Detaillierte SCP-D-basierte Kommunikation

Inhalt

Einleitung

Dieses Dokument beschreibt die SCP Model-D-Kommunikationsstrategie zwischen Cisco AMF/SMF und Drittanbieter-NF.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Funktionen der Zugangs- und Mobilitätsmanagementfunktion (AMF)
- Funktionalität der Session Management Function (SMF)
- Funktionen von Service Communication Proxy (SCP)

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Betreiber weltweit können zwischen mehreren Kommunikationsmodellen wählen, bei denen SCP für die Erkennung von Netzwerkfunktionen (NF) und die anschließende Kommunikation zwischen NF und NF verwendet wird. In diesem Thema werden Konzepte zu verschiedenen

Kommunikationsmodellen und den Anruffluss-/Konfigurationsänderungen behandelt, die bei Subscriber Microservices Infrastructure (SMI), AMF/SMF erforderlich sind, um eine SCP Model-D-basierte Kommunikation zu ermöglichen.

Architektur- und Lösungsüberblick

In der servicebasierten Architektur (SBA) fungiert der SCP als Vermittler, der die indirekte Kommunikation zwischen NFs durch die Verarbeitung von Routing, Lastenausgleich und Serviceerkennung erleichtert und so die servicebasierte Architektur letztendlich rationalisiert.

3GPP 23.501 Annex-E beschreibt die vier Kommunikationsmodelle zwischen NF in einer 5GC-Bereitstellung.

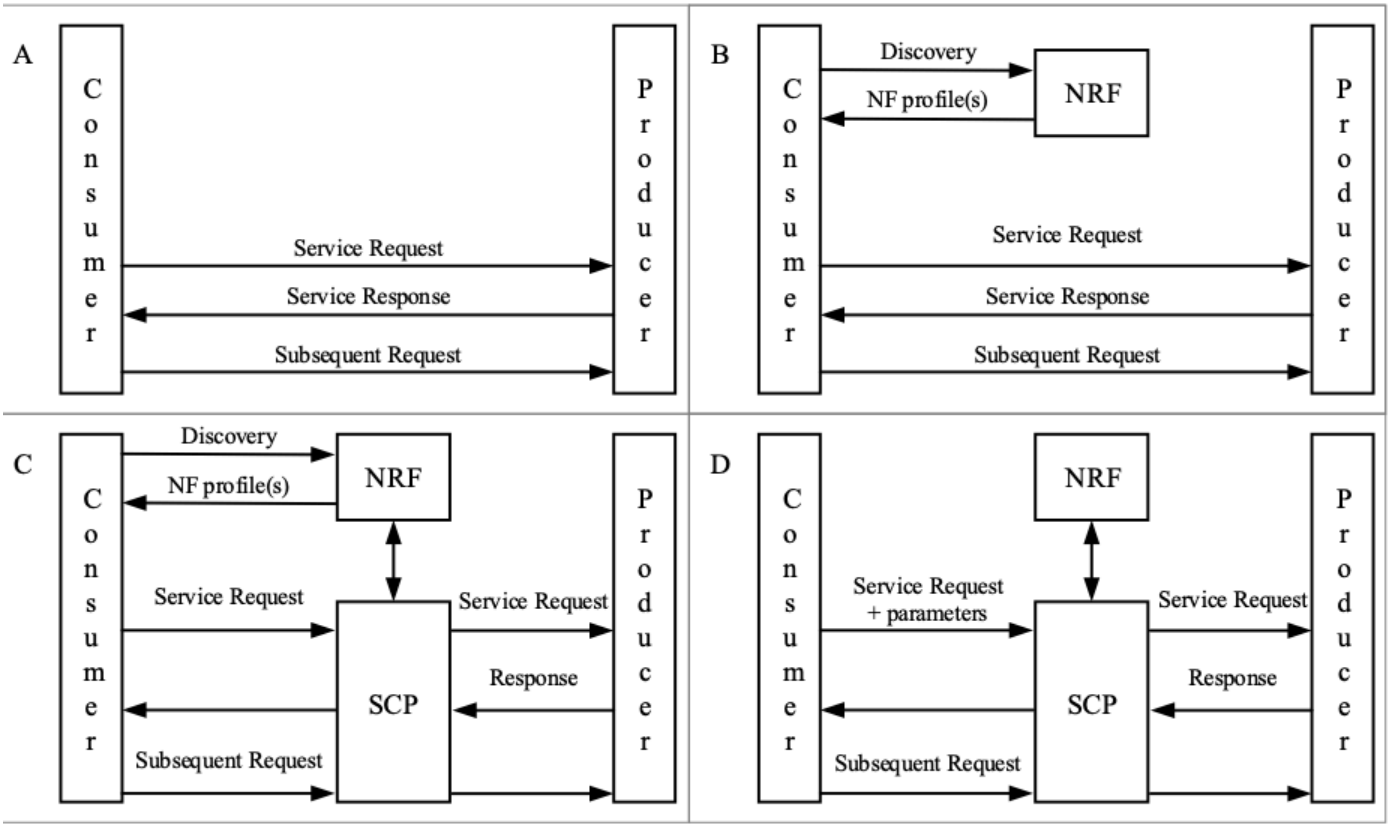


Abbildung A: (verschiedene Kommunikationsmodelle mit SCP)

Modell-A - Direkte Kommunikation ohne NRF-Interaktion (Network Repository Function): Die Verbraucher werden mit den "NF-Profilen" der Hersteller konfiguriert und kommunizieren direkt mit einem Hersteller ihrer Wahl. Hierbei handelt es sich um eine statische Auswahl, und es werden weder NRF noch SCP verwendet.

Modell B - Direkte Kommunikation mit NRF-Interaktion: Verbraucher ermitteln die Ergebnisse, indem sie die NRF abfragen. Auf der Grundlage des Erkennungsergebnisses führt der Consumer die Auswahl durch. Der Verbraucher sendet die Anfrage an den ausgewählten Hersteller.

Modell C - Indirekte Kommunikation ohne delegierte Erkennung: Verbraucher ermitteln durch Abfrage der NRF. Auf der Grundlage des Erkennungsergebnisses wählt der Consumer einen NF-Satz oder eine bestimmte NF-Instanz des NF-Satzes aus. Der Consumer sendet die Anforderung

an den SCP, der die Adresse des ausgewählten Service-Herstellers enthält und auf eine NF-Service-Instanz oder eine Gruppe von NF-Service-Instanzen verweist. Im letzteren Fall wählt das SCP eine NF Service-Instanz aus. Wenn möglich, interagiert das SCP mit NRF, um Auswahlparameter wie Standort, Kapazität usw. abzurufen. Der SCP leitet die Anforderung an die ausgewählte NF-Service-Producer-Instanz weiter.

Modell D - Indirekte Kommunikation mit delegierter Erkennung: Die Verbraucher sind nicht an der Entdeckung oder Auswahl beteiligt. Der Verbraucher fügt der Serviceanfrage alle erforderlichen Erkennungs- und Auswahlparameter hinzu, die erforderlich sind, um einen geeigneten Hersteller zu finden. Der SCP verwendet die Anforderungsadresse sowie die Ermittlungs- und Auswahlparameter in der Anforderungsnachricht, um die Anforderung an eine geeignete Erzeugerinstanz weiterzuleiten. Der SCP kann die Erkennung mit einem NRF durchführen und ein Erkennungsergebnis abrufen.

Details zur modellbasierten Kommunikation: Wenn Call Model-D verwendet wird, sendet der NF-Consumer keine direkte Anfrage an den NRF, sondern delegiert diese Erkennung an den SCP. Der NF-Client sendet eine Nachricht an den SCP und verkettet für jeden dieser Erkennungsfaktoren die Zeichenfolge "3gpp-sbi-discovery" mit dem Namen des Erkennungsfaktors, der verwendet wird, wenn die NF-Erkennung über den NRF erfolgt.

In einem Szenario, in dem SMF nach Unified Data Management (UDM) mit den Servicenamen nudm-sdm sucht, werden die Erkennungsfaktoren an den SCP übergeben:

- Autoritätsüberschrift: die Behörde entweder den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) oder die IP-Adresse trägt, wobei der Konfiguration der IP-Adresse Priorität eingeräumt wird.
- 3gpp-sbi-discovery-requester-nf-type: SMF
- 3gpp-sbi-discovery-target-nf-type: UDM
- 3gpp-Sbi-discovery-service-name: nudm-sdm

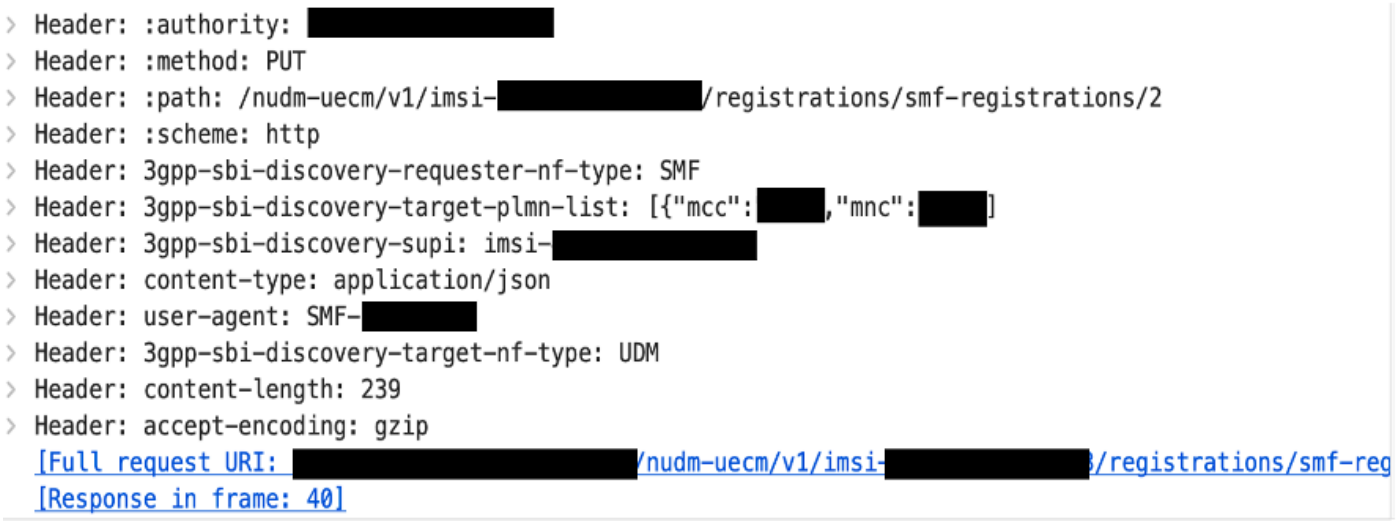
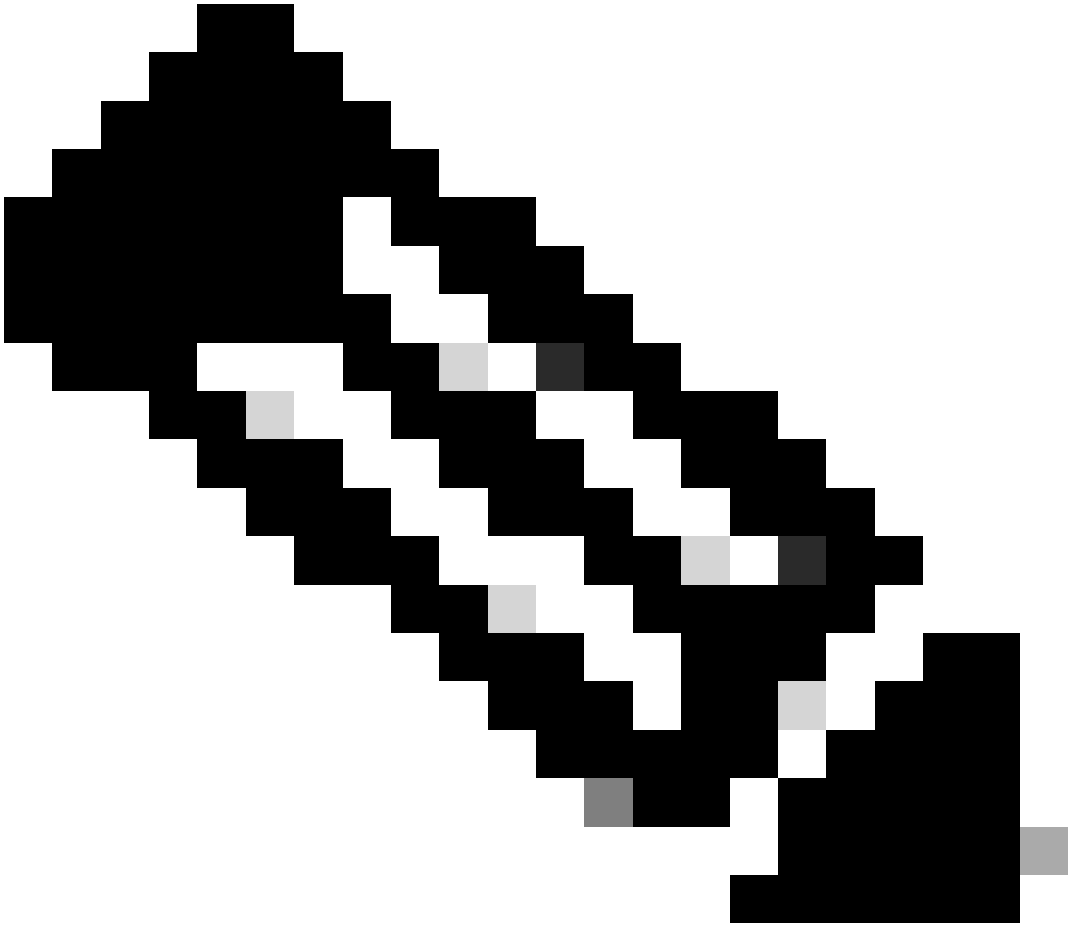


Abbildung B: (SMF-UDM Kommunikation über SCP Modell D)



Anmerkung: Das 3gpp-sbi-discovery-service Namensformat ist im reinen Zeichenfolgenformat und nicht im Arrayformat gemäß 3gpp 29.510 und offenen API-Definitionen (4.7.12.4 Style). Im 29.510 wird 3gpp-sbi-discovery-service-name als Arrayformat erwähnt.

```
- 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
```

Abbildung C: (Snapshot aus der Spezifikation 29.510)

Allerdings konvertiert style:form und explode:false das Array in einen einfachen String, der anhand eines Beispiels aus OpenAPI erklärt wird.

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(

Abbildung D: (Snapshot von Open API: (Stilbeispiele 4.7.12.4)

Sie verfügen sowohl in AMF als auch in SMF über eine CLI-Steuerung, um den Parameter "3gpp-sbi-discovery-service" zu senden, da dieser optional ist (dies kann je nach Bereitstellungsumgebung erfolgen).

Im Fall von Modell B, wenn Sie sich das Beispiel der AMF- und der Authentication Server Function (AUSF)-Kommunikation ansehen, sendet die AMF nach der Erkennung von AUSF den POST-Test an AUSF mit AUSF IP/FQDN und Port.

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

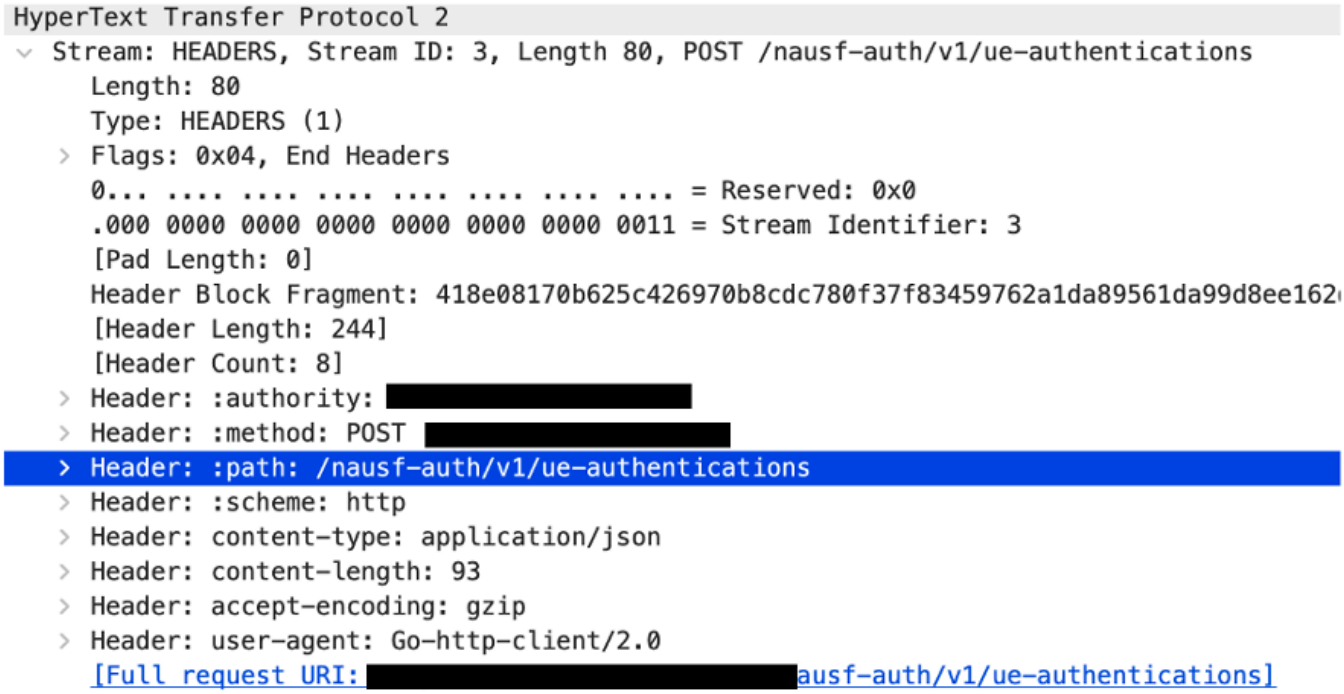


Abbildung E: (AMF-AUSF-Kommunikation über Modell B)

Da die Erkennung im Modell D vom SCP durchgeführt wird, sendet die AMF anstelle von POST-http(s)://<ausf-fqdn>:<ausf-port>/nausf-auth/v1/ue-authentifizierungen die geänderte POST-Anforderung:

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

ODER

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

Mit

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

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

3gpp-Sbi-Discovery-Dienstname

Hier sehen Sie, dass AMF die API-Root (<ausf-fqdn>:<ausf-port>) der AUSF durch die API-Root der SCP ersetzt hat.

```
> 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]
```

Abbildung F: (AMF-AUSF-Kommunikation über SCP-Modell D)

Die 3gpp-sbi-discovery-Parameter ermöglichen dem SCP, die beste NF abzurufen und dann die POST-Anforderung weiterzuleiten, bei der die api-root des SCP durch die api-root ersetzt wird, die vom NRF empfangen wurde, nachdem die Antwort auf die Ermittlungsanforderung empfangen wurde.

Erforderliche Konfigurationen für AMF/SMF

Um für jede NF (z.B. UDM) anzugeben, welches Anrufmodell verwendet werden muss, wird die Konfiguration des nf-Auswahllösungsmodells innerhalb des zugehörigen 'Profilnetzwerkelements' verwendet.

<#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
```

Nach der Auswahl von Model-D werden die für das zugeordnete Netzwerkelement konfigurierten

Abfrageparameter weiterhin verwendet und im Format '3gpp-Sbi-Discovery-<Abfrageparameter>' an den SCP übergeben.

<#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 ]
```

Schließlich wird das Profilnetzwerkelement dem Profil Datennetzwerkname (dnn) zugeordnet.

<#root>

```
profile dnn ims
```

```
 network-element-profiles udm prf-udm-scp
```

```
 network-element-profiles scp prf-scp
```

```
exit
```

SCP(s) sind als Netzwerkelement definiert.

nf-client-profile und ein Fehlerbehandlungsprofil werden dem Netzwerkelement zugeordnet.

<#root>

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

```
 nf-client-profile        <>

 failure-handling-profile <>

exit
```

Das NF-Client-Profil vom Typ "scp-profile" beschreibt die Merkmale des SCP-Endpunkts.

Hier kann nscp-route in api-root hinzugefügt werden.

<#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
```

Der SMF-FQDN wird in der Southbound-Schnittstelle (SBI) des Endpunkts konfiguriert.

<#root>

```
endpoint sbi
```

relicas 2

nodes 2

fqdn <>

Beispiel-Snap-of-Packets

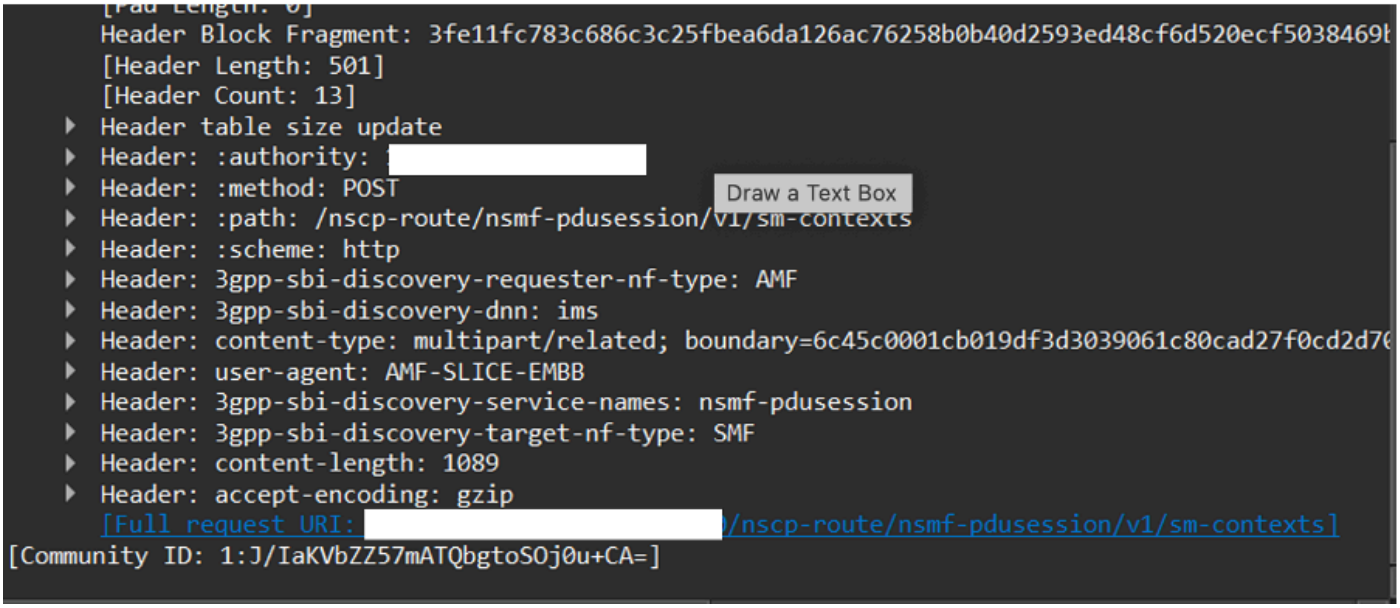


Abbildung G: (AMF- SMF nsmf-pdusession Kommunikation über SCP Modell D)

Aus dem Profil muss auf das soeben konfigurierte SCP-Netzwerkelement verwiesen werden.

<#root>

profile dnn <>

network-element-profiles udm <>

network-element-profiles scp <>

exit

Wenn die SCP-Fehlerbehandlung mit Aktion als Wiederholungsversuch konfiguriert ist, versucht SMF, die SCP auf der Grundlage der SCP-Konfiguration und der Anzahl der Wiederholungsversuche zu wechseln.

Wenn die SCP-Fehlerbehandlung mit Aktion als Retry-and-Fallback für einen bestimmten Dienstnamen und Nachrichtentyp konfiguriert ist, wird der Fallback auf Modell A ausgeführt.

Dieses Fail Handling Profile für SCP (FHSCP) wird verwendet, wenn der Fehler vom SCP (Server-Header, der den SCP angibt) ausgelöst wird und die NF-Client-Konfiguration für den Peer vorhanden ist.

<#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
```

Beispiel für das NF-Client-Profil für die Policy Control Function (PCF) für das Szenario, in dem für den Nachrichtentyp "PcfSmpolicycontrolCreate" der Wiederholungsversuch und das Failover für die Aktion konfiguriert sind:

<#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
```

Wichtige DNS-PODs und Konfiguration auf SMI-Ebene erforderlich

CoreDNS-PODs, die Teil des kube-system-Namespaces sind, werden als 2-POD-Replikat bereitgestellt. Diese PODs können auf jedem der beiden Master-/Steuerknoten geplant werden und sind unabhängig davon, wo die IP-Adresse des Namenservers im Cluster-Manager konfiguriert ist.

Es wird jedoch empfohlen, die IP-Adresse des Nameservers in allen Steuerungs-/Master-Knoten zu konfigurieren, da Sie kein Label-Steuerelement haben, um die CoreDNS-Pods nach Ihren Wünschen zu drehen. Wenn die Route zu den Nameservern auf keinem der Master-Server vorhanden ist, auf denen CoreDNS bereitgestellt ist, kann die SMF/AMF-Cluster-Synchronisierung nicht durchgeführt werden.

Derzeit leitet CoreDNS DNS-Anfragen an den Namenserver weiter, der in der Datei resolv.conf

angegeben ist.

'kubectl edit configmap coredns -n kube-system' Sie haben:

<#root>

```
 {


forward ./etc/resolv.conf{


     max_concurrent 1000


  }
```

Wenn Sie /etc/resolv.conf auf dem Master-Knoten überprüfen, auf dem der Dienst gestartet wird, muss er Folgendes enthalten:

<#root>

```
 name server <>


     name server <>
```

Beispiel für eine Namenserver-Konfiguration im Master-/Kontrollknoten:

<#root>

```
nodes <>


initial-boot netplan vlans <>
```

dhcp4 false

dhcp6 false

addresses [<>]

nameserver addresses [<>]

id <>

link <>

exit

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.