

Oracle® Communications

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



Release 1.2
F21274-02
March 2020

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Copyright © 2019, 2020, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

1	What's New in This Guide	
<hr/>		
2	Introduction	
<hr/>		
	Introduction	2-1
	Network Slice Selection Policy	2-2
	Locate Product Documentation on the Oracle Help Center Site	2-3
	My Oracle Support	2-3
	Acronyms and Terminology	2-3
3	NSSF Supported Services	
<hr/>		
	Network Slice Selection Service	3-1
	Helm Parameters	3-4
	NSSAI Availability Service	3-5
4	NSSF Architecture	
<hr/>		
	NSSF Architecture	4-1
5	Managed Objects	
<hr/>		
6	Configure NSSF using REST Interface	
<hr/>		
7	NSSF Measurements	
<hr/>		
8	NSSF Alerts	
<hr/>		

List of Figures

2-1	Policy Configuration	2-2
3-1	Initial Register	3-1
3-2	PDU Session Establishment	3-3
3-3	UE-Config-Update	3-3
3-4	Update the S-NSSAIs the AMF supports per TA	3-5
3-5	Create a Subscription	3-6
3-6	Unsubscribe a Subscription	3-6
3-7	Update the AMF with any S-NSSAI restricted per TA	3-7
3-8	Delete the NSSAI Availability Information at NSSF	3-7
4-1	Network Slice Selection Function Architecture Diagram	4-1

List of Tables

2-1	Acronyms	2-3
5-1	NSI Profile - Parameters	5-1
5-2	Supported REST APIs - NSI Profile	5-1
5-3	NSS Rule Parameters	5-2
5-4	Supported REST APIs - NSS Rule	5-2
5-5	AMF Resolution - Parameters	5-2
5-6	Supported REST APIs - AMF Resolution	5-3
5-7	Configured NSSAI - Parameters	5-3
5-8	Supported REST APIs - Configured NSSAI	5-3
5-9	TimeProfile - Parameters	5-4
5-10	Supported REST APIs - Time Profile	5-4
5-11	Auth NSSAI - Parameters	5-4
5-12	Supported REST APIs - Auth NSSAI	5-5
8-1	NSSF Alert Details	8-1

1

What's New in This Guide

- IWF to support PCF discovery to find the PCF from BSF for AAA from P-DRA
- Diameter GW Integration with IWF

2

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 serve 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 following NSSF services:

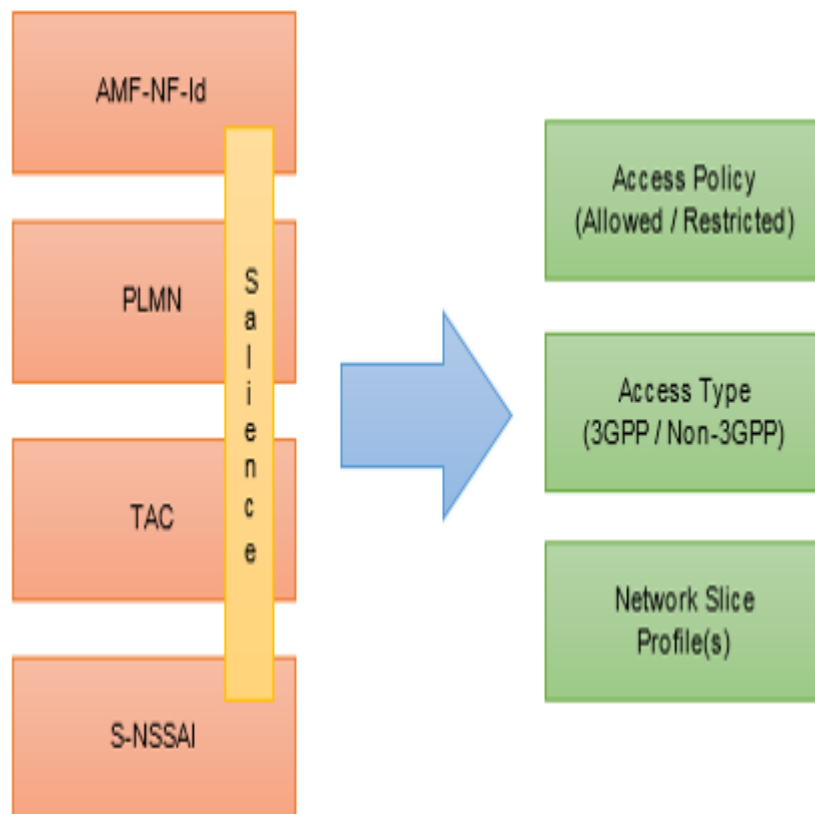
- Network Slice Selection service, *Nssf_NSSelection*. This service is used by an NF Service Consumer (AMF) to retrieve the information related to network slice. Network Slice Selection Service enables Network Slice selection in the serving Home Public Land Mobile Network (HPLMN).

- NSSAI Availability Service, Nnssf_NSSAIAvailability. This service is used by an NF Service Consumer (AMF) to update the S-NSSAI(s) the AMF supports on a per TA basis on the NSSF and to notify any change in status, on a per TA basis, of the SNSSAIs available per TA (unrestricted) and the restricted SNSSAI(s) per PLMN in that TA in the serving 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 2-1 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 NNSelection 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 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 the **Industries** link to display the **Industries Documentation** page.
3. Click **Oracle Communications**, select your product and respective release. A list of the documentation set for the selected product and release displays.
4. 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 2-1 Acronyms

Field	Description
5G-AN	5G Access Network
5GC	5G Core Network

Table 2-1 (Cont.) Acronyms

Field	Description
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
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

Table 2-1 (Cont.) Acronyms

Field	Description
UDR	Unified Data Repository
UDSF	Unstructured Data Storage Function

3

NSSF Supported Services

This section includes information about the service supported by NSSF.

Network Slice Selection Service

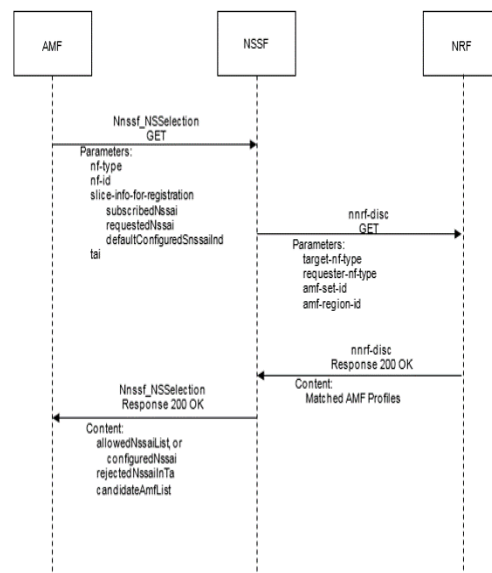
The Network Slice Selection service is identified by the service operation name, `Nnssf_NSSelection`. This service supports GET request during the following procedures by UE:

- **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:** When NSSF receives PDU-Session establishment request from NF consumer, NSSF determines network slice which can serve the requested SNSSAI, based on operator configured policies, and responds with URL of NRF which manages to the Slice and/or Slice ID of the matching Network Slice computed.
- **UE-Config-Update:** When the UDM updates the Subscribed S-NSSAI(s) to the serving AMF, based on configuration in this AMF, the NSSF determines the mapping of the configured NSSAI for the serving PLMN and ALLOWED NSSAI to the Subscribed S-NSSAI(s).

Initial Register

Following diagram illustrates the procedure of Initial Register:

Figure 3-1 Initial Register



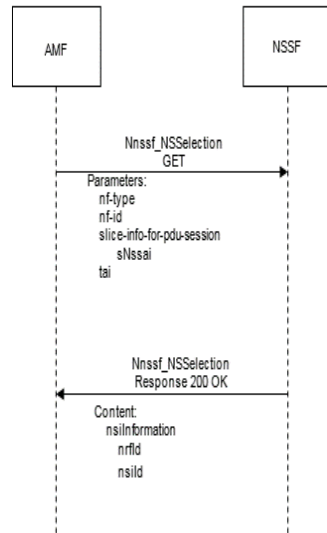
The following is performed for Initial Register:

- 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. For Helm parameters, see [Helm Parameters](#)
- 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 3-2 PDU Session Establishment



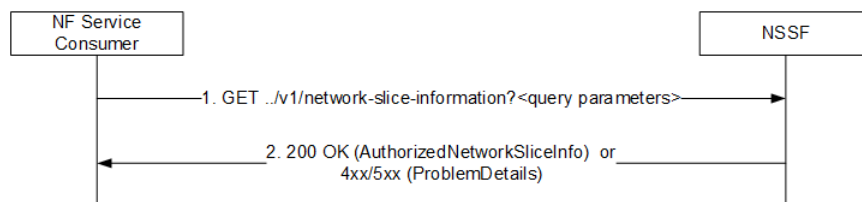
The following is performed for PDU Session Establishment:

- 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.

UE-Config-Update

When the UDM updates the Subscribed S-NSSAI(s) to the serving AMF, based on configuration in this AMF, the NSSF determines the mapping of the configured NSSAI for the serving PLMN and ALLOWED NSSAI to the Subscribed S-NSSAI(s). Following diagram illustrates the procedure of UE-Config-Update:

Figure 3-3 UE-Config-Update



The following is performed for UE-Config-Update:

- The AMF sends a UE-Config-Update (GET) request to NSSF. NSSF checks and validates the Subscribed S-NSSAI(s), Requested S-NSSAI(s), PLMN ID of the SUPI, TAI, NF type, and NF instance ID. If message is valid, NSSF searches for allowed S-NSSAI list based on policy configuration and input parameters.
- NSSF responds with 200 OK with AuthorizedNetworkSliceInfo in case NSSF finds a match.
- NSSF responds with 200 OK with empty AuthorizedNetworkSliceInfo in case there is no match found .
- NSSF responds with error code in case of incorrect parameter validation.

Helm Parameters

This section provides the information on NSSF Helm configurable parameters.

NrfDiscovery

When enabled, NSSF will send discovery request for each initial register message to get the Candidate AMF List corresponding to target AMF set selected.

- Acceptable values: True/False
- Default Value: False
- Properties:
 - Disclimit: When the **NrfDiscovery** parameter is enabled, this parameter signifies the maximum number of Candidateprofiles as discovery response.
 - Range (2,20)
 - Default 5
- Precondition: This will be applicable only when the **CandidateResolution** parameter is enabled.

Relevance

When enabled, NSSF will apply relevance algorithm to select/sort Candidate AMFs as a response to Initial register or UE-Config-Update requests which are part of selected Target AMF set.

- Acceptable values: True/False
- Default Value: False
- Preconditions:
 - This will be applicable only when the **CandidateResolution** parameter is enabled.
 - AMF must Update its capabilities to NssaiAvailability as per 29.531.

CandidateResolution

When enabled, NSSF will respond with Candidate AMF List in case when Initial Register message or UE-Config-Update message comes on NS-Selection service. When disabled NSSF will respond with Target AMF set and NRF.

- Acceptable values: True/False
- Default Value: False
- Properties:

- Maxcandidates: When the **CandidateResolution** parameter is enabled, this parameter signifies the maximum number of AMFs in Candidate AMF list returned to AMF by NSSF.
- Range (2,20)
- Default 5

NSSAI Availability Service

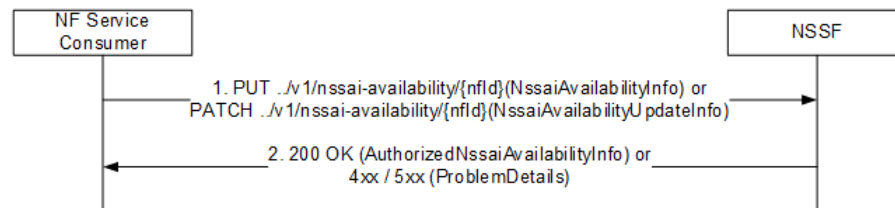
The NSSAI Availability service is identified by the service operation name, `Nnssf_NSSAIAvailability`. For the `Nnssf_NSSAIAvailability` service the following service operations are defined:

- Update
- Subscribe
- Unsubscribe
- Notify
- Delete

Update Service Operation

The AMF uses this operation to update the NSSF with the supported S-NSSAI(s) on a per TA basis and to get informed of the S-NSSAIs available per TA (unrestricted) and the restricted S-NSSAI(s) per PLMN in that TA in the serving PLMN of the UE.

Figure 3-4 Update the S-NSSAIs the AMF supports per TA



- The NF service consumer (e.g. AMF) sends a HTTP PUT message to NSSF with NSSAI availability information, identified by {nfId}, with `NssaiAvailabilityInfo` as body. Body of message contains a list of S-NSSAIs supported by AMF on a per TA basis.
- On receiving a PUT message, NSSF stores/updates the list in the session database.
- The NSSF authorizes the list based on NSSAI Auth rules and responds with the list of allowed S-NSSAIs for that AMF on a per TAI basis as per the request.

Subscribe Service Operation

The Subscribe operation is used by AMF to subscribe to a notification of any changes in status of the NSSAI availability information (e.g. S-NSSAIs available per TA and the restricted S-NSSAI(s) per PLMN in that TA in the serving PLMN of the UE) upon this is updated by another AMF.

Figure 3-5 Create a Subscription

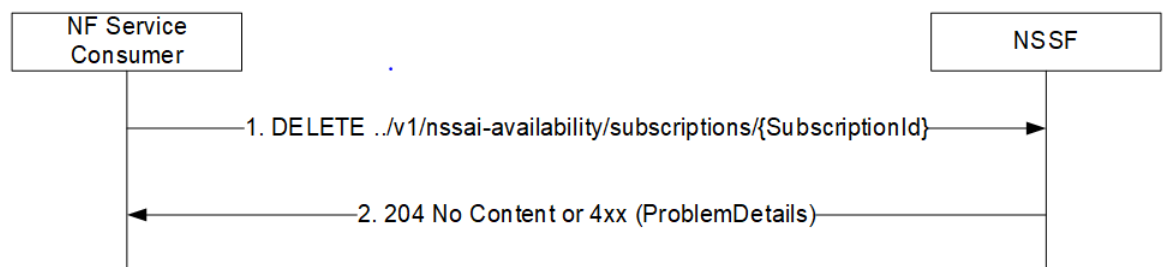


- AMF sends a POST request to NSSF with notification URL and a list of TAIs as JASON body.
- NSS stores the subscription request and responds with the list of allowed S-NSSAI/s per TAI for each TAI in the request. NSSF also returns a subscription-id and expiry (duration up to which NSSF ends notifications for any change in the status of Grant of S-NSSAI for subscribed TAI/s).

Unsubscribe Service Operation

The Unsubscribe operation is used by AMF to unsubscribe to a notification of any previously subscribed changes to the NSSAI availability information.

Figure 3-6 Unsubscribe a Subscription

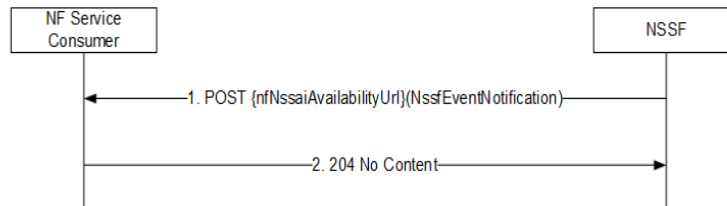


- AMF sends a Delete request to NSSF with sunscription-id.
- NSSF checks for active subscription with the id and if found, deletes the subscription. NSSF responds with 204.

Notify Service Operation

The Notify service operation shall be used by the NSSF to update the AMF with any change in status, on a per TA basis, of the S-NSSAIs available per TA (unrestricted) and the S-NSSAIs restricted per PLMN in that TA in the serving PLMN of the UE.

Figure 3-7 Update the AMF with any S-NSSAI restricted per TA

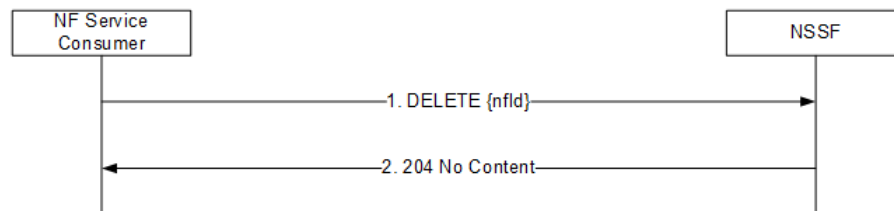


- NSSF sends notification to subscribed AMF when one or more following condition are true:
 - There is change at Grant rules on S-NSSAI corresponding to one or more of TAIs subscribed by AMF.
 - An S-NSSAI has been added or deleted for one or more of TAIs subscribed by AMF.

Delete Service Operation

The AMF uses this operation to delete the NSSAI Availability information stored for that AMF in the NSSF.

Figure 3-8 Delete the NSSAI Availability Information at NSSF



- The NF service consumer (e.g. AMF) sends a DELETE request to NSSF with {nflId}.
- The NSSF searches in session database for the NS-Availability data corresponding to nflId and deletes.

4

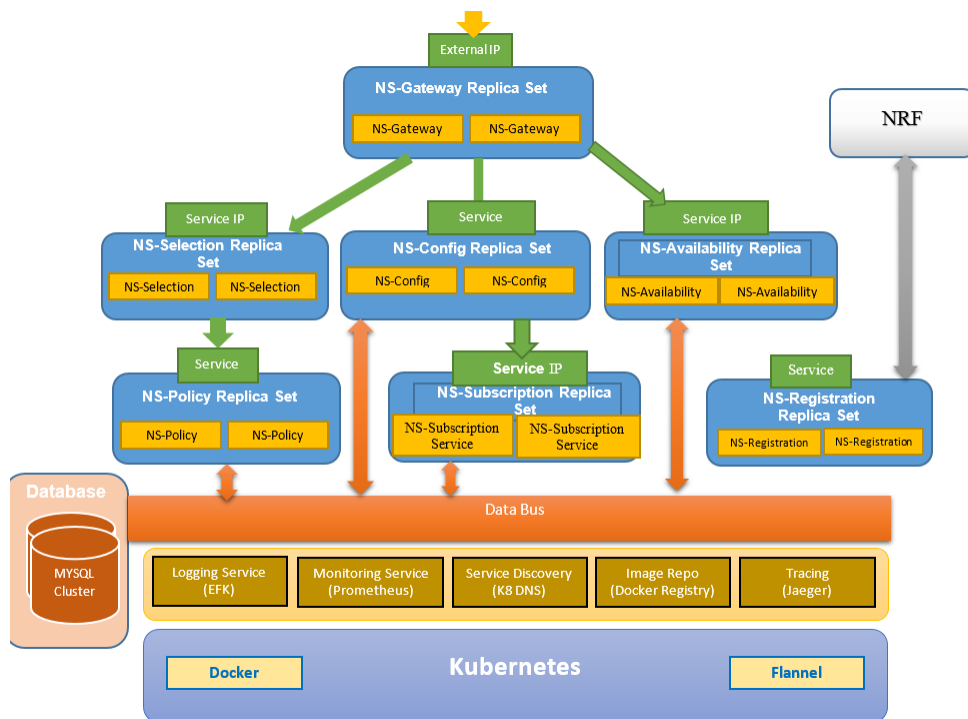
NSSF Architecture

This section provides a high-level OCNSSF architecture.

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 4-1 Network Slice Selection Function Architecture Diagram



The solution has the following components:

- **NS-Gateway (NSG):** This microservice is responsible for receiving the ingress traffic for NSSF and distribute the traffic to the appropriate NSSF Function (NSSelection, NSAvailability). NSG is also responsible to pegging traffic related measurements.

 **Note:**

API Gateway **Ambassador** is used to implement NS-Gateway.

- **NS-Selection MicroService (NSS):** This microservice receives all traffic for NS Selection Service. The microservice 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-Availability MicroService (NSA):** This microservice receives all traffic for NS Availability Service. The microservice maintains a list of allowed/rejected S-NSSAIs per TAI. It also provides AMF to get authorizes S-NSSAI list per TAI based on the S-NSSAIs supported by AMF.
- **NS-Policy MicroService (NSP):** This microservice performs the following functionalities:
 - This microservice performs the policy decision based on operator configured policy rules.
 - Initial Register/UE-Config-Update:
 - * Based on incoming requested NSSAI , Subscriber-NSSAI, PLMN, TAC, and AMF_ID, NSSF selects allowed and rejected network slices per access type.
 - * In case of successful selection of network slice, this service runs Discovery query to NRF to get candidate AMF list.
 - PDU Session Establishment:
 - * Based on incoming requested NSSAI, PLMN, TAC, and AMF_ID, AMF runs policy rules to find a single network slice.
- **NS-Subscription MicroService (NSS):** This microservice sends notifications to NF service consumer (AMF) which have subscribed for "S-NSSAI_STATUS_CHANGE_REPORT" if there is any change of allowed NSSAI on subscribed TAI list.
- **NS-Configuration MicroService (NSC):**
This microservice provides REST interface to configure NSS managed objects. For information on managed objects and REST APIs, See the *OCNSSF Cloud Native User's Guide*.
- **NS-Registration MicroService (NSR):**
This microservice registers with the NRF and sends periodic heartbeats.

1.NRF Regisration and Heartbeat

In this level, first the Registration profile is configured using helm. Then Performance service calculates load and capacity of NF. NsRegistration requests load and capacity from performance service and send it to NRF with heartbeat.

2.NRF Subscription

NSSF subscribes to NRF for AMF based on Target AMF Set and Region ID for Registration/Deregistration and load update.

5

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 5-1 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 Instance Identifier
4	targetAmfSets	array (TargetAmfSet)	array of TargetAmfSet (Refer primitive data type section)

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 5-2 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 5-3 NSS Rule Parameters

S.No	Field Name	Type	Description (With Default Values)
1	name	String	Network Slice Selection Rule Name
2	amfld	String	AMF Identifier
3	plmnId	String	Public Land Mobile Network ID (MCC:MNC)
4	tac	String	Tracking Area Code
5	snssai	Snssai	Single Network Slice Selection Assistance Information
6	saliency	Integer	Order of importance, higher saliency, more important
7	behaviour	Behaviour	

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 5-4 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}	NssfNssRule	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 5-5 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	candidateAmfList	array(candidateAmf)	Refer the primitive data type section

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 5-6 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/amfresolutions/{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 5-7 Configured NSSAI - Parameters

S.No	Field Name	Type	Description (With Default Values)
1	amfld	Integer	AMF Identifier
2	plmnid	plmn	Public Land Mobile Network ID (MCC:MNC)
3	tac	string	Tracking Area Code
4	salience	Integer	Order of importance, higher salience, more important
5	snssai	array(Snssai)	Refer to primitive datatype section

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 5-8 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 5-8 (Cont.) Supported REST APIs - Configured NSSAI

Resource Name	URI	Data Type	HTTP Method	Description
Configured NSSAI	/nssf-configuration/v1/configurednssais/{amf_id}:{mcc}:{mnc}[:{tac}[:{sst}:{sd}]]	NssfConfiguredNssai	GET	Read a configured NSSAI
			DELETE	Delete a configured NSSAI

Time Profile: The Time Profile managed object enables customer to configure time/date based slice selection policies. This allows customer to create a "Time Profile" and associate it to a network slice when creating a "NSS Rule" managed object.

Table 5-9 TimeProfile - Parameters

S.No	Field Name	Type	Description
1	name	String	Time Profile Name
2	startDate	Date	Date in the format of yy-mm-dd
3	endDate	Date	Date in the format of yy-mm-dd
4	daysOfWeek	array(DaysOfWeek)	Refer enumeration section
5	timespans	array(TimeSpan)	Refer primitive section

Customer can configure Time 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 Time Profile managed object.

Table 5-10 Supported REST APIs - Time Profile

Resource Name	URI	Data Type	HTTP Method	Description
Time Profiles	/nssf-configuration/v1/timeprofiles	array(TimeProfile)	POST	Create a time profile
			GET	Read all time profiles
Time Profile	/nssf-configuration/v1/timeprofiles	TimeProfile	GET	Read a time profile
			DELETE	Delete a time profile
			PUT	Update a time profile

Auth NSSAI: The Auth NSSAI managed object enables customer to configure network slice authentication rules by configuring Grant status (Allowed/Rejected_PLMN, Rejected_TAC) for S-Nssai on a per TAI basis.

Table 5-11 Auth NSSAI - Parameters

S.No	Field Name	Type	Description (With Default Values)
1	name	String	Network Slice Authentication Rule Name

Table 5-11 (Cont.) Auth NSSAI - Parameters

S.No	Field Name	Type	Description (With Default Values)
2	plmnId	plmnid	Public Land Mobile Network ID (MCC:MNC)
3	tac	string	Tracking Area Code
4	snssai	Snssai	Single Network Slice Selection Assistance Information
5	grant	Grant	Whether the requested s-NSSAI is allowed or restricted

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

Table 5-12 Supported REST APIs - Auth NSSAI

Resource Name	URI	Data Type	HTTP Method	Description
AuthNSSAIs	/nssf-configuration/v1/authNSSAI	array(AuthNSSAI)	POST	Create a AuthNSSAI Profile
			GET	Read all AuthNSSAI Profiles
AuthNSSAI	/nssf-configuration/v1/authNSSAI / {mcc}:{mnc}[:{tac}[:{sst}:{sd}]]	AuthNSSAI	GET	Read a AuthNSSAI Profile
			DELETE	Delete a AuthNSSAI Profile

For a sample Open API Specification, see [Open API Specification](#).

Primitive Tables

Behavior

Attribute	Datatype	Description
accessType	AccessType	Refer Enumeration section
nsiProfiles	array(NsiProfileMap)	Array of NsiProfile Map

TargetAmfSet

Attribute	Datatype	Description
regionId	string	region id of TargetAmfSet
setId	string	set id of TargetAmfSet
setFqdn	string	FQDN of TargetAmfSet

CandidateAmf

Attribute	Datatype	Description
fqdn	string	FQDN of targetamfset
instanceId	string	Instance id of Amf

Timespan

Attribute	Datatype	Description
startTime	time	start time in hh:mm:ss
endTime	time	end time in hh:mm:ss

Plmnid

Attribute	Datatype	Description
mcc	string	Mobile Country Code
mnc	string	Mobile Network Code

Snssai

Attribute	Datatype	Description
sst	integer	Slice /Service Type
sd	string	Slice Differentiator

Enumerations

Grant

Value	Description
"ALLOWED"	Allowed signifies SNSSAI is allowed in TAI
"REJECTED_IN_TA"	S-NSSAI is not allowed for Tracking Area
"REJECTED_IN_PLMN"	S-NSSAI is not allowed for PLMN

Access Type

Value	Description
"3GPP_ACCESS"	Specifies 5G network
"NON_3GPP_ACCESS"	Specifies non 5G network

DayofWeek

Value	Description
"MONDAY"	Monday, day of the week
"TUESDAY"	Tuesday, day of the week
"WEDNESDAY"	Wednesday, day of the week
"THURSDAY"	Thursday, day of the week
"FRIDAY"	Friday, day of the week
"SATURDAY"	Saturday, day of the week

Value	Description
"SUNDAY"	Sunday, day of the week

6

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 Time 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://host:port/nssf-configuration/v1/timeprofiles`
 - Body : Refer to Sample TimeProfile-Body section for sample message/s and OpenApi for schema.

REST message sample - Time Profiles

```
http://host:port/nssf-configuration/v1/timeprofiles
POST
```

```

Content-Type: application/json
BODY
{
  "name": "WEEKDAY-BUSY",
  "startDate": "2019-01-01",
  "endDate": "2019-01-01",
  "daysOfWeek":
  [
    "MONDAY", "TUESDAY", "WEDNESDAY", "THURSDAY", "FRIDAY"
  ]
  "timeSpans":
  [
    {
      "startTime": "09:00:00",
      "endTime": "12:00:00"
    },
    {
      "startTime": "16:00:00",
      "endTime": "21:00:00"
    }
  ]
}

```

3. Configure the Nssai Auth managed object:

- Request_Type: POST
- URL: *http://localhost:5755/nssf-configuration/v1/nssaiauth/*
- Body : Refer to Sample Nssai Auth -Body section for sample message/s and OpenApi for schema.

REST message sample - Nssai Auth

http://localhost:5755/nssf-configuration/v1/nssaiauth/

POST

```

{
  "name": "NSSAI-ATH-1",
  "plmnId":
  {
    "mcc": "100",
    "mnc": "101"
  },
  "tac": "100002",

  "snssai":
  {
    "sst": "1",
    "sd": "EMBB02"
  },
  "grant": "ALLOWED"
}

```

4. 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": "EMBB01"
  },
  "salience": "0",
  "behavior":
  {
    "grant": "ALLOWED",
    "accessType": "3GPP_ACCESS",
    "nsiProfiles":
    [
      {
        "name": "NSI001",
        "timeProfile": "WEEKDAY-BUSY",
        "salience": 1
      },
      {
        "name": "NSI002",
        "salience": 0
      }
    ]
  }
}

```

5. Configure the Configured NSSAI managed object: Configured NSSAI enables customer to configure default configured 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 - 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": "EMBB01"
      },
      {
        "sst": 2,
        "sd": "EMBB02"
      }
    ]
  }
}

```

6. 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 - 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": "01.102.01"
    },
    {
      "fqdn": "pt02.set001.region01.amfset.
5gc.mnc311.mcc282.3gppnetwork.org",
      "instanceId": "01.102.02"
    }
  ]
}

```

For more information on APIs and managed object parameters, see [#unique_22](#).

7

NSSF Measurements

Success Measurements

Tag	Dimensions	Description	Micro-service
nsselection_rx_total	AMF Instance Id, Message Type	Count of request messages received by NSSF for the Nnssf_NSSelection service	NSSelection
nsselection_success_tx_total	AMF Instance Id, Message Type	Count of success response messages sent by NSSF for requests for the Nnssf_NSSelection service	NSSelection
nssaiavailability_rx_total	Operation	Count of request messages received by NSSF for the Nnssf_NSSAIAvailability service	NSAvailability
nssaiavailability_success_tx_total	Operation	Count of success response messages sent by NSSF for requests for the Nnssf_NSSAIAvailability service	NSAvailability
nsselection_policy_match	AMF Instance Id, Message Type Policy Rule Name	Count of policy matches found during processing of request messages for the Nnssf_NSSelection service	NSPolicy
nsselection_time_match	AMF Instance Id, Message Type, Time Profile Name	Count of time profile matches found during processing of request messages for the Nnssf_NSSelection service	NSPolicy
nsselection_nsi_selected	AMF Instance Id, Message Type, NSI Profile Name	Count of Network Slice Instances selected during processing of request messages for the Nnssf_NSSelection service	NSPolicy
nsselection_nrf_disc	None	Count of NRF discoveries performed during processing of request messages for the Nnssf_NSSelection service	NSPolicy
nsselection_nrf_disc_success	None	Count of successful discovery results received from NRF during processing of request messages for the Nnssf_NSSelection service	NSPolicy
nssaiavailability_tx_total	Subscription- Id	Count of notification messages sent by NSSF as part of Nnssf_NSSAIAvailability service	NSSubscription

Tag	Dimensions	Description	Micro-service
nssaiavailability_succe s_rx_total	Subscription- Id	Count of success notification response messages received by NSSF for requests for the Nssf_NSSAIAvailability service	NSSubscription

Error Measurements

Tag	Dimensions	Description	Micro-service
nssf_configuration_database_read_error	None	Count of errors encountered when trying to read the configuration database	NSPolicy
nssf_configuration_database_write_error	None	Count of errors encountered when trying to write to the configuration database	NSConfig
nssf_state_data_read_error	None	Count of errors encountered when trying to read the state database	NSPolicy
nssf_state_data_write_error	None	Count of errors encountered when trying to write to the state database	NSAvailability
nsselection_nrf_disc_failure	None	Count of errors encountered when trying to reach the NRF's discovery service	NSPolicy
nsselection_policy_not_found	AMF Instance Id, Message Type	Count of request messages that did not find a configured policy	NSPolicy
nsselection_nrf_retrys	Method	Count of retry attempts sent to NRF	NRFClient
nssaiavailability_subscription_failure	Operation	Count of subscribe requests rejected by NSSF	NSAvailability
nssaiavailability_notification_failure	Subscription-Id	Count of failure notification response messages received by NSSF for requests for the Nssf_NSSAIAvailability service	NSSubscription

8

NSSF Alerts

This section includes information about alerts for OCNSSF.

Table 8-1 NSSF Alert Details

Name	Severity	Condition	Description
ocnssfPolicyNotFoundWarn	Warning	rate(nsselection_policy_match) <= 95%	Rate of messages that did not find a matching policy is above warning threshold (Threshold: \diamond, Current: \diamond)
ocnssfPolicyNotFoundMaj	Major	rate(nsselection_policy_match) <= 85%	Rate of messages that did not find a matching policy is above major threshold
ocnssfPolicyNotFoundCrit	Critical	rate(nsselection_policy_match) <= 70%	Rate of messages that did not find a matching policy is above critical threshold
ocnssfNrfDiscFailedWarn	Warning	rate(nsselection_nrf_discovery_failure) >= 10%	Rate of failed NRF discovery attempts is above warning threshold
ocnssfNrfDiscFailedMaj	Major	rate(nsselection_nrf_discovery_failure) >= 30%	Rate of failed NRF discovery attempts is above major threshold
ocnssfNrfDiscFailedCrit	Critical	rate(nsselection_nrf_discovery_failure) >= 50%	Rate of failed NRF discovery attempts is above critical threshold
ocnssfNotificationFailureWarn	Warning	rate(nssaiavailability_notification_failure) >= 10	Rate of failed attempts to send Notification to AMF
ocnssfNotificationFailureMaj	Major	rate(nssaiavailability_notification_failure) >= 30	Rate of failed attempts to send Notification to AMF
ocnssfNotificationFailureCrit	Critical	rate(nssaiavailability_notification_failure) >= 50	Rate of failed attempts to send Notification to AMF

For NSSF Alerts configuration, please refer to *OCNSSF Installation and Upgrade Guide*.

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
'/nssf-configuration/v1/nssaiauth':
  post:
    summary: "Create a network slice authentication rule"
    tags:
      - "Create a network slice authentication rule"
    requestBody:
      content:
        application/json: # Media type
          schema: # Request body contents
            $ref: '#/components/schemas/NssfNssaiAuth'

```

```

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 authentication rules"
  tags:
    - "Read all network slice authentication rules"
  responses:
    '200' :
      description: OK
      content:
        application/json:
          schema:
            type: array
            items:
              $ref: '#/components/schemas/NssfNssaiAuth'
    '403' :
      description: Forbidden
    '500' :
      description: Internal Server Error
    '503' :
      description: Service Unavailable
default:
  description: Unexpected error
'/nssf-configuration/v1/nssaiauth/{name}':
get:
  summary: "Read a network slice authentication rule"
  tags:
    - "Read a network slice selection rule"
  parameters:
    - name: name
      in: path
      description: "network slice authentication rule name"
      required: true
      schema:
        type: string
  responses:
    '200' :
      description: OK
      content:
        application/json:
          schema:
            $ref: '#/components/schemas/NssfNssaiAuth'
    '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 authentication rule"
  parameters:
    - name: name
      in: path
      description: "network slice authentication 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:
    NssfNsiAuth:
      type: object
      properties:
        name:
          type: string
          description: "Authentication Rule Name"
          minLength: 1
          maxLength: 255
          example: "AUTH-RULE-1"
        plmnId:
          $ref: '#/components/schemas/PlmnId'
        tac:
          type: string
          description: "AMF Identifier"
          minLength: 1
          maxLength: 255
        snssai:
          $ref: '#/components/schemas/Snssai'
        grant:
          $ref: '#/components/schemas/Grant'
    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
    nsId:
        type: string
        description: "Network Slice Instance 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:
        $ref: '#/components/schemas/NssfNssRuleBehavior'
required:
  - name
  - nrfUri
  - snssai
  - behavior
PlmnId:
  type: object
  properties:
    mcc:
      type: string
      description: "Mobile Country Code"
      minLength: 1
      maxLength: 3
    mnc:
      type: string
      description: "Mobile Network Code"
      minLength: 1
      maxLength: 3
  required:
    - mcc
    - mnc
Snssai:
  type: object
  properties:
    sst:
      type: integer
      minimum: 0
      maximum: 255
    sd:
      type: string
      pattern: '^[A-Za-f0-9]{6}$'
  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:
    - accessType
```