ETSI TS 123 288 V16.11.0 (2022-07)

5G;
Architecture enhancements for 5G System (5GS)
to support network data analytics services
(3GPP TS 23.288 version 16.11.0 Release 16)

Reference
RTS/TSGS-0223288vgb0

Keywords
5G

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document defines the Stage 2 architecture enhancements for 5G System (5GS) to support network data analytics services in 5G Core network.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[3] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[4] 3GPP TS 23.503: "Policy and Charging Control Framework for the 5G System; Stage 2".

[5] Void.

[6] 3GPP TS 28.532: "Management and orchestration; Generic management services".

[7] 3GPP TS 28.550: "Management and orchestration; Performance Assurance".

[8] 3GPP TS 28.552: "Management and orchestration; 5G performance measurements".

[9] 3GPP TS 28.545: "Management and orchestration; Fault Supervision (FS)".

[10] 3GPP TS 28.554: "Management and orchestration; 5G end to end Key Performance Indicators (KPI)".

[11] ITU-T Recommendation P.1203.3: "Parametric bitstream-based quality assessment of progressive download and adaptive audiovisual streaming services over reliable transport - Quality integration module".

[12] 3GPP TS 38.215: "NR; Physical layer measurements".

[13] Void.

[14] 3GPP TS 38.331: "NR; Radio Resource Control (RRC) protocol specification".

[15] 3GPP TS 36.331: "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification".

[16] 3GPP TS 38.413: "NG-RAN; NG Application Protocol (NGAP)".

[17] 3GPP TS 29.244: "Interface between the Control Plane and the User Plane Nodes".

[18] 3GPP TS 29.510: "5G System; Network function repository services; Stage 3".

[19] 3GPP TS 28.533: "Management and orchestration; Architecture framework".

[20] 3GPP TS 37.320: "Radio measurement collection for Minimization of Drive Tests (MDT); Overall description; stage 2".

[21] 3GPP TS 28.201: "Charging management; Network slice performance and analytics charging in the 5G System (5GS); stage 2".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1], TS 23.501 [2] and TS 23.503 [4]. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1], TS 23.501 [2] and TS 23.503 [4] apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

4 Reference Architecture for Data Analytics

4.1 General

The NWDAF (Network Data Analytics Function) is part of the architecture specified in TS 23.501 [2] and uses the mechanisms and interfaces specified for 5GC in TS 23.501 [2] and OAM services (see clause 6.2.3.1).

The NWDAF interacts with different entities for different purposes:

- Data collection based on subscription to events provided by AMF, SMF, PCF, UDM, AF (directly or via NEF), and OAM;
- Retrieval of information from data repositories (e.g. UDR via UDM for subscriber-related information);
- Retrieval of information about NFs (e.g. from NRF for NF-related information);
- On demand provision of analytics to consumers, as specified in clause 6.

A single instance or multiple instances of NWDAF may be deployed in a PLMN. If multiple NWDAF instances are deployed, the architecture supports deploying the NWDAF as a central NF, as a collection of distributed NFs, or as a combination of both.

NOTE 1: When multiple NWDAFs exist, not all of them need to be able to provide the same type of analytics results, i.e., some of them can be specialized in providing certain types of analytics. An Analytics ID information element is used to identify the type of supported analytics that NWDAF can generate.

NOTE 2: NWDAF instance(s) can be collocated with a 5GS NF.

4.2 Non-roaming architecture

As depicted in Figure 4.2-1, the 5G System architecture allows NWDAF to collect data from any 5GC NF. The NWDAF belongs to the same PLMN as the 5GC NF that provides the data.

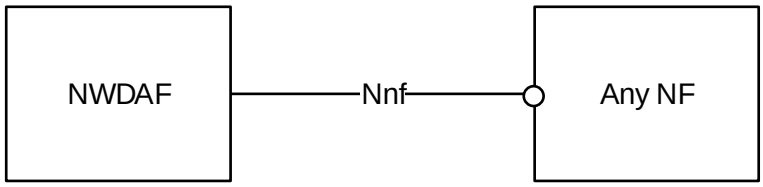

Figure 4.2-1: Data Collection architecture from any 5GC NF

The Nnf interface is defined for the NWDAF to request subscription to data delivery for a particular context, to cancel subscription to data delivery and to request a specific report of data for a particular context.

The 5G System architecture allows NWDAF to retrieve the management data from OAM by invoking OAM services.

As depicted in Figure 4.2-2, the 5G System architecture allows any 5GC NF to request network analytics information from NWDAF. The NWDAF belongs to the same PLMN as the 5GC NF that consumes the analytics information.

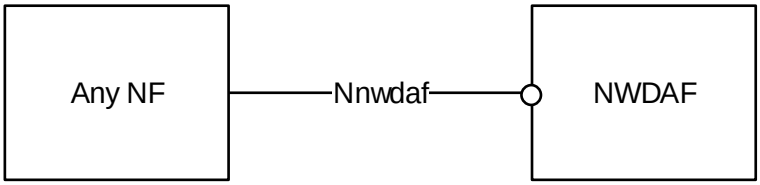

Figure 4.2-2: Network Data Analytics Exposure architecture

The Nnwdaf interface is defined for 5GC NFs, to request subscription to network analytics delivery for a particular context, to cancel subscription to network analytics delivery and to request a specific report of network analytics for a particular context.

NOTE: The 5G System architecture also allows other consumers such as OAM and CEF (Charging Enablement Function) to request network analytics information from NWDAF.

4.3 Roaming architecture

The interactions between the NWDAF and the other 5GC NFs are only considered in the same PLMN case.

Roaming architecture does not apply in this release of the specification.

5 Network Data Analytics Functional Description

5.1 General

The NWDAF provides analytics to 5GC NFs, and OAM as defined in clause 7.

Analytics information are either statistical information of the past events, or predictive information.

Different NWDAF instances may be present in the 5GC, with possible specializations per type of analytics. The capabilities of a NWDAF instance are described in the NWDAF profile stored in the NRF.

In order to support NFs that are consumers of analytics with the discovery of a NWDAF instance that is able to provide some specific type of analytics, each NWDAF instance should provide the list of Analytics ID(s) that it supports when registering to the NRF, in addition to other NRF registration elements of the NF profile. Other NFs requiring the discovery of an NWDAF instance that provides support for some specific type of analytics may query the NRF and include the Analytics ID(s) that identifies the desired type of analytics for that purpose.

The consumers i.e. 5GC NFs and OAM decide how to use the data analytics provided by NWDAF.

The interactions between 5GC NF(s) and the NWDAF take place within a PLMN.

The NWDAF has no knowledge about NF application logic. The NWDAF may use subscription data but only for statistical purpose.

5.2 NWDAF Discovery and Selection

The NWDAF service consumer selects an NWDAF that supports requested analytics information by using the NWDAF discovery principles defined in clause 6.3.13, TS 23.501 [2].

6 Procedures to Support Network Data Analytics

6.0 General

This clause specifies procedures to support network data analytics function.

Clause 6.1 and clause 6.2 specify generic procedures which apply to all type of analytics, while clause 6.3 and onwards specify procedures specific to some type of analytics.

6.1 Procedures for analytics exposure

6.1.1 Analytics Subscribe/Unsubscribe

6.1.1.1 Analytics subscribe/unsubscribe by NWDAF service consumer

This procedure is used by any NWDAF service consumer (e.g. including NFs/OAM) to subscribe/unsubscribe at NWDAF to be notified on analytics information, using Nnwdaf_AnalyticsSubscription service defined in clause 7.2. This service is also used by an NWDAF service consumer to modify existing analytics subscription(s). Any entity can consume this service as defined in clause 7.2.

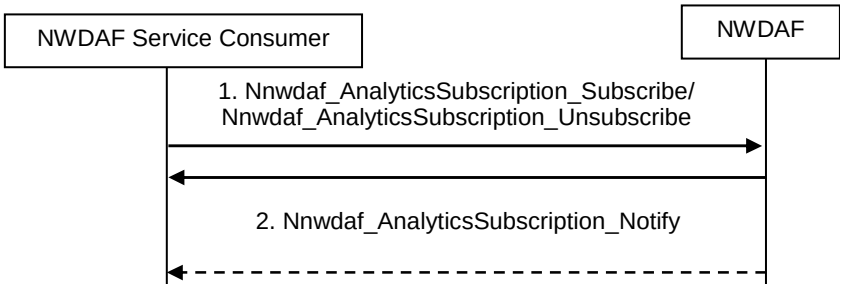

Figure 6.1.1.1-1: Network data analytics Subscribe/unsubscribe

1. The NWDAF service consumer subscribes to or cancels subscription to analytics information by invoking the Nnwdaf_AnalyticsSubscription_Subscribe/ Nnwdaf_AnalyticsSubscription_Unsubscribe service operation. The parameters that can be provided by the NWDAF service consumer are listed in clause 6.1.3.

   When a subscription to analytics information is received, the NWDAF determines whether triggering new data collection is needed.

   If the service invocation is for a subscription modification, the NF service consumer includes an identifier (Subscription Correlation ID) to be modified in the invocation of Nnwdaf_AnalyticsSubscription_Subscribe.

2. If NWDAF service consumer subscribes to analytics information, the NWDAF notifies the NWDAF service consumer with the analytics information by invoking Nnwdaf_AnalyticsSubscription_Notify service operation, based on the request from the NWDAF service consumer, e.g. Analytics Reporting Parameters.

6.1.1.2 Analytics subscribe/unsubscribe by AFs via NEF

The analytics exposure to AFs may be performed via NEF by using analytics subscription to NWDAF.

Figure 6.1.1.2-1 illustrates the interaction between AF and NWDAF performed via the NEF.

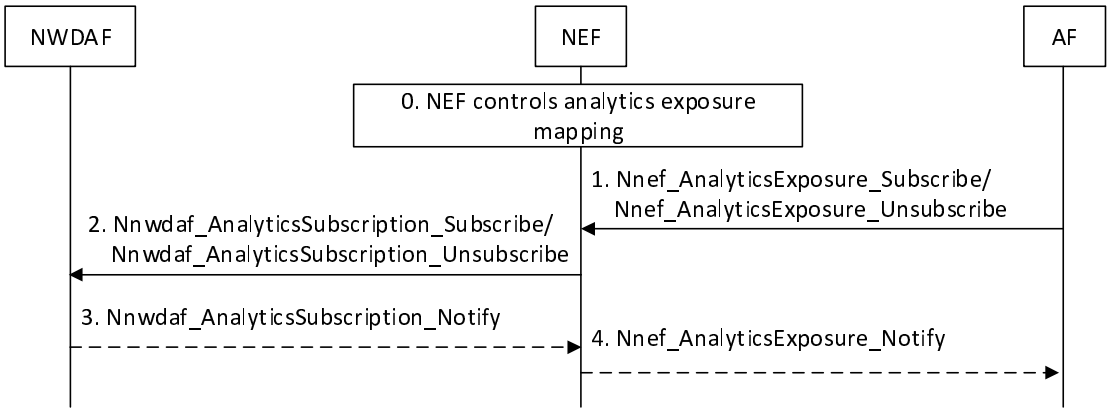

Figure 6.1.1.2-1: Procedure for analytics subscribe/unsubscribe by AFs via NEF

0. NEF controls the analytics exposure mapping among the AF identifier with allowed Analytics ID, and associated inbound restrictions (i.e, applied to subscription of the Analytics ID for an AF) and/or outbound restrictions (i.e., applied to notification of Analytics ID to an AF).

   In this Release, AF is configured with the appropriated NEF to subscribe to analytics information, the allowed Analytics ID(s), and with allowed inbound restrictions (i.e., parameters and/or parameter values) for subscription to each Analytics ID.

1. The AF subscribes to or cancels subscription to analytics information via NEF by invoking the Nnef_AnalyticsExposure_Subscribe/ Nnef_AnalyticsExposure_Unsubscribe service operation defined in TS 23.502 [3]. If the AF wants to modify an existing analytics subscription at NEF, it includes an identifier (Subscription Correlation ID) to be modified in the invocation of Nnef_AnalyticsExposure_Subscribe. If the analytics information subscription is authorized by the NEF, the NEF proceeds with the steps below.

2. Based on the request from the AF, the NEF subscribes to or cancels subscription to analytics information by invoking the Nnwdaf_AnalyticsSubscription_Subscribe/ Nnwdaf_AnalyticsSubscription_Unsubscribe service operation.

   If the parameters and/or parameters values of the AF request comply with the inbound restriction in the analytics exposure mapping, NEF forwards in the subscription to NWDAF service the Analytics ID, parameters and/or parameters values from the AF request.

   If the request from AF does not comply with the restrictions in the analytics exposure mapping, NEF may apply restrictions to the subscription request to NWDAF (e.g., restrictions to parameters or parameter values of the Nnwdaf_AnalyticsSubscription_Subscribe service operations), based on operator configuration and/or may apply parameter mapping (e.g. geo coordinate mapping to TA(s)/Cell-id(s)).

   The NEF records the association of the analytics request from the AF and the analytics request sent to the NWDAF.

   The NEF selects an NWDAF that supports analytics information requested by the AF using the NWDAF discovery procedure defined in TS 23.501 [2].

   If the AF request is for a modification of the existing analytics subscription(s), the NEF invokes Nnwdaf_AnalyticsSubscription_Subscribe to modify the analytics subscription identified by an identifier (Subscription Correlation ID) associated with the AF.

3. If the NEF has subscribed to analytics information, the NWDAF notifies the NEF with the analytics information by invoking Nnwdaf_AnalyticsSubscription_Notify service operation.

4. If the NEF receives the notification from the NWDAF, the NEF notifies the AF with the analytics information by invoking Nnef_AnalyticsExposure_Notify service operation defined in TS 23.502 [3]. NEF may apply outbound restrictions to the notifications to AFs (e.g., restrictions to parameters or parameter values of the Nnef_AnalyticsExposure_Notify service operation) based on analytics exposure mapping and may apply parameter mapping for external usage (e.g. TA(s), Cell-id(s) to geo coordinate).

6.1.2 Analytics Request

6.1.2.1 Analytics request by NWDAF service consumer

This procedure is used by the NWDAF service consumer (e.g. including NFs/OAM) to request and get from NWDAF analytics information, using Nnwdaf_AnalyticsInfo service defined in clause 7.3.

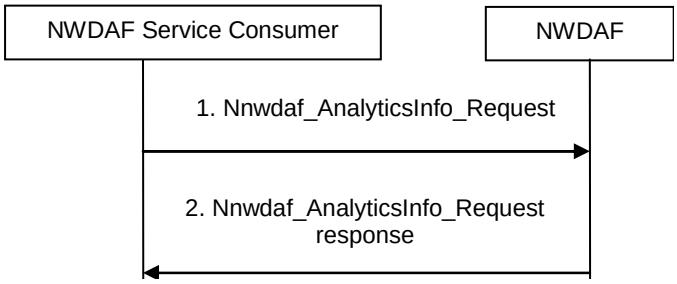

Figure 6.1.2.1-1: Network data analytics Request

1. The NWDAF service consumer requests analytics information by invoking Nnwdaf_AnalyticsInfo_Request service operation. The parameters that can be provided by the NWDAF service consumer are listed in clause 6.1.3.

   When a request for analytics information is received, the NWDAF determines whether triggering new data collection is needed.

2. The NWDAF responds with analytics information to the NWDAF service consumer.

6.1.2.2 Analytics request by AFs via NEF

The analytics exposure to AFs may be performed via NEF by using analytics request to NWDAF.

Figure 6.1.2.2-1 illustrates the interaction between AF and NWDAF performed via the NEF.

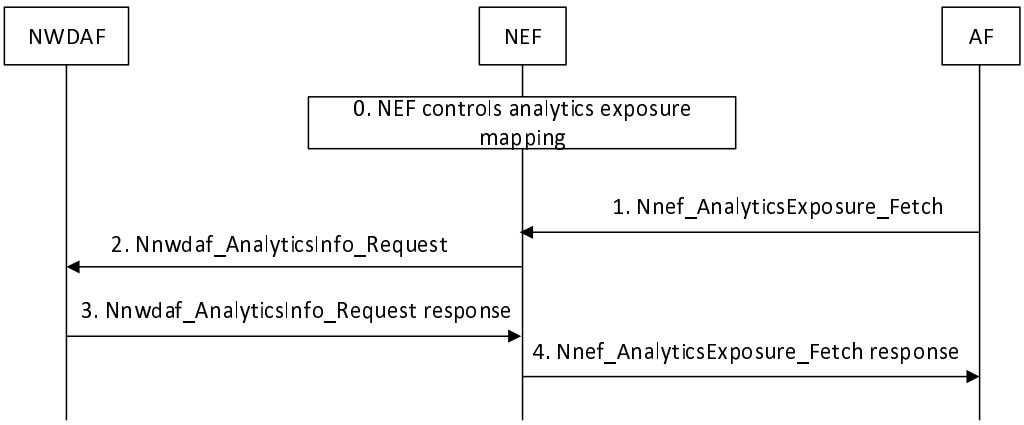

Figure 6.1.2.2-1: Procedure for analytics request by AFs via NEF

0. NEF controls the analytics exposure mapping among the AF identifier with allowed Analytics ID(s), and associated inbound restrictions (i.e., applied to the Analytics ID requested by AF, and/or outbound restrictions (i.e., applied to the response of Analytics ID to AF).

   In this Release, AF is configured, e.g., via static OAM configuration, with the appropriated NEF to subscribe to analytics information, the allowed Analytics ID(s), and with allowed inbound restrictions (i.e., parameters and/or parameter values) for requesting each Analytics ID.

1. The AF requests to receive analytics information via NEF by invoking the Nnef_AnalyticsExposure_Fetch service operation defined in TS 23.502 [3]. If the analytics information request is authorized by the NEF, the NEF proceeds with the steps below.

2. Based on the request from the AF, the NEF requests analytics information by invoking the Nnwdaf_AnalyticsInfo_Request service operation.

   If the parameters and/or parameters values of the AF request comply with the restriction in the analytics exposure mapping, NEF forwards in the subscription to NWDAF service the Analytics ID, parameters and/or parameters values from AF in the request to NWDAF.

   If the request from AF does not comply with the restrictions in the analytics exposure mapping, NEF may apply restrictions to the request to NWDAF (e.g., restrictions to parameters or parameter values of the Nnwdaf_AnalyticsInfo_Request service operations) based on operator configuration and/or may apply parameter mapping (e.g. geo coordinate mapping to TA(s), Cell-id(s)).

   The NEF records the association of the analytics request from the AF and the analytics request sent to the NWDAF.

   The NEF selects an NWDAF that supports analytics information requested by the AF using the NWDAF discovery procedure defined in TS 23.501 [2].

3. The NWDAF responds with the analytics information to the NEF.

4. The NEF responds with the analytics information to the AF. NEF may apply restrictions to the response to AFs (e.g., restrictions to parameters or parameter values of the Nnef_AnalyticsExposure_Fetch response service operation) based on operator configuration.

6.1.3 Contents of Analytics Exposure

The consumers of the Nnwdaf_AnalyticsSubscription or Nnwdaf_AnalyticsInfo service operations described in clause 7 provide the following input parameters listed below.

- A list of Analytics ID(s): identifies the requested analytics.

- Analytics Filter Information: indicates the conditions to be fulfilled for reporting Analytics Information. This set of optional parameter types and values enables to select which type of analytics information is requested. Analytics Filter Information are defined in procedures.

- Target of Analytics Reporting: indicates the object(s) for which Analytics information is requested, entities such as specific UEs, a group of UE(s) or any UE (i.e. all UEs).

- (Only for Nnwdaf_AnalyticsSubscription) A Notification Target Address (+ Notification Correlation ID) as defined in TS 23.502 [3] clause 4.15.1, allowing to correlate notifications received from NWDAF with this subscription.

- Analytics Reporting Information with the following parameters:

  - (Only for Nnwdaf_AnalyticsSubscription) Analytics Reporting Parameters as per Event Reporting parameters defined in Table 4.15.1-1, TS 23.502 [3].

  - (Only for Nnwdaf_AnalyticsSubscription) Reporting Thresholds, which indicate conditions on the level of each requested analytics that when reached shall be notified by the NWDAF. A matching direction may be provided such as below, above, or crossed. If no matching direction is provided, the default direction is crossed.

- Analytics target period: time interval [start..end], either in the past (both start time and end time in the past) or in the future (both start time and end time in the future). An Analytics target period in the past is a request or subscription for statistics. An Analytics target period in the future is a request or subscription for predictions. The time interval is expressed with actual start time and actual end time (e.g. via UTC time). When the Analytics Reporting Parameters indicate a periodic reporting mode, the time interval can also be expressed as positive or negative offsets to the reporting time, which indicates a subscription for predictions or statistics respectively. By setting start time and end time to the same value, the consumer of the analytics can request analytics or subscribe to analytics for a specific time rather than for a time interval.

- Preferred level of accuracy of the analytics (e.g. Low/High).

- (Only for Nnwdaf_AnalyticsInfo_Request) Time when analytics information is needed (if applicable). If the time is reached the consumer does not need to wait for the analytics information any longer, yet the NWDAF may send an error response to the consumer.

- [OPTIONAL] Maximum number of objects requested by the consumer (max) to limit the number of objects in a list of analytics per Nnwdaf_AnalyticsSubscription_Notify or Nnwdaf_AnalyticsInfo_Request response.

- [OPTIONAL] Maximum number of SUPIs (SUPImax) requested by the consumer to limit the number of SUPIs in an object. When SUPImax is not provided, the NWDAF shal return all SUPIs concerned by the analytics object. When SUPImax is set to 0, the NWDAF shall not provide any SUPI.

The NWDAF provides to the consumer of the Nnwdaf_AnalyticsSubscription or Nnwdaf_AnalyticsInfo service operations described in clause 7, the output information listed below:

- (Only for Nnwdaf_AnalyticsSubscription) The Notification Correlation Information.

- For each Analytics ID the analytics information in the requested Analytics target period.

- In addition, the following additional information:

  - Timestamp of analytics generation, which allows consumers to decide until when the received information shall be used. For instance, an NF can deem a received notification from NWDAF for a given feedback as invalid based on this timestamp;

  - Validity period, which defines the time period for which the analytics information is valid.

  - Probability assertion: confidence in prediction.

6.2 Procedures for Data Collection

6.2.1 General

The Data Collection feature permits NWDAF to retrieve data from various sources (e.g. NF such as AMF, SMF, PCF, and AF; OAM), as a basis of the computation of network analytics.

All available data encompass:

- OAM global NF data,

- Data available in NFs, e.g. behaviour data related to individual UEs or UE groups (e.g. UE reachability), and pre-computed metrics covering UE populations (e.g. number of UEs present in a geographical area), per spatial and temporal dimensions (e.g. per region for a period of time),

- NF data available in the 5GC (e.g. NRF),

- Data available in AF.

The NWDAF shall use at least one of the following services:

- the Generic management services as defined in TS 28.532 [6], the Performance Management services as defined in TS 28.550 [7] or the Fault Supervision services as defined in TS 28.545 [9], offered by OAM in order to collect OAM global NF data.

- the Exposure services offered by NFs in order to retrieve data and other non-OAM pre-computed metrics available in the NFs.

- Other NF services in order to collect NF data (e.g. NRF)

The NWDAF shall obtain the proper information to perform data collection for a UE, a group of UEs or any UE:

- For an Analytics ID, NWDAF is configured with the corresponding NF Type(s) and/or event ID(s) and/or OAM measurement types.

- NWDAF shall determine which NF instance(s) of the relevant NF type(s) are serving the UE, the group of UEs or any UE, taking into account the S-NSSAI(s) and area of interest as defined in clause 7.1.3, TS 23.501 [2].

- NWDAF invokes Nnf_EventExposure_Subscribe services to collect data from the determined NF instance(s), and/or triggers the procedure in clause 6.2.3.2 to subscribe to OAM services to collect the OAM measurement.

The NWDAF performs data collection from an AF directly as defined in clause 6.2.2.2 or via NEF as defined in clause 6.2.2.3.

The NWDAF shall be able to discover the events supported by a NF.

Data collection procedures enables the NWDAF to efficiently obtain the appropriate data with the appropriate granularity.

When a request or subscription for statistics or predictions is received, the NWDAF may not possess the necessary data to perform the service, including:

- Data on the monitoring period in the past, which is necessary for the provision of statistics and predictions matching the Analytics target period.

- Data on longer monitoring periods in the past, which is necessary for model training.

Therefore, in order to optimize the service quality, the NWDAF may undertake the following actions:

- The NWDAF may return a probability assertion as stated in clause 6.1.3 expressing the confidence in the prediction produced. Prediction may be returned with zero confidence as described below. This confidence is likely to grow in the case of subscriptions.

- The value of the confidence depends on the level or urgency expressed by the parameter "preferred level of accuracy of the analytics" as listed in clause 6.1.3, the parameter "time when analytics information is needed" as listed in clause 6.1.3, and the availability of data. If no sufficient data is collected to provide an estimation for the requested level of accuracy before the time deadline, the service shall return a zero confidence. Otherwise, the NWDAF may wait until enough data is collected before providing a response or a first notification.

- In order to be prepared for future requests on analytics from NFs/OAM, the NWDAF, upon operator configuration, may collect data on its own initiative, e.g. on samples of UEs, and retain the data collected in the data storage.

NOTE 1: The NWDAF can send an error response to the analytics consumer to indicate that statistics are unavailable if the NWDAF was not prepared for future requests and did not collect data on its own initiative.

The volume and maximum duration of data storage is also subject to operator configuration.

The NWDAF may decide to reduce the amount of data collected to reduce signalling load, by either prioritizing requests received from analytics consumers, or reducing the extent (e.g. duration, scope) of data collection, or modifying the sampling ratios.

The NWDAF may skip data collection phase when the NWDAF already has enough information to provide requested analytics.

The data which NWDAF may collect is listed for each analytics in input data clause and is decided by the NWDAF.

NOTE 2: NWDAF can skip data collection phase for some specific input data per the requested analytics e.g. when some of the data is already available at NWDAF for the requested analytics, or when NWDAF considers that some of the data is not needed at all to provide the requested analytics as per the analytics consumer request (e.g. based on preferred level of accuracy or based on the time when analytics are needed).

6.2.2 Data Collection from NFs

6.2.2.1 General

The Data Collection from NFs is used by NWDAF to subscribe/unsubscribe at any 5GC NF to be notified for data on a set of events.

The Data Collection from NFs is based on the services of AMF, SMF, UDM, PCF, NRF and AF (possibly via NEF):

- Event Exposure Service offered by each NF as defined in TS 23.502 [3] clause 4.15 and clause 5.2.
- other NF services (e.g. Nnrf_NFDiscovery and Nnrf_NFManagement in NRF as defined in TS 23.502 [3] clause 4.17)

This data collection service is used directly in order to retrieve behaviour data for individual UEs or groups of UEs (e.g. UE reachability), and also to retrieve global UE information (e.g. Number of UEs present in a geographical area).

Table 6.2.2.1-1: NF Services consumed by NWDAF for data collection

Service producer	Service	Reference in TS 23.502 [3]
AMF	Namf_EventExposure	5.2.2.3
SMF	Nsmf_EventExposure	5.2.8.3
PCF	Npcf_EventExposure (for a group of UEs or any UE) Npcf_PolicyAuthorization_Subscribe (for a specific UE)	5.2.5.7
UDM	Nudm_EventExposure	5.2.3.5
NEF	Nnef_EventExposure	5.2.6.2
AF	Naf_EventExposure	5.2.19.2
NRF	Nnrf_NFDiscovery	5.2.7.3
	Nnrf_NFManagement	5.2.7.2

NOTE 1: The present document specifies that NWDAF can collect some UPF input data for deriving analytics, but how NWDAF collects these UPF input data is not defined in this Release of the specification.

NOTE 2: There is no data collected from the PCF by the NWDAF defined in this Release of the specification.

To retrieve data related to a specific UE, the NWDAF shall first determine which NF instances are serving this UE as stated in table 6.2.2.1-2 unless the NWDAF has already obtained this information due to recent operations related to this UE.

Table 6.2.2.1-2: NF Services consumed by NWDAF to determine which NF instances are serving a UE

Type of NF instance (serving the UE) to determine	NF to be contacted by NWDAF	Service	Reference in TS 23.502 [3]
UDM	NRF	Nnrf_NFDiscovery	5.2.7.3
AMF	UDM	Nudm_UECM	5.2.3.2
SMF	UDM	Nudm_UECM	5.2.3.2
BSF	NRF	Nnrf_NFDiscovery	5.2.7.3
PCF	BSF	Nbsf_Management	5.2.13.2
NEF	NRF	Nnrf_NFDiscovery	5.2.7.3

The UDM instance should be determined using NRF as described in clause 4.17.4 of TS 23.502 [3] and factors to determine as described in clause 6.3.8 of TS 23.501 [2].

The AMF, SMF instances should be determined using a request to UDM providing the SUPI or the group identity. To determine the SMF serving a PDU session, the NWDAF should in addition provide the DNN and S-NSSAI of this PDU Session; otherwise the NWDAF will obtain a list of possibly multiple SMFs (e.g. one per PDU session).

The BSF instance should be discovered using NRF thanks to optional request parameters (e.g. DNN list, IP domain list, IPv4 address range, IPv6 prefix range) as stated in clause 4.17.4 of TS 23.502 [3], or based on local configuration at the NWDAF.

The PCF instance serving UE PDU Session(s) should be determined using a request to BSF with the allocated UE address, DNN and S-NSSAI.

When NWDAF receives a request addressed to an Internal Group ID from a consumer, NWDAF may need to initiate data collection from several 5GC NFs, such as AMF, SMF, UDM, PCF, NEF/AF, etc. NWDAF may first discover the instances of the required 5GC NFs deployed in the network, e.g. by querying NRF.

For discovering the UDM, NWDAF can query the NRF with the Internal Group ID as the target of the query. For discovering AMF, SMF, PCF, NEF, and AF, NWDAF may need to discover all the instances in the network by using the Nnrf_NFDiscovery service.

NOTE 3: It is assumed that all members of an Internal Group ID belong to the same UDM Group ID. NWDAF can select a UDM instance supporting the UDM Group ID of the Internal Group ID.

Then, if data needs to be collected from AMF, SMF, UDM, and PCF, NWDAF may initiate the data collection with the Internal Group ID as the target, e.g. subscribing to the event exposure in all the instances of a given type of network function. This subscription to all the instances of required source of event exposure handles, e.g. mobility of UEs across AMFs, or initiation of new PDU sessions with different allocated SMFs.

For collecting data from AMF and SMF, NWDAF may collect the data directly from AMF and/or SMF, or indirectly via UDM, according to TS 23.502 [3] clause 4.15.3.2.3.

The NWDAF determines to collect data from a trusted AF supporting specific Event ID(s) and serving specific application(s) based on internal configuration.

The NEF instance that is serving a specific network slices and/or applications of a UE should be determined using NRF using optional request parameters as defined in clause 6.3.14 of TS 23.501 [2]

If NWDAF needs to collect data from an AF deployed outside the operator's domain, the NWDAF shall contact NEF with a SUPI or Internal Group ID as the target of the data collection. NEF is responsible for translation of SUPI to GPSI, or internal to external group identifiers, by querying UDM, prior to contacting the AF.

To retrieve required data for any UE, the NWDAF may subscribe to events from the AMF and/or SMF instances it has determined, setting the target of event reporting to "any UE" and the event filter(s) according to the Analytics Filter Information. Alternatively, if the required data is communication related and for any UE within an Area of interest, the NWDAF can obtain from the AMF instances it has determined a list of UEs located within the Area of Interest. Based on the obtained UE list, for each UE in the list, the NWDAF retrieves the SMF serving the UE and the NWDAF subscribes to data from the relevant SMF per each specific UE.

To retrieve data related to "any UE" based on analytics filter information, the NWDAF shall first determine which NF instances are matching the analytics filter information (see clause 6.7.5.1) as stated in table 6.2.2.1-3 unless the NWDAF has already obtained this information due to recent operations related to this analytics filter information.

Table 6.2.2.1-3: NF Services consumed by NWDAF to determine which NF instances are matching analytics filters

Type of NF instance (matching analytics filters) to determine	NF to be contacted by NWDAF	Service	Reference in TS 23.502 [3]
AMF, SMF	NRF	Nnrf_NFDiscovery	5.2.7.3

6.2.2.2 Procedure for Data Collection from NFs

The procedure in Figure 6.2.2.2-1 is used by NWDAF to subscribe/unsubscribe at NFs in order to be notified for data collection on a related event (s), using Event Exposure Services as listed in Table 6.2.2.1-1.

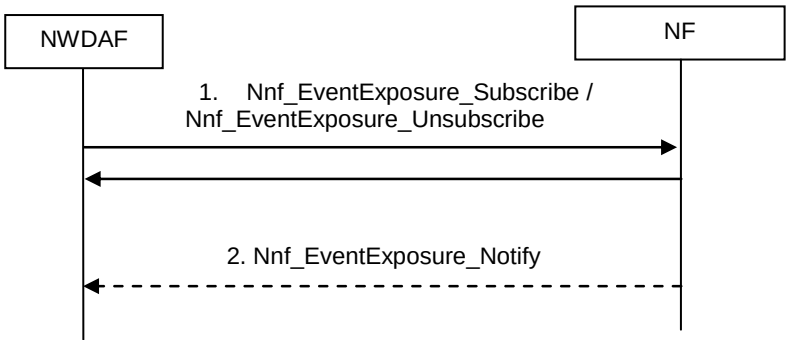

Figure 6.2.2.2-1: Event Exposure Subscribe/unsubscribe for NFs

1. The NWDAF subscribes to or cancels subscription for a (set of) Event ID(s) by invoking the Nnf_EventExposure_Subscribe / Nnf_EventExposure_Unsubscribe service operation.

NOTE 1: The Event ID (s) are defined in TS 23.502 [3].

2. If NWDAF subscribes to a (set of) Event ID(s), the NFs notify the NWDAF (e.g. with the event report) by invoking Nnf_EventExposure_Notify service operation.

NOTE 2: The NWDAF can use the immediate reporting flag as defined in Table 4.15.1-1 of TS 23.502 [3] to meet the request-response model for data collection from NFs.

NOTE 3: This procedure is also used when the NWDAF subscribes for data from a trusted AF.

6.2.2.3 Procedure for Data Collection from AF via NEF

The procedure in Figure 6.2.2.3-1 is used by NWDAF to collect information from AFs via the NEF.

NOTE 1: In this release, AF registers its available data to NWDAF via OAM configuration at NEF.

The AF collectable data information includes: AF identification, AF service identification (e.g., endpoint information of Naf_EventExposure), available data to be collected per application (e.g., identified by Event ID(s)).

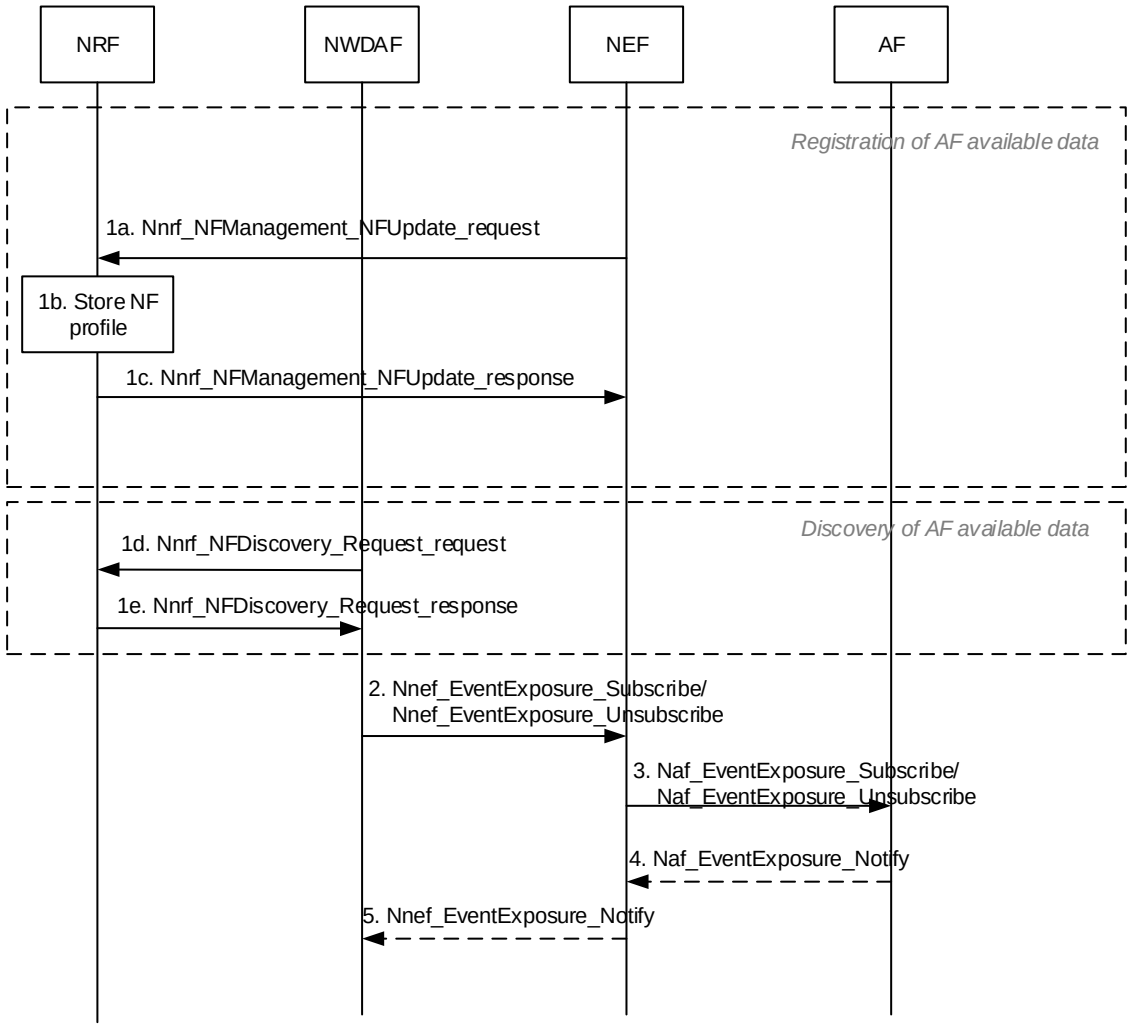

Figure 6.2.2.3-1: Data Collection from AF via NEF

1a. After the registration of AF available data at the NEF, NEF generates an event exposure with new EventID to be associated with available data to be collected from AF. NEF invokes Nnrf_NFManagement_NFUpdate_request service operation to update its registration information (i.e., NEF Profile) including the generated Event IDs, and associated AF identification, Application ID(s).

1b. NRF stores the received NEF registration information including available data to be collected from AF.

1c. NRF sends Nnrf_NFManagement_NFUpdate_response message to NEF.

1d. When NWDAF needs to discovery the available data from AFs and the appropriated NEF to collect this data, NWDAF invokes Nnrf_NFDiscovery_Request_request service operation using as parameter the NEF NF Type, a list of Event ID(s), and optionally AF identification, application ID.

1e. NRF matches the requested query for available data in AFs with the registered NEF Profiles and sends this information via Nnrf_NFDiscovery_Request_response message to NWDAF.

NOTE 2: After the registration and discovery procedure described in step 1, NWDAF identifies the available data per AF per application and the proper NEF to collect such data.

2. The NWDAF subscribes to or cancels subscription to data in AF via NEF by invoking the Nnef_EventExposure_Subscribe or Nnef_EventExposure_Unsubscribe service operation. If the event subscription is authorized by the NEF, the NEF records the association of the event trigger and the NWDAF identity.

NOTE 3: User consent for retrieving user data in AF via NEF is not specified in this Release.

3. Based on the request from the NWDAF, the NEF subscribes to or cancels subscription to data in AF by invoking the Naf_EventExposure_Subscribe/ Naf_EventExposure_Unsubscribe service operation.

4. If the NEF subscribes to data in AF, the AF notifies the NEF with the data by invoking Naf_EventExposure_Notify service operation.

5. If the NEF receives the notification from the AF, the NEF notifies the NWDAF with the data by invoking Nnef_EventExposure_Notify service operation.

6.2.2.4 Procedure for Data Collection from NRF

The NWDAF may use NRF services and Network Function service framework procedures as defined in TS 23.502 [3] clause 5.2.7 and clause 4.17:

- NF/NF service discovery procedures (in TS 23.502 [3] clause 4.17.4) and Nnrf_NFDiscovery service (in TS 23.502 [3] clause 5.2.7.3) in order to dynamically discover the NF instances and services of the 5GC. Such discovery may be performed on a periodic basis, or under specific circumstances.

- NF/NF service status subscribe/notify procedures (in TS 23.502 [3] clause 4.17.7) and Nnrf_NFManagement service (in TS 23.502 [3] clause 5.2.7.2) in order to be notified about the change of status of an NF. The service operations for obtaining status information are NFStatusSubscribe and NFStatusNotify, from the Nnrf_NFManagement service.

The information provided by the NRF to the NWDAF with the Nnrf_NFDiscovery_Request and the Nnrf_NFManagement_NFStatusNotify service operations are the NF Profiles and the NF services as defined in TS 23.502 [3] clause 5.2.7. Such information can be used to set-up and maintain a consistent network map for data collection and also, depending on use cases, to perform analytics (e.g. NF load analytics as defined in clause 6.5).

6.2.2.5 Usage of Exposure framework by the NWDAF for Data Collection

The NWDAF shall subscribe (and unsubscribe) to the Event exposure service from NF(s) reusing the framework defined in TS 23.502 [3] clause 4.15. This framework supports the possibility for the NWDAF to indicate / request:

- Events-ID: one or multiple Event ID(s) defined in TS 23.502 [3] clause 4.15.1

- Target of Event Reporting defined in TS 23.502 [3] clause 4.15.1: the objects targeted by the Events. Within a subscription, all Event ID(s) are associated with the same target of event reporting. In the case of NWDAF, the objects can be UE(s), UE group(s), any UE.

- Event Filter Information defined in TS 23.502 [3] clause 4.15.1. This provides Event Parameter Types and Event Parameter Value(s) to be matched against.

- A Notification Target Address and a Notification Correlation ID as defined in TS 23.502 [3] clause 4.15.1, allowing the NWDAF to correlate notifications received from the NF with this subscription.

- Event Reporting Information described in TS 23.502 [3] Table 4.15.1-1.

- Expiry time as defined in TS 23.502 [3] clause 4.15.1.

The notifications from NFs/AFs contain on top of the Event being reported (and of dedicated information being reported for this event):

- the Notification Correlation Information provided by the NWDAF in its request,

- (when applicable to the event) the Target Id e.g. UE ID (SUPI and if available GPSI), and

- a time stamp.

6.2.3 Data Collection from OAM

6.2.3.1 General

The NWDAF may collect relevant management data from the services in the OAM as configured by the PLMN operator.

- NG RAN or 5GC performance measurements as defined in TS 28.552 [8].
- 5G End to end KPIs as defined in TS 28.554 [10].

NWDAF shall use the following services to have access to the information provided by OAM:

- Generic performance assurance and fault supervision management services as defined in TS 28.532 [6].
- PM (Performance Management) services as defined in TS 28.550 [7].
- FS (Fault Supervision) services defined in TS 28.545 [9].

NWDAF can be configured to invoke the existing OAM services to retrieve the management data that are relevant for analytics generation, which may include NF resources usage information (e.g. usage of virtual resources assigned to NF) and NF resource configuration information (e.g. life cycle changes of NF resource configurations).

OAM perform the required configuration in order to provide the information requested by NWDAF subscription and perform the tasks, e.g. data collection, data processing, associated with the subscribed request from NWDAF.

Another usage of OAM services is when the target of data collection is a specific UE, via MDT based retrieval of information:

- Measurement collection for MDT as defined in TS 37.320 [20].

6.2.3.2 Procedure for data collection from OAM

The interactions between NWDAF and OAM for data collection are illustrated in Figure 6.2.3.2-1. The data collected depends on the use cases. This figure is an abstraction of the OAM performance data file report management service that is defined TS 28.532 [6]. The actual OAM services and reporting mechanisms that NWDAF may use are specified in TS 28.532 [6], TS 28.550 [7] or TS 28.545 [9].

The flow below assumes the NWDAF is configured on how to subscribe to the relevant OAM services.

OAM shall setup the required mechanisms to guarantee the continuous data collection requested by NWDAF.

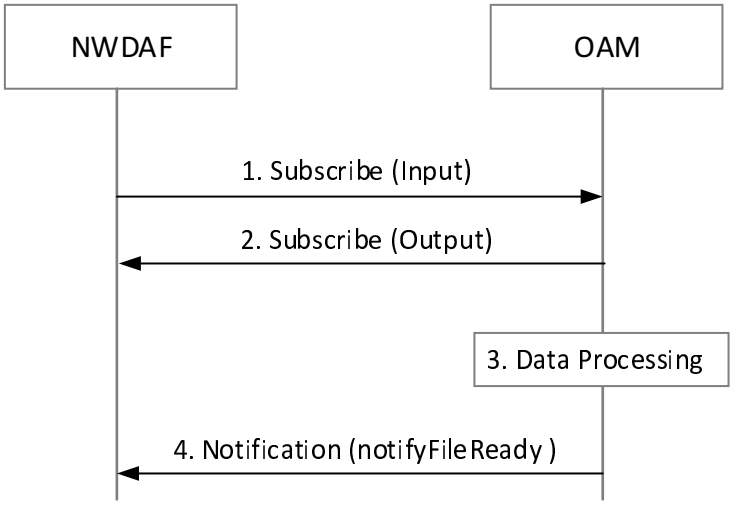

Figure 6.2.3.2-1: Data collection from OAM performance data file report management service

1. (Clause 11.3.1.1.3.2, TS 28.532 [6]), Subscribe (Input): NWDAF subscribes to the notification(s) related to the services provided by the management service producer.

2. (Clause 11.3.1.1.3.3, TS 28.532 [6]), Subscribe (Output): management service producer responses to NWDAF if the subscription is success or not.

3. Data processing: management service producer prepares the data.

4. (Clause 11.3.1.1.1, TS 28.532 [6]), Notification (notifyFileReady): management service producer notifies the data file is ready.

As the final step, NWDAF fetches data by using FTP (not specified in 3GPP, based on vendor implementation).

NOTE: The call flow in Figure 6.2.3.2-1 only shows a subscribe/notify model for the simplicity, however both request-response and subscription-notification models are supported.

6.2.4 Correlation between network data and service data

The Correlation information in each NF input data which helps NWDAF correlate data from different NFs is defined in Table 6.2.4-1, which is subject to all the network data analytics.

NOTE: For simplicity, the correlation information is not listed in the input data per network data analytics.

Table 6.2.4-1: Correlation Information

Correlation Information	Description
Timestamp, IP address 5-tuple	To correlate the data from AF and from UPF.
Timestamp, AN Tunnel Info (Clause 9.3.2.2, TS 38.413 [16])	To correlate the UPF data and OAM data which are reported by the RAN (e.g. Reference Signal Received Power or Reference Signal Received Quality as defined in Table 6.4.2-3).
Timestamp, UE IP address	To correlate the data from UPF and SMF.
Timestamp, SUPI	To correlate data from SMF and AMF.
Timestamp, SUPI, DNN, S-NSSAI or UE IP address	To correlate data from SMF and PCF.
Timestamp, RAN UE NGAP ID (Clause 9.3.3.2, TS 38.413 [16]) and Global RAN Node ID	To correlate the AMF data and OAM data reported by the RAN (e.g. Reference Signal Received Power or Reference Signal Received Quality as defined in Table 6.4.2-3).
Timestamp, Application ID, IP filter information	To correlate data from SMF and AF.

6.3 Slice load level related network data analytics

6.3.1 General

The NWDAF provides slice load level information to an NF on a Network Slice instance level. The NWDAF is not required to be aware of the current subscribers using the slice. The NWDAF notifies slice specific network status analytics information to the NFs that are subscribed to it. An NF may collect directly slice specific network status analytics information from NWDAF. This information is not subscriber specific.

The NWDAF services as defined in the clause 7.2 and clause 7.3 are used to expose slice load level analytics from the NWDAF to the consumer NF (e.g. PCF or NSSF).

The following Analytics ID is used for the slice load level related network data analytics:

- Load level information

The following Analytics Filters can be included by the consumer in the related Nnwdaf_AnalyticsSubscription_Subscribe and Nnwdaf_AnalyticsInfo_Request service operation:

- S-NSSAI and NSI ID.

NOTE: The use of NSI ID in the network is optional and depends on the deployment choices of the operator. If used, the NSI ID is associated with S-NSSAI. NSI ID is only applicable when the consumer is NSSF.

- Load Level Threshold value.

6.3.2 Void

6.3.2A Input data

There is no input data specification for support of slice load level analytics in this Release of the specification.

6.3.3 Void

6.3.3A Output analytics

The NWDAF reports when the load level of the Network Slice Instance, indicated by the S-NSSAI and the associated NSI ID (if applicable) in the Analytics Filter, crosses the threshold provided in the analytics subscription; if no threshold is provided in the subscription, the reporting (Notify operation) is assumed to be periodic.

6.4 Observed Service Experience related network data analytics

6.4.1 General

This clause specifies how NWDAF can provide Observed Service Experience (i.e. average of observed Service MoS and/or variance of observed Service MoS indicating service MOS distribution for services such as audio-visual streaming as well as services that are not audio-visual streaming such as V2X and Web Browsing services) analytics, in the form of statistics or predictions, to a service consumer.

The Observed Service Experience analytics may provide one or both of the following:

- Service Experience for a Network Slice: Service Experience for a UE or a group of UEs or any UE in a Network Slice;
- Service Experience for an Application: Service Experience for a UE or a group of UEs or any UE in an Application or a set of Applications.

Therefore, Observed Service experience may be provided individually per UE or group of UEs, or globally, averaged per Application or averaged across a set of Applications on a Network Slice.

The service consumer may be an NF (e.g. PCF), or the OAM.

The consumer of these analytics shall indicate in the request or subscription:

- Analytics Id set to "Service Experience";
- The Target of Analytics Reporting: one or more SUPI(s) or Internal Group Identifier(s), or "any UE";
- Analytics Filter Information as defined in Table 6.4.1-1; and
- optionally, maximum number of objects and maximum number of SUPIs;

Table 6.4.1-1: Analytics Filter Information related to the observed service experience

Information	Description	Mandatory	
		Application	Network Slice
Application ID (0...max)	The identification of the application(s) for which the analytics information is subscribed or requested.	Y	N
S-NSSAI	When requesting Service Experience for a Network Slice: identifies the Network Slice for which analytics information is subscribed or requested. When requesting Service Experience for an Application: identifies the S-NSSAI used to access the application together with the DNN listed below.	N	Y
NSI ID(s)	Identifies the Network Slice instance(s) for which analytics information is subscribed or requested.	N	N
Area of Interest	Identifies the Area (i.e. set of TAIs), as defined in TS 23.501 [2] for which the analytics information is subscribed or requested.	N	N
DNN	When requesting Service Experience for an Application, this is the DNN to access the application.	N	N

NOTE: A service consumer may use the Area of Interest in order to reduce the amount of signalling that the analytics subscription or request generates.

- An Analytics target period that indicates the time window for which the statistics or predictions are requested;
- In a subscription, the Notification Correlation Id and the Notification Target Address.

The NWDAF shall notify the result of the analytics to the consumer as specified in clause 6.4.3.

NWDAF collects the network data from AF (directly or via NEF) and from other 5GC NF(s) in order to calculate and provide statistics and predictions on the observed service experience to a consumer NF or to OAM.

Based on the Analytics Filter information in Table 6.4.1-1 and the Target of Analytics reporting provided by the service consumer in the analytics subscription or request, NWDAF determines whether service experience analytics should be delivered for:

i) Application(s);

ii) Network Slice;

iii) both Application(s) and Network Slice.

If NWDAF is unable to differentiate based on the analytics subscription or request, it provides service experience analytics for both Application(s) and Network Slice.

If service experience for both Application(s) and Network Slice is desired but the Target of Analytics reporting or Analytics Filter information values (e.g. Area of Interest) need to be different, separate subscriptions/requests may be provided by the service consumer.

6.4.2 Input Data

The service data collected from the AF, the network data from other 5GC NFs and the network data from OAM for observed service experience are defined in Table 6.4.2-1, Table 6.4.2-2 and Table 6.4.2-3, respectively.

Table 6.4.2-1: Service Data from AF related to the observed service experience

Information	Source	Description
Application ID	AF	To identify the service and support analytics per type of service (the desired level of service)
IP filter information	AF	Identify a service flow of the UE for the application
Locations of Application	AF/NEF	Locations of application represented by a list of DNAI(s). The NEF may map the AF-Service-Identifier information to a list of DNAI(s) when the DNAI(s) being used by the application are statically defined.
Service Experience	AF	Refers to the QoE per service flow as established in the SLA and during on boarding. It can be either e.g. MOS or video MOS as specified in ITU-T P.1203.3 [11] or a customized MOS for any kind of service including those not related to video or voice.
Timestamp	AF	A time stamp associated to the Service Experience provided by the AF, mandatory if the Service Experience is provided by the ASP.

NWDAF subscribes to the service data from AF in the Table 6.4.2-1 either directly for trusted AFs by invoking Naf_EventExposure_Subscribe service (Event ID = Service Experience information, Event Filter information = Area of Interest, Application ID) as defined in TS 23.502 [3], or indirectly for untrusted AFs via NEF by invoking Nnef_EventExposure_Subscribe service (Event ID = Service Experience information, Event Filter information = Area of Interest, Application ID) where NEF translates the Area of Interest into geographic zone identifier(s).

NOTE: When the Service Experience is expressed as a customized MOS, the customized MOS may be defined by the content provider or by the MNO and may be based on the nature of the targeted service type (e.g. web browsing, gaming, augmented reality, V2X, SMS).

Table 6.4.2-2: QoS flow level Network Data from 5GC NF related to the QoS profile assigned for a particular service (identified by an Application Id or IP filter information)

Information	Source	Description
Timestamp	5GC NF	A time stamp associated with the collected information.
Location	AMF	The UE location information.
(list of)SUPI(s)	AMF	If UE IDs are not provided as target of analytics reporting for slice service experience, AMF returns the UE IDs matching the AMF event filters.
DNN	SMF	DNN for the PDU Session which contains the QoS flow
S-NSSAI	SMF	S-NSSAI for the PDU Session which contains the QoS flow
Application ID	SMF	Used by NWDAF to identify the application service provider and application for the QoS flow
IP filter information	SMF	Provided by the SMF, which is used by NWDAF to identify the service data flow for policy control and/or differentiated charging for the QoS flow
QFI	SMF	QoS Flow Identifier
QoS flow Bit Rate	UPF	The observed bit rate for UL direction; and The observed bit rate for DL direction
QoS flow Packet Delay	UPF	The observed Packet delay for UL direction; and The observed Packet delay for the DL direction
Packet transmission	UPF	The observed number of packet transmission
Packet retransmission	UPF	The observed number of packet retransmission

NOTE 1: How NWDAF collects QoS flow Bit Rate, QoS flow Packet Delay, Packet transmission and Packet retransmission information from UPF is not defined in this Release of the specification.

NOTE 2: Care shall be taken with regards to load and major signalling caused when requesting Any UE. This could be achieved via utilization of some event filters (e.g. Area of Interest for AMF), Analytics Reporting Information (e.g. SUPImax), or sampling ratio as part of Event Reporting Information.

NWDAF subscribes to the network data from 5GC NF(s) in the Table 6.4.2-2 by invoking Nnf_EventExposure_Subscribe service operation with the following Event IDs as input parameters:

- AMF Source: Namf_EventExposure_Subscribe (Event IDs = Location Changes, Area of Interest).
- SMF Source: Nsmf_EventExposure_Subscribe (Event ID = QFI allocation).

Table 6.4.2-3: UE level Network Data from OAM related to the QoS profile

Information	Source	Description
Timestamp	OAM	A time stamp associated with the collected information.
Reference Signal Received Power	OAM	The per UE measurement of the received power level in a network cell, including SS-RSRP, CSI-RSRP as specified in clause 5.5 of TS 38.331 [14] and E-UTRA RSRP as specified in clause 5.5.5 of TS 36.331 [15]
Reference Signal Received Quality	OAM	The per UE measurement of the received quality in a network cell, including SS-RSRQ, CSI-RSRQ as specified in clause 5.5 of TS 38.331 [14] and E-UTRA RSRQ as specified in clause 5.5.5 of TS 36.331 [15]
Signal-to-noise and interference ratio	OAM	The per UE measurement of the received signal to noise and interference ratio in a network cell, including SS-SINR, CSI-SINR, E-UTRA RS-SINR, as specified in clause 5.1 of TS 38.215 [12]

NWDAF subscribes the network data from OAM in the Table 6.4.2-3 by using the services provided by OAM as described in clause 6.2.3.

The Event Filters for the service data collection from SMF, AMF and AF are defined in TS 23.502 [3].

The timestamps are provided by each NF to allow correlation of QoS and traffic KPIs. The clock reference is able to know the accuracy of the time and correlate the time series of the data retrieved from each NF.

6.4.3 Output Analytics

The NWDAF services as defined in the clause 7.2 and 7.3 are used to expose the analytics.

- Service Experience statistics information is defined in Table 6.4.3-1.
- Service Experience predictions information is defined in Table 6.4.3-2.

Table 6.4.3-1: Service Experience statistics

Information	Description
Slice instance service experiences (0…max)	List of observed service experience information for each Network Slice instance.
> S-NSSAI	Identifies the Network Slice.
> NSI ID	Identifies the Network Slice instance within the Network Slice.
> Network Slice instance service experience	Service experience across Applications on a Network Slice instance over the Analytics target period (average, variance).
> SUPI list (0..SUPImax)	List of SUPI(s) for which the slice instance service experience applies.
> Ratio	Estimated percentage of UEs with similar service experience (in the group, or among all UEs).
> Spatial validity	Area where the Network Slice service experience analytics applies.
> Validity period	Validity period for the Network Slice service experience analytics as defined in clause 6.1.3.
Application service experiences (0..max)	List of observed service experience information for each Application.
> S-NSSAI	Identifies the Network Slice used to access the Application.
> Application ID	Identification of the Application.
> Service Experience	Service Experience over the Analytics target period (average, variance).
> SUPI list (0..SUPImax)	List of SUPI(s) with the same application service experience.
> Ratio	Estimated percentage of UEs with similar service experience (in the group, or among all UEs).
> Spatial validity	Area where the Application service experience analytics applies.
> Validity period	Validity period for the Application service experience analytics as defined in clause 6.1.3.

Table 6.4.3-2: Service Experience predictions

Information	Description
Slice instance service experiences (0…max)	List of observed service experience information for each Network Slice instance.
S-NSSAI	Identifies the Network Slice.
> NSI ID	Identifies the Network Slice instance within the Network Slice.
> Network Slice instance service experience	Service experience across Applications on a Network Slice instance over the Analytics target period (average, variance).
> SUPI list (0..SUPImax)	List of SUPI(s) for which the slice instance service experience applies.
> Ratio	Estimated percentage of UEs with similar service experience (in the group, or among all UEs).
> Spatial validity	Area where the Network Slice service experience analytics applies.
> Validity period	Validity period for the Network Slice service experience analytics as defined in clause 6.1.3.
> Probability assertion	Confidence of this prediction.
Application service experiences (0..max)	List of predicted service experience information for each Application.
> S-NSSAI	Identifies the Network Slice used to access the Application.
> Application ID	Identification of the Application.
> Service Experience	Service Experience over the Analytics target period (average, variance).
> SUPI list (0..SUPImax)	List of SUPI(s) with the same application service experience.
> Ratio	Estimated percentage of UEs with similar service experience (in the group, or among all UEs).
> Spatial validity	Area where the Application service experience analytics applies.
> Validity period	Validity period for the Application service experience analytics as defined in clause 6.1.3.
> Probability assertion	Confidence of this prediction.

NOTE 1: The NSI ID is an optional parameter. If not provided the Slice instance service experience indicates the service experience for the S-NSSAI.

NOTE 2: The SUPI list and Ratio in the service experience information for an application can be omitted, if the corresponding parameter(s) is/are provided and are assigned with the same value(s) in the service experience information for the slice instance which the application belongs to. Otherwise, the SUPI list and Ratio are mandatory to be provided for an application service experience.

NOTE 3: The Spatial validity is present in the output parameters if the consumer provided the Area of Interest as defined in Table 6.4.1-1.

The number of Service Experiences and SUPIs are limited respectively by the maximum number of objects and the Maximum number of SUPIs provided as part of Analytics Reporting Information by the NWDAF Service Consumer.

6.4.4 Procedures to request Service Experience for an Application

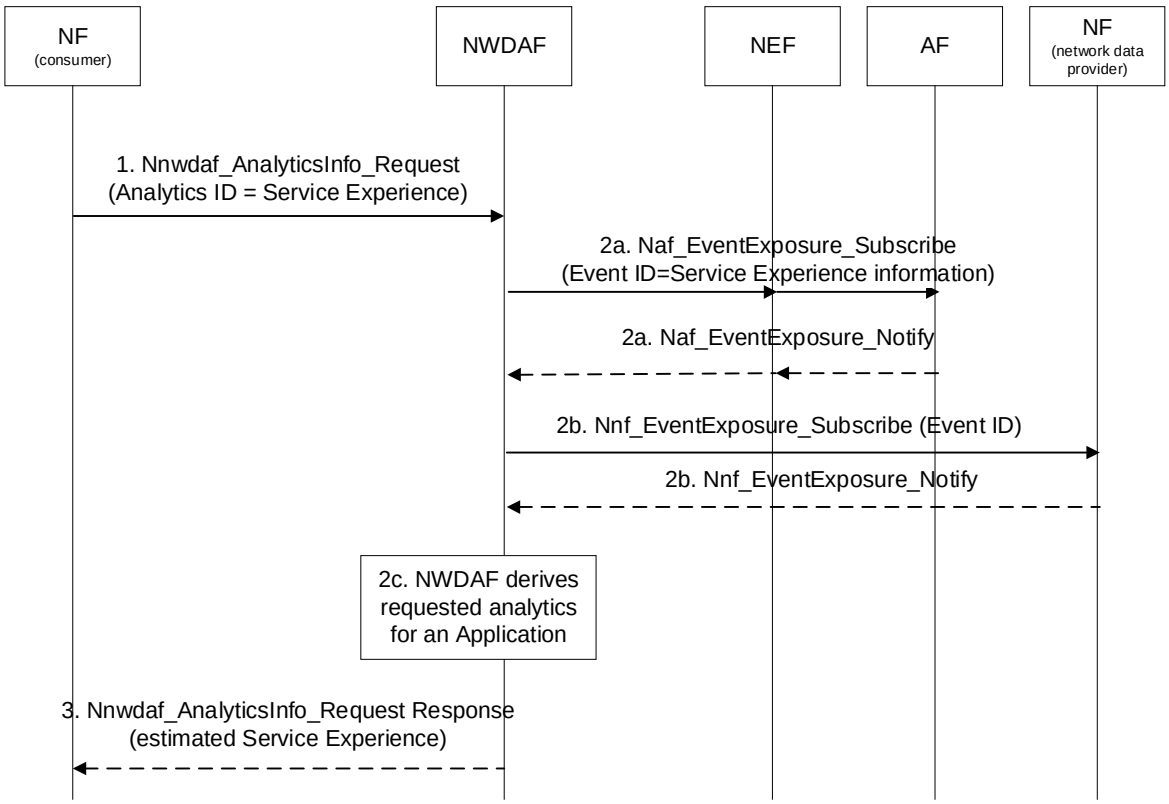

Figure 6.4.4-1: Procedure for NWDAF providing Service Experience for an Application

This procedure allows the consumer to request Analytics ID "Service Experience" for a particular Application. The consumer includes both the Application ID for which the Service Experience is requested and indicates that the Target of Analytics Reporting is "any UE". At the same time, for an Application ID, a set of initial QoS parameter combinations per service experience window (e.g. one is for 3<Service MOS<4 and another is for 4<Service MOS<5) is defined in PCF (e.g. by configuration of operator policies) that may be updated based on the Service Experience reported by NWDAF.

1. Consumer NF sends an Analytics request/subscribe (Analytics ID = Service Experience, Target of Analytics Reporting = any UE, Analytics Filter information = (Application ID, Analytics target period S-NSSAI, DNN, Area of Interest)) to NWDAF by invoking a Nnwdaf_AnalyticsInfo_Request or a Nnwdaf_AnalyticsSubscription_Subscribe.

2a. NWDAF subscribes the service data from AF in the Table 6.4.2-1 by invoking Nnef_EventExposure_Subscribe or Naf_EventExposure_Subscribe service (Event ID = Service Experience information, Application ID, Event Filter information), Target of Event Reporting = Any UE) as defined in TS 23.502 [3].

NOTE 1: In the case of trusted AF, NWDAF provides the Area of Interest as a list of TAIs to AF. In the case of untrusted AF, NEF translates the requested Area of Interest provided as event filter by NWDA into geographic zone identifier(s) that act as event filter for AF.

2b. NWDAF subscribes the network data from 5GC NF(s) in the Table 6.4.2-2 by invoking Nnf_EventExposure_Subscribe service operation.

2c. With these data, the NWDAF estimates the Service experience for the application.

NOTE 2: QoE measurements from the applications are based on outcome of the ongoing SA5 Rel-16 WID "Management of QoE measurement collection" which addresses how to collect the QoE measurements from the applications in the UE.

3. The NWDAF provides the data analytics, i.e. the observed Service Experience (which can be a range of values) to the consumer NF by means of either Nnwdaf_AnalyticsInfo_Request response or

Nnwdaf_AnalyticsSubscription_Notify, depending on the service used in step 1, indicating how well the used QoS Parameters satisfy the Service MoS agreed between the MNO and the end user or between the MNO and the external ASP.

NOTE 3: The call flow only shows a request-response model for the interaction of NWDAF and consumer NF for simplicity instead of both request-response model and subscription-notification model.

If the consumer NF is a PCF and it determines that the application SLA is not satisfied, it may take into account the Observed Service Experience and the operator policies including SLA and required Service Experience (which can be a range of values) to determine new QoS parameters to be applied for the service, as defined in clause 6.1.1.3 and clause 6.2.1.2, TS 23.503 [4].

NOTE 4: The non-real time data information from AF includes the service experience data (see Table 6.4.2-1), which indicates the service quality during the service lifetime.

6.4.5 Procedures to request Service Experience for a Network Slice

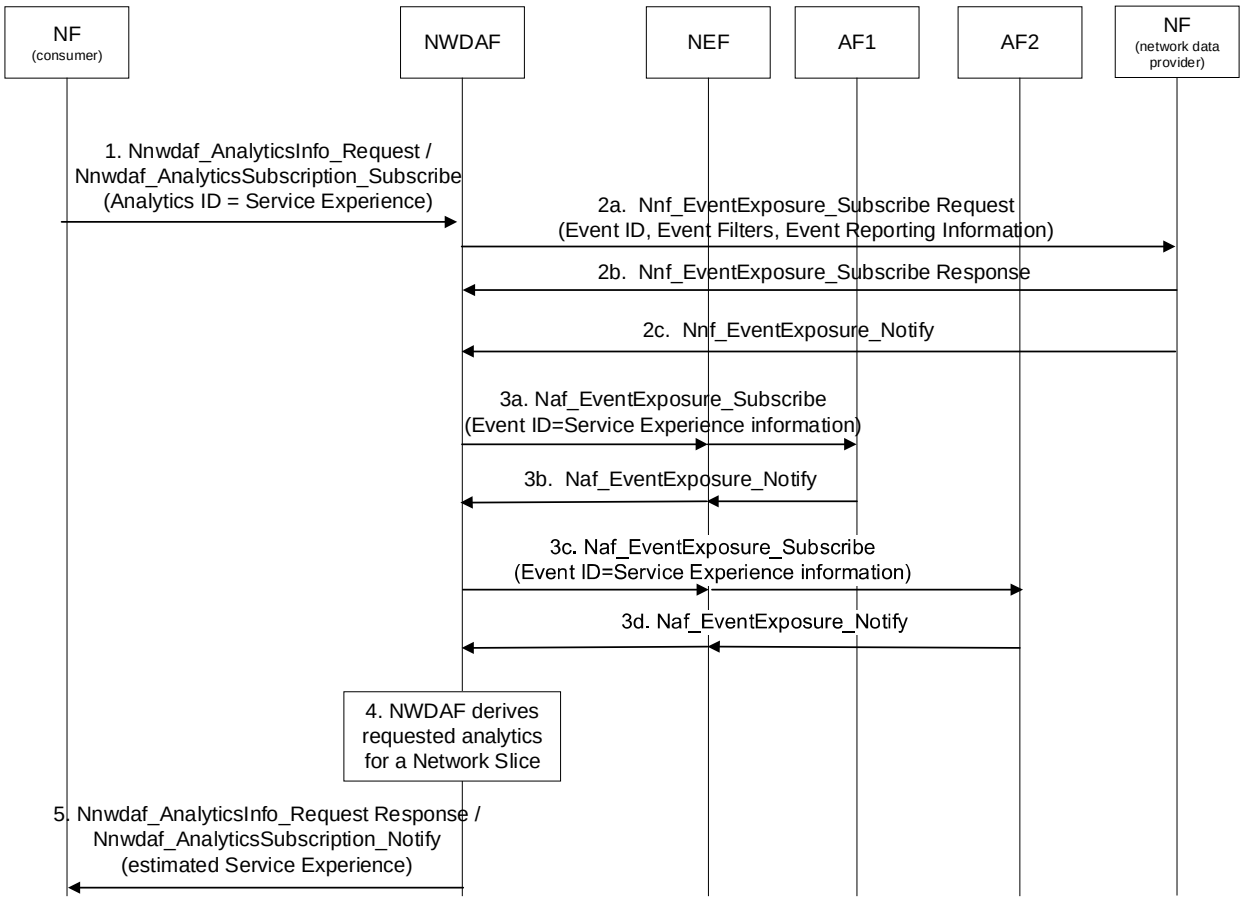

Figure 6.4.5-1: Procedure for NWDAF providing Service Experience for a UE or a group of UEs in a Network Slice

This procedure is similar to the procedure in clause 6.4.4, with the following differences. The consumer needs to request the Analytics ID "Service Experience" for all UEs or a group of UEs or a UE on a Network Slice, identified by an S-NSSAI. If multiple Network Slice instances of the same Network Slice are deployed, associated NSI ID(s) may be used in addition to S-NSSAI. If 'any UE' is the Target of Analytics Reporting, NWDAF may subscribe to UE mobility event notifications of AMF as described in clause 5.3.4.4 of TS 23.501 [2] using event ID "UE moving in or out of Area of Interest" and Event Filters as described in Table 5.2.2.3.1-1 of TS 23.502 [3] if it is needed to retrieve the list of SUPIs (and GPSIs if available) in the area of interest. The event exposure service request may also include the immediate reporting flag as Event Reporting Information as described in Table 4.15.1-1 of TS 23.502 [3].

In addition, service experience data may need to be collected from multiple Applications. If each Application is hosted in different AFs, NWDAF subscribes the service data in the Table 6.4.2-1 from the different AFs by invoking Nnef_EventExposure_Subscribe or Naf_EventExposure_Subscribe services for each Application (Event ID = Service

Experience information, Event Filter information, Application ID) as defined in TS 23.502 [3]. Figure 6.4.5-1 shows an example procedure with two AFs. If one AF provides the service experience data of multiple Applications, the set of Application IDs is provided by NWDAF to the AF with the Naf_EventExposure_Subscribe service operation, as defined TS 23.502 [3].

The Observed Service Experience for a Network Slice when consumed by OAM could be used as described in Annex H of TS 28.550 [7].

6.5 NF load analytics

6.5.1 General

The clause 6.5 describes how NWDAF can provide NF load analytics, in the form of statistics or predictions or both, to another NF.

The service consumer may be an NF, or the OAM.

The consumer of these analytics shall indicate in the request:

- Analytics ID set to "NF load information";
- The Target of Analytics Reporting: an optional SUPI;
- Analytics Filter Information:
  - optional S-NSSAI;
  - an optional list of NF Instance IDs, NF Set IDs, or NF types;
- Optional Reporting Threshold; the Reporting Threshold is unique for all NFs matching the above Analytics Filter and the reporting applies when the conditions are met for at least one of these NFs;
- An Analytics target period indicates the time period over which the statistics or predictions are requested;
- In a subscription, the Notification Correlation Id and the Notification Target Address are included.

The NWDAF shall notify the result of the analytics to the consumer as indicated in clause 6.5.3.

If a list of the NF Instance IDs (or respectively of NF Set IDs) is provided, the NWDAF shall provide the analytics for each designated NF instance (or respectively for each NF instance belonging to each designated NF Set). In such case the Target of Analytics Reporting should be ignored.

Otherwise, if a SUPI is provided, the NWDAF shall use the SUPI to determine which NF instances (AMF and SMF) are serving this specific UE, filter them according to the provided S-NSSAI and NF types using data collected from NRF or OAM, and provide analytics for these NF instances.

NOTE: Only NF instances of type AMF and SMF can be determined using a SUPI.

6.5.2 Input data

For the purpose of NF load analytics, the NWDAF may collect the information as listed in Table 6.5.2-1 for the relevant NF instance(s).

Table 6.5.2-1: Data collected by NWDAF for NF load analytics

Information	Source	Description
NF load	NRF	The load of specific NF instance(s) in their NF profile as defined per TS 29.510 [18].
NF status	NRF	The status of a specific NF instance(s) (registered, suspended, undiscoverable) as defined per TS 29.510 [18].
NF resource usage	OAM	The usage of assigned virtual resources currently in use for specific NF instance(s) (mean usage of virtual CPU, memory, disk) as defined in TS 28.552 [8] clause 5.7.
NF resource configuration	OAM	The life cycle changes of specific NF resources (e.g., NF operational or interrupted during virtual/physical resources reconfiguration) as defined in TS 28.533 [19], clause 5.2.

NOTE 1: The OAM information can be used as a complement to NRF information for some or all of the following aspects: resources utilization, NRF information correlation, and alternative source of information if NRF information on load is not available.

NOTE 2: NWDAF can request NRF for data related to NF instances, as described in TS 29.510 [18].

NOTE 3: NWDAF can correlate the NF resources configuration with NF resource usage for generating the analytics output.

If target NF type is UPF, the NWDAF may collect the information as listed in Table 6.5.2-2, in addition to information listed in Table 6.5.2-1.

Table 6.5.2-2: Data collected by NWDAF for UPF load analytics

Information	Source	Description
Traffic usage report	UPF	Report of user plane traffic in the UPF for the accumulated usage of network resources (see TS 29.244 [17])

NOTE 4: How NWDAF collects information in table 6.5.2-2 is not defined in this Release of the specification.

6.5.3 Output analytics

The NWDAF services as defined in the clause 7.2 and 7.3 are used to expose the analytics. NF load statistics information are defined in Table 6.5.3-1. NF load predictions information are defined in Table 6.5.3-2.

Table 6.5.3-1: NF load statistics

Information	Description
List of resource status (1..max)	List of observed load information for each NF instance along with the corresponding NF id / NF Set ID (as applicable)
> NF type	Type of the NF instance
> NF instance ID	Identification of the NF instance
> NF status	The availability status of the NF on the Analytics target period, expressed as a percentage of time per status value (registered, suspended, undiscoverable)
> NF resource usage	The average usage of assigned resources (CPU, memory, disk)
> NF load	The average load of the NF instance over the Analytics target period
> NF peak load (optional)	The maximum load of the NF instance over the Analytics target period

Table 6.5.3-2: NF load predictions

Information	Description
List of resource status (1..max)	List of predicted load information for each NF instance along with the corresponding NF id / NF Set ID (as applicable)
> NF type	Type of the NF instance
> NF instance ID	Identification of the NF instance
> NF status	The availability status of the NF on the Analytics target period, expressed as a percentage of time per status value (registered, suspended, undiscoverable)
> NF resource usage	The average usage of assigned resources (CPU, memory, disk)
> NF load	The average load of the NF instance over the Analytics target period
> NF peak load (optional)	The maximum load of the NF instance over the Analytics target period
> Confidence	Confidence of this prediction

NOTE: The variations on per-instance NF load and resource usage could be influenced by the number of running NF instances in addition to the load itself.

The predictions are provided with a Validity Period, as defined in clause 6.1.3.

The number of resource status is limited by the maximum number of objects provided as part of Analytics Reporting Information.

6.5.4 Procedures

The procedure depicted in Figure 6.5.4-1 allows a consumer NF to request analytics to NWDAF for NF load of various NF instances as defined in 6.5.1.

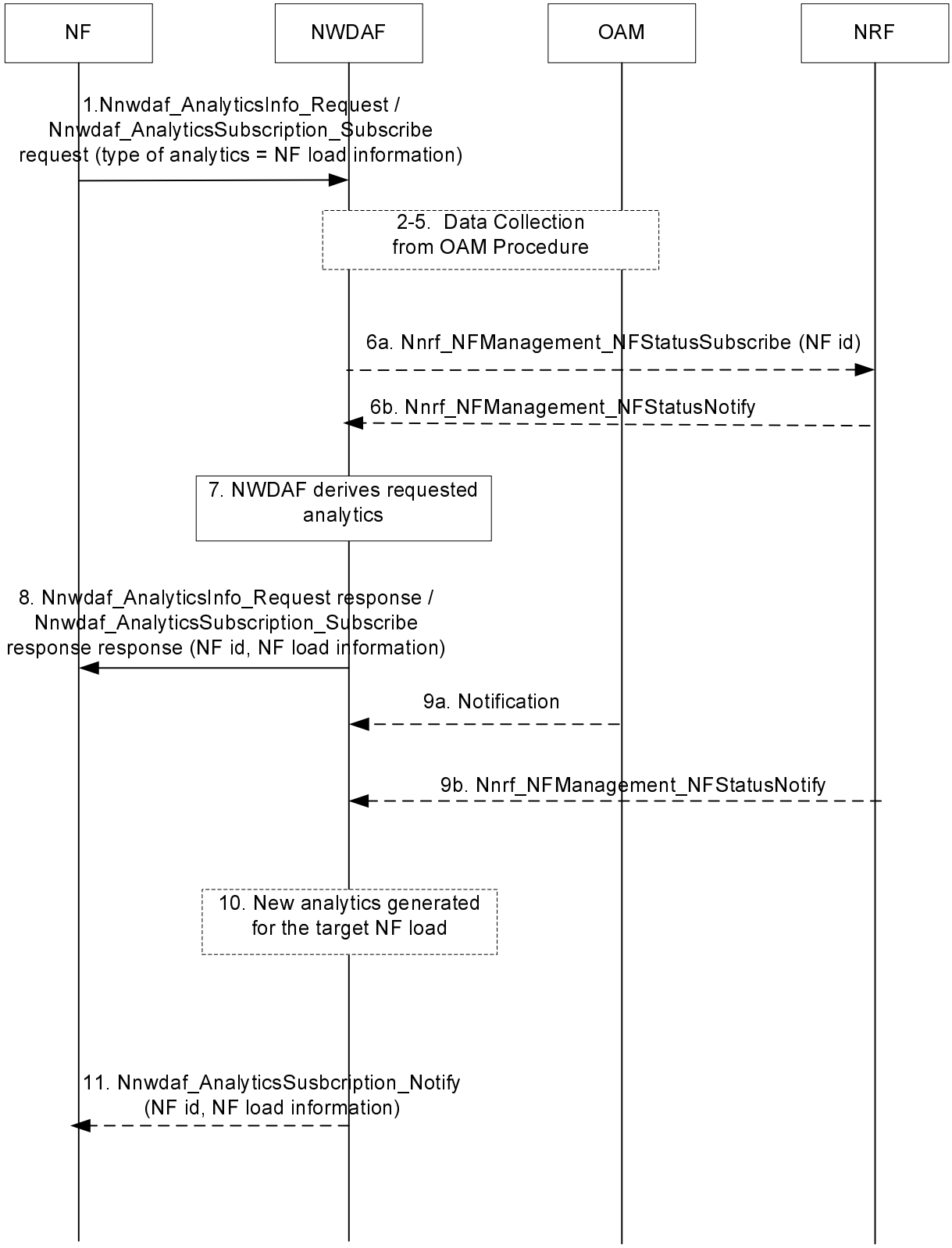

Figure 6.5.4-1: NF load analytics provided by NWDAF

1. The NF sends a request to the NWDAF for analytics for NF load for a specific NF, using either the Nnwdaf_AnalyticsInfo or Nnwdaf_AnalyticsSubscription service. The Analytics ID is set to NF load information, the target for analytics and the analytics filter are set according to clause 6.5.1. The NF can request statistics or predictions or both and can provide a time window.

2-5. If the request is authorized, and in order to provide the requested analytics, the NWDAF may need for each NF targeted instance to subscribe to OAM services to retrieve the target NF resource usage and NF resources

configuration following steps captured in clause 6.2.3.2 for data collection from OAM. Steps 2-5 may be skipped when e.g. the NWDAF already has the requested analytics.

NOTE 1: The call flow only shows a subscription/notification model for the simplicity, however both request-response and subscription-notification models should be supported.

NOTE 2: If the target NF type is UPF, the NWDAF can collect the information as listed in Table 6.5.2-2. How the NWDAF collects information is not defined in this Release of the specification.

6a. The NWDAF subscribes to changes on the load and status of NF instances registered in NRF and identified by their NF id from NRF using Nnrf_NFManagement_NFStatusSubscribe service operation for each NF instance.

6b. NRF notifies NWDAF of changes on the load and status of the requested NF instances by using Nnrf_NFManagement_NFStatusNotify service operation.

7. The NWDAF derives requested analytics.

8. The NWDAF provide requested NF load analytics to the NF along with the corresponding Validity Period, using either the Nnwdaf_AnalyticsInfo_Request response or Nnwdaf_AnalyticsSubscription_Subscribe response, depending on the service used in step 1.

9-11. If at step 1 the NF has subscribed to receive continuous reporting of NF load analytics, the NWDAF may generate new analytics and, when relevant according to the Analytics target period and Reporting Threshold, provide them along with the corresponding Validity Period to the NF upon reception of notification of new NF load information from OAM or NRF.

NOTE 3: If the target NF type at step 1 is UPF, the NWDAF can generate new analytics when receiving new information as listed in Table 6.5.2-2. How the NWDAF receives such new information is not defined in this Release of the specification.

6.6 Network Performance Analytics

6.6.1 General

With Network Performance Analytics, NWDAF provides either statistics or predictions on the gNB status information, gNB resource usage, communication performance and mobility performance in an Area of Interest; in addition, NWDAF it may provide statistics or predictions on the number of UEs that are located in that Area of Interest.

The service consumer may be an NF (e.g. PCF, NEF, AF), or the OAM.

The consumer of these analytics may indicate in the request:

- Analytics ID set to "Network Performance";
- Target of Analytics Reporting containing either a UE, or Internal Group Identifier that refers to the group for which the analytics on the number of UEs that are located in the Area of Interest at the time indicated in the Analytics target period is requested or any UE;
- Analytics Filter Information containing:
  - Area of Interest (list of TA or Cells) which restricts the area in focus (mandatory if Target Of Analytics Reporting is set to "any UE", optional otherwise);
  - Optionally, the subset of analytics that are requested among those specified in clause 6.6.3;
- Optionally, Reporting Thresholds, which apply only for subscriptions and indicate conditions on the level to be reached for respective analytics information (see clause 6.6.3) in order to be notified by the NWDAF;
- An Analytics target period indicates the time period over which the statistics or prediction are requested; and
- Optionally, maximum number of objects;
- In a subscription, the Notification Correlation Id and the Notification Target Address are included.

The NWDAF notifies the result of the analytics to the consumer as indicated in clause 6.6.3.

6.6.2 Input Data

The NWDAF collects Load and Performance information in an Area of Interest from the sources listed in Table 6.6.2-1 and number of UEs within Area of Interest from the sources listed in Table 6.6.2-2.

Table 6.6.2-1: Load and Performance information collected by NWDAF

Load information	Source	Description
Status, load and performance information	OAM	Statistics on RAN status (up/down), load (i.e. Radio Resource Utilization) and performance per Cell Id in the Area of Interest as defined in TS 28.552 [8].
NF Load information	NRF	Load per NF

Table 6.6.2-2: Number of UEs in Area of Interest information collected by NWDAF

Number of UEs information	Source	Description
Number of UEs	AMF	Number of UEs in an Area of Interest

The NWDAF shall be able to collect UE mobility information as stated in clause 6.7.2.2.

6.6.3 Output Analytics

The NWDAF shall be able to provide both statistics and predictions on Network Performance.

Network performance statistics are defined in Table 6.6.3-1.

Table 6.6.3-1: Network performance statistics

Information	Description
List of network performance information (1..max)	Observed statistics during the Analytics target period
> Area subset	TA or Cell ID within the requested area of interest as defined in clause 6.6.1
> Analytics target period subset	Time window within the requested Analytics target period as defined in clause 6.6.1.
> gNB status information	Average ratio of gNBs that have been up and running during the entire Analytics target period in the area subset
> gNB resource usage	Average usage of assigned resources (CPU, memory, disk)
> Number of UEs	Average number of UEs observed in the area subset
> Communication performance	Average ratio of successful setup of PDU Sessions
> Mobility performance	Average ratio of successful handover

Network performance predictions are defined in Table 6.6.3-2.

Table 6.6.3-2: Network performance predictions

Information	Description
List of network performance information (1..max)	Predicted analytics during the Analytics target period
> Area subset	TA or Cell ID within the requested area of interest as defined in clause 6.6.1
> Analytics target period subset	Time window within the requested Analytics target period as defined in clause 6.6.1.
> gNB status information	Average ratio of gNBs that will be up and running during the entire Analytics target period in the area subset
> gNB resource usage	Average usage of assigned resources (CPU, memory, disk) (average, peak)
> Number of UEs	Average number of UEs predicted in the area subset
> Communication performance	Average ratio of successful setup of PDU Sessions
> Mobility performance	Average ratio of successful handover
> Confidence	Confidence of this prediction

NOTE 1: The predictions are provided with a Validity Period, as defined in clause 6.1.3.

NOTE 2: The analytics on number of UEs are related to the information retrieved from the AMFs.

The number of network performance information entries is limited by the maximum number of objects provided as part of Analytics Reporting Information.

The NWDAF provides Network Performance Analytics to a consumer at the time requested by the consumer in the Analytics target period:

- Analytics ID set to "Network Performance".
- Notification Target Address including the address of the consumer.
- Notification Correlation Id, for the consumer to correlate notifications from NWDAF if subscription applies.
- Analytics specific parameters at the time indicated in the Analytics target period**.**

6.6.4 Procedures

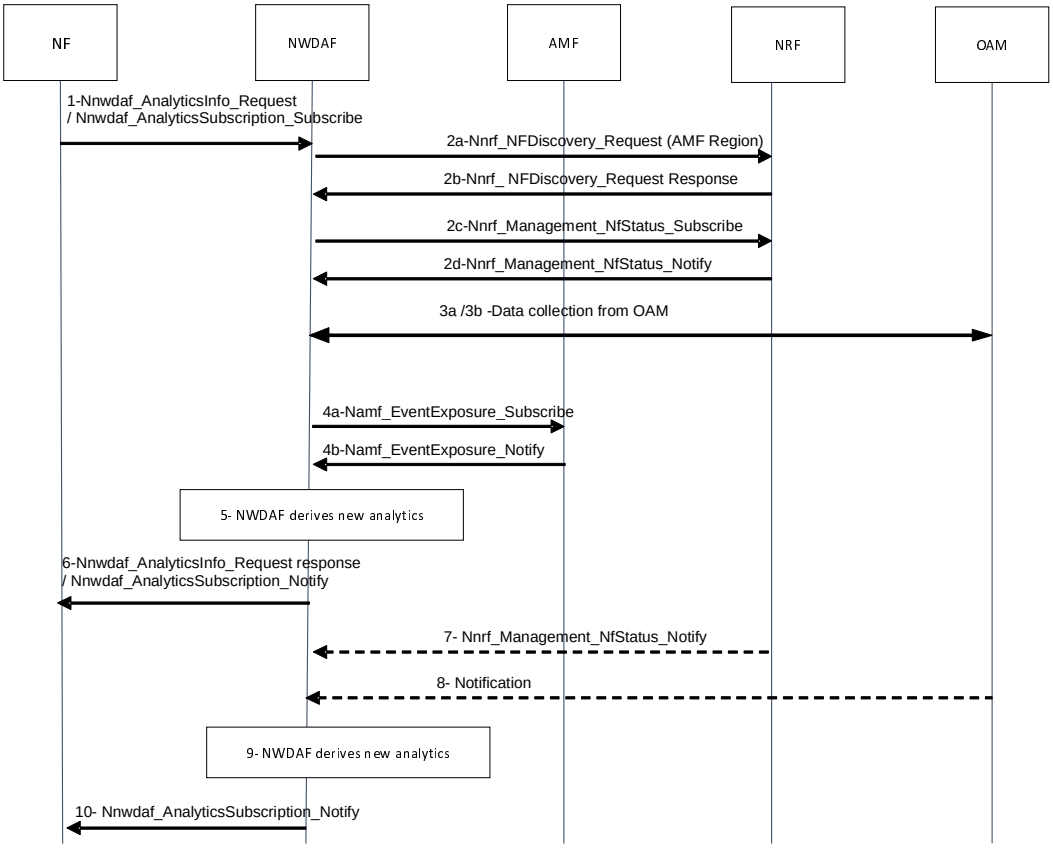

Figure 6.6.4-1: Procedure for subscription to network performance analytics

1. The NF sends Nnwdaf_AnalyticsSubscription_Subscribe or Nnwdaf_AnalyticsInfo_Request (Analytics ID="Network Performance", Target of Analytics Reporting, Analytics Filter="Area of Interest", "Reporting Thresholds" and Analytics target Period(s)) to the NWDAF.

2a-2d. The NWDAF discovers from NRF the AMF(s) belonging to the AMF Region(s) that include(s) the Area of Interest and subscribes to NF load and status information from NRF about these AMF(s).

3a-3b. The NWDAF subscribes to OAM services to get the status and load information and the resource usage on the Area of Interest in clause 6.6.2, following the procedure captured in Clause 6.2.3.2.

4a-4b. The NWDAF collects the number of UEs located in the Area of Interest from AMF using Namf_EventExposure_Subscribe service, including the Target of Event Reporting provided as an input parameter (i.e. any UE or Internal Group Identifier).

5. The NWDAF derives the requested analytics.

6. The NWDAF sends Nnwdaf_AnalyticsSubscription_Notify or Nnwdaf_AnalyticsInfo_Request response (Network Performance analytics, Subscription Correlation Id, Probability of assertion).

7-8. A change of network performance information, i.e. change in the gNB status information, gNB resource usage, communication performance and mobility performance in the area of interest at the observed period, is detected by OAM, or a change in the NF load information is reported by NRF, and is notified to NWDAF.

9. The NWDAF derives new analytics taking into account the most recent data collected.

10. When relevant according to the Analytics target period and Reporting Thresholds, the NWDAF provides a notification using Nnwdaf_AnalyticsSubscription_Notify (Network Performance analyticsSubscription Correlation Id, Probability of assertion).

6.7 UE related analytics

6.7.1 General

This clause specifies the UE related analytics which can be provided by NWDAF:

- UE mobility analytics;
- UE communication analytics;
- Expected UE behavioural parameters related network data analytics; and
- Abnormal behaviour related network data analytics.

The NWDAF service consumer may request for these analytics separately, or in a combined way. As an example, an NWDAF service consumer may learn from the NWDAF the expected UE behaviour parameters as defined in clause 4.15.6.3, TS 23.502 [3] for a group of UEs or a specific UE, by requesting analytics for both UE mobility (see clause 6.7.2) and for UE communication (see clause 6.7.3).

NOTE: Possible uses of such analytics is for the AMF to learn about expected UE behaviour to derive appropriate MICO mode configuration, or for an AF to learn about expected UE behaviour to further provision 5GC with appropriate UE parameters.

6.7.2 UE mobility analytics

6.7.2.1 General

NWDAF supporting UE mobility statistics or predictions shall be able to collect UE mobility related information from NF, OAM, and to perform data analytics to provide UE mobility statistics or predictions.

The service consumer may be a NF (e.g. AMF).

The consumer of these analytics may indicate in the request:

- The Target of Analytics Reporting which is a single UE or a group of UEs.
- Analytics Filter Information optionally containing:
  - Area of Interest;
- An Analytics target period indicates the time period over which the statistics or predictions are requested.
- Optionally, maximum number of objects.
- Preferred level of accuracy of the analytics (low/high).
- In a subscription, the Notification Correlation Id and the Notification Target Address are included.

6.7.2.2 Input Data

The NWDAF supporting data analytics on UE mobility shall be able to collect UE mobility information from OAM, 5GC and AFs. The detailed information collected by the NWDAF could be MDT data from OAM, network data from 5GC and/or service data from AFs:

- UE mobility information from OAM is UE location carried in MDT data;
- Network data related to UE mobility from 5GC is UE location information as defined in the Table 6.7.2.2-1;

Table 6.7.2.2-1: UE Mobility information collected from 5GC

Information	Source	Description
UE ID	AMF	SUPI
UE locations (1..max)	AMF	UE positions
>UE location		TA or cells that the UE enters (NOTE 1)
>Timestamp		A time stamp when the AMF detects the UE enters this location
Type Allocation code (TAC)	AMF	To indicate the terminal model and vendor information of the UE. The UEs with the same TAC may have similar mobility behaviour. The UE whose mobility behaviour is unlike other UEs with the same TAC may be an abnormal one.
Frequent Mobility Registration Update	AMF	A UE (e.g. a stationary UE) may re-select between neighbour cells due to radio coverage fluctuations. This may lead to multiple Mobility Registration Updates if the cells belong to different registration areas. The number of Mobility Registration Updates N within a period M may be an indication for abnormal ping-pong behaviour, where N and M are operator's configurable parameters.
NOTE 1: UE location includes either the last known location or the current location, under the conditions defined in Table 4.15.3.1-1 in TS 23.502 [3].		

- Service data related to UE mobility provided by AFs is defined in the Table 6.7.2.2-2;

Table 6.7.2.2-2: Service Data from AF related to UE mobility

Information	Description
UE ID	Could be external UE ID (i.e. GPSI)
Application ID	Identifying the application providing this information
UE trajectory (1..max)	Timestamped UE positions
>UE location	Geographical area that the UE enters
>Timestamp	A time stamp when UE enters this area

Depending on the requested level of accuracy, data collection may be provided on samples (e.g. spatial subsets of UEs or UE group, temporal subsets of UE location information).

NOTE: Reporting current UE location can cause AMF to request NG-RAN to report UE location and consequently extra signalling and load in NG-RAN and AMF. The consumer retrieving data from AMF needs to use current location with care to avoid excessive signalling.

The application Id is optional. If the application Id is omitted, the collected UE mobility information can be applicable to all the applications for the UE.

6.7.2.3 Output Analytics

The NWDAF supporting data analytics on UE mobility shall be able to provide UE mobility analytics to consumer NFs or AFs. The analytics results provided by the NWDAF could be UE mobility statistics as defined in table 6.7.2.3-1, UE mobility predictions as defined in Table 6.7.2.3-2:

Table 6.7.2.3-1: UE mobility statistics

Information	Description
UE group ID or UE ID	Identifies a UE or a group of UEs, e.g. internal group ID defined in TS 23.501 [2] clause 5.9.7, SUPI (see NOTE).
Time slot entry (1..max)	List of time slots during the Analytics target period
> Time slot start	Time slot start within the Analytics target period
> Duration	Duration of the time slot (average and variance)
> UE location (1..max)	Observed location statistics
>> UE location	TA or cells which the UE stays
>> Ratio	Percentage of UEs in the group (in the case of an UE group)

Table 6.7.2.3-2: UE mobility predictions

Information	Description
UE group ID or UE ID	Identifies an UE or a group of UEs, e.g. internal group ID defined in TS 23.501 [2] clause 5.9.7, or SUPI (see NOTE).
Time slot entry (1..max)	List of predicted time slots
>Time slot start	Time slot start time within the Analytics target period
> Duration	Duration of the time slot
> UE location (1..max)	Predicted location prediction during the Analytics target period
>> UE location	TA or cells where the UE or UE group may move into
>> Confidence	Confidence of this prediction
>> Ratio	Percentage of UEs in the group (in the case of an UE group)

NOTE: When target of analytics reporting is an individual UE, one UE ID (i.e. SUPI) will be included, the NWDAF will provide the analytics mobility result (i.e. list of (predicted) time slots) to NF service consumer(s) for the UE.

The results for UE groups address the group globally. The ratio is the proportion of UEs in the group at a given location at a given time.

The number of time slots and UE locations is limited by the maximum number of objects provided as part of Analytics Reporting Information

The time slots shall be provided by order of time, possibly overlapping. The locations shall be provided by decreasing value of ratio for a given time slot. The sum of all ratios on a given time slot must be equal or less than 100%. Depending on the list size limitation, the least probable locations on a given Analytics target period may not be provided.

6.7.2.4 Procedures

The NWDAF can provide UE mobility related analytics, in the form of statistics or predictions or both, to another NF. If the NF is an AF, and when the AF is untrusted, the AF will request analytics via the NEF, and the NEF will then convey the request to NWDAF.

NOTE: In the case of untrusted AF the Target of Analytics Reporting can be a GPSI or an External Group Identifier that is mapped in the 5GC to a SUPI or an Internal Group Identifier.

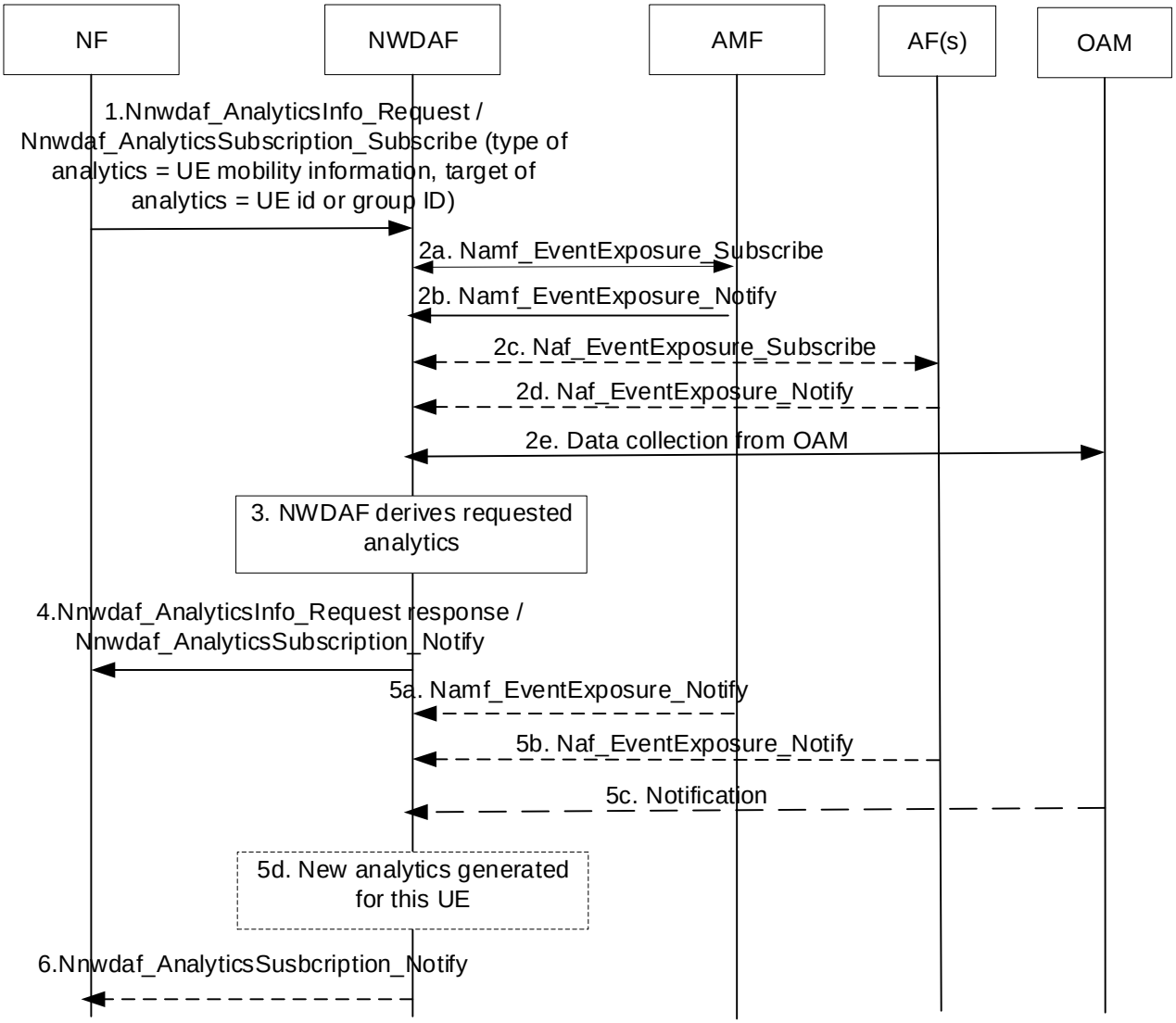

Figure 6.7.2.4-1: UE mobility analytics provided to an NF

1. The NF sends a request to the NWDAF for analytics on a specific UE or a group of UEs, using either the Nnwdaf_AnalyticsInfo or Nnwdaf_AnalyticsSubscription service. The NF can request statistics or predictions or both. The type of analytics is set to UE mobility information. The NF provides the UE id or Internal Group ID in the Target of Analytics Reporting.

2. If the request is authorized, and in order to provide the requested analytics, the NWDAF may subscribe to events with all the serving AMFs for notification of location changes. This step may be skipped when e.g. the NWDAF already has the requested analytics available.

   The NWDAF subscribes the service data from AF(s) in the Table 6.7.2.2-2 by invoking Naf_EventExposure_Subscribe service or Nnef_EventExposure_Subscribe (if via NEF)) using event ID "UE Mobility information" as defined in TS 23.502 [3].

   The NWDAF collects UE mobility information from OAM, following the procedure captured in clause 6.2.3.2.

NOTE: The NWDAF determines the AMF serving the UE or the group of UEs as described in clause 6.2.2.1.

3. The NWDAF derives requested analytics.

4. The NWDAF provide requested UE mobility analytics to the NF, using either the Nnwdaf_AnalyticsInfo_Request response or Nnwdaf_AnalyticsSubscription_Notify, depending on the service used in step 1. The details for UE mobility analytics provided by NWDAF are defined in clause 6.7.2.3.

5-6. If at step 1, the NF has subscribed to receive notifications for UE mobility analytics, after receiving event notification from the AMFs, AFs and OAM subscribed by NWDAF in step 2, the NWDAF may generate new analytics and provide them to the NF.

6.7.3 UE Communication Analytics

6.7.3.1 General

In order to support some optimized operations, e.g. customized mobility management, traffic routing handling, or QoS improvement, in 5GS, an NWDAF may perform data analytics on UE communication pattern and user plane traffic, and provide the analytics results (i.e. UE communication statistics or prediction) to NFs in the 5GC.

An NWDAF supporting UE Communication Analytics collects per-application communication description from AFs. If consumer NF provides an Application ID, the NWDAF only considers the data from AF, SMF and UPF that corresponds to this application ID.

The consumer of these analytics may indicate in the request:

- The Target of Analytics Reporting which is a single UE or a group of UEs.
- Analytics Filter Information optionally including:
  - S-NSSAI;
  - DNN;
  - Application ID;
  - Area of Interest.
- An Analytics target period indicates the time period over which the statistics or predictions are requested.
- Preferred level of accuracy of the analytics (low/high).
- Optionally, maximum number of objects;
- In a subscription, the Notification Correlation Id and the Notification Target Address are included.

6.7.3.2 Input Data

The NWDAF supporting data analytics on UE communication shall be able to collect communication information for the UE from 5GC. The detailed information collected by the NWDAF includes service data related to UE communication as defined in the Table 6.7.3.2-1.

Table 6.7.3.2-1: Service Data from 5GC related to UE communication

Information	Source	Description
UE ID	SMF, AF	SUPI in the case of SMF, external UE ID (i.e. GPSI) in the case of AF
Group ID	SMF, AF	To identify UE group if available Internal Group ID in the case of SMF, External Group ID in the case of AF
S-NSSAI	SMF	Information to identify a Network Slice
DNN	SMF	Data Network Name where PDU connectivity service is provided
Application ID	SMF, AF	Identifying the application providing this information
Expected UE Behaviour parameters	AF	Same as Expected UE Behaviour parameters specified in TS 23.502 [3]
UE communication (1..max)	UPF, AF	Communication description per application
>Communication start		The time stamp that this communication starts
>Communication stop		The time stamp that this communication stops
>UL data rate		UL data rate of this communication
>DL data rate		DL data rate of this communication
>Traffic volume		Traffic volume of this communication
Type Allocation code (TAC)	AMF	To indicate the terminal model and vendor information of the UE. The UEs with the same TAC may have similar communication behaviour. The UE whose communication behaviour is unlike other UEs with the same TAC may be an abnormal one.

NOTE: How NWDAF collects UE communication related data from UPF is not defined in this Release of the specification.

Depending on the requested level of accuracy, data collection may be provided on samples (e.g. spatial subsets of UEs or UE group, temporal subsets of UE communication information).

The application Id is optional. If the application Id is omitted, the collected UE communication information can be applicable to all the applications for the UE.

6.7.3.3 Output Analytics

The NWDAF supporting UE Communication Analytics provides the analytics results to consumer NFs. The analytics results provided by the NWDAF include the UE communication statistics as defined in Table 6.7.3.3-1 or predictions as defined in Table 6.7.3.3-2.

Table 6.7.3.3-1: UE Communication Statistics

Information	Description
UE group ID or UE ID	Identifies an UE or a group of UEs, e.g. internal group ID defined in TS 23.501 [2] clause 5.9.7 or SUPI (see NOTE).
UE communications (1..max)	List of communication time slots.
> Periodic communication indicator	Identifies whether the UE communicates periodically or not.
> Periodic time	Interval Time of periodic communication (average and variance) if periodic. Example: every hour
> Start time	Start time observed (average and variance)
> Duration time	Duration interval time of communication (average and variance).
> Traffic characterization	S-NSSAI, DNN, ports, other useful information.
> Traffic volume	Volume UL/DL (average and variance).
> Ratio	Percentage of UEs in the group (in the case of an UE group).

Table 6.7.3.3-2: UE Communication Predictions

Information	Description
UE group ID or UE ID	Identifies an UE or a group of UEs, e.g. internal group ID defined in TS 23.501 [2] clause 5.9.7 or SUPI (see NOTE).
UE communications (1..max)	List of communication time slots.
> Periodic communication indicator	Identifies whether the UE communicates periodically or not.
> Periodic time	Interval Time of periodic communication (average and variance) if periodic. Example: every hour.
> Start time	Start time predicted (average and variance).
> Duration time	Duration interval time of communication.
> Traffic characterization	S-NSSAI, DNN, ports, other useful information.
> Traffic volume	Volume UL/DL (average and variance).
> Confidence	Confidence of the prediction.
> Ratio	Percentage of UEs in the group (in the case of an UE group).

NOTE: When target of analytics reporting is an individual UE, one UE ID (i.e. SUPI) will be included, the NWDAF will provide the analytics communication result (i.e. list of (predicted) communication time slots) to NF service consumer(s) for the UE.

The results for UE groups address the group globally. The ratio is the proportion of UEs in the group for a given communication at a given time and duration.

The number of UE communication entries (1..max) is limited by the maximum number of objects provided as part of Analytics Reporting Information. The communications shall be provided by order of time, possibly overlapping.

Depending on the list size limitation, the least probable communications on a given Analytics target period may not be provided.

6.7.3.4 Procedures

The NWDAF can provide UE communication related analytics, in the form of statistics or predictions or both, to a 5GC NF.

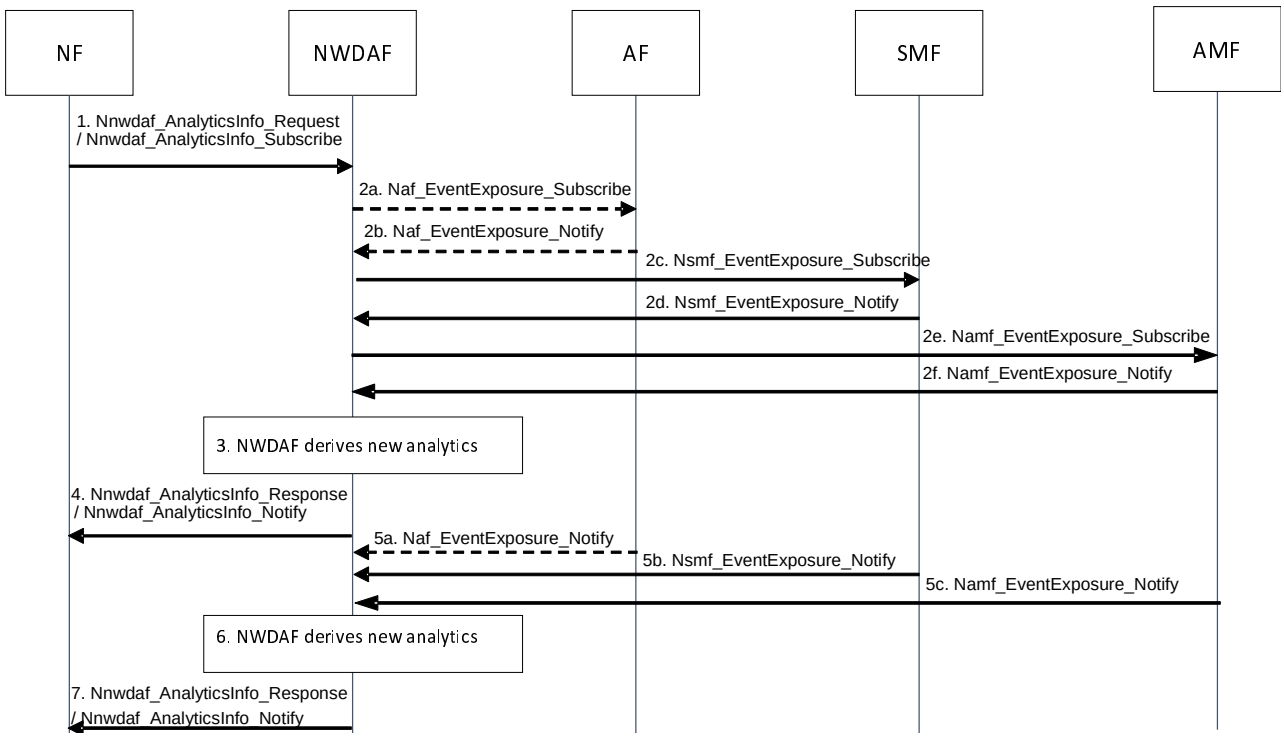

Figure 6.7.3.4-1: Procedure for UE communication analytics

1. 5GC NF to NWDAF: Nnwdaf_AnalyticsSubscription_Subscribe (Analytics ID=UE communication analytics, Target of Analytics Reporting=SUPI, Analytics Filter = (Application ID, Area of Interest, etc.)).

5GC NF sends a request to the NWDAF for analytics on a specific UE(s), using either Nnwdaf_AnalyticsInfo or Nnwdaf_AnalyticsSubscription_Subscribe service. The analytics type indicated by "Analytics ID" is set to "UE communication". The Target of Analytics Reporting is set to SUPI or an Internal Group Identifier and Analytics Filter may include Application ID and Area of Interest.

2a-b. NWDAF to AF (Optional): Naf_EventExposure_Subscribe (Event ID, external UE ID, Application ID, Area of Interest).

In order to provide the requested analytics, the NWDAF may subscribe per application communication information, which is identified by Application ID, from AFs for the UE. The Event ID "UE Communication information" as defined in TS 23.502 [3] is used, which indicates communication report for the UE which is requested by the 5GC NF in the step 1. The external UE ID is obtained by the NWDAF based on UE internal ID, i.e., SUPI. In the case of external AF, the NEF translates the requested Area of Interest into a list of geographic zone identifier(s) as described in clause 5.6.7.1 of TS 23.501 [2].

This step is skipped if the NWDAF already has the requested analytics available or has subscribed to the AF.

2c-d. NWDAF to SMF: Nsmf_EventExposure_Subscribe (Event ID, SUPI, Application ID).

In order to provide the requested analytics, the NWDAF subscribes to information of the UE from SMFs as defined in table 6.7.3.2-1.

2e-f. NWDAF to AMF: Namf_EventExposure_Subscribe (Event ID, SUPI, Area of Interest).

In order to provide the requested analytics, the NWDAF retrieves Type Allocation code from AMF.

NOTE: The NWDAF determines the SMF serving the UE as described in clause 6.2.2.1.

3. The NWDAF derives requested analytics, in the form of UE communication statistics or predictions or both.

4. NWDAF to 5GC NF: Nnwdaf_AnalyticsInfo_Request response or Nnwdaf_AnalyticsSubscription_Notify.

The NWDAF provides requested UE communication analytics to the NF, using either Nnwdaf_AnalyticsInfo_Request response or Nnwdaf_AnalyticsSubscription_Notify, depending on the service used in step 1.

5-7. If the NF subscribed UE communication analytics at step 1, when the NWDAF generates new analytics, it notifies the new generated analytics to the 5GC NF.

6.7.4 Expected UE behavioural parameters related network data analytics

6.7.4.1 General

The clause 6.7.4 defines how a service consumer learns from the NWDAF the expected UE behaviour parameters as defined in clause 4.15.6.3, TS 23.502 [3] for a group of UEs or a specific UE.

The service consumer may be an NF (e.g. AMF, AF), or the OAM.

The consumer of these analytics shall indicate in the request:

- Analytics ID set to "UE Mobility" or "UE Communication".
- The Target of Analytics Reporting can be a UE or an Internal Group Identifier.

NOTE: In the case of untrusted AF the Target of Analytics Reporting can be a GPSI or an External Group Identifier that is mapped in the 5GC to a SUPI or an Internal Group Identifier

- An Analytics target period, which indicates the time period over which the statistics or predictions are requested.
- Optional maximum number of objects;
- In a subscription, the Notification Correlation Id and the Notification Target Address are included.

The NWDAF shall notify the result of the analytics to the consumer as indicated in clause 6.7.4.3.

6.7.4.2 Input Data

In order to produce "UE Mobility" analytics, the NWDAF collects UE mobility information as defined in clause 6.7.2.2. In order to produce "UE Communication" analytics, the NWDAF collects UE communication information as defined in clause 6.7.3.2.

6.7.4.3 Output Analytics

The analytics results for "UE Mobility" are specified in Table 6.7.2.3-1 and Table 6.7.2.3-2.

The analytics results for "UE Communication" are specified in Table 6.7.3.3-1 and Table 6.7.3.3-2.

6.7.4.4 Procedures

6.7.4.4.1 NWDAF-assisted expected UE behavioural analytics

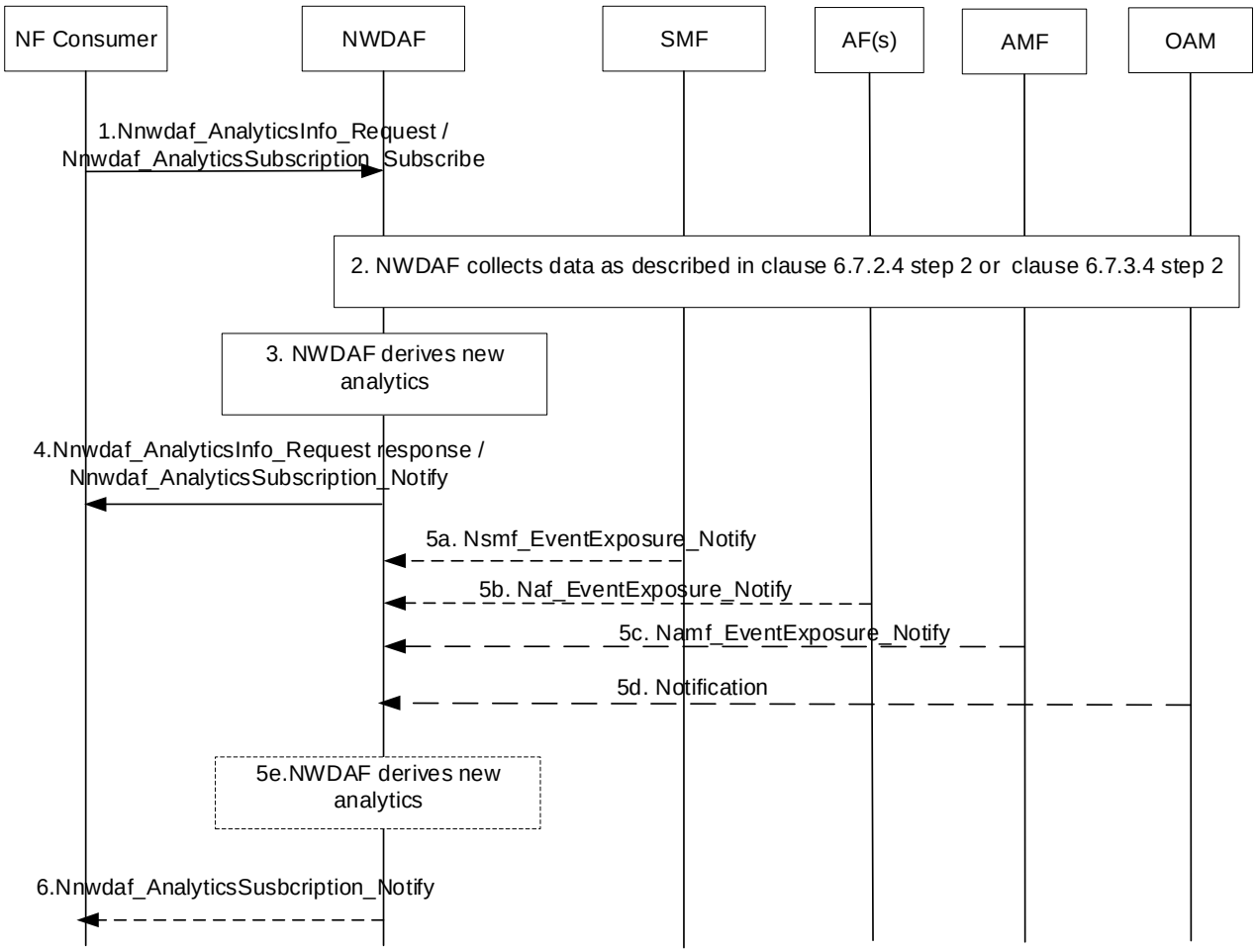

Figure 6.7.4.4.1-1: NWDAF assisted expected UE behavioural analytics procedure

1. 5GC NF (e.g., AMF, SMF and AF) to NWDAF: Nnwdaf_AnalyticsInfo_Request (Analytics ID, Target of Analytics Reporting=SUPI) or Nnwdaf_AnalyticsSubscription_Subscribe (Analytics ID, Target of Analytics Reporting =SUPI).

   The Analytics ID is set to "UE Mobility" or to "UE Communication"," and the consumer request analytics.

2. If Analytics ID is set to "UE Mobility", the NWDAF collects data from OAM, AMF and/or AF as specified in clause 6.7.2.4 step 2, unless the information is already available.

   If Analytics ID is set to "UE Communication", the NWDAF collects data from AMF, SMF and/or AF as specified in clause 6.7.3.4 step 2, unless the information is already available.

3. The NWDAF derives requested analytics.

4. NWDAF to 5GC NF: Nnwdaf_AnalyticsInfo_Request response or Nnwdaf_AnalyticsSubscription_Notify.

   The NWDAF provides requested Expected UE behaviour to the NF, using either Nnwdaf_AnalyticsInfo_Response or Nnwdaf_AnalyticsSubscription_Notify, depending on the service used in step 1.

5-6. If the NF subscribed to at step 1, when the NWDAF generates new analytics, it provides the new generated analytics to the NF.

6.7.5 Abnormal behaviour related network data analytics

6.7.5.1 General

This clause defines how to identify a group of UEs or a specific UE with abnormal behaviour, e.g. being misused or hijacked, with the help of NWDAF.

NOTE 1: The misused or hijacked UEs are UEs in which there are malicious applications running or UEs which have been stolen.

The consumer of this analytics could be a 5GC NF. The 5GC NF subscribes analytics on abnormal behaviour from a NWDAF based on the UE subscription, network configuration or application layer request.

The NWDAF performs data analytics on abnormal behaviour if there is a related subscription and returns exception reports that result from the analysis of the correlations between behavioural variables. The exception reports contain an Exception Level expressed in the form of a scalar value, possibly supplemented by additional measurements.

The consumer of this analytics shall indicate in the request:

- Analytics ID set to "Abnormal behaviour";
- The Target of Analytics Reporting can be one UE, any UE or an Internal Group Identifier;
- An Analytics target period indicates the time period over which the statistics or predictions are requested;
- Analytics Filter Information optionally including:
  - expected UE behaviour parameters;
  - expected analytics type or list of Exception IDs with associated thresholds for the Exception Level, where the expected analytics type can be mobility related, communication related or both;
  - Area of interest;
  - Application ID;
  - DNN;
  - S-NSSAI.

NOTE 2: The expected analytics type generally indicates whether mobility or communication related abnormal behaviour analytics or both are expected by the consumer, and the list of exception IDs indicates what specific analytics are expected by the consumer. Either the expected analytics type or the list of Exception IDs needs to be indicated, but they are not presented simultaneously. When the expected analytics type is indicated, the NWDAF performs corresponding abnormal behaviour analytics which are supported by the NWDAF. The relation between the expected analytics type and Exception IDs is defined in Table 6.7.5.1-1.

- Optionally, maximum number of objects and maximum number of SUPIs;
- In a subscription, the Notification Correlation Id and the Notification Target Address are included.

Table 6.7.5.1-1: Relation between expected analytics type and Exception IDs

Expected analytics type	Exception IDs matching the expected analytics type
mobility related	Unexpected UE location, Ping-ponging across neighbouring cells, Unexpected wakeup, Unexpected radio link failures.
communication related	Unexpected long-live/large rate flows, Unexpected wakeup, Suspicion of DDoS attack, Wrong destination address, Too frequent Service Access.

If the Target of Analytics Reporting is any UE, then the Analytics Filter should at least include:

- Area of Interest or S-NSSAI, if the expected analytics type or the list of Exception IDs is mobility related.
- Area of Interest, application ID, DNN or S-NSSAI, if the expected analytics type or the list of Exception IDs is communication related.

If the target of Analytics Reporting is any UE, the consumer of this analytics shall request either mobility related only or communication related only abnormal behaviour analytics, but not both at the same time.

The expected UE behaviour parameters that the consumer can indicate in the request when known depend on the Exception ID that the consumer expects. They may encompass UE behaviour parameters as defined in TS 23.502 [3] clause 4.15.6.3, and other parameters. Table 6.7.5.1-2 shows the mapping between each Exception ID and UE behaviour parameters.

Table 6.7.5.1-2: Description of Expected UE Behaviour parameters per Exception ID

Exception ID	UE behaviour parameters to provide
Unexpected UE location	Expected UE Moving Trajectory Stationary Indication
Unexpected long-live/large rate flows	Periodic Time Scheduled Communication Time Communication Duration Time
Unexpected wakeup	Periodic Time Communication Duration Time Scheduled Communication Time
Suspicion of DDoS attack	Periodic Time Communication Duration Time Scheduled Communication Time Scheduled Communication Type Traffic Profile
Too frequent Service Access	Periodic Time
Unexpected radio link failures	Expected UE Moving Trajectory
Ping-ponging across neighbouring cells	Expected UE Moving Trajectory Stationary Indication

When the NWDAF detects those UEs that deviate from the expected UE behaviour, e.g. unexpected UE location, abnormal traffic pattern, wrong destination address etc., the NWDAF shall notify the result of the analytics to the consumer as specified in clause 6.7.5.3.

6.7.5.2 Input Data

The Exceptions information from AF is as specified in Table 6.7.5.2-1.

On request of the service consumer, the NWDAF shall collect and analyse UE behavioural information from the 5GC NFs (SMF, AMF, AF), or OAM as specified in clauses 6.7.2.2 and 6.7.3.2 and/or expected UE behavioural parameters from UDM as defined in clause 4.15.6.3 of TS 23.502 [3], depending on Exception IDs.

NOTE: Care needs to be taken with regards to load by avoiding to cause major extra signalling when collecting data for any UE.

Table 6.7.5.2-1: Exceptions information from AF

Information	Description
IP address 5-tuple	To identify a data flow of a UE via the AF (such as the Firewall or a Threat Intelligence Sharing platform)
Exceptions (1..max) (NOTE 1)	
>Exception ID	Indicating the Exception ID (such as Unexpected long-live/large rate flows and Suspicion of DDoS attack as defined in Table 6.7.5.3-2) of the data flow.
>Exception Level	Scalar value indicating the severity of the abnormal behaviour.
>Exception trend	Measured trend (up/down/unknown/stable)
NOTE 1: The Exceptions information and the UE behavioural information as defined in clauses 6.7.2.2 and 6.7.3.2 could help NWDAF to train an Abnormal classifier, which could be used to classify a UE behaviour data into Normal behaviour or Exception.	

6.7.5.3 Output Analytics

Corresponding to the "abnormal behaviour" Analytics ID, the analytics result provided by the NWDAF is defined in Table 6.7.5.3-1 and Table 6.7.5.3-2. When the level of an exception trespasses above or below the threshold, the NWDAF shall notify the consumer with the exception ID associated with the exception if the exception ID is within the list of exception IDs indicated by the consumer or matches the expected analytics type indicated by the consumer. The NWDAF shall provide the Exception Level and determine which of the other information elements to provide, depending on the observed exception.

Abnormal behaviour statistics information is defined in Table 6.7.5.3-1.

Table 6.7.5.3-1: Abnormal behaviour statistics

Information	Description
Exceptions (1..max)	List of observed exceptions
> Exception ID	The risk detected by NWDAF
> Exception Level	Scalar value indicating the severity of the abnormal behaviour
> Exception trend	Measured trend (up/down/unknown/stable)
> UE characteristics	Internal Group Identifier, TAC
> SUPI list (1..SUPImax)	SUPI(s) of the UE(s) affected with the Exception
> Ratio	Estimated percentage of UEs affected by the Exception within the Target of Analytics Reporting
> Amount	Estimated number of UEs affected by the Exception (applicable when the Target of Analytics Reporting = "any UE")
> Additional measurement	Specific information for each risk (see Table 6.7.5.3-3)

Abnormal behaviour predictions information is defined in Table 6.7.5.3-2.

Table 6.7.5.3-2: Abnormal behaviour predictions

Information	Description
Exceptions (1..max)	List of predicted exceptions
> Exception ID	The risk detected by NWDAF
> Exception Level	Scalar value indicating the severity of the abnormal behaviour
> Exception trend	Measured trend (up/down/unknown/stable)
> UE characteristics	Internal Group Identifier, TAC
> SUPI list (1..SUPImax)	SUPI(s) of the UE(s) affected with the Exception
> Ratio	Estimated percentage of UEs affected by the Exception within the Target of Analytics Reporting
> Amount	Estimated number of UEs affected by the Exception (applicable when the Target of Analytics Reporting = "any UE")
> Additional measurement	Specific information for each risk (see Table 6.7.5.3-3)
> Confidence	Confidence of this prediction

The UE characteristics may provide a set of features common to all UEs affected with the exception.

The number of exceptions and the length of the SUPI list shall respectively be lower than the parameters maximum number of objects and Maximum number of SUPIs provided as part of Analytics Reporting Information.

If PCF subscribes to notifications on "Abnormal behaviour", the NWDAF shall send the PCF notifications about the risk, which may trigger the PCF to update the AM/SM policies.

The NWDAF also sends the notification directly to the AMF or SMF, if the AMF or SMF subscribes to the notification, so that the AMF or SMF may, based on operator local policies defined on a per S-NSSAI basis (for AMF) or on a per S-NSSAI, per DNN, or per (DNN,S-NSSAI) basis (for SMF), take actions for risk solving.

If the AF subscribes to notifications on "Abnormal behaviour", the NWDAF sends the notifications to the AF so that the AF may take actions for risk solving.

The following Table 6.7.5.3-3 gives examples of additional measurement provided by the NWDAF and examples of NF actions for solving each risk.

Table 6.7.5.3-3: Examples of additional measurements and NF actions for risk solving

Exception ID and description	Additional measurement	Actions of NFs
Unexpected UE location	Unexpected UE location (TA or cells which the UE stays)	PCF may extend the Service Area Restrictions with current UE location. AMF may extend the mobility restriction with current UE location.
Ping-ponging across neighbouring cells	Numbers, frequency, time and location information, assumption about the possible circumstances of the ping-ponging	If the ping-ponging are per UE, then: 1. the AMF may adjust the UE (e.g. a stationary UE) registration area. 2. the AMF and/or the AF may allow the use of Coverage Enhancement for the affected UE.
Unexpected long-live/large rate flows	Unexpected flow template (IP address 5 tuple)	SMF updates the QoS rule, e.g. decrease the MBR for the related QoS flow. PCF, if dynamic PCC applies for corresponding DNN, S-NSSAI, updates PCC Rules that triggers SMF updates the QoS rule, e.g. decrease the MBR for the related QoS flow.
Unexpected wakeup	Time of unexpected wake-up	AMF applies MM back-off timer to the UE.
Suspicion of DDoS attack	Victim's address (target IP address list)	PCF may request SMF to release the PDU session. SMF may release the PDU session and apply SM back-off timer.
Wrong destination address	Wrong destination address (target IP address list)	PCF updates the packet filter in the PCC Rules that triggers the SMF to update the related QoS flow and configures the UPF.
Too frequent Service Access	Volume, frequency, time, assumptions about the possible circumstances	AF may release the AF session. PCF may request SMF to release the PDU session. SMF may release the PDU session and apply SM back-off timer.
Unexpected radio link failures	Numbers, frequency, time and location, assumptions about the possible circumstances	If the unexpected radio link failures are per UE location bases, the AMF may allow the use of CE (Coverage Enhancement) in the affected location. Also, the Operator may improve the coverage conditions in the affected location. If the unexpected radio link failures are per UE bases, then the AMF and/or the AF may allow the use of CE for the affected UE.

6.7.5.4 Procedure

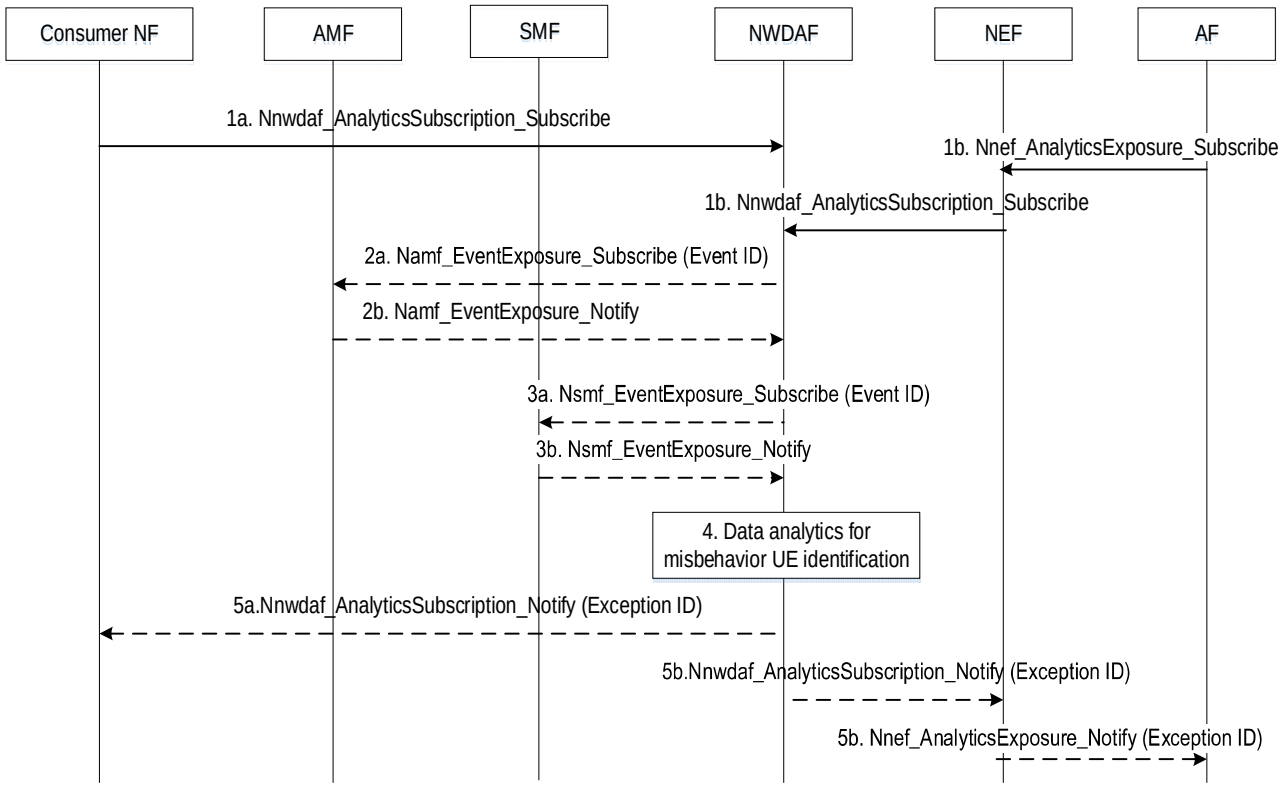

Figure 6.7.5.4-1: Procedure for NWDAF assisted misused or hijacked UEs identification

1a. A consumer NF subscribes to/requests NWDAF using Nnwdaf_AnalyticsSubscription_Subscribe/ Nnwdaf_AnalyticsInfo_Request (Analytics ID set to "Abnormal behaviour", Target of Analytics Reporting = Internal-Group-Identifier, any UE or SUPI, Analytics Filter Information).

A consumer NF may subscribe to/request abnormal behaviour notification/response from NWDAF for a group of UEs, any UE or a specific UE. The Analytics ID indicates the NWDAF to identify misused or hijacked UEs through abnormal behaviour analytic.

1b. AF to NWDAF: Nnwdaf_AnalyticsSubscription_Subscribe or Nnwdaf_AnalyticsInfo_Request (Analytics ID, Target of Analytics Reporting = External-group identifier, any UE or External UE ID, Analytics Filter Information).

For untrusted AFs, the AF sends the subscription via a NEF, where the AF invokes NEF service Nnef_AnalyticsExposure_Subscribe or Nnef_AnalyticsExposure_Fetch (Analytics ID, Target of Analytics Reporting = External-group-identifier, any UE or External UE ID, Analytics Filter Information).

An AF may also subscribe to/request abnormal behaviour notification/response from NWDAF for a group of UEs, a specific UE or any UE, where the subscription/request message may contain expected UE behaviour parameters identified on the application layer. If an External-Group-Identifier is provided by the AF, the NEF interrogates UDM to map the External-Group-Identifier to the Internal-Group-Identifier and obtain SUPI list corresponding to the Internal-Group-Identifier.

2. [Conditional] NWDAF to AMF: Namf_EventExposure_Subscribe (Event ID(s), Event Filter(s), Internal-Group-Identifier, any UE or SUPI).

The NWDAF sends subscription requests to the related AMF to collect UE behavioural information if it has not subscribed such data.

NOTE 1: The NWDAF determines the related AMF(s) as described in clause 6.2.2.1.

The AMF sends event reports to the NWDAF based on the report requirements contained in the subscription request received from the NWDAF.

If requested by NWDAF via Event Filter(s), the AMF checks whether the UE's behaviour matches its expected UE behavioural information. In this case, the AMF sends event reports to the NWDAF only when it detects that the UE's behaviour deviated from its expected UE behaviour.

Depending on the Exception ID, the NWDAF may in addition perform data collection from OAM as specified in clause 6.2.3.2.

3. [Conditional] NWDAF to SMF: Nsmf_EventExposure_Subscribe (Event ID(s), Event Filter(s), Internal-Group-Identifier, any UE or SUPI).

   The NWDAF sends subscription requests to the related SMF(s) if it has not subscribed to such data.

NOTE 2: Besides Analytics Filter Information, other mechanisms such as setting maximum number of SUPIs, and/ or using sampling ratio as part of Analytics Reporting Parameters as per Event Reporting Information (clause 4.15.1, TS 23.502 [3]) can be used by the analytics consumer to limit signalling load, e.g. when the target of analytics reporting is "any UE". The NWDAF can also use sampling ratio when subscribing towards AMF and SMF.

NOTE 3: The NWDAF determines the related SMF(s) as described in clause 6.2.2.1.

The SMF sends event reports to the NWDAF based on the report requirements contained in the subscription request received from the NWDAF.

If requested by NWDAF via Event Filter(s), the SMF checks whether the UE's behaviour matches its expected UE behavioural information. In this case, the SMF sends event reports to the NWDAF only when it detects that the UE's behaviour deviated from its expected UE behaviour.

4. The NWDAF performs data analytics for misused or hijacked UEs identification. Based on the analytics and operator's policies the NWDAF determines whether to send a notification to the consumer NF or AF.

5a. [Conditional] NWDAF to consumer NF (AMF or PCF or SMF depending on the subscription): Nnwdaf_AnalyticsSubscription_Notify or Nnwdaf_AnalyticsInfo_Response (Analytics ID, Exception ID, Internal-Group-Identifier or SUPI, Exception level) (which is used depending on the service used in step 1a).

If the NWDAF determines to send a notification/response to the consumer 5GC NFs, the NWDAF invokes Nnwdaf_EventSubscription_Notify or Nnwdaf_AnalyticsInfo_Response services. Based on the notification/response, the 5G NFs adopt configured actions to resolve/mitigate/avoid the risks as described in the Table 6.7.5.3-1.

5b. [Conditional] NWDAF to AF: Nnwdaf_AnalyticsSubscription_Notify or Nnwdaf_AnalyticsInfo_Response (Analytics ID, Exception ID, External UE ID, Exception level) (which is used depending on the service used in step 1b).

If the NWDAF determines to send a notification/response to the consumer AF, the NWDAF needs to include external UE ID of the identified UE into the notification/response message.

NOTE 3: Based on the notification, the AF can adopt corresponding actions, e.g. adjusting recommended TCP Window Size, adjusting recommended Service Start and End.

NOTE 4: The call flow only shows a subscribe-notify model for the interaction of NWDAF and consumer NF for simplicity instead of both request-response model and subscription-notification model.

6.8 User Data Congestion Analytics

6.8.1 General

The NWDAF can provide user data congestion related analytics, by one-time reporting or continuous reporting, in the form of statistics or predictions or both, to another NF. User Data Congestion related analytics can relate to congestion experienced while transferring user data over the control plane or user plane or both. A request for user data congestion analytics relates to a specific area or to a specific user. If the consumer of these analytics provides a UE ID, the NWDAF determines the area where the UE is located. The NWDAF then collects measurements per cell and uses the measurements to determine user data congestion analytics.

The request for user data congestion related analytics indicates the location area information where congestion related analytics is desired or indicates a UE Identity that can be used by the NWDAF to determine the location area information where congestion related analytics is desired. When the consumer of user data congestion related analytics subscribes to user data congestion related analytics, it may indicate a threshold and the NWDAF will provide analytics to the consumer when the congestion level crosses the threshold. The consumer can indicate an S-NSSAI in the request when congestion analytics are needed on a per slice level.

The service consumer may be an NF (e.g. NEF, AF).

The consumer of these analytics may indicate in the request or subscription:

- Analytics ID set to "User Data Congestion".
- Target of Analytics Reporting containing either a SUPI, or "any UE".
- Analytics Filter Information containing:
  - Area of Interest (list of TA or Cells) which restricts the area in focus (mandatory if Target Of Analytics Reporting is set to "any UE", optional otherwise);
  - Optional S-NSSAI, in order to obtain congestion analytics only on a given slice.
- Optional Reporting Threshold, which applies only for subscriptions and indicates conditions on the congestion level (Network Status Indication, see clause 6.8.3) to be reached in order to be notified by the NWDAF.
- Optional maximum number of objects;
- An Analytics target period indicates the time period over which the statistics or prediction are requested, either in the past or in the future.
- In a subscription, the Notification Correlation Id and the Notification Target Address are included.

The NWDAF notifies the result of the analytics to the consumer as indicated in clause 6.8.3.

6.8.2 Input data

The detailed information collected by the NWDAF is defined in Table 6.8.2-1.

NOTE: Performance Measurements defined in TS 28.552 [8] represent resource utilisation but do not, by themselves, indicate the event of congestion or congestion levels. The NWDAF collects measurements from the OAM and how the NWDAF derives Network Status Indication (NSI) is not specified.

Table 6.8.2-1: Data Collected from the NF related to User Data Congestion Analytics

Information	Source	Description
UE Location	AMF	UE location information that NWDAF can use to derive the Area of Interest.
Measurements	OAM	Performance Measurements that will be used by the NWDAF to determine congestion levels. Performance Measurements are related to information transfer over the user plane and/or the control plane (e.g. UE Throughput, DRB Setup Management, RRC Connection Number, PDU Session Management, and Radio Resource Utilization as defined in TS 28.552 [8]). The NWDAF may obtain measurements by invoking management services that are defined in TS 28.532 [6] and TS 28.550 [7].

Additionally, NWDAF may use statistics or predictions on service experience as specified in clause 6.4.3 as an input, e.g. for service experience in a given area or service experience for some specific applications such as high bandwidth applications.

6.8.3 Output analytics

The NWDAF outputs the user data congestion analytics for transfer over the user plane, for transfer over the control plane, or for both. The output may consist of statistics, predictions, or both. The detailed information provided by the NWDAF is defined in Table 6.8.3-1 for statistics and in Table 6.8.3-2 for predictions.

Table 6.8.3-1: User Data Congestion statistics

Information	Description
Area of Interest	A list of TAIs or Cell IDs
List of user data congestion Analytics (1..max)	
>Type	User Plane or Control Plane
>Applicable Time Window	The time period that the analytics applies to
>Network Status Indication	Congestion Level

Table 6.8.3-2: User Data Congestion predictions

Information	Description
Area of Interest	A list of TAIs or Cell IDs
List of user data congestion Analytics (1..max)	
>Type	User Plane or Control Plane
>Applicable Time Window	The time period that the analytics applies to
>Network Status Indication	Congestion Level
> Confidence	Confidence of this prediction

The number of user data congestion analytics entries is limited by the maximum number of objects provided as part of Analytics Reporting Information.

6.8.4 Procedures

6.8.4.1 Procedure for one-time or continuous reporting of analytics for user data congestion in a geographic area

The procedure as depicted in Figure 6.8.4.1-1 is used by an NF to retrieve congestion analytics for a specific geographic area. The procedure can be used to request a one-time or continuous reporting of congestion analytics.

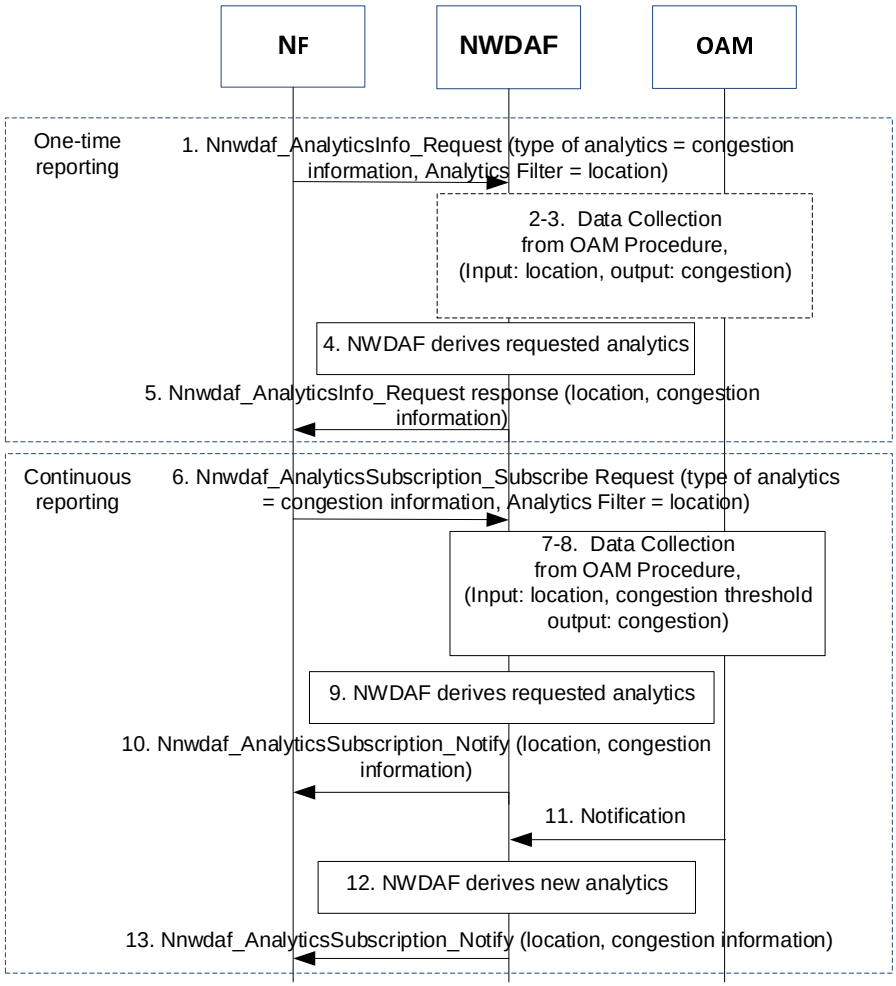

Figure 6.8.4.1-1: Procedure for one-time or continuous reporting of analytics for congestion in a geographic area

For one-time reporting:

1. The NF sends Nnwdaf_AnalyticsInfo_Request to NWDAF, indicating request for analytics for congestion in a specific location. The NF can request statistics or predictions or both. The type of analytics is set to user data congestion analytics for transfer over user plane, control plane, or both, Analytics Filter is set to a location (e.g. ECGI, TA).

2-3. If the request is authorized, and in order to provide the requested analytics, the NWDAF may request the measurement information for the requested location from OAM services following the data collection from OAM procedure as captured in 6.2.3.2. If the NWDAF already has information about the requested location, these steps are omitted. The NWDAF may obtain measurements by invoking management services that are defined in TS 28.532 [6] and TS 28.550 [7].

4. The NWDAF derives requested analytics.

5. The NWDAF provides the analytics for congestion to the NF.

For continuous reporting:

6. The NF sends Nnwdaf_AnalyticsSubscription_Subscribe Request to the NWDAF, indicating request for analytics for congestion in a specific location (e.g. ECGI, TA), possibly with thresholds. The NF can request statistics or predictions or both. The type of analytics is set to user data congestion analytics for transfer over user plane, control plane, or both.

7-8. The NWDAF subscribes to OAM services following the data collection from OAM procedure as captured in 6.2.3.2 to get measurement information for the requested location, possibly providing measurement thresholds.

The NWDAF may obtain measurements by invoking management services that are defined in TS 28.532 [6] and TS 28.550 [7].

9. The NWDAF derives requested analytics.
10. The NWDAF provides the analytics for congestion to the NF.
11. A change of user data congestion status corresponding to crossing a threshold set by the NWDAF is detected by OAM and notified to NWDAF.
12. The NWDAF derives new analytics.
13. The NWDAF provides a notification for analytics for the user data congestion to the NF.

6.8.4.2 Procedure for one-time or continuous reporting of analytics for user data congestion for a specific UE

The procedure as depicted in Figure 6.8.4.2-1 is used by an NF to retrieve user data congestion analytics for a specific UE. The procedure can be used to request a one-time or continuous reporting of user data congestion analytics.

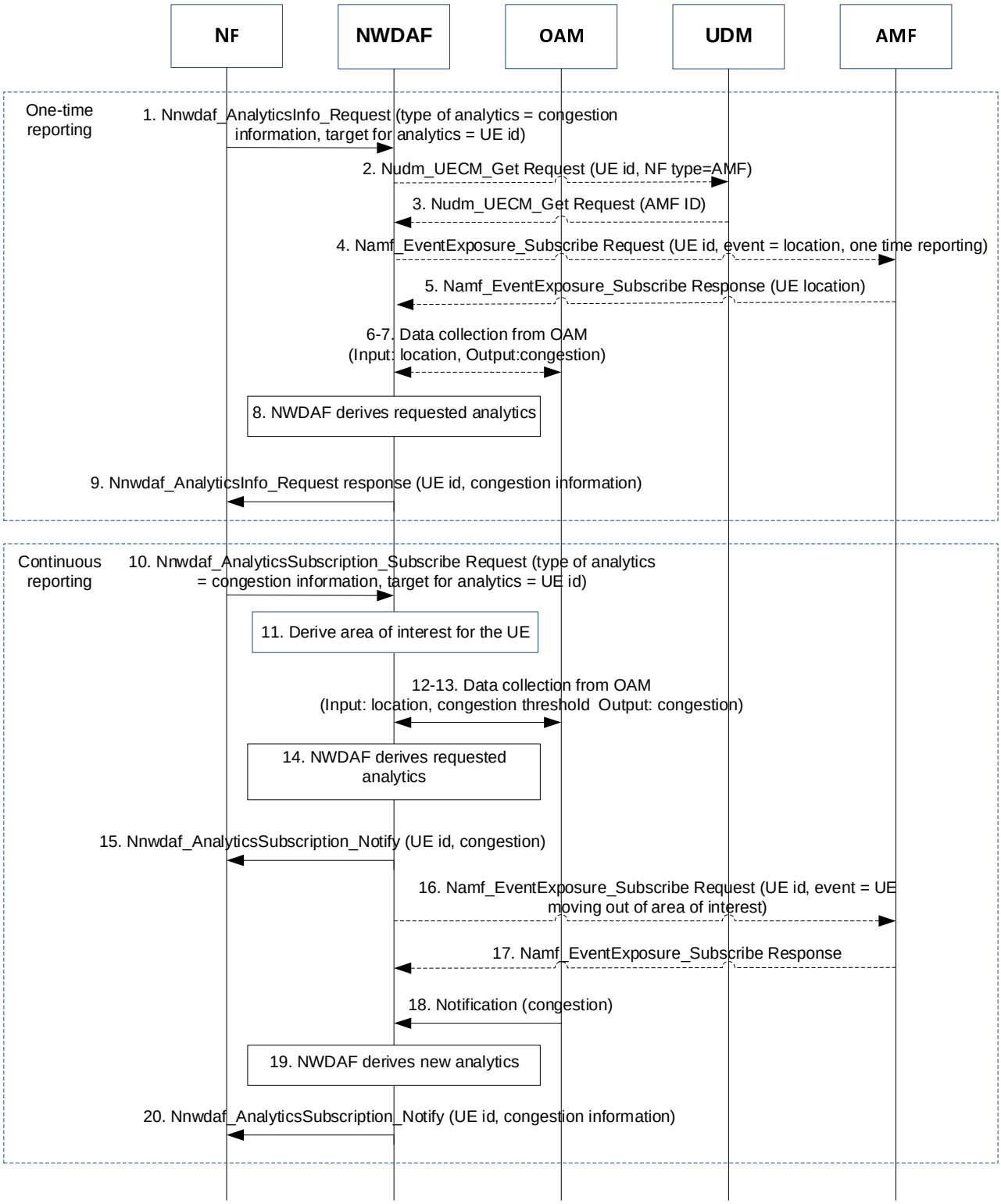

Figure 6.8.4.2-1: Procedure for one-time or continuous reporting of analytics for congestion for a specific UE

For one-time reporting:

1. The NF sends Nnwdaf_AnalyticsInfo_Request to NWDAF, requesting for analytics for user data congestion for a specific UE id. The NF can request statistics or predictions or both. The type of analytics is set to user data congestion analytics for transfer over user plane, control plane, or both, the Target of Analytics Reporting is set to UE id.

2-5. The NWDAF may already know the UE location. If not, the NWDAF checks the UE location by first retrieving the AMF serving the UE (steps 2-3) and then by interrogating the AMF about the UE location.

6-7. The NWDAF requests measurement information for the UE location from OAM services (as captured in 6.2.3.2). These steps are omitted if the NWDAF already has the information. The NWDAF may obtain measurements by invoking management services that are defined in TS 28.532 [6] and TS 28.550 [7].

8. The NWDAF derives requested analytics.

9. The NWDAF provides the analytics for congestion to the NF.

For continuous reporting:

10. The NF sends Nnwdaf_AnalyticsSubscription_Subscribe Request to the NWDAF. The NF can request for statistics or for predictions or for both. The type of analytics is set to user data congestion analytics for transfer over user plane, control plane, or both.

11. The NWDAF determines the UE location, either via internal information or by applying the same steps as steps 2 to 5. The NWDAF then determines an area of interest.

12-13. The NWDAF subscribes to OAM services (as captured in 6.2.3.2) to get the measurement information for the UE location, possibly providing measurement thresholds. The NWDAF may obtain measurements by invoking management services that are defined in TS 28.532 [6] and TS 28.550 [7].

14. The NWDAF derives requested analytics.

15. The NWDAF provides the analytics for user data congestion status information to the NF.

16-17. The NWDAF subscribes to UE mobility event notification in order to be informed when the UE moves out of the area of interest (in order to define a new area of interest and request new information to OAM if the UE moves to a different area).

18. A change of user data congestion status corresponding to crossing a threshold set by the NWDAF is detected by OAM and notified to NWDAF.

19. The NWDAF derives new analytics.

20. The NWDAF provides a notification for analytics for the user data congestion status information to the NF.

6.9 QoS Sustainability Analytics

6.9.1 General

The consumer of QoS Sustainability analytics may request the NWDAF analytics information regarding the QoS change statistics for an Analytics target period in the past in a certain area or the likelihood of a QoS change for an Analytics target period in the future in a certain area. The consumer can request either to subscribe to notifications (i.e. a Subscribe-Notify model) or to a single notification (i.e., a Request-Response model).

The service consumer may be a NF (e.g. AF).

The request includes the following parameters:

- Analytics ID = "QoS Sustainability";
- Target of Analytics Reporting: "any UE";
- Analytics Filter Information containing:
  - QoS requirements (mandatory):
    - 5QI (standardized or pre-configured), and applicable additional QoS parameters and the corresponding values (conditional, i.e. it is needed for GBR 5QIs to know the GFBR); or
    - the QoS Characteristics attributes including Resource Type, PDB, PER and their values;

  - Location information (mandatory): an area or a path of interest. The location information could reflect a list of waypoints;

NOTE: In this Release, the consumer of the "QoS Sustainability" Analytics ID will provide location information in the area of interest format (TAIs or Cell IDs) which is understandable by NWDAF.

  - S-NSSAI (optional);

- Optional maximum number of objects;

- Analytics target period: relative time interval, either in the past or in the future, that indicates the time period for which the QoS Sustainability analytics is requested;

- Reporting Threshold(s), which apply only for subscriptions and indicate conditions on the level to be reached for the reporting of the analytics, i.e. to discretize the output analytics and to trigger the notification when the threshold(s) provided in the analytics subscription are crossed by the expected QoS KPIs. The level(s) relate to value(s) of the QoS KPIs defined in TS 28.554 [10], for the relevant 5QI:

  - for a 5QI of GBR resource type, the Reporting Threshold(s) refer to the QoS flow Retainability KPI;

  - for a 5QI of non-GBR resource type, the Reporting Threshold(s) refer to the RAN UE Throughput KPI.

  An acceptable deviation from the threshold level in the non-critical direction (i.e. in which the QoS is improving) may be set to limit the amount of signalling.

- In a subscription, the Notification Correlation Id and the Notification Target Address.

The NWDAF collects the corresponding statistics information on the QoS KPI for the relevant 5QI of interests from the OAM, i.e. the QoS flow Retainability or the RAN UE Throughput as defined in TS 28.554 [10].

If the Analytics target period refers to the past:

- The NWDAF verifies whether the triggering conditions for the notification of QoS change statistics are met and if so, generates for the consumer one or more notifications.

- The analytics feedback contains the information on the location and the time for the QoS change statistics and the Reporting Threshold(s) that were crossed.

If the Analytics target period is in the future:

- The NWDAF detects the need for notification about a potential QoS change based on comparing the expected values for the KPI of the target 5QI against the Reporting Threshold(s) provided by the consumer in any cell in the requested area for the requested Analytics target period. The expected KPI values are derived from the statistics for the 5QI obtained from OAM. OAM information may also include planned or unplanned outages detection and other information that is not in scope for 3GPP to discuss in detail.

- The analytics feedback contains the information on the location and the time when a potential QoS change may occur and what Reporting Threshold(s) may be crossed.

6.9.2 Input data

Table 6.9.2-1: Data collection for "QoS Sustainability" analytics

Information	Source	Description
RAN UE Throughput	OAM TS 28.554 [10]	Average UE bitrate in the cell (Payload data volume on RLC level per elapsed time unit on the air interface, for transfers restricted by the air interface), per timeslot, per cell, per 5QI and per S-NSSAI.
QoS flow Retainability	OAM TS 28.554 [10]	Number of abnormally released QoS flows during the time the QoS Flows were used per timeslot, per cell, per 5QI and per S-NSSAI.

NOTE: The timeslot is the time interval split according to the time unit of the OAM statistics defined by operator.

6.9.3 Output analytics

The NWDAF outputs the QoS Sustainability analytics. Depending on the Analytics target period, the output consists of statistics or predictions. The detailed information provided by the NWDAF is defined in Table 6.9.3-1 for statistics and Table 6.9.3-2 for predictions.

Table 6.9.3-1: "QoS Sustainability" statistics

Information	Description
List of QoS sustainability Analytics (1..max)	
>Applicable Area	A list of TAIs or Cell IDs within the Location information that the analytics applies to.
>Applicable Time Period	The time period within the Analytics target period that the analytics applies to.
>Crossed Reporting Threshold(s)	The Reporting Threshold(s) that are met or exceeded by the statistics value or the expected value of the QoS KPI.

Table 6.9.3-2: "QoS Sustainability" predictions

Information	Description
List of QoS sustainability Analytics (1..max)	
>Applicable Area	A list of TAIs or Cell IDs within the Location information that the analytics applies to.
>Applicable Time Period	The time period within the Analytics target period that the analytics applies to.
>Crossed Reporting Threshold(s)	The Reporting Threshold(s) that are met or exceeded by the statistics value or the expected value of the QoS KPI.
>Confidence	Confidence of the prediction.

NOTE 1: The meaning of Confidence is based on the SLA, i.e. the consumer has to understand the meaning of the different values of Confidence.

NOTE 2: The Analytics can contain multiple sets of the above information if the location information reflected a list of waypoints.

The number of QoS sustainability analytics entries is limited by the maximum number of objects provided as part of Analytics Reporting Information.

6.9.4 Procedures

Figure 6.9.4-1 depicts a procedure for "QoS Sustainability" analytics provided by NWDAF.

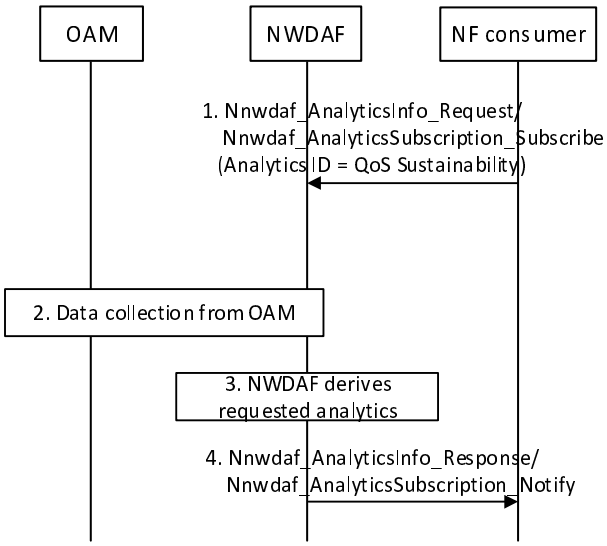

Figure 6.9.4-1: "QoS Sustainability" analytics provided by NWDAF

1. The consumer requests or subscribes to analytics information on "QoS Sustainability" provided by NWDAF. The parameters included in the request are described in clause 6.9.1.

   The consumer may include multiple sets of parameters in order to provide different combinations of "Location information" and "Analytics target period" when requesting QoS Sustainability analytics.

2. The NWDAF collects the data specified in clause 6.9.2 from the OAM, following the procedure captured in clause 6.2.3.2.

3. The NWDAF verifies whether the triggering conditions are met and derives the requested analytics. The NWDAF can detect the need for notification based on comparing the requested analytics of the target 5QI against the Reporting Threshold(s) provided by consumer in any cell over the requested Analytics target period.

4. The NWDAF provides response or notification on "QoS Sustainability" to the consumer.

7 Nnwdaf Services Description

7.1 General

The following table illustrates the NWDAF Services.

Table 7.1-1: NF services provided by NWDAF

Service Name	Service Operations	Operation Semantics	Example Consumer(s)
Nnwdaf_AnalyticsSubscription	Subscribe	Subscribe / Notify	PCF, NSSF, AMF, SMF, NEF, AF, OAM, CEF
	Unsubscribe		PCF, NSSF, AMF, SMF, NEF, AF, OAM, CEF
	Notify		PCF, NSSF, AMF, SMF, NEF, AF, OAM, CEF
Nnwdaf_AnalyticsInfo	Request	Request / Response	PCF, NSSF, AMF, SMF, NEF, AF, OAM, CEF
NOTE 1: How OAM consumes Nnwdaf services and which Analytics information is relevant is defined in TS 28.550 [7] Annex H. and out of the scope of this TS. NOTE 2: How CEF consumes Nnwdaf services and which Analytics information is relevant is defined in TS 28.201 [21] and out of the scope of this TS.			

The following table shows the analytics information provided by NWDAF service:

Table 7.1-2: Analytics information provided by NWDAF

Analytics Information	Request Description	Response Description
Slice Load level information	Analytics ID: load level information	Load level of a Network Slice Instance reported either as notification of crossing of a given threshold or as periodic notification (if no threshold is provided).
Observed Service experience information	Analytics ID: Service Experience	Observed Service experience statistics or predictions may be provided for a Network Slice or an Application. They may be derived from an individual UE, a group of UEs or any UE. For slice service experience, they may be derived from an Application, a set of Applications or all Applications on the Network Slice.
NF Load information	Analytics ID: NF load information	Load statistics or predictions information for specific NF(s).
Network Performance information	Analytics ID: Network Performance	Statistics or predictions on the load in an Area of Interest; in addition, statistics or predictions on the number of UEs that are located in that Area of Interest.
UE mobility information	Analytics ID: UE Mobility	Statistics or predictions on UE mobility.
UE Communication information	Analytics ID: UE Communication	Statistics or predictions on UE communication.
Expected UE behavioural parameters	Analytics ID: UE Mobility and/or UE Communication	Analytics on UE Mobility and/or UE Communication.
UE Abnormal behaviour information	Analytics ID: Abnormal behaviour	List of observed or expected exceptions, with Exception ID, Exception Level and other information, depending on the observed or expected exceptions.
User Data Congestion information	Analytics ID: User Data Congestion	Statistics or predictions on the user data congestion for transfer over the user plane, for transfer over the control plane, or for both.
QoS Sustainability	Analytics ID: QoS Sustainability	For statistics, the information on the location and the time for the QoS change and the threshold(s) that were crossed; or, for predictions, the information on the location and the time when a potential QoS change may occur and what threshold(s) may be crossed.

7.2 Nnwdaf_AnalyticsSubscription Service

7.2.1 General

Service Description: This service enables the consumer to subscribe/unsubscribe for network data analytics.

When the subscription is accepted by the NWDAF, the consumer NF receives from the NWDAF an identifier (Subscription Correlation ID) allowing to further manage (modify, delete) this subscription. The modification of Analytics subscription can be enforced by NWDAF based on operator policy and configuration.

7.2.2 Nnwdaf_AnalyticsSubscription_Subscribe service operation

Service operation name: Nnwdaf_AnalyticsSubscription_Subscribe.

Description: Subscribes to NWDAF analytics with specific parameters.

Inputs, Required: (Set of) Analytics ID(s) defined in Table 7.1-2, Target of Analytics Reporting, Notification Target Address (+ Notification Correlation ID), Analytics Reporting Parameters, Analytics target period.

NOTE 1: Target of Analytics Reporting can be provided per individual Analytics ID in a set of Analytics IDs.

Inputs, Optional: Analytics Filter Information, Subscription Correlation ID (in the case of modification of the analytics subscription), preferred level of accuracy of the analytics, Reporting Thresholds, Maximum number of objects requested (max), Maximum number of SUPIs requested (SUPImax).

NOTE 2: Analytics Filter Information, Reporting Thresholds, Maximum number of objects requested (max) and Maximum number of SUPIs requested (SUPImax) can be provided per individual Analytics ID in a set of Analytics IDs.

Outputs Required: When the subscription is accepted: Subscription Correlation ID (required for management of this subscription).

Outputs, Optional: None.

7.2.3 Nnwdaf_AnalyticsSubscription_Unsubscribe service operation

Service operation name: Nnwdaf_AnalyticsSubscription_Unsubscribe.

Description: unsubscribe to NWDAF analytic.

Inputs, Required: Subscription Correlation ID.

Inputs, Optional: None.

Outputs, Required: Operation execution result indication.

Outputs, Optional: None.

7.2.4 Nnwdaf_AnalyticsSubscription_Notify service operation

Service operation name: Nnwdaf_AnalyticsSubscription_Notify.

Description: NWDAF notifies the consumer instance of the analytics that has subscribed to the specific NWDAF service.

Inputs, Required: Set of the tuple (Analytics ID, Analytics specific parameters), Notification Correlation Information.

Inputs, Optional: Timestamp of analytics generation, validity period, probability assertion.

NOTE 1: Some NWDAF output analytics already include confidence of predictions, which provides the same information as probability assertion.

NOTE 2: Validity period can also be provided as part of Analytics specific parameters for some NWDAF output analytics.

Outputs, Required: Operation execution result indication.

Outputs, Optional: None.

7.3 Nnwdaf_AnalyticsInfo service

7.3.1 General

Service description: this service enables the consumer to request and get from NWDAF network data analytics.

7.3.2 Nnwdaf_AnalyticsInfo_Request service operation

Service operation name: Nnwdaf_AnalyticsInfo_Request.

Description: the consumer requests NWDAF operator specific analytics.

Inputs, Required: (Set of) Analytics ID(s) defined in Table 7.1-2, Target of Analytics Reporting, Analytics target period.

NOTE 1: Target of Analytics Reporting can be provided per individual Analytics ID in a set of Analytics IDs.

Inputs, Optional: Analytics Filter Information, preferred level of accuracy of the analytics, time when analytics information is needed, Maximum number of objects requested (max), Maximum number of SUPIs requested (SUPImax).

NOTE 2: Analytics Filter Information, Maximum number of objects requested (max) and Maximum number of SUPIs requested (SUPImax) can be provided per individual Analytics ID in a set of Analytics IDs.

Outputs, Required: Set of the tuple (Analytics ID, Analytics specific parameters).

Outputs, Optional: Timestamp of analytics generation, validity period, probability assertion.

NOTE 3: Some NWDAF output analytics already include confidence of predictions, which provides the same information as probability assertion.

NOTE 4: Validity period can also be provided as part of Analytics specific parameters for some NWDAF output analytics.

Annex A (informative): Change history

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2019-05	SP#84	SP-190456	-	-	-	MCC Editorial update for presentation to TSG SA#84 for approval	1.0.0
2019-06	SP#84	-	-	-	-	MCC editorial update for publication after approval at TSG SA#84	16.0.0
2019-09	SP#85	SP-190612	0001	3	F	Clarifications to Observed Service experience related network data analytics	16.1.0
2019-09	SP#85	SP-190612	0010	1	F	Specification clean-up	16.1.0
2019-09	SP#85	SP-190612	0012	3	F	Miscellaneous corrections to TS 23.288	16.1.0
2019-09	SP#85	SP-190612	0014	1	F	Clarification of NF and AF	16.1.0
2019-09	SP#85	SP-190612	0015	3	F	Update the Analytics information provided by NWDAF	16.1.0
2019-09	SP#85	SP-190612	0017	2	F	Closing open issue on NEF-AF interaction for data collection from AF	16.1.0
2019-09	SP#85	SP-190612	0026	1	F	Clarification of the correlation information	16.1.0
2019-09	SP#85	SP-190612	0027	4	F	Clarifications of the pre-check behaviours of the NF	16.1.0
2019-09	SP#85	SP-190612	0029	3	F	Corrections to slice load level analytics	16.1.0
2019-09	SP#85	SP-190612	0034	3	F	Clarifications on Potential QoS Change	16.1.0
2019-09	SP#85	SP-190612	0036	1	F	CR to properly separate UE identifiers from Analytics Filter	16.1.0
2019-09	SP#85	SP-190612	0037	1	F	CR for update of observed service experience	16.1.0
2019-09	SP#85	SP-190612	0039	3	F	Miscellaneous editorial corrections	16.1.0
2019-09	SP#85	SP-190612	0040	3	F	Optionality of data to be collected by NWDAF	16.1.0
2019-09	SP#85	SP-190612	0042	1	F	Clarification on Data Collection	16.1.0
2019-09	SP#85	SP-190612	0045	1	F	Probability assertion clarification on NWDAF services description	16.1.0
2019-09	SP#85	SP-190612	0046	1	F	Corrections for analytics exposure framework related parameters	16.1.0
2019-09	SP#85	SP-190612	0052	1	F	BSF and PCF selection for data collection	16.1.0
2019-09	SP#85	SP-190612	0054	-	F	Corrections to Nnwdaf_AnalyticsSubscription_Subscribe and Nnwdaf_AnalyticsInfo_Request service operations	16.1.0
2019-12	SP#86	SP-191079	0002	6	F	Clarifications to NF load data analytics	16.2.0
2019-12	SP#86	SP-191079	0003	8	F	Clarifications to Network Performance related network data analytics	16.2.0
2019-12	SP#86	SP-191079	0004	3	F	Clarifications to Abnormal behaviour analytics	16.2.0
2019-12	SP#86	SP-191079	0009	4	F	Clarifications to UE mobility and Abnormal behaviour analytics	16.2.0
2019-12	SP#86	SP-191079	0043	2	F	Remove UE related analytics for any UE	16.2.0
2019-12	SP#86	SP-191079	0044	6	F	Clarifications to UE communication and mobility analytics output	16.2.0
2019-12	SP#86	SP-191079	0047	3	F	Corrections for observed Service experience related network data analytics	16.2.0
2019-12	SP#86	SP-191079	0055	01	F	Terminology Alignment	16.2.0
2019-12	SP#86	SP-191079	0057	5	F	Editor's Notes cleanup	16.2.0
2019-12	SP#86	SP-191079	0062	-	F	Corrections to User Data Congestion Analytics	16.2.0
2019-12	SP#86	SP-191079	0063	-	F	Correction for data collection from OAM	16.2.0
2019-12	SP#86	SP-191079	0064	7	F	Corrections to general and framework parts of analytics	16.2.0
2019-12	SP#86	SP-191079	0065	-	F	Corrections to data collection from NFs	16.2.0
2019-12	SP#86	SP-191079	0066	6	F	Miscellaneous corrections/updates to TS 23.288	16.2.0
2019-12	SP#86	SP-191079	0068	4	F	Clarification of the data collection of the OSE	16.2.0
2019-12	SP#86	SP-191079	0071	3	F	Update to UE related analytics	16.2.0
2019-12	SP#86	SP-191079	0072		F	Clarifications on Supporting Modification of Analytics Subscription	16.2.0
2019-12	SP#86	SP-191079	0076	2	F	Removing Editor's note on how to find a PCF instance serving a UE	16.2.0
2019-12	SP#86	SP-191079	0078	2	F	User Data Congestion - Removal of Editor's Notes and Description Alignments	16.2.0
2019-12	SP#86	SP-191079	0081	3	F	CR to update UE communication	16.2.0
2019-12	SP#86	SP-191079	0084	3	F	Correction to Analytics Filter for slice load level analytics	16.2.0
2019-12	SP#86	SP-191079	0087	3	F	Clarification on NWDAF-assisted expected UE behavioural analytics	16.2.0
2019-12	SP#86	SP-191079	0088		F	Update the correlation information for AMF data and RAN data	16.2.0
2019-12	SP#86	SP-191079	0091	1	F	Clarification of UE related analytics	16.2.0
2019-12	SP#86	SP-191079	0092		F	Clarification of QoS requirements parameter used for QoS Sustainability Analytics	16.2.0
2019-12	SP#86	SP-191079	0093	4	F	Alignments on Analytics Filter Information and clarifications on Reporting Thresholds	16.2.0
2019-12	SP#86	SP-191079	0094	1	F	Clarification for UPF related data collection	16.2.0
2019-12	SP#86	SP-191120	0095	3	F	Alignment of User Data Congestion Analytics	16.2.0
2019-12	SP#86	SP-191079	0099	1	F	NEF parameter mapping for outbound analytics	16.2.0
2019-12	SP#86	SP-191079	0100	5	F	Alignments on QoS Sustainability Analytics	16.2.0
2020-03	SP#87E	SP-200070	0103	1	F	Clarification on definitions and NSI	16.3.0
2020-03	SP#87E	SP-200070	0104	-	F	NWDAF collect MDT/SON parameters	16.3.0
2020-03	SP#87E	SP-200070	0105	1	F	Update to Clause 6.1.3 Contents of Analytics Exposure	16.3.0
2020-03	SP#87E	SP-200070	0108	2	F	CR to update Observed Service Experience	16.3.0
2020-03	SP#87E	SP-200070	0109	3	F	Corrections on UE mobility analytics type by NWDAF service	16.3.0
2020-03	SP#87E	SP-200070	0110	3	F	Corrections on UE mobility analytics type by NWDAF service	16.3.0
2020-03	SP#87E	SP-200070	0112	2	F	Correct the filters for UE related analytics	16.3.0
2020-03	SP#87E	SP-200070	0113	4	F	A mechanism to avoid the flooding of reporting	16.3.0

2020-03	SP#87E	SP-200070	0114	1	F	Reporting information updates	16.3.0
2020-03	SP#87E	SP-200070	0115	1	F	Mega CR on editorial corrections	16.3.0
2020-03	SP#87E	SP-200070	0117	1	F	Slice service experience data collection corrections	16.3.0
2020-03	SP#87E	SP-200070	0119	1	F	Add the definition for Maximum number of results parameter into clause 6.1.3	16.3.0
2020-03	SP#87E	SP-200070	0123	1	F	Clarification of clause 6.7.2 UE mobility analytics	16.3.0
2020-03	SP#87E	SP-200070	0124	1	F	Clarification of clause 6.7.4 Expected UE behavioural parameters related network data analytics	16.3.0
2020-03	SP#87E	SP-200070	0126	1	F	Clarification on abnormal behaviour analytics	16.3.0
2020-03	SP#87E	SP-200070	0127	1	F	Clarifications on data collection	16.3.0
2020-03	SP#87E	SP-200070	0128	1	F	Corrections to Observed Service Experience analytics	16.3.0
2020-03	SP#87E	SP-200070	0129	1	F	Corrections to User Data Congestion Analytics	16.3.0
2020-03	SP#87E	SP-200070	0130	-	F	Corrections related to Analytics Filter Information and others	16.3.0
2020-03	SP#87E	SP-200070	0132	-	F	Clarifications on Inputs of NWDAF Analytics Subscription	16.3.0
2020-03	SP#87E	SP-200070	0139	-	F	Clarification of data collection from UPF	16.3.0
2020-03	SP#87E	SP-200070	0140	-	F	TS 23.288 editor's note handling	16.3.0
2020-03	SP#87E	SP-200070	0142	1	F	Clarification on the NWDAF services invoked in Abnormal behaviour	16.3.0
2020-07	SP#88E	SP-200431	0118	3	F	Abnormal analytics for any UE	16.4.0
2020-07	SP#88E	SP-200431	0146	1	F	Clarification of NF load analytics procedure	16.4.0
2020-07	SP#88E	SP-200431	0148	1	F	Clarification on Data Collection Procedure	16.4.0
2020-07	SP#88E	SP-200431	0149	1	F	Correction on Probability Assertion	16.4.0
2020-07	SP#88E	SP-200431	0150	1	F	Miscellaneous FASMO corrections to service experience analytics	16.4.0
2020-07	SP#88E	SP-200431	0153	1	F	Support of abnormal behaviour analytics for any UE	16.4.0
2020-07	SP#88E	SP-200431	0154	1	F	Support of data collection for any UE	16.4.0
2020-07	SP#88E	SP-200431	0155	2	F	Clarification on UE mobility analytics exposed to AF	16.4.0
2020-07	SP#88E	SP-200431	0156	1	F	Abnormal analytics clarifications (not any UE related)	16.4.0
2020-07	SP#88E	SP-200431	0158	1	F	Clarification on Event and Analytics Filters for some analytics types	16.4.0
2020-07	SP#88E	SP-200431	0159	-	F	The term MoS to apply for all kind of services	16.4.0
2020-07	SP#88E	SP-200431	0160	1	F	Further corrections to Observed Service Experience analytics	16.4.0
2020-07	SP#88E	SP-200431	0161	1	F	Clarifications on procedures for analytics exposure	16.4.0
2020-07	SP#88E	SP-200431	0162	1	F	Clarifications on procedures for data collection	16.4.0
2020-07	SP#88E	SP-200431	0163	1	F	Further clarifications on abnormal behaviour related network data analytics	16.4.0
2020-07	SP#88E	SP-200431	0165	1	F	Clarification for the Network Performance analytics	16.4.0
2020-07	SP#88E	SP-200431	0166	1	F	Updates of data collection for slice service experience	16.4.0
2020-07	SP#88E	SP-200431	0167	1	F	Corrections related to external UE ID	16.4.0
2020-07	SP#88E	SP-200431	0168	-	F	General clean-up for output abnormal behaviour analytics	16.4.0
2020-07	SP#88E	SP-200431	0169	-	F	Removing service provider actions for exception ID ping-ponging across neighbouring cells	16.4.0
2020-07	SP#88E	SP-200431	0170	1	F	Updated Event IDs for analytics	16.4.0
2020-07	SP#88E	SP-200431	0172	1	F	Corrections to Nnwdaf service operations	16.4.0
2020-07	SP#88E	SP-200431	0173	1	F	Adding UDM and OAM as consumers of services provided by NWDAF	16.4.0
2020-07	SP#88E	SP-200431	0176	1	F	Corrections for maximum number of objects and Maximum number of SUPIs	16.4.0
2020-09	SP#89E	SP-200679	0177	1	F	Service experience analytics discrimination	16.5.0
2020-09	SP#89E	SP-200679	0178	-	F	Corrections for wrong references for TS 28.532 clauses	16.5.0
2020-09	SP#89E	SP-200679	0179	-	F	Clarification on Target of Event Reporting	16.5.0
2020-09	SP#89E	SP-200679	0181	2	F	Clarification on Analytics Exposure	16.5.0
2020-09	SP#89E	SP-200679	0182	1	F	Clarification on data collection for statistics	16.5.0
2020-09	SP#89E	SP-200679	0183	1	F	Clarification on mapping of expected analytics type and Exception IDs	16.5.0
2020-09	SP#89E	SP-200679	0184	1	F	Clarification on NWDAF identifying the AF to collect data for an Event	16.5.0
2020-09	SP#89E	SP-200679	0186	1	F	Clarification on Multiple Parameter Sets for QoS Sustainability	16.5.0
2020-12	SP#90E	SP-200957	0188	1	F	Clarifications for Charging function as NWDAF consumer	16.6.0
2021-03	SP#91E	SP-210246	0192	-	F	Correct wrong reference	16.7.0
2021-03	SP#91E	SP-210246	0199	1	F	UE location in the AMF	16.7.0
2021-06	SP#92E	SP-210330	0264	-	F	Delete NSI ID via N7 interface	16.8.0
2021-06	SP#92E	SP-210333	0333	1	F	Clarification on output parameters in OSE	16.8.0
2021-09	SP#93E	SP-210907	0397	1	F	Clarify the data source of UE behavioural information and expected UE behavioural parameters	16.9.0
2021-12	SP#94E	SP-211275	0473	1	F	Add the description of Wrong destination address	16.10.0
2022-06	SP#96	SP-220391	0526	-	F	Removing UDM as consumer of expected UE behavioural parameters analytics	16.11.0

History

Document history		
V16.4.0	July 2020	Publication
V16.5.0	October 2020	Publication
V16.6.0	January 2021	Publication
V16.7.0	April 2021	Publication
V16.8.0	July 2021	Publication
V16.9.0	September 2021	Publication
V16.10.0	January 2022	Publication
V16.11.0	July 2022	Publication