Session Queries over LDAP

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Product(s) or Functional Area	PCF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration required to enable
Related Documentation	Not Applicable

Revision History

Table 2: Revision History

Revision Details	Release
Enhancement introduced. Added procedural information to configure the LDAP Endpoint.	2020.02.0
First introduced.	2020.01.0

Feature Description

In the policy-based network, the SPR/LDAP initiates a NAP notification towards PCF to signify a profile change. Upon receiving the notification, the PCF refreshes the subscriber profile by requerying LDAP to receive information about the modified subscriber.

If the NAP endpoint terminates on PCRF, the PCRF forwards the NAP request to PCF when it does not find the session in the local database. In situations where the NAP endpoint terminates on PCF, the PCF requeries LDAP and CHF to refresh the subscriber details.

How it Works

This section describes how this feature works.

Table 3: Feature History Table

Feature Name	Release Information	Description
Updates to LDAP Query in PCF to Perform Blocking Action	2024.02.0	PCF sends LDAP query only for the on-net and roaming sessions where the PCF needs to perform a blocking action. The blocking action allows to limit the irrelevant LDAP queries sent from PCF.

NAP Notifications

When you modify subscriber details, the NAP server, LDAP server, and PCF or PCRF perform the following operations:

NAP request termination on the PCRF

1. The LDAP server updates the NAP server with the modified details.
2. The NAP server broadcasts the Subscriber Change Notification message to the connected PCRF server. The message contains the unique identifier, and MSISDN or IMSI ID.
3. After receiving the message, the PCRF sends an acknowledgment to NAP. The PCRF then searches for the local session.
4. If the subscriber session is active on the PCRF, then PCRF requests the updated subscriber information from SPR or LDAP server. Depending upon the information it receives, PCRF updates the local session with the updated subscriber information and sends a Re-Auth-Request (RAR) for the Policy and Charging Rules Function (PCEF). For example, if PCRF identifies a session for the notification that contains the specified MSISDN in the PCRF then it triggers a Gx-RAR for the subscriber sessions.
5. If PCRF does not find the subscriber session locally, then the Policy Server forwards the Subscriber Change Notification to PCF. After receiving notification, PCF seeks the session locally and takes the appropriate action.

NAP request termination on PCF

When profile changes occur in NAP, it signifies that certain policies are added or modified. In this situation, the PCF performs the following:

1. Upon receiving a notification from NAP, the PCF initiates a requery or refresh request.
2. The PCF sends an N28 Subscribe Update request seeking the details of the policies that are added or updated.
3. After receiving the updates, the PCF reevaluates the policies to determine the updated policies and sends the Update_Notify message to SMF (over the N7 interface).

LDAP Queries

The Policy Server manages the 4G and 5G subscriber information in separate modules, which indicates that the PCRF continues to store the 4G-specific information, and PCF preserves the 5G-specific details. When the Policy Server receives a request seeking subscriber information, the LDAP with other components performs the following tasks:

1. The LDAP queries the MongoDB or Subscriber Profile Repository (SPR) by sending the "Get Subscriber Information" message.
2. After receiving the query, the Policy Server searches the subscriber information in the local MongoDB instance.
3. After receiving the search query, the Policy Server searches the subscriber information in the local MongoDB instance.
4. If the Policy Server discovers the subscriber information on PCRF, it sends the details to LDAP in the defined format. If the PCRF does not find the information, it forwards the request to PCF for further processing.
5. When PCF detects the information, it notifies PCRF with the subscriber information, which the PCRF forwards to the LDAP in the specified format.

Call Flows

This section describes the key call flows for this feature.

NAP Notification Call Flow

This section describes the NAP Notification call flow.

Figure 1: NAP Notification Call Flow

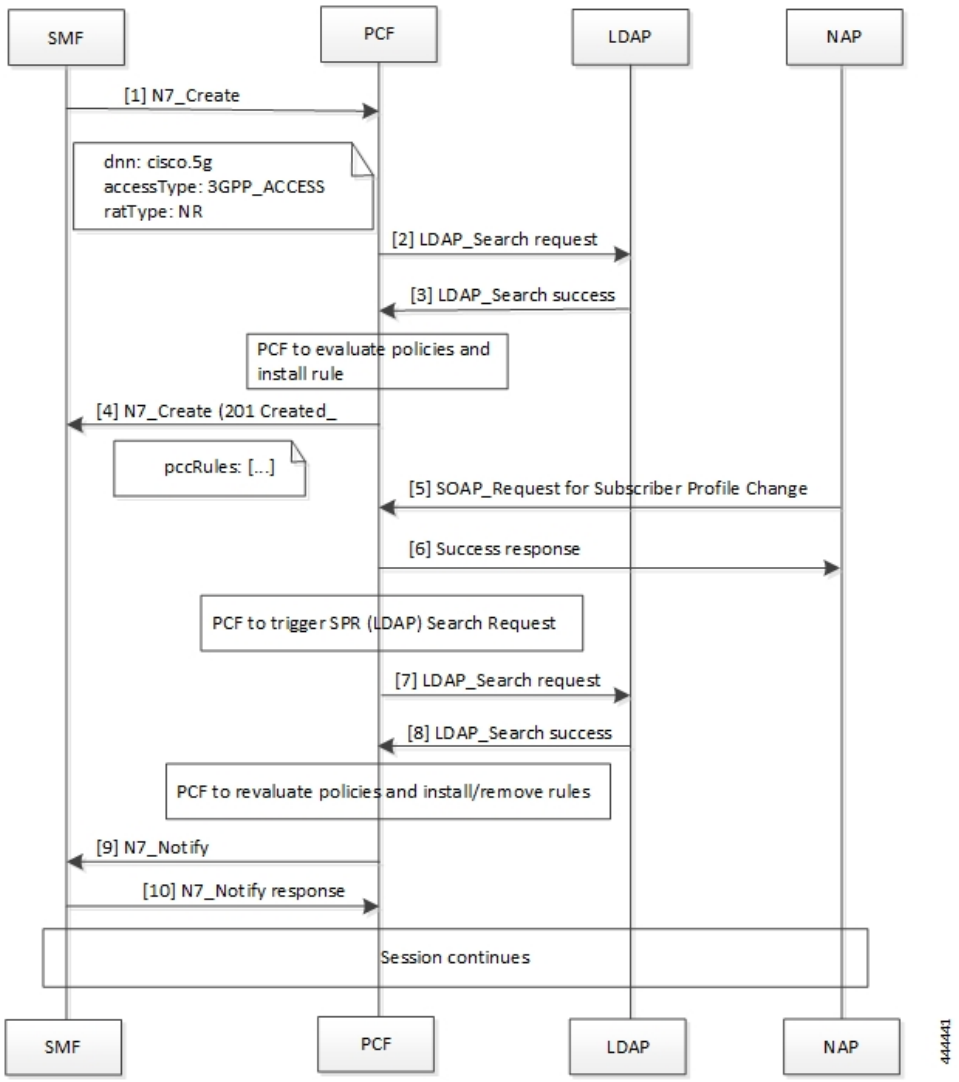

Table 4: NAP Notification Call Flow Description

Step	Description
1	The SMF sends an N7 Create request to the PCF requesting the policy details.
2	The PCF searches for the configured policies by sending the LDAP Search request towards LDAP.
3	The LDAP sends the response with search results in the LDAP Search success message to the PCF.
4	PCF evaluates the policies to determine the newly added or modified policies, and install the rules as required. The PCF responds with a set of pccRules to the original N7_Create request from the SMF with HTTP status 201.

Step	Description
5	The NAP sends a SOAP request for Subscriber Profile Change to the PCF.
6	In response to the request, PCF sends a Success response along with the requested subscriber information to NAP.
7	After PCF initiates a search request to LDAP, the PCF sends a LDAP Search request to LDAP.
8	The LDAP responds with LDAP_Search success message and the search results to the PCF.
9	PCF reevaluates the policies to determine the updated or modified policies, and installs or removes the policy rules as required. The PCF initiates an N7 Notify request to the SMF.
10	The SMF acknowledges the request with the N7 Notify response message towards the PCF.

LDAP Server Initialization Call Flow

This section describes the LDAP Server Initialization call flow.

Figure 2: LDAP Server Initialization Call Flow

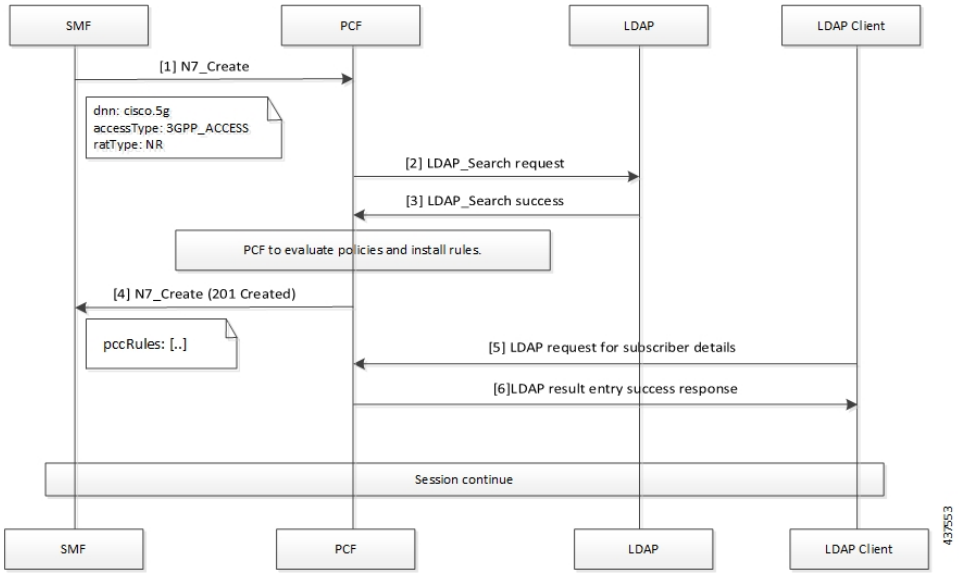

Table 5: LDAP Server Initialization Call Flow Description

Step	Description
1	The SMF sends an N7 Create request to the PCF requesting the policy details.
2	The PCF searches for the configured policies by sending the LDAP Search request towards LDAP.
3	The LDAP sends the response with search results in the LDAP Search Success message to the PCF.

Step	Description
4	PCF evaluates the policies to determine the newly added or modified policies, and install the rules as required. The PCF responds with a set of pccRules to the original N7 Create request from the SMF with the HTTP status 201.
5	The LDAP Client sends an LDAP request for Subscriber Profile Change to the PCF.
6	In response to the request, PCF sends a Success response along with the requested subscriber information to LDAP Client.

Enabling the Policy Server to Process the NAP and LDAP Queries

The configuration that enables the Policy Server to forward the NAP and LDAP queries to PCF or PCRF involves the following:

1. Configuring the gRPC Endpoint for PCF
2. Configuring the Forwarding Capability

Configuring the gRPC Endpoint for PCF

This section describes how to configure the gRPC endpoint to route the messages for PCF.

To set up the endpoint for gRPC, use the following configuration:

```
config
  engine engine_group_name
   grpc externalIPs external_ip
    port port_number
    end
```

For example,

```
engine magenta grpc externalIPs [192.0.2.18] port 8080
```

NOTES:

- **engine** *engine_group_name* —Specify the engine group name.
- **grpc externalIPs** *external_ip*—Specify the gRPC external IP address.
- **port** *port_number*—Specify the port number.

Configuring the Forwarding Capability

This section describes how to configure the forwarding capability.

For High Availability (HA) or Geographic Redundancy (GR) environments, ensure that the PCF Engine can access the Policy Server VMs. You can configure the capability responsible for routing the notification and queries by adding the following parameters to the qns.conf file.

The following table describes the application parameters.

Table 6: Application Parameters

Parameter Name	Description	Default Value	Possible Values	Example
-DsubmitToPCF	When set to true, PCRF sends NAP and LDAP requests to the PCF Engine. For HA or GR deployment, the external PCF Engine must be able to access the Policy Server VMs. Enable this feature on PCRF. This is an optional parameter.	False	True or False	-DsubmitToPCF=true
-Dpcf.host	Host or IP address of the PCF Engine on which PCRF sends the NAP and LDAP request. This parameter works when you set the submitToPCF parameter to true. Configuring this parameter is an optional step.	-	IP or host address	-Dpcf.host=192.0.2.19

Parameter Name	Description	Default Value	Possible Values	Example
-Dpcf.alternate.host	Host or IP address of the PCF Engine on which PCRF sends the NAP and LDAP requests. The NAP and LDAP requests are sent to the specified IP or host address when the address specified in the –Dpcf.host parameter is not accessible from the Policy Server. This parameter is usable only when you set the submitToPCF parameter to true. Configuring this parameter is an optional step.	-	The IP or host address	-Dpcf.alternate.host =192.0.2.20
-Dpcf.actions.sync.timeout Ms.default	The timeout period in milliseconds. Policy Server reports a timeout message when the PCRF sends a NAP and LDAP request and waits for the response until the specified interval is met. Configuring this parameter is an optional step.	350 (recommended value)	An integer value	-Dpcf.actions.sync.timeout Ms.default=350

Parameter Name	Description	Default Value	Possible Values	Example
-Dpcf.engine.port	The port number on which the PCF Engine is running. The NAP and LDAP requests are directed to this port number.	9884	An integer value	-Dpcf.engine.port=9884

Configuration Support for PCF-NAP Requests

This section describes the prerequisites and configurations that are required to support the PCF-NAP communication.

This configuration support involves the following:

- Prerequisites for PCF-NAP Requests

1. Configuring the Unified API
2. Setting a Limit on NAP Requests

Prerequisites for PCF-NAP Requests

This section describes the prerequisites that must be met for PCF-NAP communication.

For PCF-NAP interaction, make sure that the following configurations are available in your environment:

- N7 interface must be configured. For information on configuring the N7 interface, see Configuration Support for the N7 and N28 Interface.
- LDAP must be configured to operate with PCF. For information on configuring the LDAP, see Configuring PCF to use LDAP.

Configuring the Unified API

This section describes how to configure the unified API through the PCF Ops Center.

PCF receive NAP requests to requery the LDAP and reevaluate policies after receiving notification about profile change from NAP, so the new policies are applied. PCF receives the NAP requests through the unified API ingress endpoint.

To configure the unified API, use the following configuration in the Policy Ops Center console:

```
config
  api unified
    engine-group engine_group_name
    external-port external_ip
```

```
externalIPs external_ip
end
```

NOTES:

- **api unified**—Enter the unified API configuration mode.
- **engine-group** *engine_group_name* —Specify the PCF engine's group name.
- **external-port** *port_number*—(Optional) Specify the service to be accessed using an external IP instead of an Ingress endpoint. Specifies the external port number to expose the unified API endpoint.
- **externalIPs** *external_ip*—(Optional) Specify the service to be accessed using an external IP instead of an Ingress endpoint. Specifies the IP address for the external endpoint.

Setting a Limit on NAP Requests

This section describes how to set a limit on the number of NAP requests for PCF to process.

To configure the maximum number NAP requests TPS per PCF Engine deployment, use the following configuration in the Policy Ops Center console:

```
config
  engine engine_name
     properties broadcast.tps value tps
     end
```

NOTES:

- **engine** *engine_name* —Specify the engine name.
- **properties broadcast.tps value** *tps*—Specify the maximum number of NAP requests TPS that each PCF Engine must process. The default value is 20.

Configuration Support for LDAP Endpoint

This section describes how to configure the LDAP server endpoint that enables PCF to establish a connection with LDAP.

The configuration of the LDAP server endpoint involves the following steps:

1. Configuring the LDAP Endpoint
2. Setting a Limit on LDAP Search Request

Configuring the LDAP Endpoint

This section describes how to configure the LDAP server endpoint and the associated filter mappings.

Based on the LDAP endpoint configuration, the LDAP endpoint authenticates itself with PCF to retrieve the subscriber details through the search query.

Note Configuration changes to the LDAP endpoint cause the endpoint to restart automatically. Cisco recommends making such changes only within the maintenance window.

To configure the LDAP server endpoint, use the following configuration in the Policy Ops Center console:

```
config
  ldap-server-endpoint
  connect
    bind-ip ip_address
      port port_number
    binddn username
      password password
    request-timeout timeout
      replica replica_count
    max-transactions maximum_transaction
  health-check-attributes attribute_name
    valueattribute_value
  health-check-filter name attribute_name
    valueattribute_value
  ldap-clients client_name
    passwordpassword
  input-mapping filter_from_client
  internal-lookup-key [ IMSI | IP_ADDRESS | MSISDN ]
  output-mapping output_attribute_name
    input session_attribute_name
    end
```

NOTES:

- **ldap-server-endpoint**—Enters the LDAP server endpoint configuration mode.
- **connect**—Enters the LDAP connection configuration.
- **bind-ip** *ip_address* **port** *port_number* **request-timeout** *timeout*—Specify the external IP address and port number to which the LDAP client can connect to externally. The default port number is 9389.
- **binddn** *username* **password** *password*—Specify the user DN, for example: cn=manager, ou=account, so=profile, and password for connecting to the LDAP server.
- **request-timeout** *timeout_duration* —Specify the duration in milliseconds after which the request expires. The request awaits a response from the PCF engine. The default timeout value is 2000.
- **replica** *replica_count* —Specify the replica count for the LDAP server.
- **max-transactions** *maximum_transaction*—Specify the maximum number of transactions per second that each connection must process. The default value is 200.
- **health-check-attributes** *attribute_name* **value** *attribute_value*—Specify the attribute name and value that the client receives as a response to the health check request.
- **health-check-filter name** *attribute_name* **value** *attribute_value*—Specify the attribute name and value that distinguishes the health check request.

- **ldap-clients** *client_name* **password** *password*—Specify the configuration that PCF uses to configure multiple client authentication parameters.
- **input-mapping** *filter_from_client*—Specify the configuration to map the filter ID received from LDAP client and the internal-lookup-key. The accepted value must contain text string. For example, IMSI, MSISDN, framedIp, framedIpv6Prefix. You can configure the input mapping separately for frameIP, MSISDN, IMSI, and framedIpv6Prefix.
- **internal-lookup-key [IMSI | IP_ADDRESS | MSISDN]**—Configures the internal lookup key.
- **output-mapping** *output_attribute_name* **input** *session_attribute_name* —Specify the table that is used to defile the response attributes for the client. The response attribute name is mapped to the internal CPS session attributes for added flexibility.

Note PCF does not process the requests for which the output-mapping configuration is missing. The response attributes contain only those values that are configured in the output mapping as input key.

You can configure multiple supported keys only if they are available in the PCF session. The input keys can be duplicate but not the output values that you cannot configure two output-mappings with the same values.

Setting a Limit on LDAP Search Request

This section describes how to set the limit on the number of LDAP search requests for PCF to process.

To configure the maximum number LDAP requests TPS per replica, use the following configuration in the Policy Ops Center console:

```
config
  ldap-server-endpoint connect
  max-transactions max_tps
  end
```

NOTES:

- **max-transactions** *max_tps* —Specify the maximum number of LDAP requests TPS that each replica must process. The default value is 200.

OAM Support

This section describes operations, administration, and maintenance support for this feature.

Statistics

This section provides the list of statistics and counters that are involved when the Policy Server routes the LDAP queries and NAP notification to PCF or PCRF.

- PCF:

- inbound_request_total: Captures the total number of inbound LDAP search requests that PCF receives.
- incoming_request_total: Captures the total number of search results that contain the result code.
- LDAP_CHANGE-RES success: Invoked when the LDAP change message is successfully sent to the PCF Engine.
- LDAP_CHANGE-RES error: Invoked when the LDAP change message is not sent to the PCF Engine because of some exception.
- LDAP_SEARCH-RES success: Invoked when the LDAP query receives successful response from the PCF Engine.
- LDAP_SEARCH-RES error: Invoked when the LDAP queries fail to process due to an error or an exception.
- ldap_policy_request_total: Captures the total count of LDAP policy requests.
- message_total: Captures the total NAP requests such as total count of ldap_notify and ldap-change-message messages.

- PCRF:
  - ldap_change_success: Invoked when the PCRF receives success response from PCF for a NAP notification.
  - ldap_change_timeout: Invoked when the PCRF receives timeout response from PCF for a NAP notification.
  - ldap_change_<MessageType>: Invoked when the PCRF receives an error message from PCF for a NAP notification.
  - ldap_search_success: Invoked when the PCRF receives success response from the PCF for the LDAP queries.
  - ldap_search_timeout: Invoked when the PCRF receives timeout response from the PCF for the LDAP queries.
  - ldap_search_<MessageType>: Invoked when the PCRF receives an error message from the PCF for the LDAP queries.

- PCRF counters:
  - ldap_search_send: Captures the count of the cumulative number of the LDAP queries which the PCRF sends to the PCF.
  - ldap_change_send: Captures the count of the cumulative number of the NAP notifications that PCRF sends to the PCF.

For information on statistics, see *Ultra Cloud Core 5G Policy Control Function Statistics Reference*.