Approfondissement de la communication basée sur le modèle D de la SCP

Table des matières

[Introduction](#)

[Conditions préalables](#)

- [Exigences](#)
- [Composants utilisés](#)

[Informations générales](#)

[Présentation de l'architecture et des solutions](#)

[Configurations requises au niveau AMF/SMF](#)

- [Exemple d'accrochage de paquets](#)
- [POD DNS de base et configuration requise au niveau de la couche SMI](#)

Introduction

Ce document décrit l'approche approfondie de SCP Model-D Communication entre Cisco AMF/SMF et NF tiers.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Fonctionnalité de la fonction de gestion de l'accès et de la mobilité (AMF)
- Fonctionnalité de la fonction de gestion de session (SMF)
- Fonctionnalité de Service Communication Proxy (SCP)

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Les opérateurs du monde entier peuvent choisir entre plusieurs modèles de communication utilisant la SCP pour la découverte de la fonction réseau (NF) et les communications NF à NF

ultérieures. Ce sujet aborde les concepts relatifs aux différents modèles de communication et aux changements de flux d'appels/configuration requis au niveau de l'infrastructure SMI (Subscriber Microservices Infrastructure), AMF/SMF afin d'avoir une communication basée sur le modèle D de la SCP.

Présentation de l'architecture et des solutions

Dans l'architecture basée sur les services (SBA), le SCP agit en tant qu'intermédiaire, facilitant la communication indirecte entre les NF en gérant le routage, l'équilibrage de charge et la découverte de services, rationalisant ainsi l'architecture basée sur les services.

3GPP 23.501 Annexe-E détaille les quatre modèles de communication entre NF dans un déploiement 5GC.

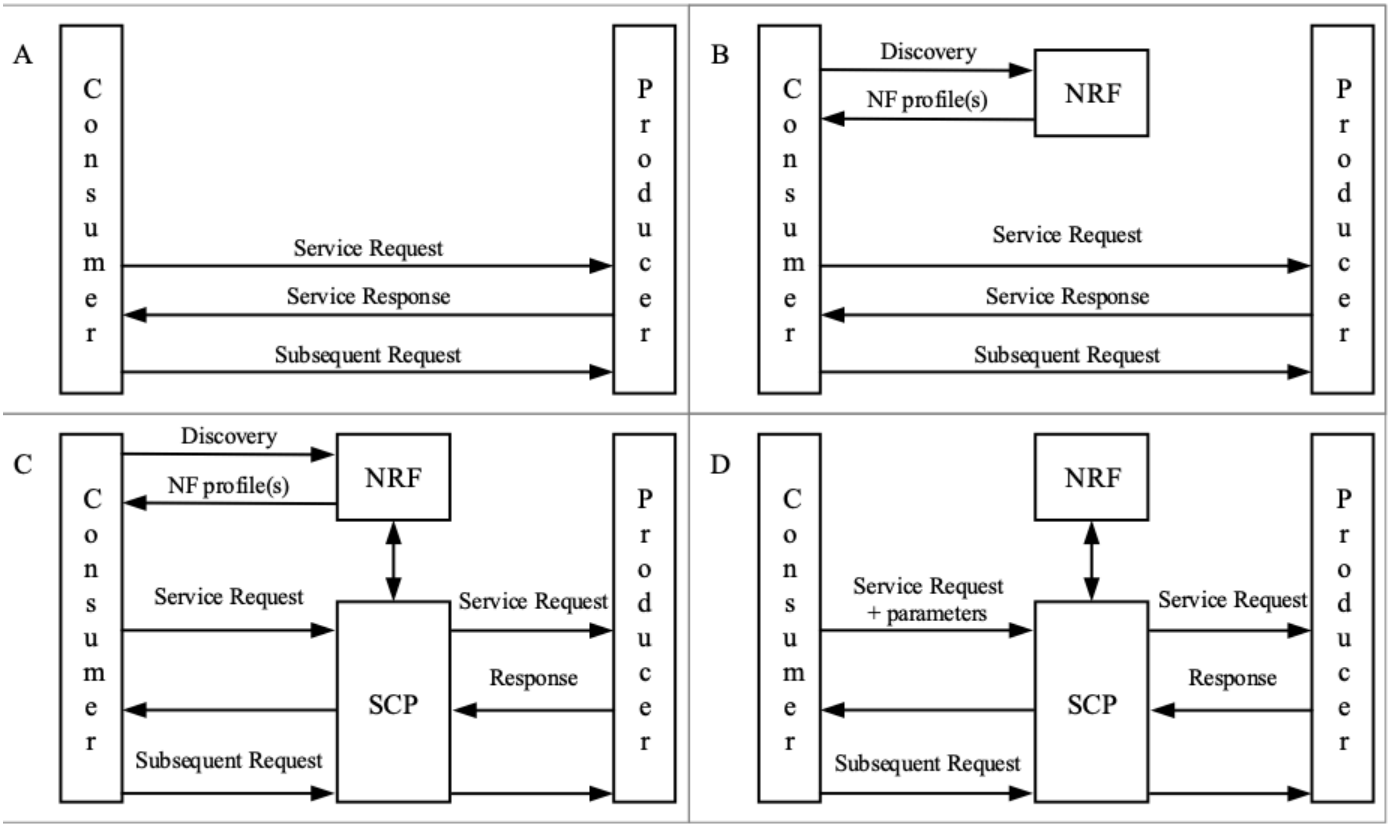


Figure A : (Différents modèles de communication impliquant la SCP)

Modèle A - Communication directe sans interaction NRF (Network Repository Function) : Les consommateurs sont configurés avec les « profils NF » des producteurs et communiquent directement avec un producteur de leur choix. Il s'agit d'un type de sélection statique et ni NRF ni SCP ne sont utilisés.

Modèle B - Communication directe avec interaction NRF : Les consommateurs effectuent la détection en interrogeant la NRF. En fonction du résultat de la détection, le consommateur effectue la sélection. Le consommateur envoie la demande au producteur sélectionné.

Modèle-C - Communication indirecte sans détection déléguée : Les consommateurs découvrent en interrogeant le NRF. En fonction du résultat de la détection, le consommateur sélectionne un

ensemble NF ou une instance NF spécifique d'un ensemble NF. Le consommateur envoie la requête au SCP contenant l'adresse du producteur de services choisi pointant vers une instance de service NF ou un ensemble d'instances de service NF. Dans ce dernier cas, le SCP choisit une instance de service NF. Si possible, le SCP interagit avec la NRF afin d'obtenir des paramètres de sélection tels que l'emplacement, la capacité, etc. Le SCP achemine la demande vers l'instance du producteur de services NF choisie.

Modèle-D - Communication indirecte avec découverte déléguée : Les consommateurs ne sont pas impliqués dans la découverte ou la sélection. Le consommateur ajoute à la demande de service tous les paramètres de découverte et de sélection nécessaires pour trouver un producteur approprié. Le SCP utilise l'adresse de demande et les paramètres de détection et de sélection dans le message de demande afin d'acheminer la demande vers une instance de producteur appropriée. Le SCP peut effectuer une détection avec un NRF et obtenir un résultat de détection.

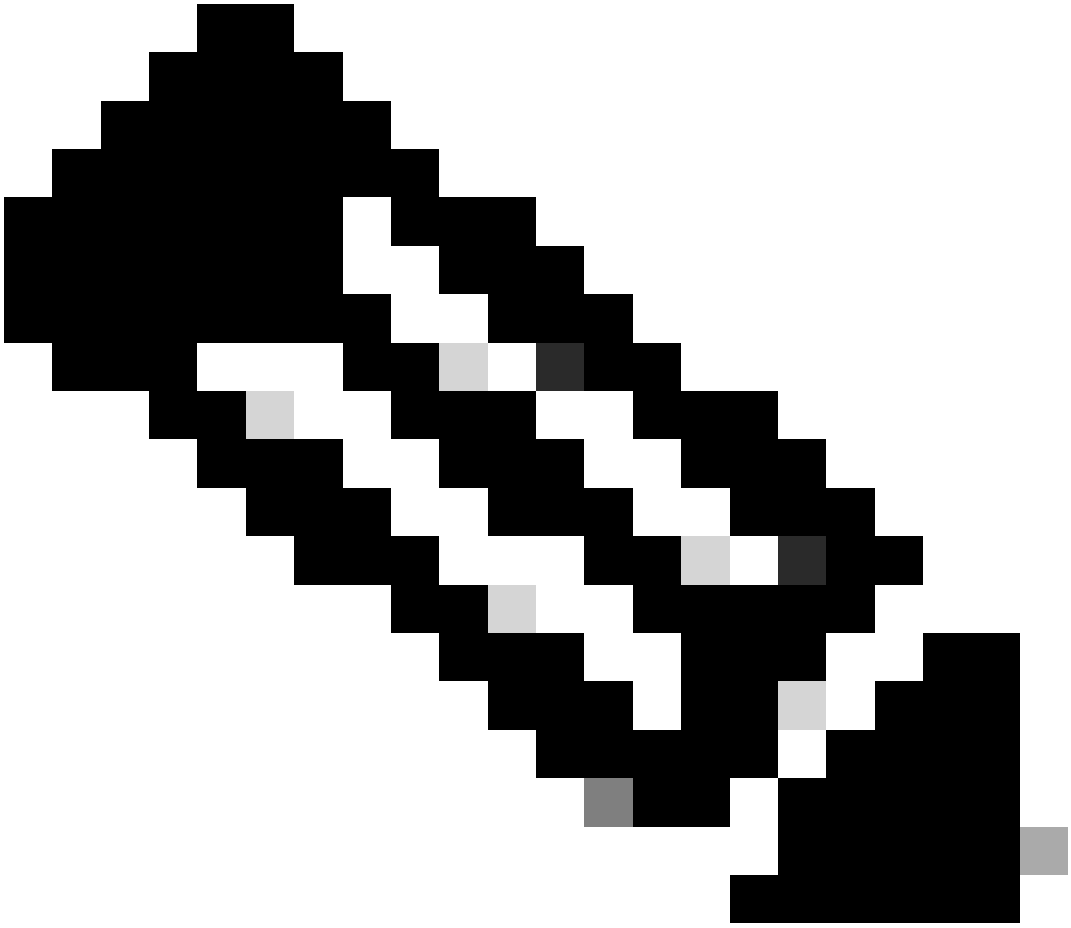
Approfondissement des communications basées sur le modèle D : Lorsque le modèle d'appel D est utilisé, le consommateur NF n'envoie pas directement une requête au NRF, mais délègue au SCP cette découverte. Le client NF envoie un message au SCP et concatène pour chacun de ces facteurs de découverte la chaîne « 3gpp-sbi-discovery » avec le nom du facteur de découverte qui sera utilisé si la découverte NF sera effectuée via le NRF.

Dans le cas d'un scénario où SMF rechercherait une gestion unifiée des données (UDM) avec des noms de service nudm-sdm, les facteurs de détection seront transmis au SCP :

- En-tête Autorité : l'autorité porte soit le nom de domaine complet (FQDN), soit l'adresse IP, la priorité étant donnée à la configuration de l'adresse IP.
- 3gpp-sbi-discovery-request-nf-type : SMF
- 3gpp-sbi-discovery-target-nf-type : UDM
- 3gpp-Sbi-discovery-service-name : nudm-sdm

```
> Header: :authority: [redacted]
> Header: :method: PUT
> Header: :path: /nudm-uecm/v1/imsi-[redacted]/registrations/smf-registrations/2
> Header: :scheme: http
> Header: 3gpp-sbi-discovery-requester-nf-type: SMF
> Header: 3gpp-sbi-discovery-target-plmn-list: [{"mcc":[redacted],"mnc":[redacted]]
> Header: 3gpp-sbi-discovery-supi: imsi-[redacted]
> Header: content-type: application/json
> Header: user-agent: SMF-[redacted]
> Header: 3gpp-sbi-discovery-target-nf-type: UDM
> Header: content-length: 239
> Header: accept-encoding: gzip
  [Full request URI: [redacted]/nudm-uecm/v1/imsi-[redacted]/registrations/smf-reg
  [Response in frame: 40]
```

Figure B : (Communication SMF-UDM via le modèle D de la SCP)



Remarque : Le format du nom du service de découverte 3gpp-sbi est au format chaîne simple et non au format tableau, conformément à la norme 3gpp 29.510 et aux définitions d'API ouvertes (style 4.7.12.4). Dans la norme 29.510, le nom du service de découverte 3gpp-sbi est mentionné sous la forme d'un format tableau.

```
- 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
```

Figure C : (Instantané de la spécification 29.510)

Cependant, le style : form et explode : false convertit le tableau en une chaîne simple qui est expliquée en prenant un exemple d'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(

Figure D : (Instantané de l'API ouverte : (4.7.12.4 Exemples de style)

Vous disposez d'un contrôle CLI dans AMF et SMF pour envoyer le paramètre 3gpp-sbi-discovery-service car il est facultatif (peut être effectué en fonction de l'environnement de déploiement).

Dans le cas du modèle B, si vous prenez l'exemple de la communication AMF et AUSF (Authentication Server Function), une fois qu'AUSF est détecté, l'AMF envoie le POST à AUSF avec AUSF IP/FQDN et Port.

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

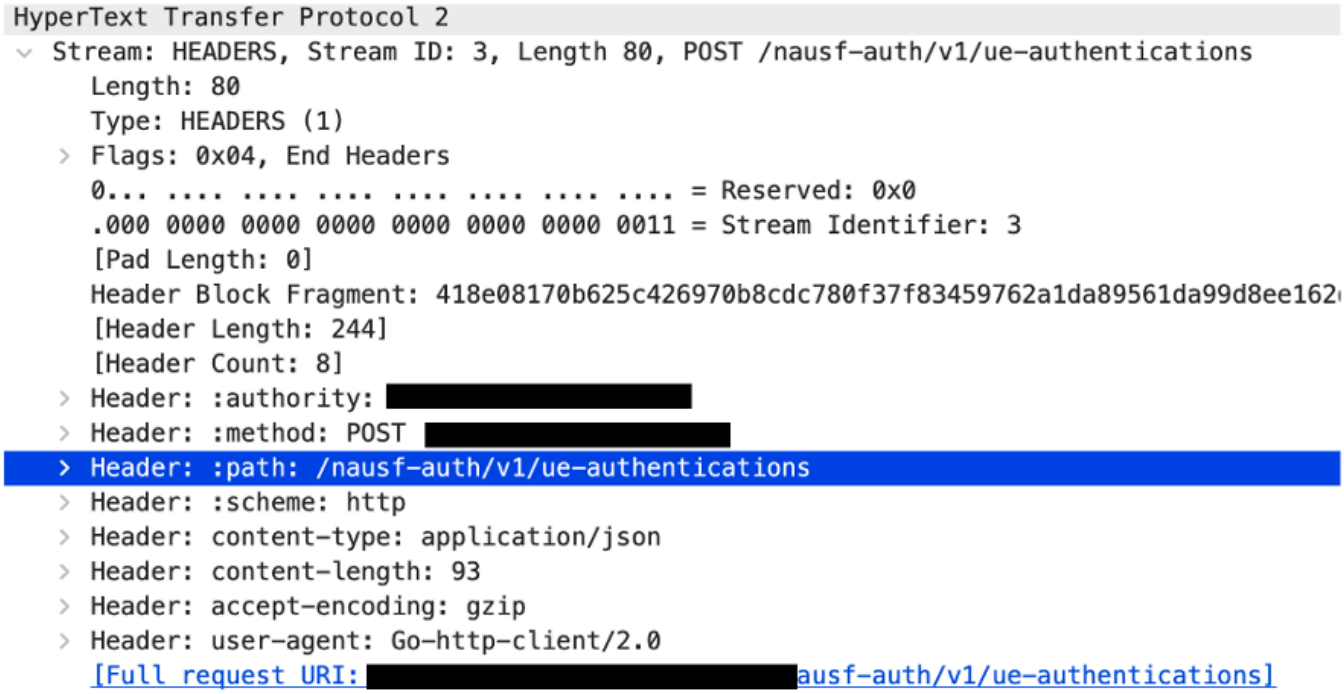


Figure E : (Communication AMF-AUSF via le modèle B)

Dans le modèle D, comme la découverte est effectuée par le SCP, au lieu des http(s)://<ausf-fqdn>:<ausf-port>/nausf-auth/v1/ue-authentifications de POST, l'AMF envoie la requête POST modifiée qui est :

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

OU

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

Avec

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

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

3gpp-Sbi-Discovery-service-name

Où vous pouvez voir qu'AMF a remplacé la racine api (<ausf-fqdn>:<ausf-port>) de l'AUSF par la racine api du 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]
```


Figure F : (Communication AMF-AUSF via SCP-Model D)

Les paramètres 3gpp-sbi-discovery permettent au SCP de récupérer le meilleur NF, puis de transférer la requête POST où il remplace la racine api du SCP par la racine api reçue du NRF après avoir reçu la réponse à sa requête de découverte.

Configurations requises au niveau AMF/SMF

Afin d'indiquer pour chaque NF (par exemple, UDM) quel modèle d'appel doit être utilisé, la configuration nf-selection-model est utilisée dans le 'profile network-element' associé.

<#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

Une fois que Model-D est choisi, les paramètres de requête configurés pour l'élément de réseau associé sont toujours utilisés et sont transmis au SCP au format « 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 ]
```

Finalement, l'élément de réseau de profil est mappé au nom de réseau de données de profil (dnn).

<#root>

```
profile dnn ims


 network-element-profiles udm prf-udm-scp


 network-element-profiles scp prf-scp


exit
```

Les SCP sont définis comme des éléments de réseau.

nf-client-profile et un profil de gestion des pannes est mappé avec network-element.

<#root>

```
profile network-element scp <>


 nf-client-profile        <>
```

```
 failure-handling-profile <>

exit
```

Le nf-client-profile de type scp-profile détaille les caractéristiques du point d'extrémité SCP.

Ici, nscp-route peut être ajouté dans 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
```

Le nom de domaine complet SMF est configuré dans l'interface de terminal en direction du sud (SBI).

<#root>

```
endpoint sbi

relicas 2
```

nodes 2

fqdn <>

Exemple d'accrochage de paquets

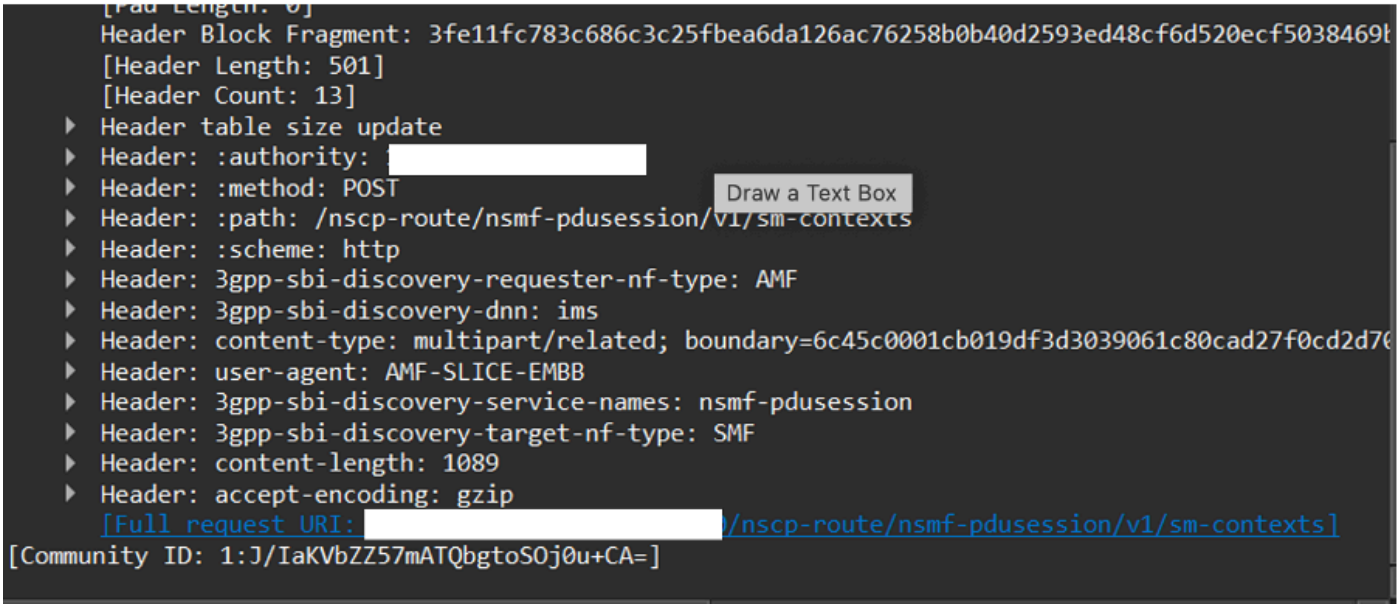


Figure G : (Communication AMF- SMF nsmf-pdusession via SCP Model D)

Vous avez besoin du profil dnn pour faire référence à l'élément réseau SCP qui vient d'être configuré.

<#root>

profile dnn <>

network-element-profiles udm <>

network-element-profiles scp <>

exit

Si la gestion des défaillances de SCP est configurée avec l'action comme une nouvelle tentative, SMF tente une SCP alternative en fonction de la configuration de SCP et du nombre de nouvelles tentatives.

Si la gestion des défaillances de SCP est configurée avec une action comme une tentative et un repli pour un nom de service et un type de message particuliers, alors le repli vers le Modèle-A se produit.

Ce profil de traitement des échecs pour SCP (FHSCP) est utilisé si l'erreur est déclenchée à partir du SCP (en-tête de serveur indiquant SCP) et si la configuration NF-client pour l'homologue est présente.

<#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
```

Exemple de profil nf-client pour la fonction de contrôle de stratégie (PCF) pour le scénario où la nouvelle tentative d'action et le retour arrière sont configurés pour le type de message 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 DNS de base et configuration requise au niveau de la couche SMI

Les pods CoreDNS, qui font partie de l'espace de noms kube-system, sont déployés en tant que réplicaset 2-pod. Ces pods peuvent être planifiés sur n'importe lequel des deux noeuds maîtres/de contrôle et ne dépendent pas de l'endroit où l'adresse IP du serveur de noms est configurée dans le gestionnaire de cluster.

Cependant, il est recommandé de configurer l'adresse IP du serveur de noms dans tous les noeuds de contrôle/maître car vous n'avez pas de contrôle d'étiquetage pour faire tourner les pods CoreDNS selon votre souhait. Si la route vers les serveurs de noms n'est pas présente sur l'un des maîtres où CoreDNS est déployé, la synchronisation du cluster SMF/AMF échoue.

Actuellement, CoreDNS transfère les requêtes DNS au serveur de noms spécifié dans le fichier resolv.conf des noeuds.

'kubectl edit configmap coredns -n kube-system' vous avez :

<#root>

```
 {


forward ./etc/resolv.conf{


     max_concurrent 1000


  }
```

Lors de la vérification de /etc/resolv.conf sur le noeud maître où le service est démarré, il doit contenir :

<#root>

```
 name server <>


     name server <>
```

Exemple de configuration de serveur de noms dans le noeud maître/de contrôle :

<#root>

```
nodes <>


initial-boot netplan vlans <>


dhcp4 false
```

dhcp6 false

addresses [<>]

nameserver addresses [<>]

id <>

link <>

exit

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.