Oracle® Communications

Network Slice Selection Function (NSSF) Cloud Native User's Guide

Release 1.0
F16990-01
April 2019

Oracle Communications Network Slice Selection Function (NSSF) Cloud Native User's Guide, Release 1.0

F16990-01

Contents

List of Figures

List of Tables

1
Introduction

Introduction

This document provides information on how to use the Oracle Communications Network Slice Selection Function (OCNSSF) in the cloud native 5G core network.

Network slices enables the operators to provide customized networks with different functionality (e.g. mobility), performance requirements (e.g. latency, availability, reliability...etc.). Network slices may differ for supported features and network functions optimisations, in which case such Network Slices may have e.g. different S-NSSAIs with different Slice/Service Types. The operator can deploy multiple Network Slice instances delivering exactly the same features but for different groups of UEs, e.g. as they deliver a different committed service and/or because they are dedicated to a customer, in which case such Network Slices may have e.g. different S-NSSAIs with the same Slice/Service Type but different Slice Differentiators. OCNSSF fulfills the requirement for determining the individual network function pertaining to a slice. This section includes information about the role of OCNSSF in the 5G Service based architecture.

Network Slice Selection Function is a functional element that supports the following functionalities:

- OCNSSF enables the Access and Mobility Management Function (AMF) to perform initial registration and PDU session establishment
- OCNSSF selects the network slicing instance (NSI) and determines the authorized Network Slice Selection Assistance Information (NSSAIs) and AMF to server the UE AMF can retrieve NRF, NSI ID, target AMFs as part of UE initial registration and PDU establishment procedure
- OCNSSF interaction with NRF allows retrieving specific NF services to be used for registration request

NSSF is responsible for providing the following information as and when queried by the AMF:

- Allowed NSSAIs
- Configured NSSAIs
- Restricted NSSAIs
- Candidate AMF List (in case of registration)
- Network Slice instance ID (for PDU registration)
- Slice-level NRF information (for PDU Connectivity)

OCNSSF supports the above functions through the Network Slice Selection service, *Nnssf_NSSelection*. This service is used by an NF Service Consumer (AMF) to retrieve the information related to network slice. Network Slice Selection Service enables Network Slice selection in the serving Home Public Land Mobile Network (HPLMN).

NSSF Supported Services

This section includes information about the service supported by NSSF.

NSSF supports the **Network Slice Selection service**.

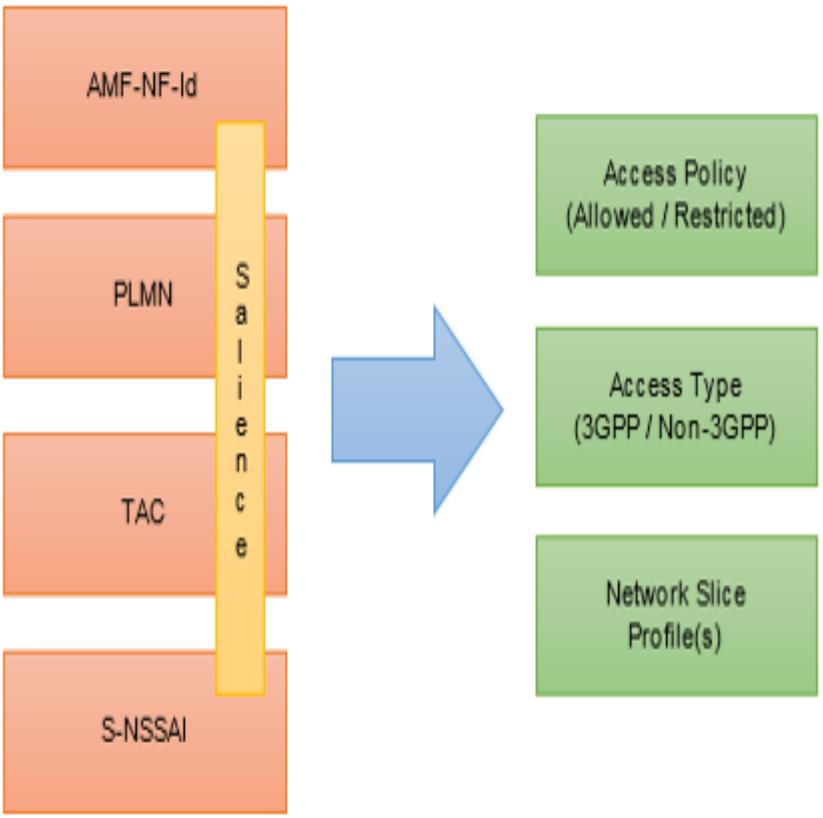
The Network Slice Selection service is identified by the service operation name `Nnssf_NSSelection`.This service supports GET request during the following procedures by UE:

- **Initial Register**: When the NSSF is able to find authorized network slice information for the requested network slice selection information, the response body includes a payload body containing at least the Allowed NSSAI, target AMF Set or the list of candidate AMF(s).
- **PDU Session Establishment:**This service is utilized by the NF service consumer (e.g AMF) to update the S-NSSAI(s) supported on a per TA basis on the NSSF. It also allows a mechanism for AMF to subscribe and notify on any update of supported/restricted S-NSSAI(s) per TA/PLMN of the UE.

Network Slice Selection Policy

NSSF allows the operator to configure network slice selection policies. Following diagram illustrates the Policy configuration.

Figure 1-1 Policy Configuration



NSSF Policy is a set of dynamic policy rules which enables NSSF to select and update Network slice mapping and availability status on time. The operator can configure policy rules such that an NSSelection request coming from a given AMF having a given PLMN and/or TAC and containing a given S-NSSAI that is both requested and subscribed can be either allowed for a certain Access Type with certain Network Slice Profile(s) or can be restricted at the PLMN or TA. The AMF, PLMN, and TAC can be configured as Don't Cares to enable policies to span geographies.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click `Industries`.
3. Under the Oracle Communications subheading, click the `Oracle Communications documentation` link.

   The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
4. Click on your Product and then the Release Number.

   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the `PDF` link, select `Save target as` (or similar command based on your browser), and save to a local folder.

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support can assist you with My Oracle Support registration.

Call the Customer Access Support main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select **2** for New Service Request.
2. Select **3** for Hardware, Networking and Solaris Operating System Support.
3. Select one of the following options:
   - For Technical issues such as creating a new Service Request (SR), select **1**.
   - For Non-technical issues such as registration or assistance with My Oracle Support, select **2**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Acronyms and Terminology

The following table provides information about the acronyms used in the document.

Table 1-1 Acronyms

Field	Description
5G-AN	5G Access Network
5GC	5G Core Network
5G-GUTI	5G Globally Unique Temporary Identifier
5QI	5G QoS Identifier
5G-S-TMSI	5G S-Temporary Mobile Subscription Identifier
5GS	5G System
5G-EIR	5G-Equipment Identity Register
(R)AN	(Radio) Access Network
AMF	Access and Mobility Management Function
AUSF	Authentication Server Function
CAPIF	Common API Framework for 3GPP northbound APIs
NEF	Network Exposure Function
NF	Network Function
NRF	Network Repository Function
NSI ID	Network Slice Instance Identifier
NSSAI	Network Slice Selection Assistance Information
NSSF	Network Slice Selection Function
Network Slice	A logical network that provides specific network capabilities and network characteristics
Network Slice instance	A set of Network Function instances and the required resources (e.g. compute, storage and networking resources) which form a deployed Network Slice
NF service	A functionality exposed by a NF through a service based interface and consumed by other authorized NFs.
NSSP	Network Slice Selection Policy
PEI	Permanent Equipment Identifier
PCF	Policy Control Function
QFI	QoS Flow Identifier
QoE	Quality of Experience
Requested NSSAI	NSSAI provided by the UE to the Serving PLMN during registration.
Allowed NSSAI	NSSAI provided by the Serving PLMN during e.g. a Registration procedure, indicating the S-NSSAIs values the UE could use in the Serving PLMN for the current registration area.
Configured NSSAI	NSSAI provisioned in the UE applicable to one or more PLMNs.
SEPP	Security Edge Protection Proxy
SBA	Service Based Architecture
SBI	Service Based Interface
SSC	Session and Service Continuity
SSCMSP	Session and Service Continuity Mode Selection Policy

Table 1-1 (Cont.) Acronyms

SST	Slice/Service type
SD	Slice Differentiator
SMF	Session Management Function
SMSF	Short Message Service Function
S-NSSAI	Single Network Slice Selection Assistance Information
UDM	Unified Data Management
UDR	Unified Data Repository
UDSF	Unstructured Data Storage Function

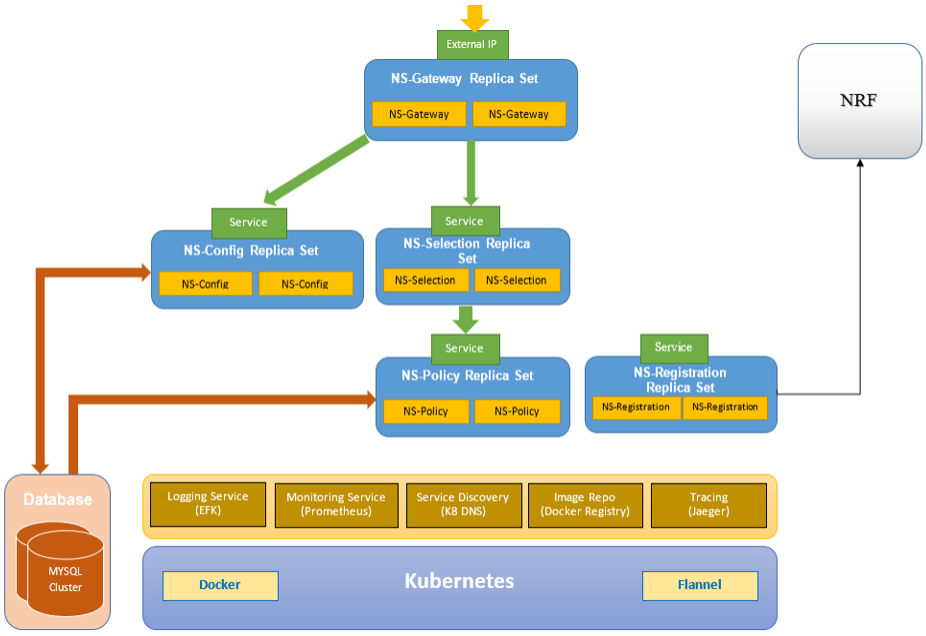
2
NSSF Functional Summary

This section provides a high-level summary of the NSFF functionality.

NSSF Architecture

NSSF comprises of various microservices deployed in Kubernetes based Cloud Native Environment (CNE, example: OC-CNE) . Some common services like logs or metrics data collection, analysis and graphs or charts visualization, etc. is provided by the environment. The microservices integrates with them and provide them necessary data. The following diagram describes the overall architecture of the NSSF:

Figure 2-1 Network Slice Selection Function Architecture Diagram



The solution has the following components:

- **NS-Gateway (NSG):**This microservice distributes among the NSSelection and NSConfig microservices. NSG is also responsible to pegging traffic related measurements. It also provides support for API life cycle.

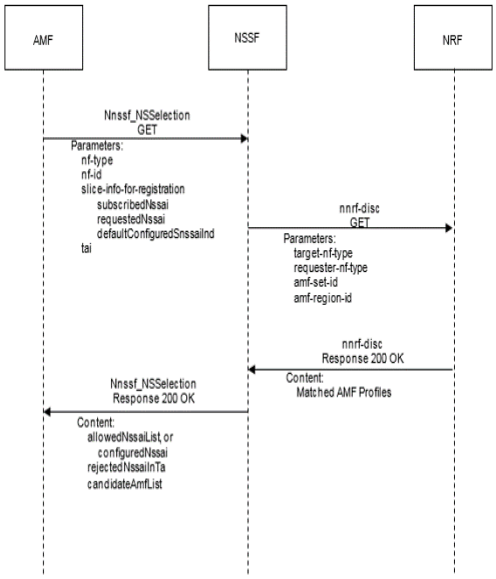
> **Note:**
>
> API Gateway **Ambassador** is used to implement NS-Gateway.

- **NS-Selection MicroService (NSS):** This micro-service receives all traffic for NS Selection Service. The micro-service validates and pre-processes NS Selection query requests before forwarding it to NSPolicy service. NSS parses and validates Get request parameters for initial registration and PDU session establishment messages. It also forwards response back to NS-Gateway.
- **NS-Policy MicroService (NSP):**
  This microservice performs the policy decision based on operator configured policy rules.
- **NS-Config MicroService (NSC):**
  This microservice is responsible for configuring NSSF managed objects. NSC also implements a REST messaging server that receives configuration HTTP messages, validates and stores the configuration in the database.
- **NS-Registration MicroService (NSR):**
  This microservice registers with the NRF and sends periodic heartbeats.
- **Data Service**
  The data service is deployed by the CNE provider. It is a common CNE service with persistent data storage and highly available clustered MySql. The OCNSSF microservices create their data store using the Data Service upon initialization.

NSSF Initial Register

Following diagram illustrates the procedure of Initial Register:

Figure 2-2 Initial Register



The following is performed for Initial Register:

- The AMF sends a GET request to the NSSF. The AMF queries the NSSF, with Requested NSSAI, mapping of Requested NSSAI to Configured NSSAI for the HPLMN, the Subscribed S-NSSAIs (with an indication if marked as default S-NSSAI), any Allowed NSSAI it might have for the other Access Type (including its mapping to the Configured

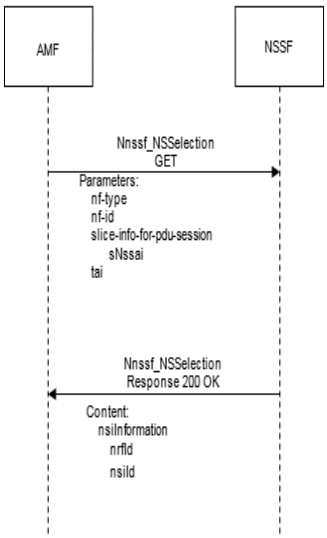
NSSAI for the HPLMN), PLMN ID of the SUPI, UE's current tracking area, NF type of the NF service consumer, and AMF ID.

- Based on this information, local configuration, and other locally available information including RAN capabilities in the current Tracking Area for the UE , the NSSF does the following:
  - It selects the Network Slice instance(s) to serve the UE. When multiple Network Slice instances in the UE's Tracking Areas are able to serve a given S-NSSAI, based on operator's configuration, the NSSF may select one of them to serve the UE, or the NSSF may defer the selection of the Network Slice instance until a NF/service within the Network Slice instance needs to be selected.
  - It determines the target AMF Set to be used to serve the UE, or, based on configuration, the list of candidate AMF(s), possibly after querying the NRF.
  - It determines the Allowed NSSAI(s) for the applicable Access Type(s), taking also into account the availability of the Network Slice instances that are able to serve the S-NSSAI(s) in the Allowed NSSAI in the current UE's tracking areas.
  - Based on operator configuration, the NSSF may determine the NRF(s) to be used to select NFs/services within the selected Network Slice instance(s).
- When the NSSF is able to find authorized network slice information for the requested network slice selection information, NSSF sends Discovery Request for AMF to NRF.
- The NRF responds with list of candidate AMFs to NSSF.
- The NSSF returns to the current AMF the Allowed NSSAI for the applicable Access Type(s) , the target AMF Set, or, based on configuration, the list of candidate AMF(s). The NSSF returns the NRF(s) to be used to select NFs/services within the selected Network Slice instance(s), and the NRF to be used to determine the list of candidate AMF(s) from the AMF Set. The NSSF returns NSI ID(s) to be associated to the Network Slice instance(s) corresponding to certain S-NSSAIs. NSSF also returns the rejected S-NSSAI(s) and the Configured NSSAI for the Serving PLMN.

PDU Session Establishment

The PDU Session Establishment in a Network Slice to a DN allows data transmission in a Network Slice. A PDU Session is associated to an S-NSSAI and a DNN. Following diagram illustrates the procedure of PDU Session Establishment:

Figure 2-3 PDU Session Establishment



The following is performed for PDU Session Establishment:

- If the AMF is not able to determine the appropriate NRF to query for the S-NSSAI provided by the UE, the AMF sends a GET request to the NSSF. The AMF queries the NSSF with this specific S-NSSAI , the NF type of the NF service consumer, Requester ID, PLMN ID of the SUPI and location information.
- The NSSF determines and returns the appropriate NRF to be used to select NFs/services within the selected Network Slice instance. The NSSF may also return an NSI ID identifying the Network Slice instance to use for this S-NSSAI.
  When a PDU Session for a given S-NSSAI is established using a specific Network Slice instance, the CN provides to the (R)AN the S-NSSAI corresponding to this Network Slice instance to enable the R(AN) to perform access specific functions.

3
Managed Objects

The following NSSF managed objects can be configured using REST APIs :

- **NSI Profile:** The NSI Profile managed object enables customer to configure Network Slice Instance profile. This allows customer to create an Network Slice , by providing a name ,id, NRF url corresponding to the slice and list of Target AMF sets which support this slice.

Table 3-1 NSI Profile - Parameters

S.No	Field Name	Type	Description (With Default Values)
1	name	String	Network Slice Instance Profile Name.
2	nrfUri	String	URI of the Network Resource Function
3	nsiId	String	Network Slice Intance Identifier
5	regionId	String	Target AMF Region Id
6	setId	String	Target AMF Set Id
7	setFqdn	String	Target AMF Set Fqdn

Customer can configure NSI Profiles by following the information provided in the table below. The supported operations are **POST**, **GET**, **DELETE**, and **PUT**. The following table provides information about the REST APIs supported by the NSI Profile managed object.

Table 3-2 Supported REST APIs - NSI Profile

Resource Name	URI	Data Type	HTTP Method	Description
NSI Profiles	/nssf-configuration/v1/nsiprofiles	array(NssfNsiProfile)	POST	Create a network slice instance profile
			GET	Read all network slice instance profiles
NSI Profile	/nssf-configuration/v1/nsiprofiles/{name}	NsiProfile	GET	Read a network slice instance profile
			DELETE	Delete a network slice instance profile
			PUT	Update a network slice instance profile

- **NSS Rule:** The NSS Rule managed object enables customer to configure policy rules, NSS Rule allows customer to allow/reject/associate a Network slice based on NSSAI(SST and SD) , PLMN(MCC and MNC) ,TAC , AMF_ID. Operator can configure salience value to prioritize one rule over other.

Table 3-3 NSS Rule Parameters

S.No	Field Name	Type	Description (With Default Values)
1	name	String	Network Slice Selection Rule Name
2	amfId	String	AMF Identifier
3	plmnId	String	AMF Identifier
4	mcc	String	Mobile Country Code
5	mnc	String	Mobile Network Code
6	tac	String	AMF Identifier
8	sst	Integer	Slice/Service type
9	sd	String	Slice Differentiator
10	salience	Integer	Order of importance, higher salience, more important
12	grant	String	Whether the requested s-NSSAI is allowed or restricted
13	accesstype	String	Access Type in which the grant applies

Customer can configure NSS Rules by following the information provided in the table below. The supported operations are **POST**, **GET**, **DELETE**, and **PUT**. The following table provides information about the REST APIs supported by the NSS Rule managed object.

Table 3-4 Supported REST APIs - NSS Rule

Resource Name	URI	Data Type	HTTP Method	Description
NSS Rules	/nssf-configuration/v1/nssrules	array(NssfNssRule)	POST	Create a network slice selection rule
			GET	Read all network slice selection rules
NSS Rule	/nssf-configuration/v1/nssrules/{name}	NssRule	GET	Read a network slice selection rule
			DELETE	Delete a network slice selection rule
			PUT	Update a network slice selection rule

- **AMF Resolution:** The AMF Resolution managed object enables customer to configure mapping of list of candidate AMFs to a pair Target AMF set ID and Region ID. This enables operator to give static candidate AMF list. This configuration is used in cases where customer has disabled discovery service with NRF.

Table 3-5 AMF Resolution - Parameters

S.No	Field Name	Type	Description (With Default Values)
1	regionId	Integer	Region ID of the target AMF list
2	setId	Integer	Set ID of the target AMF list
3	fqdn	String	Fqdn of the target AMF list
4	instanceId	String	Instance ID of the target AMF list

Customer can configure AMF Resolution by following the information provided in the table below. The supported operations are **POST**, **GET**, **DELETE**, and **PUT**. The

following table provides information about the REST APIs supported by the AMF Resolution managed object.

Table 3-6 Supported REST APIS - AMF Resolution

Resource Name	URI	Data Type	HTTP Method	Description
AMF Resolutions	/nssf-configuration/v1/amfresolutions	array(NssfAmfResolution)	POST	Create a AMF resolution
			GET	Read all AMF resolutions
AMF Resolution	/nssf-configuration/v1/amfresoltuions/{region_id}[:{set_id}[:{instance_id}]]	NssfAmfResolution	GET	Read a AMF resolution
			DELETE	Delete a AMF resolution
			PUT	Update a AMF resolution

- **Configured NSSAI:** The Configured NSSAI managed object enables customer to configure default NSSAI based on one or more of the following parameters PLMN, TAC, AMF-ID. This enables operator to configure default behavior when none of the rules match and UE has set default indication flag to true.

Table 3-7 Configured NSSAI - Parameters

S.No	Field Name	Type	Description (With Default Values)
1	amfId	Integer	AMF Identifier
2	mcc	Integer	Mobile Country Code
3	mnc	Integer	Mobile Network Code
4	tac	Integer	AMF Identifier
5	salience	Integer	Order of importance, higher salience, more important
6	sst	Integer	Slice/Service type
	sd	String	Slice Differentiator

Customer can configure Configured NSSAI by following the information provided in the table below. The supported operations are **POST**, **GET**, **DELETE**, and **PUT**. The following table provides information about the REST APIs supported by the Configured NSSAI managed object.

Table 3-8 Supported REST APIs - Configured NSSAI

Resource Name	URI	Data Type	HTTP Method	Description
Configured NSSAIs	/nssf-configuration/v1/configurednssais	array(NssfConfiguredNssai)	POST	Create a configured NSSAI
			GET	Read all configured NSSAIs

Table 3-8 (Cont.) Supported REST APIs - Configured NSSAI

Configured NSSAI	/nssf-configuration/v1/configurednssais/{amf_id}:{mcc}:{mnc}[:{tac}[:{sst}:{sd}]]]	NssfConfiguredNssai	GET	Read a configured NSSAI
			DELETE	Delete a configured NSSAI

For a sample Open API Specification, see Open API Specification.

4
Configure NSSF using REST Interface

Before configuring NSSF using REST APIs, ensure that the NSSF is installed. For information on how to install NSSF, see the *OCNSSF Cloud Native Installation Guide*.

To Configure NSSF using REST APIs:

1. Configure the NSI-Profile managed object: NSI-Profile consists of network slice name and ID and NRF-ID ,Target AMF lists which are associated to the slice.
   - Request_Type: POST
   - URL: *http:///{apiRoot}/nssf-configuration/v1/nsiprofiles*
   - Body : Refer to Sample NSI-Profile-Body section for sample message/s and OpenApi for schema.

   REST message sample - NSI Profiles

   ```
   https://host:port/v1/nssf/configurations/nsiprofiles
   POST
   Content-Type: application/json
   BODY
   {
       "name": "NSI001",
       "nrfUri": "https://nrf.oracle.com",
       "nsiId": "1",
       "targetAmfSets":
       [
           {
               "regionId": "01",
               "setId": "001",
               "setFqdn": "set001.region01.amfset.
   5gc.mnc311.mcc282.3gppnetwork.org"
           },
           {
               "regionId": "01",
               "setId": "002",
               "setFqdn": "set002.region01.amfset.
   5gc.mnc311.mcc282.3gppnetwork.org"
           }
       ]
   }
   ```

2. Configure the NSS Rule managed object: NSS Rules are policy rules which enable operator to ALLOW/REJECT a request for Network Slice Selection request and If allowed then map to a Network Slice.
   - Request_Type: POST
   - URL: *http:///{apiRoot}/nssf-configuration/v1/nssrules*
   - Body : Refer to Sample NSS-Rule -Body section for sample message/s and OpenApi for schema.

   REST message sample - NSS Rules

```
https://host:port/v1/nssf/configurations/nssrules
POST
Content-Type: application/json
BODY
{
    "name": "NSSRULE01",
    "amfId": "1",
    "plmnId":
    {
        "mcc": "311",
        "mnc": "282",
    },
    "tac": "123",
    "snssai":
    {
        "sst": "1",
        "sd": "ABCDEF"
    },
    "salience": "0",
    "behavior":
    {
        "grant": "ALLOWED",
        "accessType": "3GPP_ACCESS",
        "nsiProfiles":
        [
            {
                "name": "NSI001",
                "salience": 1
            },
            {
                "name": "NSI002",
                "salience": 0
            }
        ]
    }
}
```

3. Configure the Configured NSSAI managed object: Configured NSSAI enables customer to configure default configures NSSAI based on one or more of the following parameters PLMN, TAC, AMF-ID .
   - Request_Type: POST
   - URL: *http://{apiRoot}/nssf-configuration/v1/configuredsnssais*
   - Body : Refer to Sample Configured-NSSAI-Body section for sample message/s and OpenApi for schema.

   REST message sample - AMF Resolutions

```
https://host:port/v1/nssf/configurations/amfresolutions
POST
Content-Type: application/json
BODY
{
    "regionId": "1",
    "setId": "1",
    "candidateAmfList":
    [
        {
            "fqdn": "pt01.set001.region01.amfset.
5gc.mnc311.mcc282.3gppnetwork.org",
            "instanceId": "ABCDEF"
```

```
        },
        {
            "fqdn": "pt02.set001.region01.amfset.
5gc.mnc311.mcc282.3gppnetwork.org",
            "instanceId": "ABCDEG"
        }
    ]
}
```

4. Configure the AMF Resolution managed object: AMF Resolution enables customer to configure mapping candidate amf list to a Target AMF set ID and Region ID.

   - Request_Type: POST
   - URL: *http:///{apiRoot}/nssf-configuration/v1/amfresolutions*
   - Body : Refer to Sample AMF Resolution-Body section for sample message/s and OpenApi for schema.

   REST message sample - Configured NSSAIs

```
https://host:port/v1/nssf/configurations/configuredsnssais
POST
Content-Type: application/json
BODY
{
    "amfId": "1",
    "plmn":
    {
        "mcc": "1",
        "mnc": "1",
    },
    "tac": "1",
    "salience": 0
    "nssai":
    [
        {
            "sst": 1,
            "sd": "ABC"
        },
        {
            "sst": 2,
            "sd": "DEF"
        }
    ]
}
```

For more information on APIs and managed object parameters, see Managed Objects.

5
NSSF Measurements

This section provides information about NSSF measurements. The NSSF application has added the following measurements.

- nsselection_reg_rx_total: Count of incoming Initial Register messages
- nsselection_reg_success_tx_total: Count of Initial Registration messages for which success response is sent
- nsselection_pdu_session_rx_total: Count of incoming PDU Session Establishment messages
- nsselection_pdu_session_success_tx_total: Count of PDU Session Establishment messages for which success response is sent

A

Open API Specification

This appendix provides a sample of Open API specification in NSSF.

Open API 3.0

```
openapi: 3.0.0
info:
  title: "NSSF-CONFIGURATION"
  version: v0.1
servers:
  - url: 'https://{apiRoot}/'
    variables:
      apiRoot:
        default: nssf
        description: >-
          apiRoot should be mentioned as defined in NSSF configuration script
paths:
  '/nssf-configuration/v1/nsiprofiles':
    post:
      summary: "Create a network slice instance profile"
      tags:
        - "Create a network slice instance profile"
      requestBody:
        content:
          application/json:    # Media type
            schema:            # Request body contents
              $ref: '#/components/schemas/NssfNsiProfile'
      responses:
        '201' :
          description: Created
        '403' :
          description: Forbidden
        '409' :
          description: Conflict
        '500' :
          description: Internal Server Error
        '503' :
          description: Service Unavailable
        default:
          description: Unexpected error
    get:
      summary: "Read all network slice instance profiles"
      tags:
        - "Read all network slice instance profiles"
      responses:
        '200' :
          description: OK
          content:
            application/json:
              schema:
                type: array
                items:
                  $ref: '#/components/schemas/NssfNsiProfile'
        '403' :
```

```
        description: Forbidden
      '500' :
        description: Internal Server Error
      '503' :
        description: Service Unavailable
      default:
        description: Unexpected error
'/nssf-configurations/v1/nsiprofiles/{name}':
  get:
    summary: "Read a network slice instance profile"
    tags:
      - "Read a network slice instance profile"
    parameters:
      - name: name
        in: path
        description: "network slice instance profile name"
        required: true
        schema:
          type: string
    responses:
      '200' :
        description: OK
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/NssfNsiProfile'
      '400' :
        description: Bad Request
      '403' :
        description: Forbidden
      '404' :
        description: Not Found
      '405' :
        description: Method Not Allowed
      '409' :
        description: Conflict
      '500' :
        description: Internal Server Error
      '502' :
        description: Bad Gateway
      '503' :
        description: Service Unavailable
      default:
        description: Unexpected error
  delete:
    summary: "Delete a network slice instance profile"
    tags:
      - "Delete a network slice instance profile"
    parameters:
      - name: name
        in: path
        description: "network slice instance profile name"
        required: true
        schema:
          type: string
    responses:
      '204' :
        description: No Content
      '403' :
        description: Forbidden
      '404' :
```

```
        description: No Found
      '500' :
        description: Internal Server Error
      '503' :
        description: Service Unavailable
      default:
        description: Unexpected error
'/nssf-configuration/v1/nssrules':
  post:
    summary: "Create a network slice selection rule"
    tags:
      - "Create a network slice selection rule"
    requestBody:
      content:
        application/json:    # Media type
          schema:            # Request body contents
            $ref: '#/components/schemas/NssfNssRule'
    responses:
      '201' :
        description: Created
      '403' :
        description: Forbidden
      '409' :
        description: Conflict
      '500' :
        description: Internal Server Error
      '503' :
        description: Service Unavailable
      default:
        description: Unexpected error
  get:
    summary: "Read all network slice selection rules"
    tags:
      - "Read all network slice selection rules"
    responses:
      '200' :
        description: OK
        content:
          application/json:
            schema:
              type: array
              items:
                $ref: '#/components/schemas/NssfNssRule'
      '403' :
        description: Forbidden
      '500' :
        description: Internal Server Error
      '503' :
        description: Service Unavailable
      default:
        description: Unexpected error
'/nssf-configuration/v1/nssrule/{name}':
  get:
    summary: "Read a network slice selection rule"
    tags:
      - "Read a network slice selection rule"
    parameters:
      - name: name
        in: path
        description: "network slice selection rule name"
        required: true
```

```
            schema:
              type: string
        responses:
          '200' :
            description: OK
            content:
              application/json:
                schema:
                  $ref: '#/components/schemas/NssfNssRule'
          '400' :
            description: Bad Request
          '403' :
            description: Forbidden
          '404' :
            description: Not Found
          '405' :
            description: Method Not Allowed
          '409' :
            description: Conflict
          '500' :
            description: Internal Server Error
          '502' :
            description: Bad Gateway
          '503' :
            description: Service Unavailable
          default:
            description: Unexpected error
      delete:
        summary: "Delete a network slice selection rule"
        tags:
          - "Delete a network slice selection rule"
        parameters:
          - name: name
            in: path
            description: "network slice selection rule name"
            required: true
            schema:
              type: string
        responses:
          '204' :
            description: No Content
          '403' :
            description: Forbidden
          '404' :
            description: No Found
          '500' :
            description: Internal Server Error
          '503' :
            description: Service Unavailable
          default:
            description: Unexpected error
  components:
    schemas:
      NssfNsiProfile:
        type: object
        properties:
          name:
            type: string
            description:  "Network Slice Instance Profile Name"
            minLength: 1
            maxLength: 255
```

```
          example: "Slice01"
        nrfUri:
          type:  string
          description: "URI of the Network Resource Function"
          minLength: 1
          maxLength: 255
          example: nrf.oracle.com
        nsiId:
          type: string
          description: "Network Slice Intance Identifier"
          minLength: 1
          maxLength: 255
        targetAmfSets:
          type: array
          description: "List of Target AMF Sets mapped to this Network Slice
Instance"
          items:
              $ref: '#/components/schemas/NssfTargetAmfSet'
          minItems: 1
      required:
        - name
        - nrfUri
        - targetAmfSets
    NssfTargetAmfSet:
      type: object
      properties:
        regionId:
          type: string
          description:  "Target AMF Region Id"
          minLength: 1
          maxLength: 2
          example: "01"
        setId:
          type: string
          description:  "Target AMF Set Id"
          minLength: 1
          maxLength: 3
          example: "001"
        setFqdn:
          type: string
          description: "Target AMF Set Fqdn"
          pattern: "^(([a-zA-Z0-9]|[a-zA-Z0-9][a-zA-Z0-9\\-]*[a-zA-Z0-9])\\.){2,}
([A-Za-z0-9]|[A-Za-z0-9][A-Za-z0-9\\-]*[A-Za-z0-9]){2,}$"
          example: "set001.region01.amfset.5gc.mnc311.mcc282.3gppnetwork.org"
      required:
        - regionId
        - setId
    NssfNssRule:
      type: object
      properties:
        name:
          type: string
          description:  "Network Slice Selection Rule Name"
          minLength: 1
          maxLength: 255
          example: "NSS-Rule01"
        amfId:
          type:  string
          description: "AMF Identifier"
          minLength: 1
          maxLength: 255
```

```
    plmnId:
      $ref: '#/components/schemas/PlmnId'
    tac:
      type: string
      description: "AMF Identifier"
      minLength: 1
      maxLength: 255
    snssai:
      $ref: '#/components/schemas/Snssai'
    salience:
      type: integer
      description: "Order of importance, higher salience, more important"
      minimum: 0
      maximum: 65535
    behavior:
      $ref: '#/components/schemas/NssfNssRuleBehavior'
  required:
    - name
    - nrfUri
    - snssai
    - behavior
PlmnId:
  type: object
  properties:
    mcc:
      type: string
      description: "Mobile Country Code"
      minLength: 1
      maxLength: 3
    mnc:
      type: string
      description: "Mobile Network Code"
      minLength: 1
      maxLength: 3
  required:
    - mcc
    - mnc
Snssai:
  type: object
  properties:
    sst:
      type: integer
      minimum: 0
      maximum: 255
    sd:
      type: string
      pattern: '^[A-Fa-f0-9]{6}$'
  required:
    - sst
NssfNssRuleBehavior:
  type: object
  properties:
    grant:
      type: string
      enum:
        - ALLOWED
        - RESTRICTED
      description: "Whether the requested S-NSSAI is allowed or restricted"
    accessType:
      type: string
      enum:
```

```
            - 3GPP_ACCESS
            - NON_3GPP_ACCESS
          description: "Access Type in which the grant applies"
        nsiProfiles:
          type: array
          items:
            properties:
              name:
                type: string
                description: "Network Slice Instance profile name"
              salience:
                type: integer
                description: "Order of importance, higher salience, more
important"
            required:
              - name
      required:
        - grant
        - accessType
```

This is the start of your topic.