Approfondimento della comunicazione basata sul modello D SCP

Sommario

Introduzione

Questo documento descrive l'approccio di comunicazione SCP-D tra Cisco AMF/SMF e NF di terze parti.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Funzionalità della funzione di gestione degli accessi e della mobilità (AMF)
- Funzionalità della funzione di gestione delle sessioni (SMF)
- Funzionalità di Service Communication Proxy (SCP)

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Gli operatori di tutto il mondo possono scegliere tra diversi modelli di comunicazione utilizzando

SCP per il rilevamento della funzione di rete (NF) e le successive comunicazioni da NF a NF. In questo argomento vengono illustrati i concetti relativi ai diversi modelli di comunicazione e le modifiche al flusso di chiamata e alla configurazione necessarie in Subscriber Microservices Infrastructure (SMI), AMF/SMF per consentire la comunicazione basata su SCP Model-D.

Panoramica dell'architettura e della soluzione

Nell'architettura SBA (Service Based Architecture), SCP funge da intermediario, facilitando la comunicazione indiretta tra le NF gestendo routing, bilanciamento del carico e individuazione dei servizi, semplificando in ultima analisi l'architettura basata sui servizi.

3GPP 23.501 L'Allegato-E descrive i quattro modelli di comunicazione tra NF in una distribuzione 5GC.

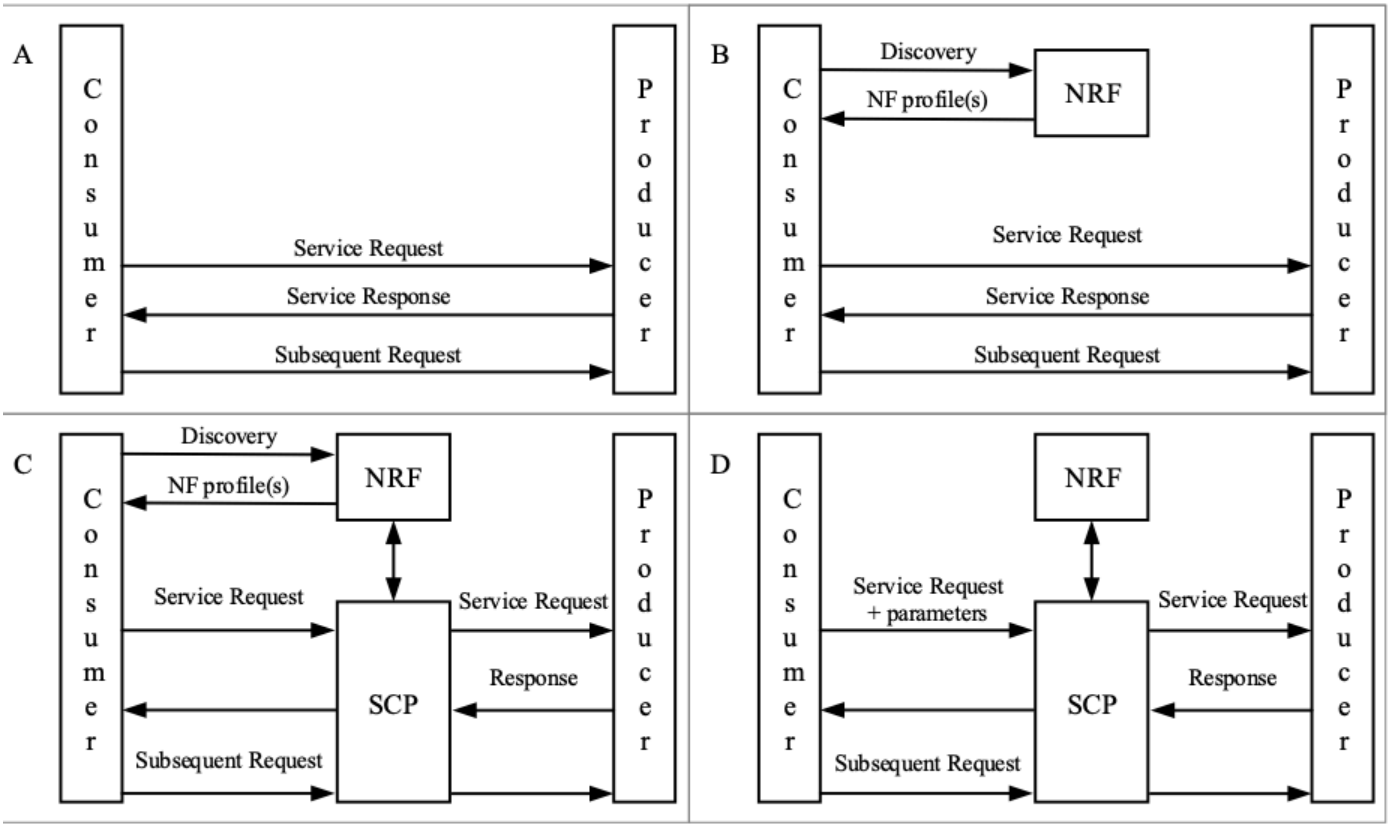


Figura A: (Diversi modelli di comunicazione con SCP)

Modello A - Comunicazione diretta senza interazione NRF (Network Repository Function): I consumatori sono configurati con i "profili NF" dei produttori e comunicano direttamente con un produttore di loro scelta. Si tratta di un tipo di selezione statica in cui non vengono utilizzati NRF o SCP.

Modello B - Comunicazione diretta con interazione NRF: I consumatori eseguono il discovery interrogando il NRF. In base al risultato del rilevamento, il consumatore effettua la selezione. Il consumatore invia la richiesta al produttore selezionato.

Modello C - Comunicazione indiretta senza individuazione delegata: I consumatori lo scoprono interrogando il NRF. In base al risultato del rilevamento, il consumer seleziona un set NF o

un'istanza NF specifica del set NF. Il consumatore invia la richiesta all'SCP contenente l'indirizzo del produttore del servizio scelto che punta a un'istanza del servizio NF o a un set di istanze del servizio NF. In quest'ultimo caso, l'SCP sceglie un'istanza del servizio NF. Se possibile, l'SCP interagisce con l'NRF per ottenere parametri di selezione quali posizione, capacità e così via. L'SCP instrada la richiesta all'istanza del produttore di servizi NF prescelta.

Modello D - Comunicazione indiretta con individuazione delegata: I consumatori non sono coinvolti nell'individuazione o nella selezione. Il consumatore aggiunge tutti i parametri di individuazione e selezione necessari per trovare un produttore idoneo alla richiesta di assistenza. L'SCP utilizza l'indirizzo della richiesta e i parametri di individuazione e selezione nel messaggio di richiesta per instradare la richiesta a un'istanza del producer appropriata. SCP può eseguire il rilevamento con un NRF e ottenere un risultato del rilevamento.

Approfondimento sulla comunicazione basata sul modello D: Quando si utilizza Call Model-D, il consumer NF non invia direttamente una richiesta al NRF, ma delega al SCP questa individuazione. Il client NF invia un messaggio all'SCP e concatena per ciascuno di questi fattori di rilevamento la stringa '3gpp-sbi-discovery' con il nome del fattore di rilevamento che verrà utilizzato se il rilevamento NF verrà eseguito tramite l'NRF.

In uno scenario in cui SMF cercherà Unified Data Management (UDM) con i nomi di servizio nudm-sdm, i fattori di rilevamento verranno passati all'SCP:

- Intestazione autorità: l'autorità dispone del nome di dominio completo (FQDN) o dell'indirizzo IP, con priorità assegnata alla configurazione dell'indirizzo IP.
- tipo 3gpp-sbi-discovery-requester-nf: SMF
- 3gpp-sbi-discovery-target-nf-type: UDM
- 3gpp-Sbi-discovery-service-name: nudm-sdm

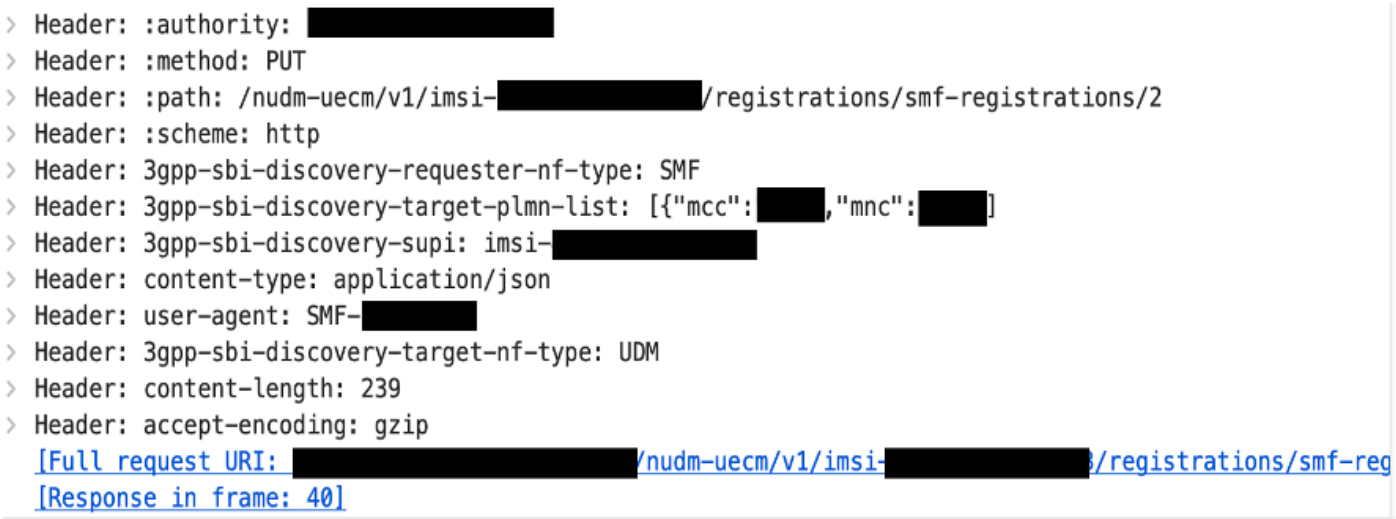
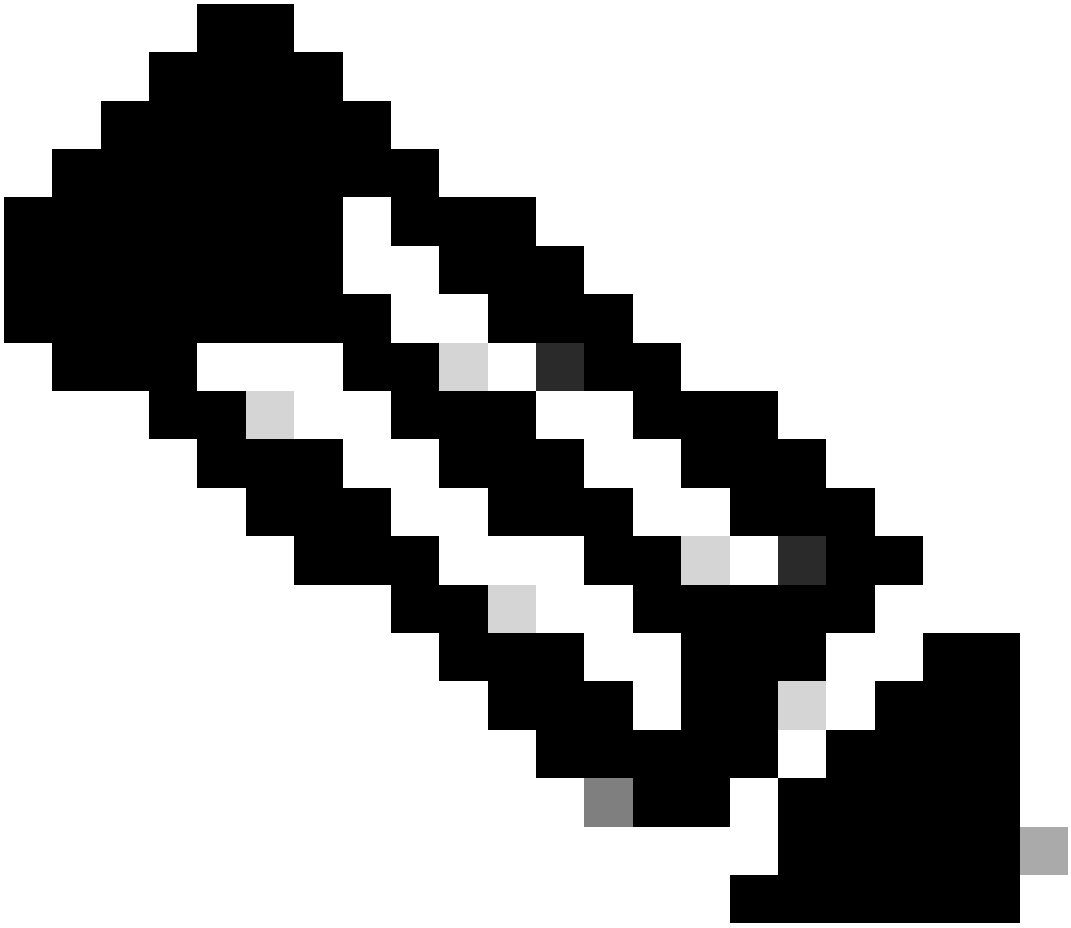


Figura B: (Comunicazione SMF-UDM tramite SCP modello D)



Nota: Il formato del nome del servizio 3gpp-sbi-discovery è in formato di stringa semplice e non in formato di array come in 3gpp 29.510 e nelle definizioni API aperte (4.7.12.4 Style). Nel 29.510 3gpp-sbi-discovery-service-name è indicato come formato di array.

```
- 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: (Snapshot da Spec. 29.510)

Tuttavia, style:form ed explode:false converte l'array in una stringa semplice che viene spiegata

prendendo un esempio da 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: (Snapshot da API aperta: (4.7.12.4 Esempi di stile)

È possibile controllare la CLI sia in AMF che in SMF per inviare il parametro 3gpp-sbi-discovery-service, in quanto opzionale (a seconda dell'ambiente di distribuzione).

Nel caso del modello B, se si prende l'esempio della comunicazione AMF e Authentication Server Function (AUSF), una volta individuato AUSF, l'AMF invia il POST ad AUSF con IP/FQDN e porta AUSF.

POST http://<ausf-fqdn>:<porta>/nausf-auth/v1/ue-authentication.

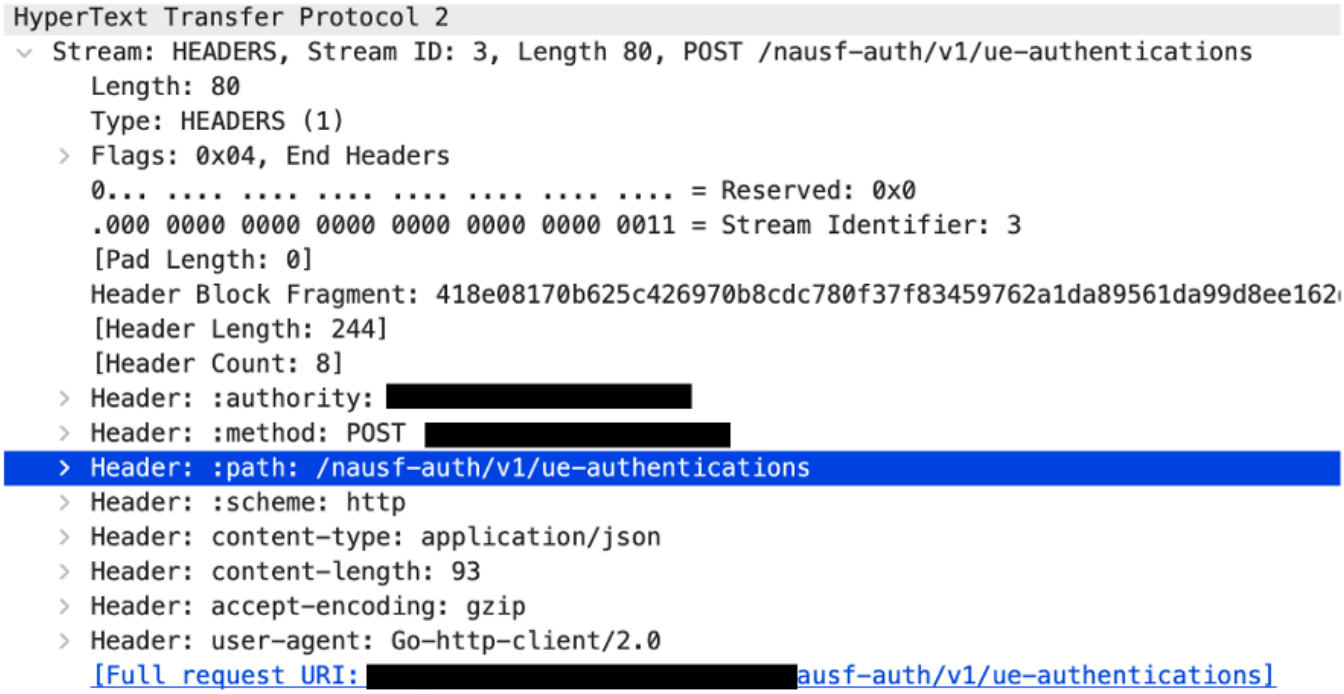


Figura E: (Comunicazione AMF-AUSF tramite modello B)

In Model-D, poiché il rilevamento viene eseguito dall'SCP, invece di POST http(s)://<ausf-fqdn>:<ausf-port>/nausf-auth/v1/ue-authentication l'AMF invia la richiesta POST modificata, ovvero:

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

O

POST http(s)://<scp-fqdn>:<porta-scp>/nscp-route/nausf-auth/v1/ue-authentication(se apiroot=nscp-route)

Con

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

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

3gpp-Sbi-Discovery-service-name

Come si può notare, AMF ha sostituito la radice api (<ausf-fqdn>:<ausf-port>) dell'AUSF con la radice api dell'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: (Comunicazione AMF-AUSF tramite SCP-modello D)

I parametri 3gpp-sbi-discovery consentono all'SCP di recuperare l'NF migliore e inoltrare la richiesta POST dove sostituisce l'api-root dell'SCP con l'api-root ricevuta dall'NRF dopo aver ricevuto la risposta alla sua richiesta di rilevamento.

Configurazioni richieste in AMF/SMF

Per indicare per ogni NF (ad esempio, UDM) quale modello di chiamata deve essere utilizzato, la configurazione del modello di selezione nf viene utilizzata nell'elemento di rete del profilo associato.

<#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

Dopo aver scelto Model-D, i parametri di query configurati per l'elemento di rete associato vengono ancora utilizzati e passati all'SCP nel 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 ]
```

Infine, l'elemento di rete del profilo viene mappato al nome della rete di dati (dnn) del profilo.

<#root>

```
profile dnn ims
```

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

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

```
exit
```

Gli SCP sono definiti come elementi di rete.

nf-client-profile e un profilo di gestione degli errori sono mappati con l'elemento di rete.

<#root>

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

```
 nf-client-profile        <>
```

```
 failure-handling-profile <>

exit
```

Il profilo client-nf di tipo profilo-scp descrive in dettaglio le caratteristiche dell'endpoint SCP.

In questo caso, è possibile aggiungere nscp-route in 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
```

Il nome di dominio completo (FQDN) di SMF è configurato nell'interfaccia SBI (Southbound Interface) dell'endpoint.

<#root>

```
endpoint sbi

relicas 2
```

nodes 2

fqdn <>

Snap di esempio dei pacchetti

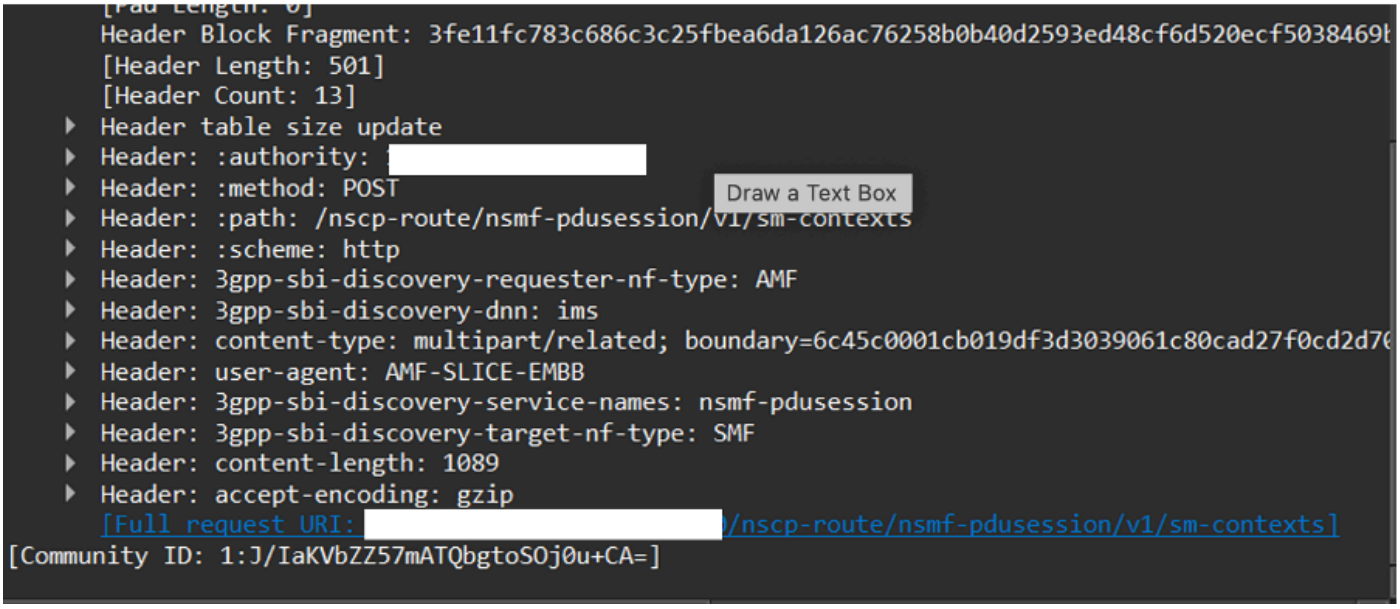


Figura G: (AMF- SMF nsmf-pdusession communication via SCP modello D)

Dal profilo dnn è necessario fare riferimento all'elemento di rete SCP appena configurato.

<#root>

profile dnn <>

network-element-profiles udm <>

network-element-profiles scp <>

exit

Se la gestione degli errori SCP è configurata con l'azione Riprova, SMF tenta di eseguire un SCP alternativo in base alla configurazione SCP e al conteggio dei tentativi.

Se la gestione degli errori SCP è configurata con l'azione retry-and-fallback per un particolare nome di servizio e tipo di messaggio, si verifica il fallback al modello A.

Questo profilo di gestione degli errori per SCP (FHSCP) viene utilizzato se l'errore viene generato dall'SCP (intestazione server che indica SCP) e se è presente la configurazione client NF per il peer.

<#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
```

Esempio del profilo nf-client per la funzione di controllo dei criteri (PCF) per lo scenario in cui i tentativi di azione e il fallback sono configurati per il tipo di messaggio 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
```

Configurazione e POD DNS di base richiesti al livello SMI

I pod CoreDNS, che fanno parte dello spazio dei nomi kube-system, vengono distribuiti come replicaset a 2 pod. Questi pod possono essere pianificati su uno qualsiasi dei due nodi master/di controllo e non dipendono dalla posizione in cui è configurato l'indirizzo IP del server dei nomi in Gestione cluster.

Tuttavia, si consiglia di configurare l'indirizzo IP del server dei nomi in tutti i nodi di controllo/master in quanto non si dispone di un controllo di etichettatura per la rotazione dei pod CoreDNS secondo le proprie esigenze. Se la route ai server dei nomi non è presente in nessuno dei master in cui viene distribuito CoreDNS, la sincronizzazione del cluster SMF/AMF non riesce.

Al momento, CoreDNS inoltra le richieste DNS al server dei nomi specificato nel file resolv.conf dei nodi.

'kubectl edit configmap coredns -n kube-system' si dispone di:

```
<#root>
 {
```

```
forward ./etc/resolv.conf{

    max_concurrent 1000

  }
```

Quando si seleziona /etc/resolv.conf nel nodo master in cui viene avviato il servizio, è necessario che contenga:

<#root>

```
 name server <>

    name server <>
```

Esempio di configurazione del server dei nomi nel nodo master/controllo:

<#root>

```
nodes <>

initial-boot netplan vlans <>

dhcp4 false

dhcp6 false
```

addresses [<>]

nameserver addresses [<>]

id <>

link <>

exit

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).