Sumérjase en la comunicación basada en el modelo D de SCP

Contenido

Introducción

Este documento describe en profundidad el enfoque de comunicación SCP Model-D entre Cisco AMF/SMF y NF de terceros.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Funcionalidad de la función de gestión de acceso y movilidad (AMF)
- Funcionalidad de la función de administración de sesiones (SMF)
- Funcionalidad del proxy de comunicación de servicio (SCP)

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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

Antecedentes

Los operadores de todo el mundo pueden elegir entre varios modelos de comunicación mediante SCP para la detección de funciones de red (NF) y las comunicaciones NF a NF posteriores. En este tema se tratan conceptos relacionados con diversos modelos de comunicación y los cambios de configuración/flujo de llamadas necesarios en Subscriber Microservices Infrastructure (SMI), AMF/SMF para disponer de una comunicación basada en el modelo D de SCP.

Descripción general de la arquitectura y la solución

En la arquitectura basada en servicios (SBA), la SCP actúa como intermediaria, facilitando la comunicación indirecta entre NF gestionando el routing, el equilibrio de carga y el descubrimiento de servicios, lo que en última instancia simplifica la arquitectura basada en servicios.

3GPP 23.501 Annex-E detalla los cuatro modelos de comunicación entre NF en una implementación 5GC.

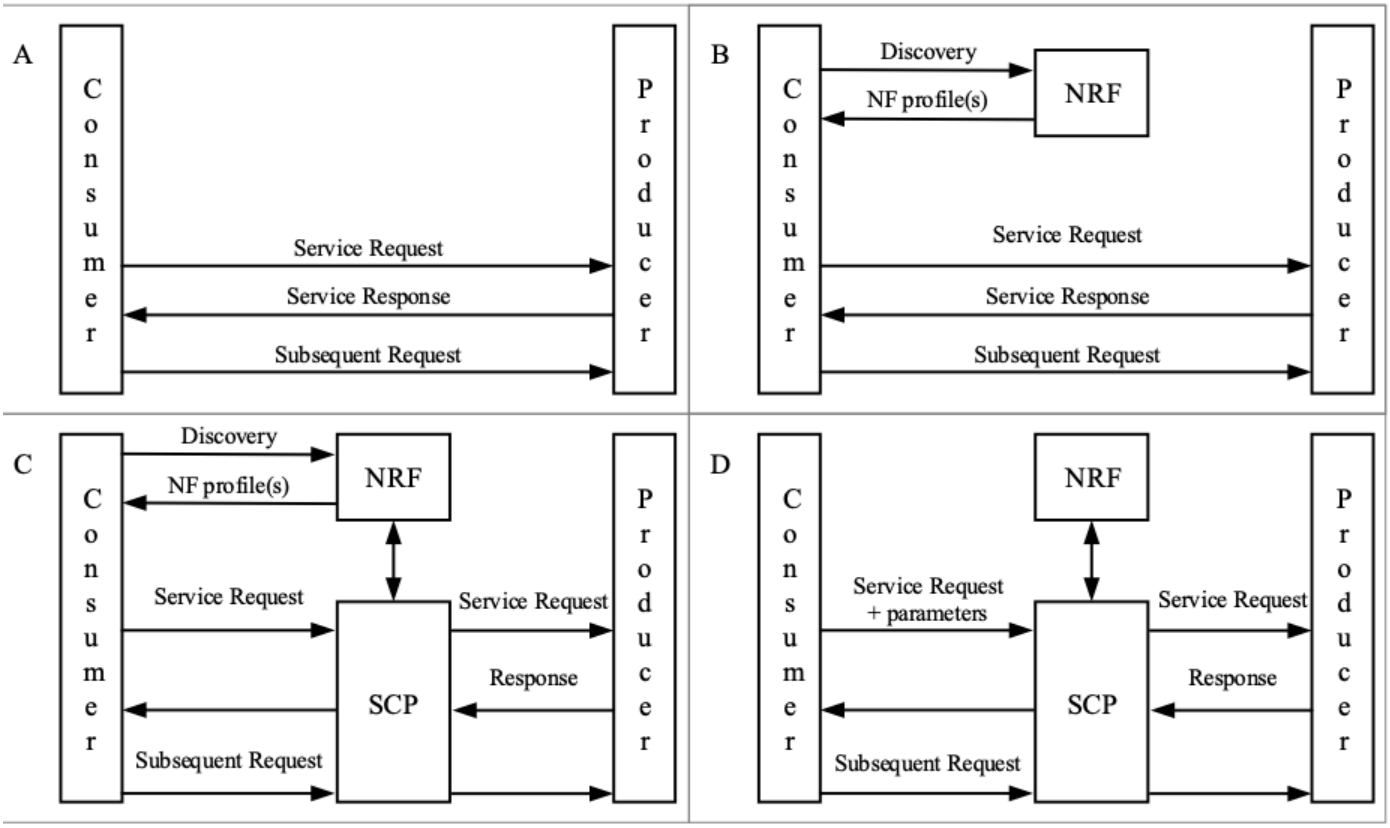


Figura A: (Diferentes modelos de comunicación que implican a SCP)

Modelo A: comunicación directa sin interacción con la función de repositorio de red (NRF): Los consumidores se configuran con los "perfiles NF" de los productores y se comunican directamente con un productor de su elección. Este es un tipo de selección estática y no se utilizan NRF ni SCP.

Modelo B: comunicación directa con interacción NRF: Los consumidores realizan la detección consultando el NRF. En función del resultado de la detección, el consumidor realiza la selección. El consumidor envía la solicitud al productor seleccionado.

Modelo C: comunicación indirecta sin detección delegada: Los consumidores lo descubren

consultando el NRF. En función del resultado de la detección, el consumidor selecciona un conjunto NF o una instancia NF específica del conjunto NF. El consumidor envía la solicitud a la SCP que contiene la dirección del productor de servicios seleccionado que apunta a una instancia de servicio de NF o a un conjunto de instancias de servicio de NF. En este último caso, la SCP elige una instancia del servicio NF. Si es posible, el SCP interactúa con el NRF para obtener parámetros de selección como la ubicación, la capacidad, etc. El SCP dirige la solicitud a la instancia del productor de servicios de NF seleccionada.

Modelo D: comunicación indirecta con detección delegada: Los consumidores no participan en la detección ni en la selección. El consumidor añade a la solicitud de servicio todos los parámetros de detección y selección necesarios para encontrar un productor adecuado. El SCP utiliza la dirección de solicitud y los parámetros de detección y selección en el mensaje de solicitud para enrutar la solicitud a una instancia de productor adecuada. El SCP puede realizar la detección con un NRF y obtener un resultado de detección.

Perspectiva en profundidad de la comunicación basada en el modelo D: Cuando se utiliza Call Model-D, el consumidor de NF no envía directamente una solicitud al NRF, sino que delega en el SCP esta detección. El cliente de NF envía un mensaje a SCP y concatenar para cada uno de estos factores de detección la cadena '3gpp-sbi-discovery' con el nombre del factor de detección que se utilizará si la detección de NF se realiza a través de NRF.

En el caso de un escenario en el que SMF busque Unified Data Management (UDM) con service-names nudm-sdm, los factores de detección se pasarán a SCP:

- Encabezado de autoridad: la autoridad lleva el nombre de dominio completamente calificado (FQDN) o la dirección IP, con prioridad dada a la configuración de la dirección IP.
- 3gpp-sbi-discovery-requester-nf-type: SMF
- 3gpp-sbi-discovery-target-nf-type: UDM
- 3gpp-Sbi-discovery-service-name: nudm-sdm

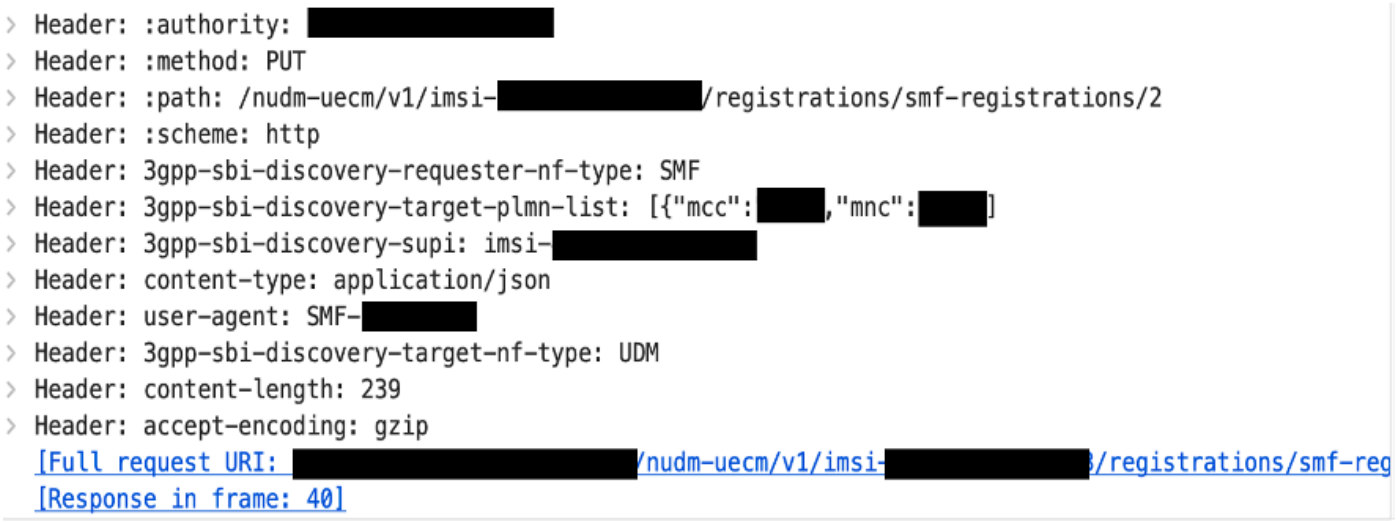
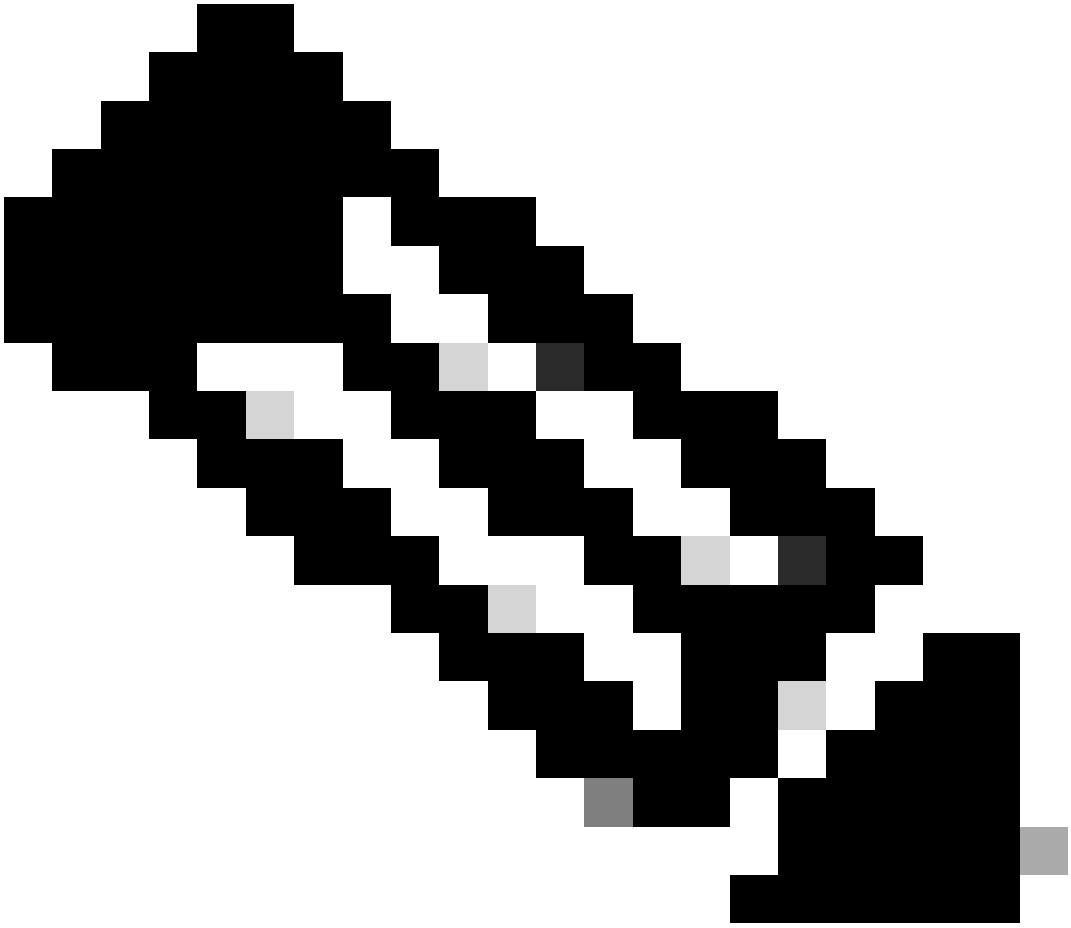


Figura B: (Comunicación SMF-UDM a través del modelo D de SCP)



Nota: El formato del nombre de 3gpp-sbi-discovery-service está en formato de cadena simple y no en formato de matriz según 3gpp 29.510 y las definiciones de API abiertas (estilo 4.7.12.4). En 29.510, 3gpp-sbi-discovery-service-name se menciona como formato de matriz.

```
- name: service-names
  in: query
  description: Names of the services offered by the NF
  schema:
    type: array
    items:
      $ref: 'TS29510_Nnrf_NFManagement.yaml#/components/schemas/ServiceName'
    minItems: 1
    uniqueItems: true
  style: form
  explode: false
```

Figura C: (Instantánea desde 29.510 espec.)

Sin embargo, style:form y explode:false convierten la matriz en una cadena sin formato que se explica tomando un ejemplo de OpenAPI.

Assume a parameter named `color` has one of the following values:

```
string -> "blue"
array -> ["blue","black","brown"]
object -> { "R": 100, "G": 200, "B": 150 }
```

The following table shows examples of rendering differences for each value.

style	explode	empty	string	array	object
matrix	false	;color	;color=blue	;color=blue,black,brown	;color=R,1(
matrix	true	;color	;color=blue	;color=blue;color=black;color=brown	;R=100;G=
label	false	.	.blue	.blue.black.brown	.R.100.G.2
label	true	.	.blue	.blue.black.brown	.R=100.G=
form	false	color=	color=blue	color=blue,black,brown	color=R,10
form	true	color=	color=blue	color=blue&color=black&color=brown	R=100&G=
simple	false	n/a	blue	blue,black,brown	R,100,G,2(
simple	true	n/a	blue	blue,black,brown	R=100,G=2
spaceDelimited	false	n/a	n/a	blue%20black%20brown	R%20100%
pipeDelimited	false	n/a	n/a	blue|black|brown	R|100|G|2(
deepObject	true	n/a	n/a	n/a	color[R]=1(

Figura D: (Instantánea de API abierta: (Ejemplos de estilo de 4.7.12.4)

Dispone de control CLI en AMF y SMF para enviar el parámetro 3gpp-sbi-discovery-service, ya que es opcional (se puede realizar en función del entorno de implementación).

En el caso del Modelo B, si toma el ejemplo de la comunicación AMF y Authentication Server Function (AUSF), una vez que se descubre AUSF, el AMF envía el POST a AUSF con AUSF IP/FQDN y el puerto.

POST http://<ausf-fqdn>:<port>/nausf-auth/v1/ue-authentications.

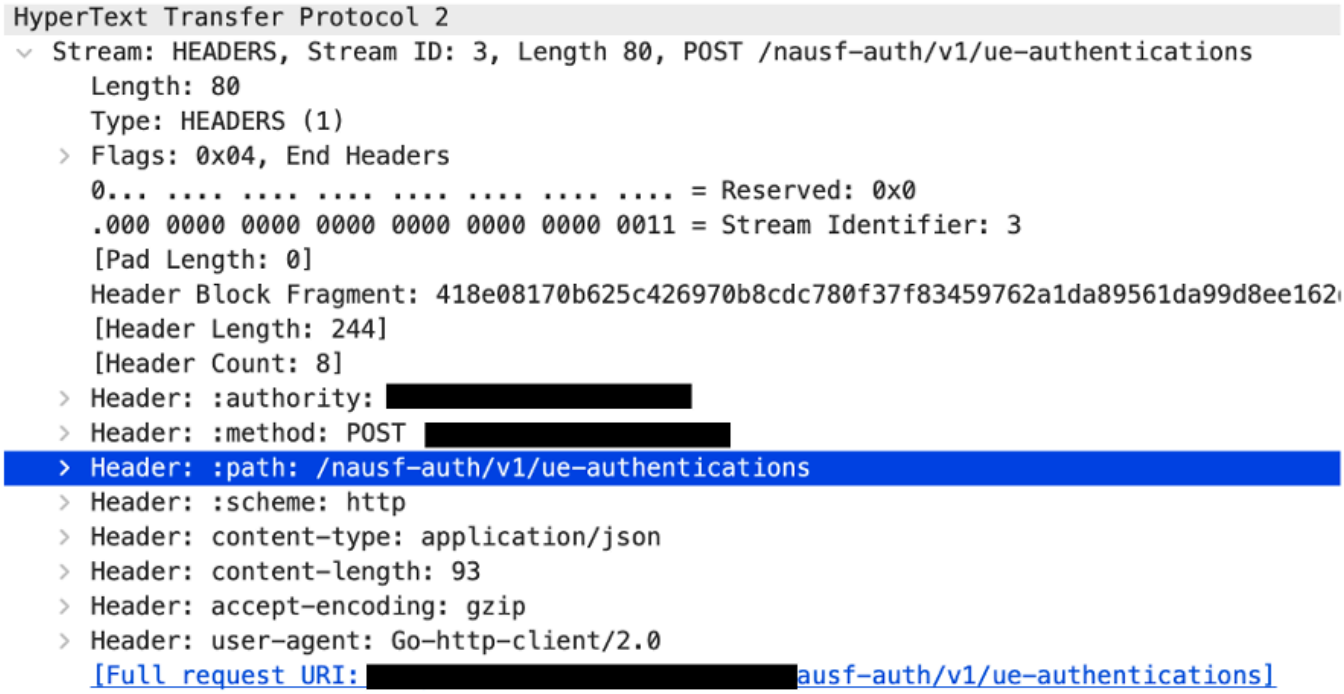


Figura E: (Comunicación AMF-AUSF a través del modelo B)

En el Modelo D, como la detección es realizada por el SCP, en lugar de POST http(s)://<ausf-fqdn>:<ausf-port>/nausf-auth/v1/ue-authentications el AMF envía la solicitud POST modificada que es:

POST http(s)://<scp-fqdn>:<scp-port>/nausf-auth/v1/ue-authentications

O bien

POST http(s)://<scp-fqdn>:<scp-port>/nscp-route/nausf-auth/v1/ue-authentications(if apiroot=nscp-route)

Con

3gpp-Sbi-Discovery-target-nf-type: AUSF

3gpp-Sbi-Discovery-Preferred-locality: LOC1

3gpp-Sbi-Discovery-service-name

Donde puede ver que AMF ha reemplazado la api-root (<ausf-fqdn>:<ausf-port>) del AUSF con la api-root del SCP.

```
> Header: :authority: [redacted]
> Header: :method: POST
> Header: :path: /nscp-route/nausf-auth/v1/ue-authentications
> Header: :scheme: http
> Header: 3gpp-sbi-discovery-service-names: ["nausf-auth"]
> Header: 3gpp-sbi-discovery-target-nf-type: AUSF
> Header: 3gpp-sbi-discovery-requester-nf-type: AMF
> Header: user-agent: AMF-SLICE-EMBB
> Header: 3gpp-sbi-discovery-target-plmn-list: [{"mcc":[redacted],"mnc":[redacted]]
> Header: content-type: application/json
> Header: content-length: 183
> Header: accept-encoding: gzip
  [Full request URI: http://[redacted]/nscp-route/nausf-auth/v1/ue-authentications]
```

Figura F: (Comunicación AMF-AUSF a través del modelo D de SCP)

Los parámetros 3gpp-sbi-discovery permiten que el SCP recupere el mejor NF y luego reenvíe la solicitud POST donde reemplaza la api-root del SCP por la api-root recibida del NRF después de haber recibido la respuesta a su solicitud de detección.

Configuraciones necesarias en AMF/SMF

Para indicar para cada NF (por ejemplo, UDM) qué modelo de llamada se debe utilizar, la configuración del modelo de selección de nf se utiliza dentro del 'elemento de red de perfil' asociado.

<#root>

profile network-element udm prf-udm-scp

[...]

nf-selection-model priority <>[local | nrf-query | nrf-query-peer-input | nrf-query-and-scp | scp]

exit

Una vez que se elige el Model-D, los parámetros de consulta configurados para el elemento de red asociado se siguen utilizando y se pasan al SCP en el formato '3gpp-Sbi-Discovery-<query-

param>'.

<#root>

```
[smf] smf(config)# profile network-element udm prf-udm-scp


[smf] smf(config-udm-udm1)# query-params


Possible completions:


 [  chf-supported-plmn  dnn  requester-snssais  tai  target-nf-instance-id  target-plmn ]
```

Finalmente, el elemento de red del perfil se asigna al nombre de red de datos (dnn) del perfil.

<#root>

```
profile dnn ims


 network-element-profiles udm prf-udm-scp


 network-element-profiles scp prf-scp


exit
```

Las SCP se definen como elemento de red.

nf-client-profile y un perfil de control de errores se asignan con network-element.

<#root>

```
profile network-element scp <>
```

```
 nf-client-profile        <>

 failure-handling-profile <>

exit
```

El nf-client-profile del tipo scp-profile detalla las características del punto final SCP.

Aquí nscp-route se puede agregar en api-root.

<#root>

```
profile nf-client nf-type scp

 scp-profile <>

  locality LOC1

   priority 30

   service name type <>

    responsetimeout 4000

    endpoint-profile EP1

     capacity   30
```

```
     api-root   nscp-route

     priority   10

     uri-scheme http

     endpoint-name scp-customer.com

      priority 10

      capacity 50

      primary ip-address ipv4

      primary ip-address port

      fqdn name <>

      fqdn port <>


exit
```

El FQDN de SMF se configura en la interfaz descendente (SBI) del terminal.

<#root>

```
endpoint sbi
```

relicas 2

nodes 2

fqdn <>

Ejemplo de un paquete

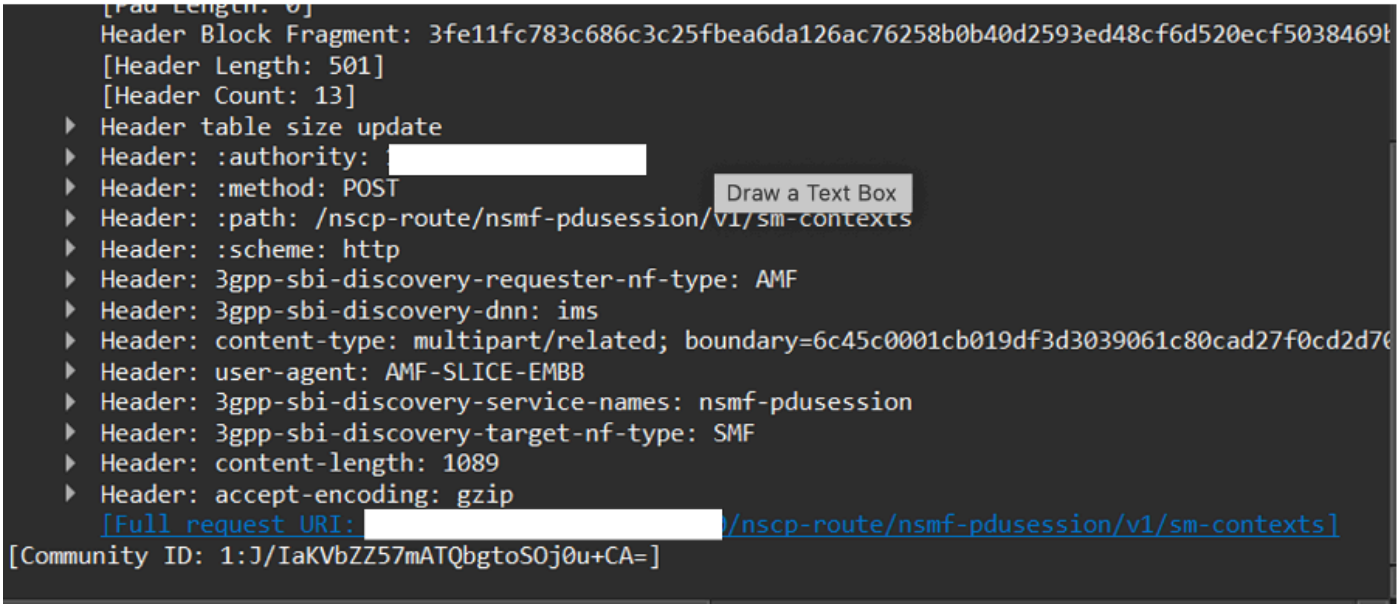


Figura G: (comunicación AMF-SMF nsmf-pdusession a través del modelo D de SCP)

Necesita del dnn de perfil hacer referencia al elemento de red SCP recién configurado.

<#root>

profile dnn <>

network-element-profiles udm <>

network-element-profiles scp <>

exit

Si la gestión de fallos de SCP se configura con la acción de reintento, SMF intenta alternar SCP en función de la configuración de SCP y del número de reintentos.

Si la gestión de fallos de SCP se configura con la acción de reintentar y fallar para un nombre de servicio y tipo de mensaje determinados, se produce la reincidencia en el modelo A.

Este perfil de control de errores para SCP (FHSCP) se utiliza si el error se desencadena desde SCP (el encabezado del servidor indica SCP) y está presente la configuración del cliente NF para el par.

<#root>

```
profile nf-client-failure nf-type scp


   profile failure-handling <>


   service name type npcf-smpolicycontrol


    responsetimeout 1800


    message type PcfSmpolicycontrolCreate


    status-code httpv2 0,307,429,500,503-504


     retry  1


     action retry-and-fallback


     exit
```

Ejemplo del perfil de cliente de nf para la función de control de políticas (PCF) para el escenario

en el que se configura el reintento de acción y la reserva para el tipo de mensaje PcfSmpolicycontrolCreate:

<#root>

```
profile nf-client nf-type pcf


 pcf-profile <>


  locality LOC1


   priority 1


   service name type npcf-smpolicycontrol


    endpoint-profile epprof


     capacity   10


     priority   1


     uri-scheme http


     endpoint-name ep1


      priority 1


      capacity 10


      primary ip-address ipv4 <>
```

```
 primary ip-address port <>

exit

endpoint-name ep2

 priority 1

 capacity 10

 primary ip-address ipv4 <>

 primary ip-address port <>

exit
```

POD de DNS de núcleo y configuración requerida en la capa SMI

Los grupos de dispositivos CoreDNS, que forman parte del espacio de nombres del sistema Kube, se implementan como un conjunto de réplicas de 2 grupos. Estos grupos de dispositivos se pueden programar en cualquiera de los dos nodos maestro/de control y no dependen de dónde esté configurada la IP del servidor de nombres en el administrador de clústeres.

Sin embargo, se recomienda configurar la IP del servidor de nombres en todos los nodos de control/maestro ya que no tiene un control de etiquetado para girar los grupos de dispositivos CoreDNS según su deseo. Si la ruta a los servidores de nombres no está presente en ninguno de los servidores maestros donde se implementa CoreDNS, la sincronización del clúster SMF/AMF falla.

Actualmente, CoreDNS reenvía las solicitudes DNS al servidor de nombres especificado en el archivo resolv.conf de los nodos.

'kubectl edit configmap coredns -n kube-system' tiene:

<#root>

```
 {


forward ./etc/resolv.conf{


     max_concurrent 1000


  }
```

Al verificar /etc/resolv.conf en el nodo maestro donde se inicia el servicio, debe contener:

<#root>

```
 name server <>


     name server <>
```

Ejemplo de configuración del servidor de nombres en el nodo maestro/de control:

<#root>

```
nodes <>


initial-boot netplan vlans <>


dhcp4 false
```

dhcp6 false

addresses [<>]

nameserver addresses [<>]

id <>

link <>

exit

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

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

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