128 bits
`amf`	binary	Campo de Gerenciamento de Autenticação	16 bits (2 bytes)
`sqn`	bigint	Número de sequência (anti-replay)	48 bits
`authentication_algorithm`	string	Nome do algoritmo	Atualmente "milenage"
`ota_counter`	bigint	Contador de operação OTA	Inteiro

Pontos Chave:

- Múltiplos assinantes podem compartilhar o mesmo conjunto de chaves
- Ki é o segredo mestre compartilhado com o SIM
- Ou OPC ou OP devem ser fornecidos (OPC pode ser derivado de OP)
- SQN é incrementado a cada autenticação
- Milenage é atualmente o único algoritmo suportado

Algoritmo de Autenticação:

MSISDN

O **MSISDN** representa um número de telefone.

Campos:

Campo	Tipo	Descrição	Formato
`msisdn`	string	Número ISDN da Estação Móvel	1-15 dígitos, formato E.164

Pontos Chave:

- MSISDN é o número de telefone no formato internacional

- Múltiplos MSISDNs podem ser atribuídos a um assinante
- Um MSISDN não pode ser compartilhado entre múltiplos assinantes
- Formato: Código do país + Número nacional (por exemplo, "14155551234" para +1 415-555-1234)

Padrão Multi-MSISDN:

Entidades de Perfil

Perfil EPC

O **Perfil EPC** define as características do serviço de dados para LTE.

Campos:

Campo	Tipo	Descrição	Unidades
`name`	string	Nome do perfil	Texto
`ue_ambr_dl_kbps`	integer	Limite de largura de banda de download	Kbps
`ue_ambr_ul_kbps`	integer	Limite de largura de banda de upload	Kbps
`network_access_mode`	integer	Restrições de acesso	Enum
`tracking_area_update_interval_seconds`	integer	Intervalo de TAU	Segundos

Modos de Acesso à Rede:

AMBR (Taxa Máxima Agregada de Bits):

Perfil IMS

O **Perfil IMS** define as características do serviço de voz/vídeo.

Campos:

Campo	Tipo	Descrição	Formato
`name`	string	Nome do perfil	Texto
`ifc_template`	text	Modelo XML de Critérios de Filtro Inicial	XML com variáveis

Variáveis do Modelo IFC:

Pontos Chave:

- IFC (Critérios de Filtro Inicial) controla o roteamento de chamadas no IMS

- O modelo é renderizado quando o assinante se registra
- As variáveis são substituídas pelos dados reais do assinante
- Enviado para S-CSCF durante o registro IMS

Perfil APN

O **Perfil APN** define características para um ponto de acesso de dados específico.

Entidades Relacionadas:

Identificador APN

Campo	Tipo	Descrição	Exemplo
`apn`	string	Nome APN	"internet", "ims", "mms"
`ip_version`	integer	Suporte ao protocolo IP	Veja abaixo

Opções de Versão IP:

Perfil QoS APN

Parâmetros de QoS:

Parâmetro	Descrição	Faixa	Portadora Padrão
`qci`	Identificador de Classe QoS	1-9	QCI 9 (Internet)
`allocation_retention_priority`	Prioridade ARP	1-15	8 (prioridade mais baixa)
`apn_ambr_dl_kbps`	Limite de download APN	0+	Varia
`apn_ambr_ul_kbps`	Limite de upload APN	0+	Varia
`pre_emption_capability`	Pode preemptar outros	true/ false	false
`pre_emption_vulnerability`	Pode ser preemptado	true/ false	true

Valores de QCI:

Perfil de Roaming

O **Perfil de Roaming** controla o acesso quando o assinante visita outras redes.

Regra de Roaming:

Avaliação da Regra:

Entidades de Estado

Estado do Assinante

O **Estado do Assinante** rastreia o status do assinante em tempo real.

Campos Chave:

Informações de Localização:

- `last_seen_mcc`, `last_seen_mnc` - Rede visitada
- `last_seen_tac` - Código da Área de Rastreamento
- `last_seen_cell_id` - ID da Célula
- `last_seen_enodeb_id` - ID do eNodeB
- `last_seen_eci` - Identificador da Célula E-UTRAN

Elementos de Rede:

- `last_seen_mme` - MME atual atendendo o assinante
- `last_seen_realm` - Reino Diameter do MME
- `last_seen_rat_type` - Tecnologia de Acesso Rádio (LTE, 5G, etc.)

Informações IMS:

- `assigned_scscf` - S-CSCF atual atendendo o assinante
- `ims_public_identity` - SIP URI (por exemplo, sip:+14155551234@ims.example.com)
- `sh_repository_data` - Dados de perfil IMS personalizados

Carimbos de Data/Hora:

- `last_seen_at` - Última mensagem Diameter recebida
- Vários carimbos de data/hora `last_*_at` para diferentes procedimentos

Sessão PDN

A **Sessão PDN** representa uma conexão de dados ativa.

Ciclo de Vida da Sessão PDN:

Chamada LTE

A **Chamada LTE** representa uma chamada de voz/vídeo VoLTE ativa.

Tipos de Chamada:

Fluxo da Chamada VoLTE:

Diagramas de Relacionamento de Entidade

Relacionamentos Completos de Entidade

Relacionamentos de Provisionamento

Este diagrama mostra o que deve existir antes de criar um assinante:

Relacionamentos de Estado da Sessão

Ciclo de Vida da Entidade

Ciclo de Vida do Provisionamento do Assinante

Ciclo de Vida da Sessão

Padrões de Fluxo de Dados

Fluxo de Autenticação

Fluxo de Atualização de Localização

Fluxo de Registro IMS

Fluxo de Estabelecimento de Sessão

Padrões de Otimização de Consulta

OmniHSS otimiza consultas ao banco de dados pré-carregando seletivamente apenas as associações necessárias para cada operação:

Consulta Mínima (Autentica��ão)

Caso de Uso: S6a AIR - Apenas precisa de chaves criptográficas e regras de roaming

Consulta Moderada (Atualização de Localização)

Caso de Uso: S6a ULR - Necessita de dados completos do perfil EPC

Consulta Completa (Registro IMS)

Caso de Uso: Cx SAR - Necessita do perfil IMS e todos os números de telefone

---

← Voltar para o Guia de Operações | Próximo: Referência da API →

Mapeamento de Dados da Resposta Diameter

← Voltar ao Índice da Documentação

Este documento fornece diagramas mermaid detalhados mostrando de onde cada campo nas respostas do protocolo Diameter é originado no sistema OmniHSS.

Índice

Resposta de Atualização de Localização (S6a ULA)

A Resposta de Atualização de Localização é enviada pelo HSS para o MME durante os procedimentos de anexação LTE. Este diagrama mostra o fluxo completo de dados das tabelas do banco de dados para os AVPs Diameter.

Mapeamento da Fonte de Dados

Mapeamento Detalhado de Campos

Fonte do Banco de Dados	Campo	AVP Diameter	Transformação
subscriber.enabled	`true/false`	Subscriber-Status	`true` → `0` (`active`), `false` → `1` (`barred`)
msisdn.msisdn	`'14155551234'`	MSISDN	Primeiro MSISDN, codificado em TBCD
epc_profile.ue_ambr_ul_kbps	`50000`	Max-Requested-Bandwidth-UL	Multiplicar por 1000 (kbps → bps)
epc_profile.ue_ambr_dl_kbps	`100000`	Max-Requested-Bandwidth-DL	Multiplicar por 1000 (kbps → bps)
epc_profile.network_access_mode	`0`	Network-Access-Mode	Mapeamento direto
apn_identifier.apn	`'internet'`	Service-	String direta

Fonte do Banco de Dados	Campo	AVP Diameter	Transformação
		Selection	
apn_identifier.ip_version	`2`	PDN-Type	`0=IPv4, 1=IPv6, 2=IPv4v6, 3=IPv4_or_IPv6`
apn_qos_profile.qci	`9`	QoS-Class-Identifier	Valor direto
apn_qos_profile.allocation_retention_priority	`8`	Priority-Level	Valor direto
apn_qos_profile.pre_emption_capability	`false`	Pre-emption-Capability	`false → 0`, `true → 1`
apn_qos_profile.pre_emption_vulnerability	`true`	Pre-emption-Vulnerability	`false → 0`, `true → 1`
apn_qos_profile.apn_ambr_ul_kbps	`25000`	APN AMBR UL	Multiplicar por 1000 (kbps → bps)
apn_qos_profile.apn_ambr_dl_kbps	`50000`	APN AMBR DL	Multiplicar por 1000 (kbps → bps)
static_ip.ipv4_static_ip	`'100.64.1.1'`	Served-Party-IP-Address (IPv4)	Somente se atribuído ao assinante
static_ip.ipv6_static_ip	`'2606:4700::1111'`	Served-Party-IP-Address (IPv6)	Somente se atribuído ao assinante

Transformações Chave:

1. **Largura de banda AMBR**: O banco de dados armazena em kbps, o Diameter espera bps (multiplicar por 1000)
2. **Codificação da Versão IP**: `0=IPv4, 1=IPv6, 2=IPv4v6, 3=IPv4_or_IPv6`
3. **Status do Assinante**: `enabled: true → 0 (SERVICE_GRANTED)`, `enabled: false → 1 (OPERATOR_DETERMINED_BARRING)`
4. **Context-Identifier**: Numeração sequencial (0, 1, 2...) para cada APN no perfil
5. **IP Estático**: Incluído apenas se atribuído via relação muitos-para-muitos `static_ips`

Validação da Lógica de Negócios:

- Verificação de Roaming: Combinar PLMN visitado com `roaming_profile.roaming_rules`
- Verificação de assinante habilitado: `subscriber.enabled == true`
- Filtrar APNs: Pode excluir APNs IMS se a política de roaming negar IMS

Resposta de Informação de Autenticação (S6a AIA)

A Resposta de Informação de Autenticação fornece vetores de autenticação para assinantes LTE/EPC.

Mapeamento da Fonte de Dados

Componentes Chave:

1. **Chaves Criptográficas**: Todas as chaves armazenadas como strings hexadecimais na tabela `key_set`
2. **Gerenciamento de SQN**: Número de sequência incrementado após cada geração de vetor de autenticação (previne ataques de repetição)
3. **Algoritmo Milenage**: 3GPP TS 35.206 - gera vetores de autenticação
4. **Derivação de KASME**: Chave derivada de CK||IK usando KDF conforme TS 33.401

Recursos de Segurança:

- SQN armazenado por assinante (não global)
- Ki/OPc nunca saem do HSS (apenas valores derivados transmitidos)
- AUTN inclui número de sequência (SQN) e AMF para autenticação de rede
- O algoritmo Milenage fornece autenticação mútua entre UE e rede

---

Resposta de Atribuição de Servidor (Cx SAA)

A Resposta de Atribuição de Servidor é enviada pelo HSS para o S-CSCF durante o registro IMS.

Mapeamento da Fonte de Dados

Recursos Chave:

1. **Template IFC**: Template XML armazenado em `ims_profile.ifc_template`
2. **Substituição Dinâmica**: Substitui `{{msisdn}}`, `{{imsi}}`, `{{impu}}` em tempo de execução
3. **Atribuição S-CSCF**: Armazena S-CSCF atribuído em `subscriber_state.assigned_scscf`
4. **Identidade Pública IMS**: Formato: `sip:+{msisdn}@{ims_domain}` ou `tel:+{msisdn}`

Parâmetros do Template IFC:

- `{{msisdn}}` - Primeiro MSISDN do assinante
- `{{imsi}}` - IMSI do assinante
- `{{impu}}` - Identidade Pública do Usuário IMS (do subscriber_state)
- `{{impi}}` - Identidade Privada do Usuário IMS (tipicamente IMSI@realm)

Resposta de Controle de Crédito (Gx CCA)

A Resposta de Controle de Crédito é enviada pela função PCRF para o PGW durante o estabelecimento do bearer.

Mapeamento da Fonte de Dados

Recursos Chave:

1. **Rastreamento de Sessão**: Cria/atualiza registro `pdn_session` para cada bearer
2. **Imposição de QoS**: Fornece QCI e limites de largura de banda do perfil APN QoS
3. **Regras de Cobrança**: Retorna regras de cobrança padrão para integração de faturamento
4. **CC-Request-Type**: Trata INITIAL (1), UPDATE (2), TERMINATION (3)

Gerenciamento do Estado da Sessão:

- `INITIAL_REQUEST`: Cria novo registro de sessão PDN
- `UPDATE_REQUEST`: Atualiza sessão PDN existente
- `TERMINATION_REQUEST`: Deleta registro de sessão PDN

Resposta de Dados do Usuário (Sh UDA)

A Resposta de Dados do Usuário é enviada pelo HSS para o AS (Servidor de Aplicação) via interface Sh.

Mapeamento da Fonte de Dados

Recursos Chave:

1. **Dados do Repositório**: Pode armazenar XML personalizado em `subscriber_state.sh_repository_data`
2. **Indicação de Serviço**: Filtra dados pelo serviço solicitado (por exemplo, presença, mensagens)
3. **Identidades Públicas**: Retorna todas as identidades públicas IMS para o assinante
4. **Dados de Referência vs Transparente**: Suporta modos de dados de referência e transparente

---

Resposta de Verificação de Identidade do ME (S13 ECA)

A Resposta de Verificação de Identidade do ME é enviada pela função EIR para o MME para validação de IMEI.

Mapeamento da Fonte de Dados

Recursos Chave:

1. **Correspondência Regex IMEI**: Regras usam expressões regulares para correspondência flexível
2. **Regras baseadas em TAC**: Podem corresponder ao Código de Alocação de Tipo (primeiros 8 dígitos)
3. **Comportamento Padrão**: Configurável para IMEIs desconhecidos (aceitar ou rejeitar)
4. **Valores de Status do Equipamento**:
    - `0` = WHITELIST (explicitamente permitido)
    - `1` = BLACKLIST (roubado/bloqueado)
    - `2` = GREYLIST (permitido, mas monitorado)
    - `5` = UNKNOWN (sem regra correspondente)

Casos de Uso:

- Bloquear dispositivos roubados por IMEI exato
- Bloquear modelos de dispositivos por padrão TAC
- Apenas dispositivos aprovados na lista branca
- Rastrear dispositivos do mercado cinza

Elementos Comuns de Resposta

Todas as respostas Diameter compartilham estes AVPs comuns:

Exemplo de Configuração:

```
config :diameter_ex,
  diameter_host: "hss",
  diameter_realm: "example.com",
  diameter_service_name: "OmniHSS"
```

Resumo do Fluxo de Dados

Pipeline de Processamento de Solicitações

Otimização de Consulta ao Banco de Dados

OmniHSS usa **pré-carregamento consciente do contexto** para minimizar consultas ao banco de dados:

```
# Exemplo: ULR pré-carrega tudo que é necessário para dados de assinatura
def get_subscriber_data(:update_location_request, imsi) do
  from(s in Subscriber, where: s.imsi == ^imsi)
  |> join(:left, [s], epc in assoc(s, :epc_profile))
  |> join(:left, [s, epc], apn in assoc(epc, :apn_profiles))
  |> join(:left, [s, epc, apn], qos in assoc(apn, :apn_qos_profile))
  |> join(:left, [s], msisdn in assoc(s, :msisdns))
  |> join(:left, [s], sip in assoc(s, :static_ips))
  |> preload([s, epc, apn, qos, msisdn, sip], [
    epc_profile: {epc, apn_profiles: {apn, apn_qos_profile: qos}},
    msisdns: msisdn,
    static_ips: sip
  ])
  |> Repo.one()
end

# Resultado: Consulta única com todos os joins - sem problema N+1
```

Notas de Implementação

Manipuladores de Protocolo

O sistema implementa manipuladores para os seguintes protocolos Diameter:

- **S6a** - Interface LTE/MME para autenticação e atualizações de localização
- **Cx** - Interface IMS/CSCF para registro IMS e atribuição de servidor
- **Sh** - Interface IMS/AS para recuperação de dados do assinante
- **Gx** - Interface PCRF para controle de políticas e cobrança
- **Rx** - Interface IMS/AF para autorização de mídia
- **S13** - Interface EIR para validação de IMEI
- **SWx** - Interface WiFi/IMS para autenticação de acesso não-3GPP

Modelos de Dados

O esquema do banco de dados inclui as seguintes entidades principais:

- **Subscriber** - Registro central do assinante com IMSI
- **Key Set** - Chaves criptográficas para autenticação
- **EPC Profile** - Configuração de serviço LTE
- **APN Profile** - Configuração do ponto de acesso
- **IMS Profile** - Configuração de serviço IMS com templates IFC
- **Roaming Profile** - Regras e restrições de roaming
- **Subscriber State** - Rastreamento dinâmico de sessão e estado
- **PDN Session** - Rastreamento de sessão de bearer ativa
- **Static IP** - Atribuições de endereço IP estático

- **EIR Rule** - Regras de validação de IMEI

← Voltar ao Índice da Documentação | Referência da API → | Fluxos de Protocolo →

Guia de Métricas e Monitoramento do OmniHSS

← Voltar para o Guia de Operações

Índice

Visão Geral do Monitoramento

O OmniHSS fornece vários mecanismos para monitorar a saúde do sistema, desempenho e atividade dos assinantes. A equipe de operações deve utilizar uma combinação dessas ferramentas para uma visibilidade abrangente.

Camadas de Monitoramento

Monitoramento do Painel de Controle

O Painel de Controle fornece a interface principal de monitoramento em tempo real.

Monitoramento da Página de Visão Geral

URL: `https://[hostname]:7443/overview`

Métricas Chave Disponíveis

Estados dos Assinantes Monitorados

Estado	Indicador	O Que Isso Significa
Ocioso	Sem informações de localização	Assinante desligado ou fora de cobertura
Conectado	MME presente	Assinante registrado na rede
PDN Ativo	Contagem de sessões PDN > 0	Conexão de dados ativa
IMS Registrado	S-CSCF atribuído	Serviços de voz prontos
Em Chamada	Contagem de chamadas ativas > 0	Chamada VoLTE em andamento

Extraindo Métricas da Visão Geral

Embora o Painel de Controle não exporte métricas diretamente, você pode:

1. **Contar linhas visíveis** para o total de assinantes
2. **Procurar por marcas de verificação verdes** para contar assinantes habilitados
3. **Revisar detalhes expandidos** para informações de estado
4. **Anotar timestamps da última visualização** para responsividade

Monitoramento da Página Diameter

URL: `https://[hostname]:7443/diameter`

Métricas Chave

Monitoramento de Pares Críticos

Identifique pares críticos e monitore seu status:

Tipo de Par	Criticidade	Impacto se Fora do Ar
MME	Alta	Sem novas conexões LTE
P-GW	Alta	Sem sessões de dados
S-CSCF	Alta	Sem registros IMS
P-CSCF	Alta	Sem chamadas VoLTE
I-CSCF	Média	Problemas de roteamento IMS
AS	Baixa-Média	Serviço específico indisponível

Monitoramento da Página de Aplicação

URL: `https://[hostname]:7443/application`

Métricas Chave

Métrica	Descrição	Faixa Normal	Limite de Ação
Contagem de Processos	Processos Erlang ativos	Varia conforme a carga	> 90% do limite
Uso de Memória	Memória total consumida	< 80%	> 90%
Tempo de Atividade	Tempo desde a última reinicialização	N/A	Monitorar para estabilidade

Monitoramento do Banco de Dados

Consultas Diretas ao Banco de Dados

Conecte-se ao Banco de Dados SQL para extrair métricas detalhadas:

Contagens de Assinantes

Consulte o banco de dados para recuperar:

- Contagem total de todos os assinantes
- Contagem de assinantes habilitados
- Contagem de assinantes habilitados para IMS

Estatísticas de Sessão

Consulte o banco de dados para recuperar:

- Contagem de sessões PDN ativas
- Contagem de chamadas VoLTE ativas
- Distribuição de sessões PDN por perfil de APN

Estatísticas de Localização

Consulte o banco de dados para recuperar:

- Contagem de assinantes agrupados por rede visitada (combinação MCC-MNC)
- Contagem de assinantes atualmente em roaming (não na PLMN 001-001)
- Distribuição de assinantes em diferentes redes visitadas

Atividade Recente

Consulte o banco de dados para recuperar:

- Contagem de assinantes vistos na última hora
- Distribuição de assinantes por MME de serviço
- Análise de timestamps da última atividade do assinante

Monitoramento da Saúde do Banco de Dados

Monitore a saúde do banco de dados consultando:

- Tamanho total do banco de dados e tendências de crescimento
- Tamanhos de tabelas individuais e contagens de linhas
- Contagem atual de conexões ao banco de dados
- Desempenho de consultas e uso de recursos

Monitoramento de Logs

Saída de Logs

O OmniHSS gera logs para **stdout/stderr**, que devem ser capturados pelo seu gerenciador de processos.

Níveis de Log

Padrões de Log Chave a Monitorar

Eventos de Par Diameter:

```
[info] Par Diameter conectado: mme01.epc.example.com
[warn] Par Diameter desconectado: pgw01.epc.example.com
[error] Falha na conexão do par Diameter: timeout
```

Eventos de Banco de Dados:

```
[info] Conexão com o banco de dados estabelecida
[error] Conexão com o banco de dados perdida: timeout
[error] Consulta ao banco de dados falhou: deadlock detectado
```

Eventos de Autenticação:

```
[info] Autenticação bem-sucedida: IMSI 001001123456789
[warn] Falha na autenticação: IMSI 001001123456789, vetor inválido
[error] Roaming negado: IMSI 001001123456789, MCC 310 MNC 410
```

Agregação de Logs

Para implantações em produção, implemente a agregação de logs:

Integração de Monitoramento Externo

Endpoint de Verificação de Saúde

Verificação de Saúde da API: `GET /api/status`

```
curl -k https://hss.example.com:8443/api/status
```

Resposta Esperada:

```
{"status": "ok"}
```

Status HTTP: 200 OK

Integração com Ferramentas de Monitoramento

Exemplo Nagios/Icinga

```
#!/bin/bash
# check_omnihss.sh

API_URL="https://hss.example.com:8443/api/status"

response=$(curl -k -s -o /dev/null -w "%{http_code}" "$API_URL" --
max-time 5)

if [ "$response" = "200" ]; then
    echo "OK - API do OmniHSS respondendo"
    exit 0
else
    echo "CRÍTICO - API do OmniHSS não respondendo (HTTP $response)"
    exit 2
fi
```

Integração com Prometheus

Exportadores personalizados podem ser criados para exportar métricas do OmniHSS para o Prometheus consultando a API e o banco de dados.

Integração SNMP

Para monitoramento baseado em SNMP, scripts de extensão SNMP

personalizados podem consultar o banco de dados ou a API para métricas e retornar valores via OIDs SNMP.

Indicadores-Chave de Desempenho

KPIs Operacionais

Limites Recomendados para KPIs

KPI	Meta	Aviso	Crítico
Tempo de Atividade do Sistema	99.99%	< 99.95%	< 99.9%
Tempo de Atividade do Par Diameter	99.9%	< 99.5%	< 99%
Taxa de Sucesso de Autenticação	> 99%	< 99%	< 95%
Tempo de Resposta do Diameter	< 100ms	> 200ms	> 500ms
Tempo de Consulta ao Banco de Dados	< 50ms	> 100ms	> 500ms
Taxa de Erro	< 0.1%	> 0.5%	> 1%

KPIs de Capacidade

Métrica	Monitorar	Planejar Ação em
Total de Assinantes	Contagem atual	80% da capacidade esperada
Sessões PDN Concorrentes	Sessões ativas	70% do máximo esperado
Tamanho do Banco de Dados	MB usados	80% do armazenamento alocado
Conexões ao Banco de Dados	Conexões ativas	80% do tamanho do pool

---

Estratégias de Alerta

Prioridades de Alerta

Definições de Alerta

Alertas Críticos (P1)

Sistema Indisponível:

- Falha na verificação de saúde da API
- Painel de Controle inacessível
- Falha na conexão com o banco de dados
- Ação: Investigação e escalonamento imediatos

Todos os Pares Diameter Desconectados:

- Zero pares conectados

- Ação: Verificar rede, reiniciar se necessário

Banco de Dados Fora do Ar:

- Não é possível conectar ao Banco de Dados SQL
- Ação: Investigar servidor de banco de dados, reiniciar se necessário

Alertas de Alta Prioridade (P2)

Par Diameter Crítico Fora do Ar:

- MME primário desconectado
- P-GW primário desconectado
- S-CSCF primário desconectado
- Ação: Investigar conectividade do par em até 15 minutos

Uso Elevado de Memória:

- Memória > 95%
- Ação: Investigar vazamento de memória, planejar reinicialização

Alta Taxa de Falha de Autenticação:

    - 10% das solicitações de autenticação falham

- Ação: Verificar provisionamento de assinantes, investigar causa

Alertas de Média Prioridade (P3)

Par Não Crítico Fora do Ar:

- Par secundário desconectado
- Servidor de Aplicação desconectado
- Ação: Investigar em até 1 hora

Uso Elevado de Memória:

- Memória > 85%
- Ação: Monitorar tendência, planejar atualização de capacidade

Taxa Elevada de Erro:

- Taxa de erro > 1%
- Ação: Revisar logs, identificar causa raiz

Alertas de Baixa Prioridade (P4)

Aviso de Capacidade:

- Assinantes > 80% da capacidade
- Banco de Dados > 80% do armazenamento alocado
- Ação: Planejar expansão de capacidade

Degradação de Desempenho:

- Tempos de resposta elevados, mas aceitáveis
- Ação: Monitorar e otimizar consultas

Canais de Notificação de Alerta

Checklist de Monitoramento

Verificações Diárias

- [ ] Revisar Visão Geral do Painel de Controle - contagens de assinantes normais
- [ ] Revisar página Diameter - todos os pares críticos conectados
- [ ] Revisar página de Aplicação - memória e processos dentro dos limites
- [ ] Verificar logs de erro - sem erros críticos nas últimas 24 horas
- [ ] Verificar se o backup foi concluído com sucesso

Verificações Semanais

- [ ] Revisar tendências de capacidade - crescimento de assinantes
- [ ] Revisar tendências de desempenho - tempos de resposta
- [ ] Revisar tamanho do banco de dados - taxa de crescimento aceitável
- [ ] Revisar taxas de erro - identificar padrões
- [ ] Testar notificações de alerta - garantir funcionamento

Verificações Mensais

- [ ] Revisão do planejamento de capacidade - projetar 6 meses à frente
- [ ] Revisão de otimização de desempenho - identificar consultas lentas
- [ ] Revisão de segurança - expiração de certificados, vulnerabilidades
- [ ] Revisão de documentação - atualizar runbooks
- [ ] Teste de recuperação de desastres - verificar se os backups restauram corretamente

---

← Voltar para o Guia de Operações | Próximo: Multi-Funcionalidades →

Recursos Multi-MSISDN e Multi-IMSI do OmniHSS

← Voltar ao Guia de Operações

Índice

Visão Geral

O OmniHSS suporta capacidades avançadas de provisionamento que permitem configurações de serviço flexíveis:

Suporte Multi-MSISDN

Um IMSI → Vários Números de Telefone

Um único assinante (identificado por um IMSI) pode ter múltiplos MSISDNs (números de telefone) atribuídos. Todos os números tocam no mesmo dispositivo e compartilham os mesmos perfis de serviço.

Suporte Multi-IMSI SIM

Uma SIM → Múltiplos IMSIs

Um único cartão SIM físico pode conter múltiplos IMSIs, permitindo que o dispositivo se conecte a diferentes redes usando diferentes identidades de rede. Isso é útil para roaming internacional e cenários de MVNO.

Multi-MSISDN: Vários Números de Telefone

Como Funciona

Um registro de assinante no HSS possui múltiplos MSISDNs vinculados através de uma tabela de junção. Quando o assinante se registra no IMS, todos os MSISDNs são

incluídos no perfil IMS, permitindo que chamadas recebidas para qualquer número cheguem ao dispositivo.

Características Principais

- **Um IMSI** - O assinante possui um único IMSI vinculado ao seu cartão SIM
- **Múltiplos MSISDNs** - O assinante pode ter vários números de telefone
- **Integração IMS** - Todos os MSISDNs estão registrados no IMS
- **Serviço Compartilhado** - Todos os números compartilham os mesmos perfis de serviço (EPC, IMS, Roaming)

Modelo de Dados

Importante: Um MSISDN pode ser atribuído a UM único assinante por vez. No entanto, um assinante pode ter VÁRIOS MSISDNs.

Casos de Uso

1. Linhas Empresariais e Pessoais

Um assinante possui números de telefone empresariais e pessoais no mesmo dispositivo:

2. Números Internacionais

Um assinante que viaja frequentemente possui números em vários países:

3. Planos Familiares

Um dos pais gerencia múltiplos números de membros da família:

Nota: No OmniHSS, isso exigiria múltiplos assinantes (um por SIM/IMSI), cada um potencialmente tendo múltiplos MSISDNs.

4. Portabilidade de Linha Legada

Quando um assinante muda de número, mas deseja manter o número antigo ativo durante a transição:

Configuração

Criando MSISDNs

Os MSISDNs devem ser criados antes de serem atribuídos aos assinantes.

```
# Criar primeiro MSISDN
curl -k -X POST https://hss.example.com:8443/api/msisdn \
  -H "Content-Type: application/json" \
  -d '{"msisdn": {"msisdn": "14155551001"}}'

# Criar segundo MSISDN
```

```
curl -k -X POST https://hss.example.com:8443/api/msisdn \
  -H "Content-Type: application/json" \
  -d '{"msisdn": {"msisdn": "14155551002"}}'
```

Atribuindo MSISDNs a Assinantes

A atribuição é feita através da tabela de junção no banco de dados.

Método de Banco de Dados:

1. Consulte o banco de dados para obter o ID do assinante para o IMSI alvo
2. Consulte o banco de dados para obter os IDs dos MSISDNs para os números de telefone
3. Insira registros na tabela de junção vinculando subscriber_id a cada msisdn_id

Isso cria a relação muitos-para-muitos entre o assinante e seus números de telefone.

Fluxo de Trabalho de Provisionamento

Verificando Atribuição

Consulte o banco de dados para recuperar o assinante junto com todos os MSISDNs vinculados por:

- Unir a tabela de assinantes com a tabela de junção
- Unir a tabela de junção com a tabela msisdn
- Agrupar resultados por assinante para ver todos os números de telefone juntos

Isso mostrará o ID do assinante, IMSI e uma lista de todos os MSISDNs atribuídos.

Integração IMS

Registro IMS

Quando um assinante se registra no IMS, **todos os MSISDNs atribuídos são incluídos** no perfil IMS enviado ao S-CSCF.

Renderização do Modelo IFC

O modelo IFC do IMS pode referenciar todos os MSISDNs usando a variável `{{msisdns}}`.

Exemplo de Modelo IFC:

```
<ServiceProfile>
  <PublicIdentity>

<Identity>sip:{{imsi}}@ims.mnc{{mnc}}.mcc{{mcc}}.3gppnetwork.org</Identity>
  </PublicIdentity>
  <!-- Repetir para cada MSISDN -->
  <PublicIdentity>
```

```
    <Identity>sip:+14155551001@ims.example.com</Identity>
  </PublicIdentity>
  <PublicIdentity>
    <Identity>tel:+14155551001</Identity>
  </PublicIdentity>
  <PublicIdentity>
    <Identity>sip:+14155551002@ims.example.com</Identity>
  </PublicIdentity>
  <PublicIdentity>
    <Identity>tel:+14155551002</Identity>
  </PublicIdentity>
  <!-- ... -->
</ServiceProfile>
```

Variável do Modelo:

- `{{msisdns}}` - Lista de todos os MSISDNs atribuídos ao assinante

Identidades Públicas

Cada MSISDN normalmente resulta em duas identidades públicas IMS:

Roteamento de Chamadas Recebidas

Quando alguém liga para um dos números do assinante, a rede IMS roteia para o URI SIP correto:

Apresentação de Chamadas de Saída

O telefone pode escolher qual número apresentar como ID do chamador para chamadas de saída.

Exemplo SIP INVITE:

```
INVITE sip:+15105551234@ims.example.com SIP/2.0
From: "+14155551002" <sip:+14155551002@ims.example.com>;tag=123
To: <sip:+15105551234@ims.example.com>
P-Asserted-Identity: <sip:+14155551002@ims.example.com>
```

Os cabeçalhos `From` e `P-Asserted-Identity` indicam qual dos números do assinante está sendo usado.

Resolução de Problemas Multi-MSISDN

Problema: MSISDN Não Aparece no Registro IMS

Sintomas:

- S-CSCF mostra apenas uma identidade pública
- Chamadas para o segundo número falham

Passos de Resolução:

1. **Verificar Atribuição de MSISDN no Banco de Dados:**
    - Consulte o banco de dados para recuperar todos os MSISDNs vinculados ao IMSI do assinante
    - Verifique a tabela de junção para garantir que as relações existam
2. **Verificar Modelo de Perfil IMS:**
    - Verifique se o modelo inclui a variável `{{msisdns}}`
    - Confirme se a sintaxe do modelo é um XML válido
3. **Revisar Logs do HSS:**
    - Procure por mensagens de registro IMS (Cx SAR)
    - Verifique se todos os MSISDNs estão incluídos na resposta
4. **Testar Registro IMS:**
    - Acione o re-registro no telefone
    - Verifique os logs do S-CSCF para identidades públicas registradas

Problema: Não é Possível Atribuir MSISDN ao Assinante

Sintomas:

- Falha na inserção do banco de dados
- Erro: "Entrada duplicada" ou "Restrição de chave estrangeira"

Possíveis Causas:

1. **MSISDN Já Atribuído:**
    - Consulte o banco de dados para verificar se o MSISDN já está vinculado a outro assinante
    - **Solução:** Remova a atribuição existente primeiro, depois crie a nova atribuição
2. **MSISDN Não Existe:**
    - Consulte o banco de dados para verificar se o registro do MSISDN existe
    - **Solução:** Crie o registro do MSISDN primeiro via API ou inserção no banco de dados

Problema: Chamadas para Um Número Funcionam, Outro Não

Sintomas:

- Chamadas para o número principal funcionam
- Chamadas para o número secundário falham ou roteiam incorretamente

Passos de Resolução:

1. **Verificar Ambos os Números no Registro IMS:**
    - Verifique as identidades públicas registradas no S-CSCF
    - Confirme se ambos os URIs SIP estão presentes
2. **Verificar Regras de Roteamento IMS:**
    - Verifique se as regras de roteamento do modelo IFC se aplicam a todas as identidades
    - Verifique se um número específico precisa de roteamento especial
3. **Testar Ambos os Números:**

```
# Testar a partir do cliente SIP
sip:+14155551001@ims.example.com  # Deve funcionar
sip:+14155551002@ims.example.com  # Também deve funcionar
```

Problema: Consulta API por MSISDN Retorna Assinante Errado

Sintomas:

- Consulta API `/api/subscriber/msisdn/:msisdn` retorna assinante inesperado

Verificação:

Consulte o banco de dados para descobrir a qual assinante o MSISDN está atribuído. Isso deve retornar exatamente um assinante. Se retornar múltiplos ou o assinante errado, a tabela de junção tem dados incorretos que precisam ser corrigidos.

Melhores Práticas

Ordem de Provisionamento

1. Crie todos os MSISDNs primeiro
2. Crie o assinante
3. Atribua MSISDNs ao assinante
4. Verifique a atribuição antes da ativação

Gestão de MSISDN

- **Documentar números primários vs secundários** em custom_attributes do assinante
- **Portar números sequencialmente** ao portar para evitar interrupção de serviço
- **Testar todos os números** após o provisionamento antes de entregar ao cliente

Configuração IMS

- Garantir que o modelo IFC trate corretamente múltiplas identidades públicas
- Testar roteamento de entrada para todos os números

- Verificar apresentação de ID do chamador para chamadas de saída

Migração

Ao migrar de um único para múltiplos MSISDNs:

Multi-IMSI SIM: Múltiplas Identidades de Rede

Como Funciona

Um SIM multi-IMSI contém múltiplos perfis completos de assinante, cada um com seu próprio IMSI, chaves e credenciais. O dispositivo pode alternar entre IMSIs para se conectar a diferentes redes, muitas vezes automaticamente com base na localização ou disponibilidade da rede.

Importante: Apenas **um IMSI pode estar ativo a qualquer momento**. Quando um dispositivo muda para um IMSI diferente no mesmo cartão SIM, o HSS automaticamente desregistrará o IMSI anteriormente ativo.

Implementação do OmniHSS

No OmniHSS, cada IMSI em um SIM multi-IMSI é provisionado como um **registro de assinante separado**, mas todos referenciam o **mesmo cartão SIM**:

Casos de Uso

1. Otimização de Roaming Internacional

- IMSI Doméstico: 001-001 (taxas de rede doméstica)
- IMSI de Roaming nos EUA: 310-410 (taxas locais dos EUA)
- IMSI de Roaming na UE: 234-015 (taxas locais da UE)
- Dispositivo alterna IMSI com base na localização

2. Serviço MVNO

- IMSI Primário: rede MVNO (revendedor)
- IMSI de Fallback: rede hospedeira (operadora mãe)
- Failover automático se a cobertura MVNO não estiver disponível

3. IoT/M2M Multi-Rede

- IMSI 1: Operadora primária
- IMSI 2: Operadora de backup para redundância
- IMSI 3: Fallback de emergência/custo baixo
- Dispositivos críticos mantêm conectividade

4. Conformidade Regulamentar

- Diferentes IMSIs para diferentes zonas regulatórias
- Cumprir requisitos locais de residência de dados

- Usar identidade de rede local por jurisdição

Recursos Multi-IMSI

Autenticação Independente

- Cada IMSI tem seu próprio Ki, OPC e conjunto de chaves
- Vetores de autenticação separados por IMSI
- Credenciais de segurança diferentes por rede

Perfis de Serviço Separados

- Diferentes perfis EPC (largura de banda, APNs)
- Diferentes perfis IMS (serviços de voz)
- Regras de roaming diferentes por IMSI

Identidade Física Compartilhada

- Todos os IMSIs referenciam o mesmo SIM (via sim_id)
- Mesmo ICCID em todos os registros de assinante
- Agrupamento lógico via cartão SIM

Seleção de Rede

- Dispositivo ou cartão SIM decide qual IMSI usar
- Com base em redes disponíveis, localização, política
- HSS autentica qualquer IMSI que o dispositivo apresentar

Configuração

```
# 1. Criar cartão SIM (capaz de multi-IMSI)
SIM_ID=$(curl -k -X POST https://hss.example.com:8443/api/sim \
  -d '{"sim": {"iccid": "8991101200003204510", "is_esim": false}}' \
  | jq -r '.data.id')

# 2. Criar conjunto de chaves para IMSI 1 (rede doméstica)
KEYSET1=$(curl -k -X POST https://hss.example.com:8443/api/key_set \
  -d '{"key_set": {"ki": "0123456789ABCDEF...", "opc": "FEDCBA9876..."}}' \
  | jq -r '.data.id')

# 3. Criar assinante 1 (IMSI doméstico)
curl -k -X POST https://hss.example.com:8443/api/subscriber \
  -d "{\"subscriber\": {
    \"imsi\": \"001001111111111\",
    \"sim_id\": $SIM_ID,
    \"key_set_id\": $KEYSET1,
    \"epc_profile_id\": 1
  }}"

# 4. Criar conjunto de chaves para IMSI 2 (parceiro de roaming)
KEYSET2=$(curl -k -X POST https://hss.example.com:8443/api/key_set \
  -d '{"key_set": {"ki": "1111111111111111...", "opc": "2222222222..."}}' \
```

```
  | jq -r '.data.id')

# 5. Criar assinante 2 (IMSI de roaming)
curl -k -X POST https://hss.example.com:8443/api/subscriber \
  -d "{\"subscriber\": {
    \"imsi\": \"310410222222222\",
    \"sim_id\": $SIM_ID,
    \"key_set_id\": $KEYSET2,
    \"epc_profile_id\": 2
  }}"

# 6. Repetir para IMSIs adicionais no SIM...
```

Fluxo de Autenticação

Quando um dispositivo multi-IMSI se conecta:

O HSS não precisa saber que é um SIM multi-IMSI—ele apenas autentica qualquer IMSI que o dispositivo apresentar.

Troca de IMSI e Desregistro Automático

Quando um SIM multi-IMSI muda de um IMSI para outro, apenas um IMSI pode estar registrado na rede a qualquer momento. O OmniHSS lida automaticamente com isso enviando uma **Solicitação de Cancelamento de Localização (CLR)** para desregistrar o IMSI anteriormente ativo quando um novo IMSI do mesmo cartão SIM se registra.

Regra de IMSI Único Ativo

Conceito Chave: Apenas um assinante (IMSI) por cartão SIM pode estar ativo a qualquer momento.

- Se um assinante está registrado em um MME usando **IMSI X**
- E o HSS recebe uma Solicitação de Atualização de Localização para **IMSI Y** (no mesmo SIM que IMSI X)
- O HSS envia automaticamente uma **Solicitação de Cancelamento de Localização** para desregistrar **IMSI X**

Isso garante uma transferência limpa entre IMSIs e evita conflitos na rede.

Fluxo de Troca de IMSI

Por Que Isso Importa

Integridade da Rede:

- Evita registros duplicados do mesmo SIM físico
- Garante que os recursos da rede sejam liberados corretamente
- Mantém dados de localização de assinante precisos

Precisão de Cobrança:

- Apenas um IMSI é cobrado pelo acesso à rede a qualquer momento
- Limites de sessão claros entre trocas de IMSI
- Geração precisa de CDR (Registro de Detalhes de Chamadas)

Gestão de Recursos:

- Recursos do MME para o IMSI antigo são liberados
- Contextos PDP e portadores são limpos
- O rastreamento de localização permanece preciso

Gatilhos de Troca de IMSI

O dispositivo/SIM decide quando trocar IMSIs com base em:

1. **Disponibilidade da Rede**
    - Rede do IMSI doméstico não disponível
    - Mudar para IMSI do parceiro de roaming
2. **Seleção Manual**
    - Usuário seleciona manualmente a rede
    - SIM muda para o IMSI correspondente
3. **Baseado em Política**
    - O cartão SIM tem regras internas (por exemplo, preferir IMSI local em certos países)
    - Troca automática com base em MCC/MNC
4. **Otimização de Custos**
    - Mudar para IMSI com taxas de roaming mais baixas
    - Usar IMSI local para evitar cobranças de roaming

Considerações IMS

O mesmo comportamento de Solicitação de Cancelamento de Localização se aplica ao registro IMS:

Impacto Operacional

Para a Equipe de Operações:

1. **Assinante aparece offline:** Quando o IMSI troca, o IMSI antigo aparecerá como "desregistrado" no HSS. Isso é um comportamento normal.
2. **Dois registros de assinante para um SIM:** SIMs multi-IMSI terão múltiplos registros de assinante compartilhando o mesmo `sim_id`. Apenas um estará no estado "registrado" a qualquer momento.
3. **Rastreamento de localização:** A tabela `subscriber_state` rastreia qual MME/

SGSN cada IMSI está registrado. Quando o IMSI troca, a localização antiga é limpa.

4. **Resolução de Problemas:** Se um dispositivo não puder ser alcançado:
    - Verifique qual IMSI está atualmente registrado
    - Verifique se o IMSI correto está sendo usado para a rede atual
    - Confirme que apenas um IMSI por SIM está no estado registrado

---

Cenários Combinados

Multi-IMSI + Multi-MSISDN

Você pode combinar ambos os recursos: múltiplos IMSIs em um SIM, cada um com múltiplos MSISDNs.

Exemplo de Caso de Uso:

- **Rede Doméstica (IMSI 1):**
    - Número pessoal: +1-415-555-1001
    - Número empresarial: +1-415-555-1002
- **Rede de Roaming nos EUA (IMSI 2):**
    - Número pessoal: +1-212-555-2001
    - Número empresarial: +1-212-555-2002

Quando o dispositivo está em território doméstico, usa IMSI 1 com seus MSISDNs. Quando está em roaming nos EUA, muda para IMSI 2 com diferentes MSISDNs otimizados para a rede dos EUA.

Procedimentos Operacionais

Gerenciando Assinantes Multi-MSISDN

Visualize todos os MSISDNs para um assinante:

```
Consulta via API: GET /api/subscriber/imsi/:imsi
```

A resposta inclui todos os MSISDNs vinculados.

Resolução de Problemas Multi-IMSI

Dispositivo não se conectando com o segundo IMSI:

1. Verifique se o segundo registro de assinante existe para esse IMSI
2. Verifique se o key_set está configurado corretamente para esse IMSI

3. Verifique se o perfil EPC está atribuído
4. Confirme se as regras de roaming permitem a conexão

Dispositivo trocando IMSIs inesperadamente:

- Isso é controlado pela lógica do dispositivo/SIM, não pelo HSS
- O HSS autentica qualquer IMSI apresentado
- Verifique as configurações de seleção de IMSI do dispositivo

Resolução de Problemas Multi-MSISDN

Segundo número não tocando:

1. Verifique se o MSISDN está vinculado na tabela de junção
2. Verifique se o modelo de perfil IMS inclui a variável `{{msisdns}}`
3. Confirme se o registro IMS inclui todas as identidades públicas
4. Revise os logs do S-CSCF para identidades registradas

Chamadas de saída mostram apenas um número:

- O dispositivo seleciona qual número apresentar como ID do chamador
- Isso é configuração do dispositivo, não do HSS
- O HSS fornece todas as identidades; o dispositivo escolhe

Resumo dos Benefícios

Benefícios Multi-MSISDN

✓ Um SIM, múltiplos números de telefone
✓ Linhas empresariais e pessoais separadas
✓ Presença local internacional
✓ Gestão simplificada do dispositivo
✓ Todos os números compartilham o mesmo serviço de dados
✓ Faturamento centralizado por IMSI

Benefícios do SIM Multi-IMSI

✓ Custos de roaming otimizados
✓ Seleção automática de rede
✓ Redundância e failover
✓ Identidade de rede local
✓ Conformidade regulatória
✓ Continuidade de serviço entre redes

Benefícios Combinados

✓ Máxima flexibilidade
✓ Diferentes conjuntos de números por rede
✓ Otimizado para cada caso de uso
✓ Cenários empresariais complexos

✓ Otimização internacional e local

← Voltar ao Guia de Operações

Gerenciamento de Perfis do OmniHSS

← Voltar para o Guia de Operações

Visão Geral

O OmniHSS utiliza **perfis** para definir características de serviço para assinantes. Os perfis permitem criar modelos de serviço reutilizáveis que podem ser atribuídos a múltiplos assinantes, simplificando o provisionamento e garantindo consistência.

Tipos de Perfis

Perfis EPC

Os Perfis EPC (Evolved Packet Core) definem características de serviço de dados para assinantes LTE.

Parâmetros Chave

Parâmetro	Descrição	Valores Típicos
`ue_ambr_dl_kbps`	Limite de velocidade de download	10.000 - 1.000.000 Kbps
`ue_ambr_ul_kbps`	Limite de velocidade de upload	5.000 - 500.000 Kbps
`network_access_mode`	Tipo de serviço	0 (Apenas Pacote), 2 (Pacote+CS)
`tracking_area_update_interval_seconds`	Temporizador TAU	54 segundos (típico)

Criando Perfis EPC

```
curl -k -X POST https://hss.example.com:8443/api/epc/profile \
  -H "Content-Type: application/json" \
  -d '{
    "epc_profile": {
      "name": "Premium 100Mbps",
      "ue_ambr_dl_kbps": 100000,
      "ue_ambr_ul_kbps": 50000,
      "network_access_mode": 0
    }
  }'
```

Modelos Comuns de Perfis EPC

Internet Básica:

- Download: 10 Mbps (10.000 Kbps)
- Upload: 5 Mbps (5.000 Kbps)

Padrão:

- Download: 50 Mbps (50.000 Kbps)
- Upload: 25 Mbps (25.000 Kbps)

Premium:

- Download: 100 Mbps (100.000 Kbps)
- Upload: 50 Mbps (50.000 Kbps)

Ilimitado:

- Download: 1 Gbps (1.000.000 Kbps)
- Upload: 500 Mbps (500.000 Kbps)

Perfis IMS

Os Perfis IMS definem características de serviço de voz, principalmente através de modelos IFC (Initial Filter Criteria).

Modelos IFC

Os modelos IFC são documentos XML que definem regras de roteamento de chamadas para o S-CSCF.

Variáveis do Modelo:

- `{{imsi}}` - IMSI do Assinante
- `{{msisdns}}` - Lista de números de telefone
- `{{mcc}}` - Código do país de origem
- `{{mnc}}` - Código da rede de origem

Criando Perfis IMS

```
curl -k -X POST https://hss.example.com:8443/api/ims/profile \
  -H "Content-Type: application/json" \
  -d '{
    "ims_profile": {
      "name": "Padrão VoLTE",
      "ifc_template": "<InitialFilterCriteria>...</InitialFilterCriteria>"
    }
  }'
```

Exemplo de Modelo IFC

```
<ServiceProfile>
  <PublicIdentity>

<Identity>sip:{{imsi}}@ims.mnc{{mnc}}.mcc{{mcc}}.3gppnetwork.org</Identity>
  </PublicIdentity>
  <InitialFilterCriteria>
    <Priority>0</Priority>
    <TriggerPoint>
      <ConditionTypeCNF>0</ConditionTypeCNF>
      <SPT>
        <ConditionNegated>0</ConditionNegated>
        <Group>0</Group>
        <Method>INVITE</Method>
      </SPT>
    </TriggerPoint>
    <ApplicationServer>
      <ServerName>sip:as.ims.example.com</ServerName>
      <DefaultHandling>0</DefaultHandling>
    </ApplicationServer>
  </InitialFilterCriteria>
</ServiceProfile>
```

Perfis APN

Os Perfis APN (Access Point Name) definem pontos de acesso à rede para conexões de dados.

Componentes APN

Identificador APN

Define o nome da APN e o suporte ao protocolo IP.

APNs Comuns:

- `internet` - Acesso geral à internet
- `ims` - Sinalização IMS/VoLTE
- `mms` - Mensagens multimídia
- `vzwadmin` - Específico do operador

Opções de Versão IP:

- 0: Apenas IPv4
- 1: Apenas IPv6
- 2: IPv4v6 (pilha dupla)
- 3: IPv4 ou IPv6 (escolha da rede)

Perfil QoS APN

Define parâmetros de qualidade de serviço.

Valores de QCI (Identificador de Classe de QoS):

QCI	Tipo	Caso de Uso	Prioridade
1	GBR	Voz conversacional	Mais Alto
2	GBR	Vídeo conversacional	Alto
4	GBR	Streaming de vídeo	Alto
5	Non-GBR	Sinalização IMS	Médio
9	Non-GBR	Internet (padrão)	Mais Baixo

Criando Configuração Completa de APN

```
# 1. Criar Identificador APN
APN_ID=$(curl -k -X POST https://hss.example.com:8443/api/apn/identifier \
  -H "Content-Type: application/json" \
  -d '{"apn_identifier": {"apn": "internet", "ip_version": 2}}' \
  | jq -r '.data.id')

# 2. Criar Perfil QoS APN
QOS_ID=$(curl -k -X POST https://hss.example.com:8443/api/apn/qos_profile \
  -H "Content-Type: application/json" \
  -d '{
    "apn_qos_profile": {
      "name": "Melhor Esforço",
      "qci": 9,
      "allocation_retention_priority": 8,
      "apn_ambr_dl_kbps": 50000,
      "apn_ambr_ul_kbps": 25000,
      "pre_emption_capability": false,
      "pre_emption_vulnerability": true
    }
  }' | jq -r '.data.id')

# 3. Criar Perfil APN
curl -k -X POST https://hss.example.com:8443/api/apn/profile \
  -H "Content-Type: application/json" \
  -d "{
    \"apn_profile\": {
      \"name\": \"Perfil APN Internet\",
      \"apn_identifier_id\": $APN_ID,
      \"apn_qos_profile_id\": $QOS_ID
    }
  }"
```

Atribuindo APNs ao Perfil EPC

As APNs estão vinculadas aos Perfis EPC através da tabela `join_epc_profile_to_apn_profile`.

Insira registros na tabela de junção para vincular IDs de perfil APN ao ID do perfil EPC. Múltiplos perfis APN podem ser atribuídos a um perfil EPC.

Perfis de Roaming

Veja a documentação detalhada no Guia de Controle de Roaming.

Atribuição de Perfis

Relações de Perfil de Assinante

Atribuindo Perfis a Assinantes

```
# Atribuir perfis EPC e IMS durante a criação do assinante
curl -k -X POST https://hss.example.com:8443/api/subscriber \
  -H "Content-Type: application/json" \
  -d '{
    "subscriber": {
      "imsi": "001001123456789",
      "key_set_id": 1,
      "epc_profile_id": 1,
      "ims_profile_id": 1,
      "roaming_profile_id": 1
    }
  }'

# Atualizar perfil do assinante
curl -k -X PUT https://hss.example.com:8443/api/subscriber/1 \
  -H "Content-Type: application/json" \
  -d '{
    "subscriber": {
      "epc_profile_id": 2
    }
  }'
```

Melhores Práticas para Gerenciamento de Perfis

Princípios de Design

1. **Criar Perfis Padrão** - Definir níveis de serviço comuns (Básico, Padrão, Premium)
2. **Reutilizar Perfis** - Atribuir o mesmo perfil a múltiplos assinantes
3. **Documentar Alterações** - Rastrear modificações de perfil
4. **Testar Antes da Produção** - Verificar se o perfil funciona primeiro com assinante de teste

Convenção de Nomenclatura de Perfis

```
[Nível de Serviço]-[Velocidade]-[Recursos]

Exemplos:
- "Básico-10Mbps-Internet"
- "Premium-100Mbps-VoLTE"
- "Empresarial-1Gbps-MultiAPN"
```

Migração de Perfis

Ao alterar o perfil de um assinante:

Importante: Alterações de perfil entram em vigor na próxima:

- Atualização de Área de Rastreamento (TAU)
- Anexação
- Registro IMS (para alterações de perfil IMS)

Solução de Problemas de Perfis

Assinante não obtendo a velocidade esperada:

1. Verifique os valores AMBR do perfil EPC atribuído
2. Verifique os valores AMBR do perfil QoS APN
3. Verifique se o MME/P-GW está aplicando QoS corretamente
4. Verifique se há congestionamento na rede

Falha no registro IMS:

1. Verifique se o perfil IMS está atribuído
2. Verifique a validade do XML do modelo IFC
3. Revise os logs do S-CSCF para erros de processamento do IFC
4. Confirme a configuração de seleção do S-CSCF

APN não disponível:

1. Verifique se o perfil APN está vinculado ao perfil EPC
2. Verifique se o identificador APN corresponde à solicitação da rede
3. Revise a solicitação de conectividade PDN do UE

← Voltar para o Guia de Operações | Próximo: Controle de Roaming →

Fluxos de Protocolo OmniHSS

← Voltar ao Guia de Operações

Visão Geral

Este documento detalha os fluxos de mensagens do protocolo Diameter suportados pelo OmniHSS. Compreender esses fluxos é essencial para solução de problemas e operações.

Interface S6a (LTE/EPC)

Solicitação de Informação de Autenticação (AIR/AIA)

MME solicita vetores de autenticação para o assinante.

AVPs Chave:

- Solicitação: User-Name (IMSI), Visited-PLMN-Id, Número de Vetores Solicitados
- Resposta: Authentication-Info (RAND, AUTN, XRES, KASME)

Solicitação de Atualização de Localização (ULR/ULA)

MME notifica HSS sobre a localização do assinante e recupera dados de assinatura.

AVPs Chave:

- Solicitação: User-Name (IMSI), RAT-Type, ULR-Flags, Visited-PLMN-Id, UE-SRVCC-Capability
- Resposta: Subscription-Data (AMBR, APN-Configuration, Network-Access-Mode)

Solicitação de Purga de UE (PUR/PUA)

MME notifica HSS quando o contexto do assinante é excluído.

Solicitação de Notificação (NOR/NOA)

MME informa HSS sobre vários eventos.

Solicitação de Cancelamento de Localização (CLR/CLA)

HSS inicia o cancelamento de localização para informar ao MME que o assinante deve ser desassociado. O OmniHSS suporta tanto o envio automático quanto programático de CLR.

CLR Automático (Transferência de MME)

Quando um assinante realiza uma Solicitação de Atualização de Localização de um novo MME, o OmniHSS envia automaticamente um CLR para o MME anterior para limpar registros obsoletos.

AVPs Chave (CLR Automático):

- User-Name: IMSI do assinante
- Destination-Host: Nome do host do MME anterior
- Destination-Realm: Reino do MME anterior
- Tipo-de-Cancelamento: 0 (Procedimento de Atualização do MME)
- CLR-Flags: 0
- Subscription-Data: Perfil completo de assinatura

Implementação: `lib/hss/control/diameter/s6a.ex:216-256`

CLR Programático (Acionado por API)

Administradores podem acionar CLR via a API programática para desassociar assinantes à força (por exemplo, para retirada de assinatura, prevenção de fraudes ou ações administrativas).

AVPs Chave (CLR Programático):

- User-Name: IMSI do assinante
- Destination-Host: Nome do host do último MME visto
- Destination-Realm: Reino do último MME visto
- Tipo-de-Cancelamento: `:subscription_withdrawal` (codificado como inteiro conforme 3GPP TS 29.272)
- CLR-Flags:
  - s6a_indicator: 1 (indica interface S6a)
  - reattach_required: 1 (UE deve re-autenticar para reanexar)

Implementação:

- Função da API: `lib/hss/control/common.ex:557-583`
- Construtor de Mensagem: `lib/hss/control/diameter/s6a.ex:542-578`

Tipos de Cancelamento

O OmniHSS suporta múltiplos tipos de cancelamento conforme 3GPP TS 29.272:

Tipo	Valor	Descrição	Caso de Uso
Procedimento de Atualização do MME	0	Mudança normal de MME	Automático durante ULR de novo MME
Procedimento de Atualização do SGSN	1	Transferência de SGSN	Cenários de transferência 3G/2G
Retirada de Assinatura	2	Término administrativo	Desassociação manual via API
Procedimento de Atualização IWF	3	Atualização da função de interconexão	Interoperabilidade de rede legada
Procedimento de Anexação Inicial	4	Registro fresco	Forçar re-autenticação

CLR-Flags

O AVP CLR-Flags é uma máscara de bits com os seguintes campos:

Flag	Bit	Descrição
Indicador S6a/S6d	0	1 = interface S6a usada
Reanexação Necessária	1	1 = UE deve realizar novo anexo

Exemplo de Configuração de CLR-Flags:

```
clr_flags: %{
  s6a_indicator: 1,        # Usando interface S6a
  reattach_required: 1     # Forçar re-autenticação
}
```

Cenários Multi-IMSI

O OmniHSS rastreia o registro do MME **por assinante (IMSI)**, não por MSISDN. Isso é crítico para entender o comportamento do CLR em cenários multi-IMSI:

Cenário 1: Múltiplos MSISDNs, Um Único IMSI

```
Assinante A:
  - IMSI: 999000123456789
  - MSISDNs: ["+1234567890", "+9876543210"]
  - last_seen_mme: "mme01.operator.com"
```

Quando este assinante se move para um novo MME:

- **Um CLR enviado** para "mme01.operator.com" com IMSI 999000123456789

- Ambos os MSISDNs são afetados (mesmo assinante, mesmo SIM)
- O AVP User-Name contém o IMSI, não os MSISDNs

Cenário 2: Múltiplos Assinantes (IMSI Diferentes), Mesmo MSISDN

O OmniHSS impõe a **restrição de MSISDN único** (um MSISDN não pode pertencer a múltiplos assinantes simultaneamente). No entanto, durante portabilidade/migração:

```
Assinante A:
  - IMSI: 999000111111111
  - MSISDN: "+1234567890"
  - last_seen_mme: "mme01.operator.com"

Assinante B (após portabilidade):
  - IMSI: 999000222222222
  - MSISDN: "+1234567890"  # Mesmo MSISDN, SIM/IMSI diferente
  - last_seen_mme: "mme02.operator.com"
```

Quando o Assinante B se registra:

- **Nenhum CLR enviado** (IMSI diferente = assinante diferente)
- O Assinante A permanece registrado no mme01
- O Assinante B se registra no mme02
- Ambos podem estar ativos simultaneamente (dispositivos físicos diferentes)

Cenário 3: CLR Programático para Assinante Multi-MSISDN

```
# Chamada da API para desassociar assinante
Hss.Control.Common.send_cancel_location_request(:imsi,
"999000123456789")
```

Resultado:

- **Um CLR enviado** para o last_seen_mme do assinante
- **Todos os MSISDNs** associados a esse IMSI são efetivamente desassociados
- O IMSI é a chave primária para rastrear o registro do MME

Notas Importantes

1. **IMSI é a Chave:** As operações de CLR são sempre **por IMSI**, nunca por MSISDN. A tabela `subscriber_state` rastreia `last_seen_mme` por assinante (IMSI).

2. **Operação Atômica:** Cada assinante pode estar registrado em apenas um MME por vez. O CLR automático garante isso limpando o registro antigo.

3. **Sem CLR se Não Houver MME Anterior:** Se `last_seen_mme` for `nil` (assinante nunca registrado), nenhum CLR é enviado durante ULR.

4. **Dados de Assinatura Incluídos:** O CLR automático (durante ULR) inclui o AVP completo `Subscription-Data` para ajudar o MME antigo a limpar corretamente o contexto.

5. **Assíncrono:** O CLR é enviado de forma assíncrona (fire-and-forget). A resposta ULA para o novo MME não espera pelo CLA do MME antigo.

6. **Tratamento de CLA:** O OmniHSS recebe respostas CLA, mas atualmente as descarta (`:discard` na linha 398). Isso previne loops de mensagens e é um comportamento padrão do HSS.

Interface Cx (IMS)

Solicitação de Autorização de Usuário (UAR/UAA)

I-CSCF consulta se o usuário está autorizado a registrar.

Solicitação de Atribuição de Servidor (SAR/SAA)

S-CSCF registra/desregistra usuário e recupera perfil IMS.

Renderização do Template IFC:

- `{{imsi}}` → IMSI real
- `{{msisdns}}` → Lista de números de telefone
- `{{mcc}}, {{mnc}}` → Códigos do PLMN de origem

Solicitação de Autenticação Multimídia (MAR/MAA)

S-CSCF solicita vetores de autenticação para registro IMS.

Solicitação de Informação de Localização (LIR/LIA)

I-CSCF consulta qual S-CSCF está atendendo o usuário.

Interface Sh (Dados do Perfil IMS)

Solicitação de Dados do Usuário (UDR/UDA)

O Servidor de Aplicação solicita dados do perfil do assinante.

Solicitação de Atualização de Perfil (PUR/PUA)

O Servidor de Aplicação atualiza dados do perfil do assinante.

Solicitação de Notificações de Inscrição (SNR/SNA)

O Servidor de Aplicação se inscreve para mudanças de perfil.

Interface Gx (Controle de Política)

O OmniHSS funciona como o PCRF (Função de Regras de Política e Cobrança) via a interface Gx.

Veja Documentação do PCRF para arquitetura detalhada, configuração de políticas e gerenciamento de QoS.

Solicitação de Controle de Crédito - Inicial (CCR-I/CCA-I)

P-GW solicita regras de política quando a sessão PDN é estabelecida.

AVPs Chave:

- Solicitação: Subscription-Id (IMSI), Called-Station-Id (APN), RAT-Type, IP-CAN-Type
- Resposta: QoS-Information (QCI, ARP, AMBR), Charging-Rule-Install

Solicitação de Controle de Crédito - Atualização (CCR-U/CCA-U)

P-GW notifica sobre mudanças na sessão.

Solicitação de Controle de Crédito - Terminar (CCR-T/CCA-T)

P-GW notifica quando a sessão PDN termina.

Solicitação de Reautenticação (RAR/RAA)

OmniHSS (PCRF) inicia atualização de política para P-GW.

Interface Rx (Política de Mídia IMS)

OmniHSS funciona como o PCRF via a interface Rx para autorização de mídia IMS.

Veja Documentação do PCRF para fluxos de chamadas VoLTE detalhados e

autorização de mídia.

Solicitação AA (AAR/AAA)

P-CSCF solicita autorização de mídia para sessão IMS.

Informações Chave:

- Analisar SDP para determinar codec e largura de banda
- Calcular largura de banda necessária (UL/DL)
- Criar filtros SDF para fluxos de mídia
- Acionar bearer dedicado via Gx RAR

Solicitação de Término de Sessão (STR/STA)

P-CSCF notifica quando a sessão IMS termina.

Interface S13 (EIR)

OmniHSS funciona como o EIR (Registro de Identidade de Equipamento) via a interface S13.

Veja Documentação do EIR para verificação detalhada de identidade de equipamentos, validação de IMEI e gerenciamento de listas negras.

Solicitação de Verificação de Identidade de ME (ECR/ECA)

Cliente EIR externo (ou MME) solicita validação de equipamento.

Valores de Status do Equipamento:

- **Equipamento Desconhecido (0)** - Dispositivo permitido (lista branca)
- **Equipamento na Lista Negra (1)** - Dispositivo bloqueado
- **Equipamento na Lista Cinza (2)** - Dispositivo permitido, mas monitorado

---

Fluxo de Chamada Completo: Chamada VoLTE

Configuração de chamada VoLTE de ponta a ponta mostrando múltiplas interfaces.

Resolução de Problemas de Protocolo

Falhas de Autenticação (S6a AIR)

Verifique:

1. Conjunto de chaves configurado corretamente (Ki, OPC, AMF)
2. Sincronização de SQN (se falhas repetidas)
3. Regras de roaming permitem rede visitada

Falhas de Atualização de Localização (S6a ULR)

Verifique:

1. Perfil EPC existe e tem APNs configurados
2. Roaming permitido para serviços de dados
3. Formato da identidade do MME correto

Falhas de Registro IMS (Cx SAR)

Verifique:

1. Perfil IMS atribuído ao assinante
2. Template IFC XML válido
3. Seleção de S-CSCF configurada
4. MSISDNs atribuídos se usados no template

Falhas de Conexão PDN (Gx CCR-I)

Verifique:

1. APN existe na lista de APNs do perfil EPC
2. Perfil de QoS do APN configurado
3. Tabela de sessão PDN não está cheia (se limites existirem)

← Voltar ao Guia de Operações

Controle de Roaming do OmniHSS

← Voltar para o Guia de Operações

Visão Geral

O OmniHSS fornece controle de roaming granular, permitindo que você defina quais redes os assinantes podem acessar para serviços de dados e IMS ao roaming.

Fluxo de Controle de Roaming

Estrutura do Perfil de Roaming

Componentes

Regra de Roaming

Cada regra especifica a ação para uma rede específica (combinação de MCC/MNC).

Campos:

- `name` - Nome descritivo
- `mcc` - Código do País Móvel (3 dígitos)
- `mnc` - Código da Rede Móvel (2-3 dígitos)
- `data_action` - 0 (Permitir) ou 1 (Negar)
- `ims_action` - 0 (Permitir) ou 1 (Negar)

Perfil de Roaming

Define o comportamento padrão e vincula às regras.

Campos:

- `name` - Nome do perfil
- `data_action_if_no_rules_match` - 0 (Permitir) ou 1 (Negar)
- `ims_action_if_no_rules_match` - 0 (Permitir) ou 1 (Negar)

Exemplos de Configuração

Permitir Todo o Roaming

```
# Criar perfil que permite tudo
curl -k -X POST https://hss.example.com:8443/api/roaming/profile \
  -H "Content-Type: application/json" \
  -d '{
    "roaming_profile": {
      "name": "Permitir Tudo",
      "data_action_if_no_rules_match": 0,
      "ims_action_if_no_rules_match": 0
    }
  }'
```

Negar Todo o Roaming

```
# Criar perfil que bloqueia tudo
curl -k -X POST https://hss.example.com:8443/api/roaming/profile \
  -H "Content-Type: application/json" \
  -d '{
    "roaming_profile": {
      "name": "Sem Roaming",
      "data_action_if_no_rules_match": 1,
      "ims_action_if_no_rules_match": 1
    }
  }'
```

Permitir Redes Específicas (Lista Branca)

```
# Criar perfil com negação por padrão
PROFILE_ID=$(curl -k -X POST https://hss.example.com:8443/api/
roaming/profile \
  -H "Content-Type: application/json" \
  -d '{
    "roaming_profile": {
      "name": "Apenas Operadoras dos EUA",
      "data_action_if_no_rules_match": 1,
      "ims_action_if_no_rules_match": 1
    }
  }' | jq -r '.data.id')

# Permitir AT&T
RULE1=$(curl -k -X POST https://hss.example.com:8443/api/roaming/rule
\
  -H "Content-Type: application/json" \
  -d '{
```

```
    "roaming_rule": {
      "name": "Permitir AT&T",
      "mcc": "310",
      "mnc": "410",
      "data_action": 0,
      "ims_action": 0
    }
  }' | jq -r '.data.id')

# Permitir Verizon
RULE2=$(curl -k -X POST https://hss.example.com:8443/api/roaming/rule
\
  -H "Content-Type: application/json" \
  -d '{
    "roaming_rule": {
      "name": "Permitir Verizon",
      "mcc": "311",
      "mnc": "480",
      "data_action": 0,
      "ims_action": 0
    }
  }' | jq -r '.data.id')

# Vincular regras ao perfil (via banco de dados)
# Inserir registros na tabela join_roaming_profile_to_roaming_rule
# para vincular cada ID de regra ao ID do perfil de roaming
```

Permitir Dados, Bloquear Voz

```
# Criar regra que permite dados, mas bloqueia IMS
curl -k -X POST https://hss.example.com:8443/api/roaming/rule \
  -H "Content-Type: application/json" \
  -d '{
    "roaming_rule": {
      "name": "Apenas Dados - T-Mobile",
      "mcc": "310",
      "mnc": "260",
      "data_action": 0,
      "ims_action": 1
    }
  }'
```

Bloquear Redes Específicas (Lista Negra)

```
# Criar perfil com permissão por padrão
PROFILE_ID=$(curl -k -X POST https://hss.example.com:8443/api/
roaming/profile \
  -H "Content-Type: application/json" \
```

```
  -d '{
    "roaming_profile": {
      "name": "Bloquear Redes Caras",
      "data_action_if_no_rules_match": 0,
      "ims_action_if_no_rules_match": 0
    }
  }' | jq -r '.data.id')

# Bloquear rede cara específica
curl -k -X POST https://hss.example.com:8443/api/roaming/rule \
  -H "Content-Type: application/json" \
  -d '{
    "roaming_rule": {
      "name": "Bloquear Rede Cara",
      "mcc": "206",
      "mnc": "01",
      "data_action": 1,
      "ims_action": 1
    }
  }'
```

Cenários Comuns de Roaming

Cenário 1: Apenas Roaming Doméstico

O assinante pode roaming dentro do país de origem, mas não internacionalmente.

Configuração:

- Padrão: Negar tudo
- Regras: Permitir todos os códigos MCC dos EUA (310, 311, 312, 313, 314, 315, 316)

Cenário 2: Apenas Parceiros de Roaming

O assinante só pode roaming em redes com acordos comerciais.

Configuração:

- Padrão: Negar tudo
- Regras: Permitir cada rede parceira explicitamente (por MCC/MNC)

Cenário 3: Roaming de Dados, Sem Roaming de Voz

O assinante pode usar dados no exterior, mas deve usar Wi-Fi para chamadas de voz.

Configuração:

- Regras: `data_action: 0` (permitir), `ims_action: 1` (negar)

Cenário 4: Acesso a Serviços de Emergência

Sempre permitir serviços de emergência, mesmo que o roaming esteja bloqueado.

Nota: O manuseio de serviços de emergência é tipicamente feito no nível do MME/rede. As regras de roaming do OmniHSS se aplicam a serviços normais.

Referência MCC/MNC

Códigos de País Comuns (MCC)

MCC	País	Redes
310-316	EUA	AT&T, Verizon, T-Mobile, etc.
302	Canadá	Rogers, Bell, Telus
234-235	Reino Unido	Vodafone, O2, EE
262	Alemanha	Deutsche Telekom, Vodafone
208	França	Orange, SFR, Bouygues
222	Itália	TIM, Vodafone, Wind
214	Espanha	Movistar, Vodafone

Operadoras Comuns dos EUA (MCC 310-316)

MCC	MNC	Operadora
310	410	AT&T
311	480	Verizon
310	260	T-Mobile
310	120	Sprint
313	380	(Rede de teste de exemplo)

Listas Completas: Veja ITU-T E.212 ou bancos de dados MCC/MNC

Pontos de Aplicação de Roaming

Interface S6a (Dados)

Quando o assinante se conecta à rede visitada:

Interface Cx (IMS)

Quando o assinante se registra no IMS na rede visitada:

Solução de Problemas de Roaming

Assinante Não Consegue Conectar na Rede Visitada

Verifique a atribuição do perfil de roaming:

- Consulte o banco de dados para visualizar o perfil de roaming atribuído ao assinante
- Verifique o nome do perfil e as configurações da ação padrão

Verifique se a regra existe para a rede visitada:

- Consulte o banco de dados para regras de roaming correspondentes ao MCC/MNC da rede visitada
- Verifique se uma regra existe para o perfil de roaming do assinante
- Verifique o valor de data_action para essa rede específica

Assinante Consegue Conectar, Mas Não Registrar IMS

Verifique a ação IMS separadamente:

- Consulte as regras de roaming para a rede visitada
- Verifique os valores de data_action e ims_action
- Procure casos em que os dados são permitidos, mas IMS é negado

Comportamento de Roaming Inesperado

Revise os logs para verificações de roaming:

```
[info] Verificação de roaming: IMSI 001001123456789, PLMN Visitado
310-410
[info] Regra de roaming correspondente: "Permitir AT&T"
[info] Ação de dados: permitir, Ação IMS: permitir
```

Melhores Práticas

Design de Perfil

1. **Comece restritivo** - Negar por padrão, permitir explicitamente parceiros
2. **Teste minuciosamente** - Verifique regras em laboratório antes da

produção
3. **Documente regras** - Mantenha uma lista de redes permitidas e por quê
4. **Revise regularmente** - Atualize conforme os acordos de roaming mudam

Gestão de Regras

1. **Use nomes descritivos** - "Permitir-ATT-Apenas-Dados" não "Regra1"
2. **Verifique MCC/MNC** - Verifique os códigos contra bancos de dados oficiais
3. **Considere ambos os serviços** - Pense em dados e IMS separadamente
4. **Monitore o uso** - Acompanhe quais redes os assinantes realmente visitam

Procedimentos Operacionais

1. **Mudanças de Emergência** - Tenha um procedimento para habilitar/desabilitar rapidamente o roaming
2. **Atualizações em Massa** - Planeje para atualizar os perfis de roaming de múltiplos assinantes
3. **Relatórios** - Acompanhe o uso de roaming e tentativas negadas
4. **Comunicação com Clientes** - Notifique os clientes sobre mudanças na política de roaming

---

← Voltar para o Guia de Operações | Próximo: Fluxos de Protocolo →

Guia de Solução de Problemas do OmniHSS

← Voltar ao Guia de Operações

Índice

Visão Geral da Solução de Problemas

Abordagem Geral de Solução de Problemas

Informações a Coletar

Antes de solucionar qualquer problema, colete:

1. **Informações do Assinante** (se específico do assinante)
    - IMSI
    - MSISDN (número de telefone)
    - Último estado conhecido
    - Mensagens de erro do dispositivo
2. **Informações de Tempo**
    - Quando o problema começou?
    - É intermitente ou constante?

    - Hora da última operação bem-sucedida

3. **Escopo do Impacto**
    - Assinante único ou múltiplos?
    - Rede específica ou todas as redes?
    - Serviço específico (dados/vóz) ou ambos?

4. **Estado do Sistema**
    - Verifique o Painel de Controle para o status do sistema
    - Revise o status do par Diameter
    - Verifique a conectividade do banco de dados

Falhas de Autenticação

Sintomas

- Assinante não consegue se conectar à rede
- Erros "Autenticação rejeitada"
- Tentativas de autenticação repetidas

Causas Comuns e Soluções

Causa 1: Conjunto de Chaves Incorreto

Sintomas:

- Falha de autenticação consistente para assinante específico
- Funciona para outros assinantes com o mesmo perfil

Passos de Diagnóstico:

1. Consultar assinante para verificar key_set_id:

   ```
   curl -k https://hss.example.com:8443/api/subscriber/imsi/[IMSI]
   ```

2. Verificar se o conjunto de chaves existe e possui valores corretos:

   ```
   curl -k https://hss.example.com:8443/api/key_set/[KEY_SET_ID]
   ```

3. Comparar valores de Ki e OPC com a documentação do cartão SIM

Solução:

- Atualizar assinante com o conjunto de chaves correto

- Se as chaves estiverem corretas, o cartão SIM pode estar com defeito

Causa 2: SQN Fora de Sincronização

Sintomas:

- Autenticação falha após ter funcionado anteriormente
- Erro: "Falha de sincronização SQN"
- Funciona intermitentemente

Passos de Diagnóstico:

1. Verificar estado do assinante para o valor SQN no banco de dados
2. Procurar erros relacionados ao SQN nos logs
3. Verificar o valor SQN do conjunto de chaves do assinante

Solução:

- O SQN será automaticamente re-sincronizado após o assinante enviar AUTS
- Se persistir, redefinir SQN para 0 no conjunto de chaves (requer re-conexão do assinante)

Aviso: Redefinir SQN pode causar problemas de segurança. Faça isso apenas durante a manutenção.

Causa 3: Assinante Desativado

Sintomas:

- Autenticação rejeitada imediatamente
- Nenhum vetor de autenticação gerado

Passos de Diagnóstico:

1. Verificar status de habilitação do assinante:

   ```
   curl -k https://hss.example.com:8443/api/subscriber/imsi/[IMSI]
   ```

2. Verificar se o campo `enabled` é `true`

Solução:

- Habilitar assinante:

  ```
  curl -k -X PUT https://hss.example.com:8443/api/subscriber/[ID]
  \
    -H "Content-Type: application/json" \
  ```

```
  -d '{"subscriber": {"enabled": true}}'
```

Causa 4: Perfil EPC Ausente

Sintomas:

- Consulta de assinante bem-sucedida, mas autenticação falha
- Erro: "Nenhum perfil EPC atribuído"

Passos de Diagnóstico:

1. Verificar o campo `epc_profile_id` do assinante
2. Verificar se o perfil EPC existe:

```
curl -k https://hss.example.com:8443/api/epc/
profile/[PROFILE_ID]
```

Solução:

- Atribuir um perfil EPC válido ao assinante

Fluxograma de Solução de Problemas de Autenticação

Problemas de Conectividade do Diameter

Sintomas

- Pares Diameter mostrando como desconectados no Painel de Controle
- Erros "Sem rota para o host"
- Serviços falhando para todos os assinantes

Causas Comuns e Soluções

Causa 1: Conectividade de Rede

Sintomas:

- Par nunca se conecta
- Erros de tempo limite de conexão
- Ping falha para o par

Passos de Diagnóstico:

1. Verificar conectividade de rede do OmniHSS para o par:

```
ping [PEER_IP]
```

2. Verificar se a porta Diameter é acessível:

   ```
   telnet [PEER_IP] 3868
   ```

3. Verificar se as regras do firewall permitem tráfego Diameter (porta 3868)

Solução:

- Corrigir roteamento de rede
- Atualizar regras do firewall
- Verificar se o par está em execução e ouvindo

Causa 2: Configuração Diameter Incorreta

Sintomas:

- Tentativas de conexão falham
- Troca CER/CEA falha
- Par rejeita conexão

Passos de Diagnóstico:

1. Revisar configuração Diameter em runtime.exs:
   - Verificar se origin_host do par corresponde ao valor esperado
   - Verificar configuração origin_realm
   - Verificar se o endereço IP do par está correto
2. Verificar logs para erros CER/CEA
3. Verificar se a configuração do par espera o origin_host do OmniHSS

Solução:

- Atualizar runtime.exs com a configuração Diameter correta
- Reiniciar o OmniHSS após a alteração de configuração
- Coordenar com o administrador do par para verificar as configurações

Causa 3: Problemas de Certificado (TLS Diameter)

Sintomas:

- Conexão falha durante a negociação TLS
- Erros de validação de certificado
- Erros "Certificado expirado" ou "Certificado inválido"

Passos de Diagnóstico:

1. Verificar se os arquivos de certificado existem em `priv/cert/`
2. Verificar a expiração do certificado:

   ```
   openssl x509 -in priv/cert/diameter.crt -noout -dates
   ```

3. Verificar se a cadeia de certificados está completa
4. Verificar o certificado do par se TLS mútuo

Solução:

- Renovar certificados expirados
- Instalar a cadeia de certificados correta
- Atualizar arquivos de certificado e reiniciar o OmniHSS

Causa 4: Incompatibilidade de Suporte de Aplicação do Par

Sintomas:

- Par se conecta, mas não suporta aplicativos necessários
- Troca de capacidades é bem-sucedida, mas operações falham
- Erros "Aplicação não suportada"

Passos de Diagnóstico:

1. Verificar a página Diameter do Painel de Controle para aplicativos do par
2. Verificar se o par suporta o aplicativo necessário (S6a, Cx, Sh, etc.)
3. Revisar troca CER/CEA nos logs

Solução:

- Verificar se a configuração do par inclui os aplicativos Diameter necessários
- Verificar se o tipo de par corresponde à funcionalidade esperada:
  - MME deve suportar S6a (16777251)
  - S-CSCF deve suportar Cx (16777216)
  - P-GW deve suportar Gx (16777238)

Fluxograma de Solução de Problemas do Diameter

Problemas de Banco de Dados

Sintomas

- API retorna erros 500

- Painel de Controle falha ao carregar
- Erros "Falha na conexão com o banco de dados"
- Desempenho de consulta lento

Causas Comuns e Soluções

Causa 1: Servidor de Banco de Dados Offline

Sintomas:

- Todas as chamadas de API falham
- Painel de Controle mostra erro
- Erros "Conexão recusada"

Passos de Diagnóstico:

1. Testar conectividade com o banco de dados:

   ```
   # Se estiver usando PostgreSQL
   psql -h [DB_HOST] -U [DB_USER] -d [DB_NAME]

   # Se estiver usando MySQL
   mysql -h [DB_HOST] -u [DB_USER] -p [DB_NAME]
   ```

2. Verificar status do serviço de banco de dados no servidor de banco de dados

3. Verificar conectividade de rede com o servidor de banco de dados

Solução:

- Iniciar o serviço de banco de dados
- Corrigir problemas no servidor de banco de dados
- Verificar roteamento de rede para o servidor de banco de dados

Causa 2: Credenciais de Banco de Dados Incorretas

Sintomas:

- Erros "Autenticação falhou"
- OmniHSS não consegue conectar na inicialização

Passos de Diagnóstico:

1. Revisar configuração do banco de dados em runtime.exs
2. Testar credenciais manualmente com cliente de banco de dados
3. Verificar permissões do usuário do banco de dados

Solução:

- Atualizar configuração do banco de dados em runtime.exs
- Conceder permissões corretas ao usuário do banco de dados
- Reiniciar o OmniHSS após a alteração de configuração

Causa 3: Pool de Conexões Exaurido

Sintomas:

- Erros 500 intermitentes
- Erros "Sem conexões disponíveis"
- Períodos de alta carga acionam falhas

Passos de Diagnóstico:

1. Verificar contagem atual de conexões no banco de dados
2. Revisar tamanho do pool de banco de dados em runtime.exs
3. Monitorar uso de conexões durante carga máxima

Solução:

- Aumentar o tamanho do pool na configuração de runtime.exs
- Investigar vazamentos de conexão se o pool se exaurir repetidamente
- Considerar escalonamento do banco de dados se a carga for consistentemente alta

Causa 4: Consultas Lentas

Sintomas:

- Respostas da API muito lentas
- Timeouts em consultas de assinantes
- CPU do banco de dados alta

Passos de Diagnóstico:

1. Consultar banco de dados para log de consultas lentas
2. Identificar consultas específicas lentas
3. Verificar se faltam índices
4. Verificar contagem de assinantes e tamanhos das tabelas

Solução:

- Otimizar consultas lentas
- Adicionar índices ausentes
- Considerar ajuste de desempenho do banco de dados
- Planejar escalonamento do banco de dados se necessário

Falhas de Registro EPC

Sintomas

- Assinante não consegue se conectar à rede LTE
- MME rejeita a conexão
- Nenhuma sessão PDN estabelecida

Causas Comuns e Soluções

Causa 1: Roaming Negado

Sintomas:

- Assinante funciona na rede doméstica, mas falha ao roaming
- Erros "Roaming não permitido"
- Funciona para algumas redes, mas não para outras

Passos de Diagnóstico:

1. Verificar `roaming_profile_id` do assinante
2. Consultar perfil de roaming e regras
3. Verificar MCC/MNC da rede visitada
4. Verificar se a regra de roaming existe para essa rede

Solução:

- Adicionar regra de roaming para MCC/MNC da rede visitada
- Ou atualizar a ação padrão do perfil de roaming para permitir
- Ver Documentação de Roaming para configuração

Causa 2: Configuração APN Ausente

Sintomas:

- Conexão bem-sucedida, mas sessão PDN falha
- Erros "APN desconhecido" do MME
- Assinante não consegue obter conexão de dados

Passos de Diagnóstico:

1. Verificar se o perfil EPC tem perfis APN vinculados
2. Verificar se o identificador APN corresponde ao que o dispositivo solicita
3. Consultar configuração do perfil APN

Solução:

- Vincular perfis APN ao perfil EPC do assinante
- Garantir que o nome APN corresponda à configuração do dispositivo
- Verificar se o perfil de QoS do APN existe

Causa 3: MME Não Conectado

Sintomas:

- Todos os assinantes falham ao se conectar
- Sem comunicação com o MME
- Par Diameter offline

Passos de Diagnóstico:

1. Verificar a página Diameter do Painel de Controle
2. Verificar se o status do par MME está "Conectado"
3. Verificar se o MME suporta a aplicação S6a

Solução:

- Solucionar conectividade Diameter
- Verificar configuração do MME
- Contatar o administrador do MME

Causa 4: Corrupção do Estado do Assinante

Sintomas:

- Assinante aparece como conectado, mas não consegue se conectar novamente
- Estado não corresponde à realidade
- Desconexão e reconexão falham

Passos de Diagnóstico:

1. Consultar estado do assinante no banco de dados
2. Verificar se há atribuições de MME obsoletas
3. Verificar o timestamp da última atualização

Solução:

- Limpar o estado do assinante (procedimento de desconexão)
- Redefinir o MME em serviço no estado do assinante
- Pode exigir ciclo de energia do assinante

Falhas de Registro IMS

Sintomas

- Assinante não consegue registrar para VoLTE
- "Falha no registro IMS" no dispositivo
- Dados funcionam, mas voz não

Causas Comuns e Soluções

Causa 1: IMS Desativado para o Assinante

Sintomas:

- Assinante tem dados, mas sem IMS
- Registro rejeitado imediatamente

Passos de Diagnóstico:

1. Consultar assinante e verificar o campo `ims_enabled`
2. Verificar se o assinante tem `ims_profile_id` atribuído

Solução:

- Habilitar IMS para o assinante
- Atribuir perfil IMS

Causa 2: S-CSCF Não Conectado

Sintomas:

- Todos os registros IMS falham
- Sem tráfego Diameter relacionado ao IMS

Passos de Diagnóstico:

1. Verificar a página Diameter do Painel de Controle
2. Verificar se o par S-CSCF está conectado
3. Verificar se o S-CSCF suporta a aplicação Cx

Solução:

- Corrigir conectividade Diameter para o S-CSCF
- Verificar configuração do S-CSCF

Causa 3: Modelo IFC Ausente ou Inválido

Sintomas:

- Registro falha durante User-Authorization-Answer
- Erros relacionados ao IFC nos logs

Passos de Diagnóstico:

1. Consultar perfil IMS do assinante
2. Verificar se o modelo IFC está presente
3. Verificar a sintaxe XML do IFC

Solução:

- Atualizar perfil IMS com modelo IFC válido
- Ver Documentação de Perfis para exemplos de IFC

Causa 4: Roaming Negado para IMS

Sintomas:

- IMS funciona na rede doméstica
- Falha ao roaming
- Roaming de dados funciona, mas não IMS

Passos de Diagnóstico:

1. Verificar ação IMS do perfil de roaming
2. Verificar se as regras de roaming têm `ims_action` correto

Solução:

- Atualizar regras de roaming para permitir IMS
- Ou atualizar a ação padrão de IMS do perfil de roaming

Fluxograma de Solução de Problemas de Registro IMS

Falhas de Chamada VoLTE

Sintomas

- Registro IMS bem-sucedido, mas chamadas falham
- Áudio em uma direção
- Chamada cai imediatamente
- Erro "Chamada falhou" no dispositivo

Causas Comuns e Soluções

Causa 1: P-CSCF Não Conectado

Sintomas:

- Registro funciona, mas chamadas falham
- Autorização de mídia falha

Passos de Diagnóstico:

1. Verificar a página Diameter do Painel de Controle
2. Verificar se o par P-CSCF está conectado
3. Verificar se o P-CSCF suporta a aplicação Rx (função PCRF do OmniHSS)

Solução:

- Corrigir conectividade Diameter para o P-CSCF
- Verificar configuração do P-CSCF que aponta para o OmniHSS para Rx

Causa 2: Autorização de Mídia Ausente

Sintomas:

- Configuração de chamada começa, mas falha
- Troca AAR/AAA falha
- Erros na interface Rx

Passos de Diagnóstico:

1. Verificar logs para mensagens Diameter Rx
2. Verificar se AAR (AA-Request) foi recebido
3. Verificar resposta AAA (AA-Answer)

Solução:

- Verificar se o P-CSCF está enviando AAR para autorização de mídia
- Verificar configuração da aplicação Rx do OmniHSS
- Verificar se o assinante tem registro IMS ativo

Causa 3: Problemas de QoS/Bearer

Sintomas:

- Chamada conecta, mas sem áudio
- Áudio em uma direção
- Problemas de qualidade

Passos de Diagnóstico:

1. Verificar perfil QoS do APN para APN de voz
2. Verificar se QCI está configurado corretamente (tipicamente QCI 1 para voz)
3. Verificar se o P-GW está conectado para Gx (função PCRF)

Solução:

- Verificar perfil QoS do APN para APN IMS
- Garantir que QCI 1 esteja configurado para bearer de voz
- Corrigir conectividade Diameter para o P-GW, se necessário

Fluxograma de Solução de Problemas de Chamada VoLTE

Problemas de Roaming

Sintomas

- Assinante funciona em casa, mas não quando está em roaming
- Algumas redes de roaming funcionam, outras não
- Roaming de dados funciona, mas não voz (ou vice-versa)

Causas Comuns e Soluções

Causa 1: Nenhum Perfil de Roaming Atribuído

Sintomas:

- Roaming falha para o assinante
- Outros assinantes rodam com sucesso

Passos de Diagnóstico:

1. Consultar `roaming_profile_id` do assinante
2. Verificar se o campo é nulo

Solução:

- Atribuir perfil de roaming ao assinante

Causa 2: Roaming Negado pela Política

Sintomas:

- Roaming falha consistentemente em rede específica

- Erro indica rejeição da política

Passos de Diagnóstico:

1. Identificar MCC/MNC da rede visitada a partir do dispositivo do assinante ou MME
2. Consultar perfil de roaming do assinante
3. Verificar regras de roaming para MCC/MNC correspondente
4. Verificar ação padrão do perfil

Solução:

- Adicionar regra de roaming para permitir a rede visitada:

```
curl -k -X POST https://hss.example.com:8443/api/roaming/rule \
  -H "Content-Type: application/json" \
  -d '{
    "roaming_rule": {
      "name": "Permitir Rede Visitada",
      "mcc": "310",
      "mnc": "410",
      "data_action": 0,
      "ims_action": 0
    }
  }'
```

Causa 3: Dados Permitidos, mas IMS Negado

Sintomas:

- Roaming de dados funciona
- Roaming de voz/IMS falha
- Disponibilidade de serviço dividida

Passos de Diagnóstico:

1. Consultar regras de roaming para a rede visitada
2. Verificar valores de `data_action` vs `ims_action`
3. Verificar ações padrão do perfil de roaming

Solução:

- Atualizar regra de roaming para permitir IMS:
  - Definir `ims_action: 0` para permitir
- Ou atualizar `ims_action_if_no_rules_match` do perfil

Ver Documentação de Roaming para configuração detalhada.

Problemas de EIR

Sintomas

- Dispositivos bloqueados inesperadamente
- Dispositivos roubados não bloqueados
- Verificação EIR falhando

Causas Comuns e Soluções

Causa 1: Regex IMEI Incorreto

Sintomas:

- Dispositivos errados bloqueados/permitidos
- Regra corresponde incorretamente

Passos de Diagnóstico:

1. Consultar regras EIR
2. Identificar qual regra está correspondendo
3. Testar padrão regex contra IMEI real
4. Verificar prioridade/ordem da regra

Solução:

- Atualizar regra EIR com regex correto
- Testar regex minuciosamente antes de aplicar
- Considerar ordem da regra (primeira correspondência vence)

Causa 2: MME Não Enviando Solicitações S13

Sintomas:

- Verificação EIR nunca acontece
- Todos os dispositivos permitidos independentemente das regras

Passos de Diagnóstico:

1. Verificar se o MME está configurado para usar a interface S13
2. Verificar se o par Diameter do MME está conectado
3. Verificar suporte à aplicação S13
4. Revisar configuração do MME

Solução:

- Configurar MME para realizar verificações EIR via S13

- Verificar se o par Diameter suporta a aplicação S13 (16777252)
- Contatar o administrador do MME, se necessário

Causa 3: Sem Regra Padrão

Sintomas:

- Dispositivos que não correspondem a nenhuma regra têm comportamento inesperado

Passos de Diagnóstico:

1. Consultar todas as regras EIR
2. Verificar se existe uma regra catch-all
3. Verificar a ordenação das regras

Solução:

- Adicionar regra padrão com regex `.*` para corresponder a todos os IMEIs
- Definir ação apropriada (whitelist ou blacklist)
- Garantir que regras específicas sejam verificadas antes da catch-all

---

Problemas de Desempenho

Sintomas

- Respostas lentas da API
- Timeouts de solicitação Diameter
- Alto uso de CPU ou memória
- Painel de Controle lento para carregar

Causas Comuns e Soluções

Causa 1: Alta Carga no Banco de Dados

Sintomas:

- Todas as operações lentas
- CPU do banco de dados alta
- Timeouts de consulta

Passos de Diagnóstico:

1. Verificar uso de recursos do servidor de banco de dados
2. Identificar consultas lentas
3. Verificar se faltam índices

4. Monitorar padrões de consulta

Solução:

- Otimizar consultas lentas
- Adicionar índices ao banco de dados
- Aumentar recursos do banco de dados
- Considerar escalonamento do banco de dados
- Ver Problemas de Banco de Dados

Causa 2: Alto Número de Assinantes

Sintomas:

- Desempenho degradado ao longo do tempo
- Lerdeza correlacionada com o crescimento do assinante
- Operações de lista especialmente lentas

Passos de Diagnóstico:

1. Consultar contagem total de assinantes
2. Verificar tamanhos das tabelas
3. Revisar planos de execução de consultas
4. Monitorar tendências de uso de recursos

Solução:

- Planejar atualização de capacidade
- Otimizar consultas para grandes conjuntos de dados
- Considerar paginação para grandes resultados
- Implementar cache, se necessário

Causa 3: Problemas com Pares Diameter

Sintomas:

- Operações Diameter lentas
- Timeouts em par específico
- Alguns pares rápidos, outros lentos

Passos de Diagnóstico:

1. Verificar a página Diameter do Painel de Controle
2. Identificar par lento
3. Testar latência de rede para o par
4. Verificar uso de recursos do par

Solução:

- Investigar problemas de desempenho do par
- Verificar caminho de rede para congestionamento
- Considerar adicionar pares redundantes
- Aumentar tempo limite Diameter, se necessário

Causa 4: Problemas de Memória

Sintomas:

- Uso de memória do OmniHSS alto
- Erros de falta de mem��ria
- Desempenho degrada ao longo do tempo

Passos de Diagnóstico:

1. Verificar uso de memória do OmniHSS na página de Aplicação
2. Monitorar tendência de memória
3. Verificar se há vazamentos de memória
4. Revisar configurações da VM Erlang

Solução:

- Reiniciar o OmniHSS para limpar condição temporária
- Investigar vazamento de memória se o uso crescer continuamente
- Ajustar configurações de memória da VM Erlang em runtime.exs
- Planejar atualização de hardware se consistentemente alto

Problemas de Estado do Assinante

Sintomas

- Assinante aparece como conectado, mas não está
- Informações de estado obsoletas
- Informações de localização incorretas
- Não consegue desconectar o assinante

Causas Comuns e Soluções

Causa 1: Queda/Reinício do MME

Sintomas:

- Assinante mostra MME em serviço que não está mais servindo
- Assinante não consegue se conectar após reinício do MME
- Estado está obsoleto

Passos de Diagnóstico:

1. Verificar estado do assinante para MME em serviço
2. Verificar se o MME reiniciou
3. Verificar o último horário de conexão do MME

Solução:

- Aguardar o assinante se conectar novamente (o estado será atualizado)
- Ou limpar manualmente o estado do assinante
- O MME deve enviar Cancel-Location no reinício

Causa 2: Desconexão de Rede Não Recebida

Sintomas:

- Assinante desligado, mas aparece como conectado
- Sessões PDN permanecem no banco de dados
- Localização não é limpa

Passos de Diagnóstico:

1. Verificar timestamp last_seen do assinante
2. Verificar se o estado é antigo (horas ou dias)
3. Verificar se o dispositivo do assinante é acessível

Solução:

- O estado será limpo quando o assinante se conectar novamente
- Ou aguardar o timeout do estado (se implementado)
- Limpeza manual pode ser necessária para estado muito obsoleto

Causa 3: Corrupção do Banco de Dados

Sintomas:

- Estado inconsistente entre tabelas
- Violações de chave estrangeira
- Estado não faz sentido

Passos de Diagnóstico:

1. Consultar estado do assinante diretamente do banco de dados
2. Verificar registros órfãos
3. Verificar integridade referencial

Solução:

- Identificar e corrigir dados inconsistentes
- Pode exigir limpeza manual do banco de dados
- Contatar suporte se a corrupção for generalizada

Problemas de API

Sintomas

- API retorna erros
- Respostas lentas da API
- Não é possível criar/atualizar entidades
- Erros 500

Causas Comuns e Soluções

Causa 1: Dados de Solicitação Inválidos

Sintomas:

- Erros 400 ou 422
- Mensagens de erro de validação
- Campo rejeitado

Passos de Diagnóstico:

1. Revisar resposta de erro para erros de campo específicos
2. Verificar formato da solicitação da API
3. Verificar se os campos obrigatórios estão presentes
4. Verificar tipos de dados

Solução:

- Corrigir dados da solicitação para corresponder à referência da API
- Garantir que todos os campos obrigatórios estejam incluídos
- Verificar se referências de chave estrangeira existem (IDs de perfil, etc.)

Causa 2: Restrição de Chave Estrangeira

Sintomas:

- Não é possível criar assinante
- Erro: "key_set_id não existe"
- Entidade referenciada não encontrada

Passos de Diagnóstico:

1. Identificar qual chave estrangeira está falhando
2. Verificar se a entidade referenciada existe:
    - key_set_id → conjuntos de chaves
    - epc_profile_id → perfis EPC
    - ims_profile_id → perfis IMS

Solução:

- Criar a entidade referenciada primeiro
- Ou usar o ID da entidade existente
- Seguir fluxo de provisionamento completo

Causa 3: Conectividade com o Banco de Dados

Sintomas:

- Erros 500
- Todas as chamadas de API falham
- Erros de conexão com o banco de dados

Solução:

- Ver Problemas de Banco de Dados

Ferramentas e Comandos de Diagnóstico

Verificações Rápidas do Painel de Controle

1. **Visão Geral do Sistema**
    - URL: `https://[hostname]:7443/overview`
    - Verificar: Contagens de assinantes, sessões ativas, status do sistema
2. **Status do Diameter**
    - URL: `https://[hostname]:7443/diameter`
    - Verificar: Todos os pares críticos conectados
3. **Saúde da Aplicação**
    - URL: `https://[hostname]:7443/application`
    - Verificar: Uso de memória, contagem de processos, tempo de atividade

Comandos de Diagnóstico da API

Verificar Saúde do Sistema:

```
curl -k https://hss.example.com:8443/api/status
```

Consultar Assinante:

```
# Por IMSI
curl -k https://hss.example.com:8443/api/subscriber/imsi/
001001123456789

# Por MSISDN
curl -k https://hss.example.com:8443/api/subscriber/msisdn/
14155551234

# Por ID
curl -k https://hss.example.com:8443/api/subscriber/1
```

Listar Todos os Assinantes:

```
curl -k https://hss.example.com:8443/api/subscriber
```

Verificar Configuração do Perfil:

```
# Perfil EPC
curl -k https://hss.example.com:8443/api/epc/profile/1

# Perfil IMS
curl -k https://hss.example.com:8443/api/ims/profile/1

# Perfil de Roaming
curl -k https://hss.example.com:8443/api/roaming/profile/1
```

Comandos de Diagnóstico de Rede

Testar Conectividade da Porta Diameter:

```
telnet [PEER_IP] 3868
```

Verificar Certificado TLS:

```
openssl s_client -connect [hostname]:8443 -showcerts
```

Testar Conectividade com o Banco de Dados:

```
# PostgreSQL
psql -h [DB_HOST] -U [DB_USER] -d [DB_NAME] -c "SELECT COUNT(*) FROM
```

```
subscriber;"

# MySQL
mysql -h [DB_HOST] -u [DB_USER] -p -e "SELECT COUNT(*) FROM
subscriber;" [DB_NAME]
```

Análise de Logs

Pesquisar Logs para IMSI Específico:

```
grep "001001123456789" /var/log/omnihss/omnihss.log
```

Encontrar Falhas de Autenticação:

```
grep "authentication.*fail" /var/log/omnihss/omnihss.log
```

Verificar Eventos do Par Diameter:

```
grep "Diameter peer" /var/log/omnihss/omnihss.log
```

Encontrar Erros de Banco de Dados:

```
grep -i "database.*error" /var/log/omnihss/omnihss.log
```

Diretrizes de Escalonamento

Quando Escalonar

Escalone para suporte de engenharia/vendedor quando:

1. **Falhas em todo o sistema** que não podem ser resolvidas com procedimentos documentados
2. **Corrupção de dados** ou estado inconsistente do banco de dados
3. **Suspeitas de bugs de software** ou comportamento inesperado
4. **Problemas de desempenho** que não podem ser resolvidos com ajustes
5. **Incidentes de segurança** ou acesso não autorizado
6. **Questões sobre comportamento não documentado**

Informações a Fornecer

Ao escalonar, inclua:

1. **Sintomas detalhados** - O que está falhando, quando, para quem
2. **Passos tomados** - O que você já fez de solução de problemas
3. **Logs** - Trechos de log relevantes mostrando o problema
4. **Configuração** - Porções relevantes de runtime.exs (redigir dados sensíveis)

5. **Ambiente** - Versão do OmniHSS, versão do banco de dados, versão do SO
6. **Impacto** - Quantos assinantes afetados, impacto nos negócios
7. **Exemplos de Assinantes** - IMSIs específicos mostrando o problema

Crítico vs Não Crítico

Problemas Críticos (Escalonar Imediatamente):

- Sistema completamente fora do ar
- Todos os assinantes incapazes de se conectar
- Corrupção de banco de dados
- Violação de segurança

Problemas Não Críticos (Documentar e Escalonar Durante o Horário Comercial):

- Problemas de assinante único que podem ser contornados
- Degradação de desempenho que é gerenciável
- Solicitações de melhoria
- Questões de documentação

Referência de Mensagens de Erro Comuns

Erros de Autenticação

Mensagem de Erro	Causa	Solução
"Falha na geração de vetores de autenticação"	Conjunto de chaves ausente ou inválido	Verificar configuração do conjunto de chaves
"Falha de sincronização SQN"	SQN fora de sincronia	Aguardar re-sincronização
"Assinante não encontrado"	IMSI inválido	Verificar IMSI, provisionar assinante
"Assinante desativado"	enabled=false	Habilitar assinante

Erros de Diameter

Mensagem de Erro	Causa	Solução
"Timeout de conexão do par Diameter"	Problema de rede	Verificar conectividade de rede
"Troca CER/CEA falhou"	Incompatibilidade de configuração	Verificar configuração Diameter
"Aplicação não suportada"	Par não suporta aplicativo necessário	Verificar aplicativos do par
"Falha na negociação TLS"	Problema de certificado	Verificar certificados

Erros de Banco de Dados

Mensagem de Erro	Causa	Solução
"Conexão recusada"	Banco de dados offline	Iniciar banco de dados
"Autenticação falhou"	Credenciais erradas	Corrigir credenciais
"Sem conexões disponíveis"	Pool exaurido	Aumentar tamanho do pool
"Timeout de consulta"	Consulta lenta	Otimizar consultas

Erros de API

Mensagem de Erro	Causa	Solução
"key_set_id não existe"	Chave estrangeira inválida	Criar conjunto de chaves primeiro
"IMSI já foi utilizado"	IMSI duplicado	Usar IMSI diferente ou excluir existente
"Erro de validação"	Entrada inválida	Verificar formato e requisitos do campo

---

← Voltar ao Guia de Operações | Próximo: Referência da API →

Integração de Webhook do OmniHSS

← Voltar ao Guia de Operações

Índice

Visão Geral

OmniHSS suporta **webhooks** para notificar sistemas externos sobre eventos de assinantes em tempo real. Quando eventos específicos ocorrem (como atualizações de localização, solicitações de autenticação ou registros IMS), o OmniHSS pode enviar uma solicitação HTTP POST para o seu endpoint de webhook configurado com os dados completos do perfil do assinante.

O Que São Webhooks?

Webhooks são callbacks HTTP que permitem que o OmniHSS envie notificações de eventos para sua aplicação à medida que acontecem, em vez de exigir que sua aplicação consulte a API do HSS em busca de alterações.

Principais Benefícios

- **Notificações em tempo real** - Receba atualizações instantâneas quando eventos de assinantes ocorrem
- **Dados completos do assinante** - Cada webhook inclui o perfil completo do assinante (o mesmo que `GET /api/subscriber`)
- **Automação orientada a eventos** - Acione fluxos de trabalho, análises ou provisionamento com base em eventos da rede
- **Redução de polling** - Não há necessidade de consultar continuamente a API para alterações no status do assinante
- **Flexibilidade de integração** - Conecte o OmniHSS a sistemas de cobrança, plataformas de análise ou aplicações personalizadas

Como Funcionam os Webhooks

Fluxo de Eventos

1. **Evento ocorre** - Um assinante realiza uma ação (anexação, atualização de localização, registro IMS, etc.)
2. **HSS processa o evento** - O OmniHSS lida com a solicitação/resposta Diameter normalmente
3. **Webhook acionado** - Se um webhook estiver registrado para este tipo de evento, o HSS envia um POST HTTP para seu endpoint
4. **Dados do assinante incluídos** - A carga útil do webhook contém o perfil completo do assinante em JSON
5. **Sua aplicação responde** - Seu endpoint deve retornar HTTP 200-299 para reconhecer o recebimento

Garantias de Entrega

- **Entrega de melhor esforço** - Webhooks são enviados de forma assíncrona e não bloqueiam operações de rede
- **Timeout** - Solicitações de webhook expiram após 5 segundos
- **Sem tentativas** - Se seu endpoint estiver indisponível ou retornar um erro, o webhook não será tentado novamente
- **Ordem não garantida** - Eventos podem chegar fora de ordem em alta carga

Importante: Operações de rede (autenticação, atualizações de localização, etc.) **não** dependem da entrega do webhook. Se seu endpoint de webhook estiver fora do ar, o serviço do assinante continua normalmente.

Eventos de Webhook

OmniHSS pode acionar webhooks para os seguintes eventos:

Eventos EPC/LTE

Evento	Acionador	Descrição
`update_location_request`	S6a ULR	Assinante se anexa ou realiza Atualização de Área de Rastreamento
`authentication_information_request`	S6a AIR	Rede solicita vetores de autenticação para o assinante
`purge_request`	S6a PUR	MME remove o contexto do assinante (dispositivo desligado, desanexado)
`cancel_location_answer`	S6a CLA	MME reconhece a desregistro do assinante

Eventos IMS

Evento	Acionador	Descrição
`ims_registration`	Cx SAR	Assinante se registra para serviço IMS/VoLTE
`ims_deregistration`	Cx SAR (desreg)	Assinante se desregistra do IMS
`ims_profile_request`	Sh UDR	Servidor de Aplicação solicita perfil IMS do assinante

Eventos de Política (PCRF)

Evento	Acionador	Descrição
`policy_request`	Gx CCR	P-GW solicita política para sessão de dados do assinante
`media_authorization`	Rx AAR	P-CSCF solicita autorização de mídia para chamada IMS

Eventos Multi-IMSI

Evento	Acionador	Descrição
`imsi_switch`	ULR para IMSI diferente no mesmo SIM	Dispositivo muda para IMSI diferente em SIM multi-IMSI

Carga Útil do Webhook

Formato da Solicitação

Quando um evento ocorre, o OmniHSS envia uma solicitação HTTP POST para a URL do webhook configurada:

```
POST /your-webhook-endpoint HTTP/1.1
Host: your-server.com
Content-Type: application/json
X-OmniHSS-Event: update_location_request
X-OmniHSS-Event-ID: 550e8400-e29b-41d4-a716-446655440000
X-OmniHSS-Timestamp: 2025-01-15T14:30:00Z

{
  "event": "update_location_request",
  "event_id": "550e8400-e29b-41d4-a716-446655440000",
  "timestamp": "2025-01-15T14:30:00Z",
  "subscriber": {
    "id": 1234,
    "imsi": "001001123456789",
    "enabled": true,
    "ims_enabled": true,
    "msisdns": [
```

```
      {"id": 1, "msisdn": "14155551001"},
      {"id": 2, "msisdn": "14155551002"}
    ],
    "sim": {
      "id": 5678,
      "iccid": "89911012000003204510",
      "is_esim": false
    },
    "key_set": {
      "id": 100,
      "amf": "8000"
    },
    "epc_profile": {
      "id": 1,
      "name": "Premium 100Mbps",
      "ue_ambr_dl_kbps": 100000,
      "ue_ambr_ul_kbps": 50000
    },
    "ims_profile": {
      "id": 1,
      "name": "Standard VoLTE"
    },
    "roaming_profile": {
      "id": 1,
      "name": "Roaming Internacional Permitido"
    },
    "subscriber_state": {
      "mme_host": "mme-01.example.com",
      "mme_realm": "epc.mnc001.mcc001.3gppnetwork.org",
      "visited_plmn": "001001",
      "last_update": "2025-01-15T14:30:00Z"
    },
    "custom_attributes": {
      "account_type": "premium",
      "billing_plan": "unlimited"
    }
  },
  "event_context": {
    "visited_plmn": "310410",
    "mme_host": "mme-roaming.example.com",
    "location_update_type": "initial_attach"
  }
}
```

Estrutura da Carga Útil

Campo	Tipo	Descrição
`event`	string	Tipo de evento (ex: `update_location_request`)
`event_id`	string	UUID único para esta entrega de webhook

Campo	Tipo	Descrição
`timestamp`	string	Timestamp ISO 8601 quando o evento ocorreu
`subscriber`	object	**Perfil completo do assinante** (o mesmo que `GET /api/subscriber/:id`)
`event_context`	object	Dados de contexto adicionais específicos do evento

Campos do Contexto do Evento

O objeto `event_context` contém informações específicas do evento:

Para `update_location_request`:

```
{
  "visited_plmn": "310410",
  "mme_host": "mme-roaming.example.com",
  "mme_realm": "epc.mnc410.mcc310.3gppnetwork.org",
  "location_update_type": "initial_attach"
}
```

Para `imsi_switch`:

```
{
  "previous_imsi": "001001111111111",
  "new_imsi": "310410222222222",
  "sim_id": 5678,
  "previous_mme_host": "mme-home.example.com",
  "new_mme_host": "mme-roaming.example.com"
}
```

Para `ims_registration`:

```
{
  "scscf_host": "scscf-01.ims.example.com",
  "public_identities": [
    "sip:001001123456789@ims.mnc001.mcc001.3gppnetwork.org",
    "sip:+14155551001@ims.example.com",
    "tel:+14155551001"
  ]
}
```

Cabeçalhos HTTP

Cabeçalho	Descrição	Exemplo
`Content-Type`	Sempre `application/json`	`application/json`
`X-OmniHSS-Event`	Tipo de evento	`update_location_request`
`X-OmniHSS-Event-ID`	Identificador único do evento	UUID
`X-OmniHSS-Timestamp`	Timestamp do evento	Formato ISO 8601
`User-Agent`	Versão do OmniHSS	`OmniHSS/1.0`

Configuração

Registrando Webhooks

Webhooks são configurados via API do OmniHSS.

Registrar um Webhook

```
curl -k -X POST https://hss.example.com:8443/api/webhook \
  -H "Content-Type: application/json" \
  -d '{
    "webhook": {
      "url": "https://your-server.com/omnihss-webhook",
      "events": [
        "update_location_request",
        "ims_registration",
        "imsi_switch"
      ],
      "enabled": true,
      "description": "Webhook do sistema de cobrança em produção"
    }
  }'
```

Resposta:

```
{
  "data": {
    "id": 1,
    "url": "https://your-server.com/omnihss-webhook",
    "events": [
      "update_location_request",
      "ims_registration",
      "imsi_switch"
    ],
    "enabled": true,
    "description": "Webhook do sistema de cobrança em produção",
    "created_at": "2025-01-15T14:00:00Z"
  }
}
```

Listar Webhooks

```
curl -k https://hss.example.com:8443/api/webhook
```

Atualizar Webhook

```
curl -k -X PUT https://hss.example.com:8443/api/webhook/1 \
  -H "Content-Type: application/json" \
```

```
  -d '{
    "webhook": {
      "enabled": false
    }
  }'
```

Deletar Webhook

```
curl -k -X DELETE https://hss.example.com:8443/api/webhook/1
```

Requisitos do Endpoint de Webhook

Seu endpoint de webhook deve:

1. **Aceitar solicitações POST** com `Content-Type: application/json`
2. **Responder rapidamente** - Retornar HTTP 200-299 dentro de 5 segundos
3. **Ser idempotente** - Lidar com entregas duplicadas de forma adequada
4. **Usar HTTPS** - Para segurança, use endpoints TLS/SSL (recomendado)
5. **Validar cargas úteis** - Verificar se a solicitação é do OmniHSS (veja a seção de Segurança)

Exemplo de Manipulador de Webhook (Node.js/Express):

```
const express = require('express');
const app = express();

app.post('/omnihss-webhook', express.json(), (req, res) => {
  const { event, subscriber, event_context } = req.body;

  console.log(`Evento recebido: ${event}`);
  console.log(`IMSI do assinante: ${subscriber.imsi}`);

  // Processar os dados do assinante
  // ... sua lógica de negócios aqui ...

  // Responder imediatamente para reconhecer o recebimento
  res.status(200).json({ received: true });

  // Lidar com processamento assíncrono após a resposta
  processWebhook(req.body).catch(console.error);
});

async function processWebhook(payload) {
  // Sua lógica de processamento assíncrono
  // ex: atualizar sistema de cobrança, acionar análises, etc.
}

app.listen(3000);
```

Casos de Uso

1. Cobrança em Tempo Real e Rastreamento de Uso

Rastrear o uso da rede pelo assinante e acionar eventos de cobrança em tempo real.

Benefícios:

- Detectar instantaneamente quando assinantes estão em roaming internacional
- Aplicar tarifas de roaming apropriadas em tempo real
- Rastrear horários de início/fim de sessão com precisão
- Gerar alertas de uso quando os limites são alcançados

2. Análise e Monitoramento

Enviar dados de atividade do assinante para plataformas de análise para painéis e relatórios em tempo real.

Caso de Uso: Rastrear assinantes ativos por região

```
// Manipulador de webhook enviando dados para plataforma de análise
app.post('/omnihss-webhook', async (req, res) => {
  const { event, subscriber, event_context } = req.body;

  if (event === 'update_location_request') {
    await analytics.track({
      event: 'subscriber_location_update',
      imsi: subscriber.imsi,
      visited_plmn: event_context.visited_plmn,
      timestamp: req.body.timestamp,
      profile: subscriber.epc_profile.name
    });
  }

  res.status(200).send();
});
```

Painel de Análise:

- Assinantes ativos por MME
- Assinantes em roaming por país
- Distribuição de níveis de serviço
- Taxas de sucesso de registro IMS

3. Detecção de Fraude e Segurança

Detectar padrões de atividade suspeita em tempo real e acionar respostas automatizadas.

Cenários de Detecção de Fraude:

1. **Mudanças Rápidas de Localização**
    - Assinante se anexa no País A
    - 30 minutos depois, se anexa no País B (fisicamente impossível)
    - Ação: Marcar conta, enviar alerta para equipe de segurança
2. **Abuso de Troca de IMSI**
    - Múltiplas trocas rápidas de IMSI no mesmo SIM
    - Possível clonagem de SIM ou uso não autorizado de multi-IMSI
    - Ação: Desativar todos os IMSIs no SIM, notificar equipe de fraude
3. **Roaming Não Autorizado**
    - Assinante faz roaming para país bloqueado (sanções, risco de fraude)
    - Ação: Desativar assinante automaticamente, bloquear acesso à rede

Exemplo de Implementação:

```
@app.route('/omnihss-webhook', methods=['POST'])
def webhook_handler():
    data = request.json
    subscriber = data['subscriber']
    event_context = data.get('event_context', {})

    if data['event'] == 'update_location_request':
        visited_plmn = event_context.get('visited_plmn')

        # Verificar países bloqueados
        if visited_plmn in BLOCKED_PLMNS:
            disable_subscriber(subscriber['imsi'])
            alert_security_team(subscriber, 'Roaming para PLMN
bloqueado')

        # Verificar viagem impossível
        if is_impossible_travel(subscriber['imsi'], visited_plmn):
            flag_for_review(subscriber['imsi'])
            alert_fraud_team(subscriber, 'Viagem impossível detectada')

    return jsonify({'status': 'ok'}), 200
```

4. Automação de Provisionamento

Provisionar ou atualizar automaticamente os serviços do assinante com base em eventos da rede.

Caso de Uso: Ativar IMS automaticamente quando o assinante usa VoLTE pela primeira vez

```
app.post('/omnihss-webhook', async (req, res) => {
  const { event, subscriber } = req.body;

  if (event === 'ims_registration' && !subscriber.ims_enabled) {
    // Primeiro usuário de IMS - habilitar IMS permanentemente
    await omnihss.updateSubscriber(subscriber.id, {
      ims_enabled: true,
      custom_attributes: {
        ...subscriber.custom_attributes,
        volte_activated_at: new Date().toISOString()
      }
    });

    // Atualizar CRM
    await crm.updateCustomer(subscriber.imsi, {
      features: ['volte']
    });
  }

  res.status(200).send();
});
```

5. Notificações ao Cliente

Enviar notificações em tempo real aos clientes sobre seus serviços.

Caso de Uso: Mensagem de boas-vindas quando em roaming internacional

Exemplo de Notificações:

- "Bem-vindo ao [País]! Tarifas de roaming se aplicam."
- "Você usou 80% da sua cota de dados"
- "Serviço VoLTE agora ativo em seu dispositivo"
- "Sua conta foi atualizada para Premium"

6. Gerenciamento de SIM Multi-IMSI

Rastrear e gerenciar assinantes com SIMs multi-IMSI, recebendo notificações quando trocam IMSIs.

```
app.post('/omnihss-webhook', async (req, res) => {
```

```
  const { event, subscriber, event_context } = req.body;

  if (event === 'imsi_switch') {
    const { previous_imsi, new_imsi, sim_id } = event_context;

    // Registrar troca de IMSI para análise
    await db.logImsiSwitch({
      sim_id,
      from_imsi: previous_imsi,
      to_imsi: new_imsi,
      timestamp: req.body.timestamp
    });

    // Atualizar sistema de cobrança
    await billing.endSession(previous_imsi);
    await billing.startSession(new_imsi);

    // Alertar se troca excessiva (potencial fraude)
    const switchCount = await db.getSwitchCount(sim_id, '24h');
    if (switchCount > 10) {
      await alertFraudTeam(`Troca excessiva de IMSI: SIM ${sim_id}`);
    }
  }

  res.status(200).send();
});
```

7. Integração com Sistemas Externos

Conectar o OmniHSS a sistemas de terceiros sem polling.

Exemplos de Integrações:

- **Sistemas de CRM** - Atualizar registros de clientes com uso de serviços
- **Monitoramento de Rede** - Enviar dados de assinantes para plataformas de análise de rede
- **Sistemas de Cobrança** - Acionar cobranças com base em eventos da rede
- **Sistemas de Ticketing** - Criar tickets automaticamente para falhas de autenticação
- **Armazéns de Dados** - Transmitir eventos de assinantes para análise de big data

---

Considerações de Segurança

Segredo/Assinatura do Webhook

Para verificar se os webhooks são do OmniHSS, implemente a verificação de

assinatura:

```
# Configurar webhook com segredo
curl -k -X POST https://hss.example.com:8443/api/webhook \
  -H "Content-Type: application/json" \
  -d '{
    "webhook": {
      "url": "https://your-server.com/omnihss-webhook",
      "events": ["update_location_request"],
      "secret": "sua-chave-secreta-aqui"
    }
  }'
```

O OmniHSS incluirá um cabeçalho `X-OmniHSS-Signature`:

```
X-OmniHSS-Signature:
sha256=5d7a8f9b2c1e3a4d6f7e8b9c0a1b2c3d4e5f6a7b8c9d0e1f2a3b4c5d6e7f8a9b
```

Verifique a assinatura:

```
const crypto = require('crypto');

function verifyWebhook(req) {
  const signature = req.headers['x-omnihss-signature'];
  const secret = process.env.WEBHOOK_SECRET;
  const payload = JSON.stringify(req.body);

  const expectedSignature = 'sha256=' +
    crypto.createHmac('sha256', secret)
      .update(payload)
      .digest('hex');

  return crypto.timingSafeEqual(
    Buffer.from(signature),
    Buffer.from(expectedSignature)
  );
}

app.post('/omnihss-webhook', (req, res) => {
  if (!verifyWebhook(req)) {
    return res.status(401).json({ error: 'Assinatura inválida' });
  }

  // Processar webhook...
  res.status(200).send();
});
```

Melhores Práticas

1. **Use HTTPS** - Sempre use TLS para endpoints de webhook
2. **Valide assinaturas** - Verifique assinaturas de webhook para evitar spoofing
3. **Limitação de taxa** - Implemente limitação de taxa em endpoints de webhook
4. **Lista de IPs permitidos** - Restringir acesso ao webhook a endereços IP do OmniHSS
5. **Monitore falhas** - Rastrear falhas e erros de entrega de webhook
6. **Sanitize dados** - Validar e sanitizar cargas úteis de webhook antes do processamento
7. **Credenciais seguras** - Armazenar segredos de webhook em configuração segura (variáveis de ambiente, gerenciador de segredos)

Privacidade de Dados

As cargas úteis do webhook contêm **informações sensíveis do assinante**:

- IMSI (identidade do assinante)
- MSISDNs (números de telefone)
- Dados de localização (PLMN visitado, MME)
- Informações do perfil de serviço

Requisitos de Conformidade:

- **GDPR** - Garantir que os dados do webhook sejam processados em conformidade com o GDPR
- **Retenção de dados** - Implementar políticas de retenção de dados apropriadas
- **Controle de acesso** - Restringir acesso ao endpoint de webhook
- **Criptografia** - Usar TLS para transporte de webhook
- **Registro de auditoria** - Registrar todas as entregas de webhook para conformidade

---

Solução de Problemas

Webhook Não Recebido

Sintomas:

- Eventos ocorrem, mas webhook não é acionado
- Endpoint de webhook nunca recebe solicitações

Passos de Solução de Problemas:

1. **Verifique se o webhook está habilitado:**

```
curl -k https://hss.example.com:8443/api/webhook
# Verifique "enabled": true
```

2. **Verifique a configuração dos eventos do webhook:**
   - Certifique-se de que o tipo de evento está incluído na lista de `events` do webhook
   - Exemplo: Se você deseja eventos `ims_registration`, verifique se está no array de eventos

3. **Revise os logs do HSS:**
   - Verifique se há erros de entrega de webhook
   - Procure por problemas de conectividade de rede
   - Verifique se não há falhas de resolução de DNS

4. **Teste a acessibilidade do endpoint:**

```
curl -X POST https://your-server.com/omnihss-webhook \
  -H "Content-Type: application/json" \
  -d '{"test": true}'
```

Timeout do Webhook

Sintomas:

- Logs do HSS mostram erros de timeout de webhook
- Endpoint de webhook recebe solicitação, mas HSS marca como falha

Solução:

1. **Responda imediatamente:**
   - Retorne HTTP 200 dentro de 5 segundos
   - Processar dados de forma assíncrona após responder

2. **Otimize o desempenho do endpoint:**

```
// RUIM - Processamento síncrono lento
app.post('/webhook', (req, res) => {
  processData(req.body); // Bloqueia por 10 segundos
  res.status(200).send();
});

// BOM - Processamento assíncrono após resposta
app.post('/webhook', (req, res) => {
  res.status(200).send(); // Responder imediatamente
  processData(req.body); // Processar assíncrono
});
```

Webhooks Duplicados

Sintomas:

- Mesmo evento entregue várias vezes
- `event_id` é idêntico para entregas duplicadas

Causa:

- Tentativas de rede (embora o OmniHSS não tente novamente, a infraestrutura de rede pode)
- Múltiplos webhooks registrados para o mesmo evento

Solução:

Implemente idempotência usando `event_id`:

```
const processedEvents = new Set();

app.post('/omnihss-webhook', (req, res) => {
  const eventId = req.body.event_id;

  if (processedEvents.has(eventId)) {
    // Já processado, pular
    return res.status(200).json({ status: 'duplicado' });
  }

  processedEvents.add(eventId);

  // Processar webhook...
  processWebhook(req.body);

  res.status(200).json({ status: 'processado' });
});
```

Webhook Retorna Erro

Sintomas:

- Endpoint retorna HTTP 4xx ou 5xx
- Logs do HSS falha de entrega de webhook

Erros Comuns:

1. **401 Não Autorizado** - Falha na verificação da assinatura
    - Verifique se o segredo do webhook corresponde à configuração
    - Verifique o algoritmo de cálculo da assinatura

2. **400 Solicitação Inválida** - Carga útil inválida
    - Verifique o parsing da carga útil do webhook
    - Certifique-se de que o cabeçalho Content-Type está sendo tratado
3. **500 Erro Interno do Servidor** - Endpoint falhou
    - Revise os logs de erro do endpoint
    - Adicione tratamento de erros e registro

Solução:

Adicione tratamento de erros abrangente:

```
app.post('/omnihss-webhook', async (req, res) => {
  try {
    // Verificar assinatura
    if (!verifyWebhook(req)) {
      return res.status(401).json({ error: 'Assinatura inválida' });
    }

    // Validar carga útil
    if (!req.body.event || !req.body.subscriber) {
      return res.status(400).json({ error: 'Carga útil inválida' });
    }

    // Processar webhook
    await processWebhook(req.body);

    res.status(200).json({ status: 'ok' });

  } catch (error) {
    console.error('Erro no processamento do webhook:', error);
    // Retornar 200 para evitar nova tentativa, registrar erro para
investigação
    res.status(200).json({ status: 'erro', message: error.message });
  }
});
```

Dados do Assinante Ausentes

Sintomas:

- Webhook recebido, mas objeto do assinante está incompleto
- Campos esperados estão nulos ou ausentes

Causas Possíveis:

1. **Assinante não totalmente provisionado** - Alguns perfis podem ser

opcionais (IMS, roaming)
2. **Condição de corrida de dados** - Assinante atualizado entre o acionamento do evento e o envio do webhook

Solução:

Lidar com campos opcionais de forma adequada:

```
const { subscriber } = req.body;

// Verificar campos opcionais
const imsProfile = subscriber.ims_profile || { name: 'Sem IMS' };
const roamingProfile = subscriber.roaming_profile || { name: 'Sem
Roaming' };

// Lidar com MSISDNs ausentes
const msisdns = subscriber.msisdns || [];
```

Monitoramento e Observabilidade

Métricas de Webhook

Rastrear o desempenho e a confiabilidade do webhook:

Métricas a Monitorar:

- Taxa de entrega de webhook (bem-sucedida vs. falhada)
- Latência do webhook (tempo do evento até a resposta do endpoint)
- Tempos de resposta do endpoint
- Taxas de erro por endpoint
- Eventos por segundo

Exemplo de Consulta de Painel (Prometheus/Grafana):

```
# Taxa de sucesso do webhook
rate(omnihss_webhook_success_total[5m]) /
rate(omnihss_webhook_attempts_total[5m])

# Latência do webhook
histogram_quantile(0.95, omnihss_webhook_duration_seconds)
```

Logs de Webhook

Ativar registro detalhado de webhook para solução de problemas:

Formato de Log:

```
{
```

```
  "timestamp": "2025-01-15T14:30:00Z",
  "level": "info",
  "component": "webhook",
  "event_id": "550e8400-e29b-41d4-a716-446655440000",
  "webhook_id": 1,
  "event_type": "update_location_request",
  "subscriber_imsi": "001001123456789",
  "endpoint": "https://your-server.com/omnihss-webhook",
  "http_status": 200,
  "duration_ms": 145,
  "error": null
}
```

← Voltar ao Guia de Operações | Próximo: Referência da API →