

# Installation Instruction for SAPC Application in UDC

## Installation Instructions



**Copyright**

© Ericsson AB 2017, 2018. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

**Disclaimer**

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.



# Contents

<b>1</b>	<b>Installation Instruction for SAPC Application for UDC</b>	<b>1</b>
1.1	UDC Installation Instruction Overview	1
1.2	Related Information	2
<b>2</b>	<b>General Installation Preparations</b>	<b>3</b>
<b>3</b>	<b>UDC Maiden Installation and Configuration With SAPC</b>	<b>4</b>
3.1	UDC Maiden Installation of SAPC Workflow	4
3.2	Prepare CUDB	4
3.3	Prepare EDA/PG	12
3.4	Prepare SAPC	15
3.5	Install CUDB	16
3.6	Install EDA/PG	16
3.7	Install SAPC	17
3.8	Configure CUDB for UDC	17
3.9	Configure EDA/PG for UDC	22
3.10	Configure SAPC	23
<b>4</b>	<b>Introduction of SAPC into an Existing UDC</b>	<b>24</b>
4.1	Introduction of SAPC into UDC Workflow	24
4.2	Prepare CUDB	25
4.3	Prepare EDA/PG	28
4.4	Prepare SAPC	29
4.5	Install SAPC	30
4.6	Configure CUDB for UDC	31
4.7	Configure EDA/PG for UDC	39
4.8	Configure SAPC	39
<b>5</b>	<b>Addition of SAPC in UDC</b>	<b>40</b>
5.1	Adding a New SAPC in UDC Workflow	40
5.2	Prepare CUDB	40
5.3	Prepare SAPC	42
5.4	Install SAPC	43
5.5	Configure CUDB for UDC	44
5.6	Configure SAPC	49



<b>Installation Instruction for SAPC Application in UDC Reference List</b>	<b>51</b>
--	-----------



# 1 Installation Instruction for SAPC Application for UDC

This guide provides installation and startup instructions for the Service-Aware Policy Controller (SAPC) application in the Ericsson User Data Consolidation (UDC) system.

This information is intended for Ericsson personnel doing the installation and startup procedures.

**Note:** This document cites several other UDC and node documents. Their corresponding document numbers are found in the reference section of this document. Refer to each Node Product Revision Information or Release Notes to determine the exact revision of the Support Libraries to be used.

## 1.1 UDC Installation Instruction Overview

There are three types of installation scenarios in UDC:

Table 1 Scenarios for Installing Applications

Scenarios	Description
UDC Maiden Installation	This involves the installation and configuration of a new Centralized User Database (CUDB) system, Ericsson Dynamic Activation Provisioning Gateway (EDA/PG) and application Front End (FE).
Introduction of an Application FE into an Existing UDC	This describes how to install and configure an application FE in a UDC system which does not contain any of this type of application FE in its current state.
Addition of an Application FE in UDC	This describes how to add a application FE into a UDC system which already includes at least one application FE for this type in its current state.

Each has its own workflow, preparation, installation and configuration procedures.

The deployed UDC system listed in the scenarios can include other FE applications. For a detailed description of the UDC system, refer to the *UDC System Description*.



The components considered in this document are the CUDB, EDA/PG and SAPC.

## 1.2 Related Information

The definition and explanation of acronyms and terminology, trademark information, and typographic conventions can be found in the following documents:

- Glossary of Terms and Acronyms
- Trademark Information
- Typographic Conventions



## 2 General Installation Preparations

Before the start of the installation, the following prerequisites must be met:

- Software installation technicians must have the appropriate training in UDC system deployments.
- Software installation technicians must be able to modify the managed object model in CUDB using the *Configuration Modification Procedure* in the *CUDB Node Configuration Data Model Description*.
- Information related to the planning of all Network Elements (NE) such as IP address allocations and infrastructure must be available.
- The site infrastructure and backbone, comprised of switches and routers, must be cabled, configured, and working.

**Note:** VLAN tagging is required at both ends in all external ports and links that connect the CMX boards towards the Site Routers because of the incompatibility with some routers. For more details, refer to [EIN – UDC](#) or [EIN – vUDC](#).

- The appropriate hardware is installed and accessible.
- The appropriate Cloud environment is deployed and in operation if applicable.
- The UDC software components are downloaded.
- Valid license keys for all UDC applications are downloaded.



## 3 UDC Maiden Installation and Configuration With SAPC

The UDC Maiden Installation and Configuration describes how to install and configure a UDC system that includes a CUDB, SAPC, and EDA/PG.

### 3.1 UDC Maiden Installation of SAPC Workflow

The complete UDC Maiden Installation workflow instruction is outlined below.

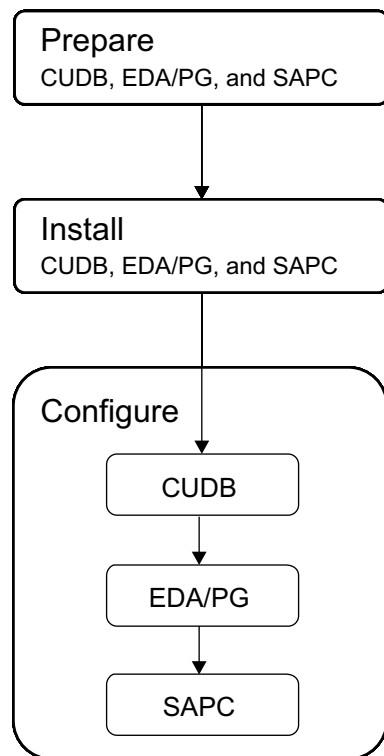


Figure 1 UDC Maiden Installation Workflow

It is recommended to perform the procedure in the order of the sections appear in this chapter.

### 3.2 Prepare CUDB

When preparing the CUDB in a UDC deployment, consider the planning and preparations in this section along with those in [CUDB Installation Instruction for native environment](#), or [Virtualized CUDB Installation Instruction for cloud environment](#).





### 3.2.1 CUDB License

License keys grant the usage of purchased functionality or capacity.

---

---

#### Do!

Ensure the appropriate license keys are available before installing the CUDB.

---

---

### 3.2.2 CUDB Templates

Installation templates are required as an input to the installation and configuration activities. Network information regarding remote CUDB nodes, EDA/PG, and FE applications are referenced in these templates.

Refer to the section *Configuration Files* in CUDB Installation Instruction for native environment, or Virtualized CUDB Installation Instruction for cloud environment.

---

---

#### Do!

Ensure all templates are updated to reflect the site-specific network plan of the customer.

---

---

### 3.2.3 CUDB Router Redundancy Mechanism

Bidirectional Forwarding Detection (BFD) and Virtual Router Redundancy Protocol (VRRP) are the supported router protocols used to provide a redundancy mechanism towards the customer network.

The protocol selected is site-specific and serves as an input to the network configuration templates.

For more information, refer to:

- *CUDB Node Network Configuration*
- *Virtualized CUDB Node Network Configuration*



---

---

### Do!

Prepare the network configuration templates using the site-specific protocol.

---

---

## 3.2.4 Common Schema Files for SAPC

The following files are required:

- *UDC Identities (openLDAP loadable) schema file.*  
Download and rename as `identities.schema`.
  - *UDC MultiService Consumer Identities (openLDAP loadable) schema file.*  
Download and rename as `mscIdentities.schema`.
  - *UDC Association Administrative Data (openLDAP loadable) schema file.*  
Download and rename as `assoc.schema`.
- 
- 

### Do!

Refer to the section *Identities Schema Files* in *UDC Product Revision Information* to download the appropriate revision of these files.

---

---

## 3.2.5 SAPC Schema Files

The following input is required for the FE.

- *SAPC LDAP schema for UDC*  
**Note:** Download and rename `sapc.schema`.
- 
- 

### Do!

Refer to the Release Information applicable to the SAPC software level to be installed for the specific revisions of the SAPC documents to use. Release Information is available through SAPC PLM.

---

---

## 3.2.6 Root Distinguished Name

The following information is required as part of the CUDB installation:



- The rootdn is operator-specific. It is recommended to use the following structure:

```
cn=manager,dc=<operator_id>,dc=com
```

Note that the rootdn cannot be changed once the installation is completed and the database is initialized. The rootdn needs to be defined in lower case.

---

## Do!

Obtain the operator-specific id to create the rootdn.

---

### 3.2.7 CUDB Initial Configuration Preparation for UDC

The CUDB initial configuration files are prepared by using the CUDB Installation Files generator tool. The installation of this tool creates input template files which must be edited to correspond to the desired CUDB system. Follow instructions as described in chapter *Configuration Files* in *CUDB Installation Instruction for native environment*, or *Virtualized CUDB Installation Instruction for cloud environment*.

#### 3.2.7.1 SAPC SOAP Notifications

Notifications are used for notifying applications after specific attributes are modified in CUDB.

SAPC notifications configuration requires update of the CUDB configuration model with a new instance of the CudbNotificationEndPoint class for the SAPC that is added in the UDC system. This class defines an endpoint receiving the notification event.

The procedure how to configure the SAPC SOAP notifications are described in the document *Configuration Guide for SAPC Application in UDC*.

The following inputs are required:

- The document *Configuration Guide for SAPC Application in UDC*.
- SAPC Node VIP address of the SAPCs available in the UDC system
 

**Note:** SAPC uses the same VIP address for LDAP traffic and SOAP traffic.
- Port number for SOAP over HTTP, in this case port:8080
- *SOAP notifications configuration in UDC* file.
- *SAPC SOAP notifications installation in UDC* script.



— *SAPC input for SOAP notifications installation in UDC* file.

---

---

### Do!

Download the *SOAP notifications configuration in UDC* file and rename to `sapc_notifications.txt`.

Download the *SAPC SOAP notifications installation in UDC* file and rename to `sapc_notifications_gen.sh`.

Download the *SAPC input for SOAP notifications installation in UDC* file and rename to `sapc_notifications_conf.conf`.

---

---

## 3.2.8

### SAPC LDAP User

The LDAP user is required for both CUDB and FE configuration to establish an LDAP session between them.

CUDB imposes restrictions on the minimum password length. All security-related configuration is captured in the `CudbSystemSecurity` object class. Refer to the *CUDB Security and Privacy Management* for information about password restrictions.

The LDAP user information such as authentication credentials and configuration parameters are stored in the CUDB administrative branch `ou=admin,<rootdn>`.

The LDAP authentication bind DN request is presented in the following format:  
`cudbUser=<LDAP_user_name>,ou=admin,<rootdn>`

---

---

### Do!

Select the SAPC LDAP `userid` and password.

---

---

## 3.2.9

### EDA/PG Users in CUDB

EDA/PG and CUDB exchange data on different interfaces, for each of this interface one or more EDA/PG `userid` needs to be defined in CUDB. Below is a list of interfaces and appropriate `userid` that are used between EDA/PG and CUDB.

— Provisioning

LDAP user for provisioning in CUDB from EDA/PG.

- EDA/PG provisioning LDAP `userid`



- EDA/PG provisioning LDAP user password
- Provisioning assurance (Data Durability)
 

LDAP user for provisioning assurance (data durability) between CUDB and EDA/PG.

  - EDA/PG replay LDAP userid
  - EDA/PG replay LDAP user password
- HTTP/REST used to notify EDA/PG to start provisioning assurance (data durability).
  - Replay userid set in attribute pg\_Http\_user
  - Replay user password set in attribute pg\_Http\_password
- Provisioning Blocking for Backup
 

JMX/JNDI used for CUDB to inform EDA about backup in operation.

  - pgUserName: should be set to cudb
  - pgPassword to be set.

---



---

### Do!

Obtain the EDA/PG userids and passwords to be used in CUDB listed above.

---



---

## 3.2.10

### EDA/PG Backup Notification Configuration in CUDB

Backup in progress notifications prevent possible data inconsistencies by temporarily halting provisioning from EDA/PG to CUDB. For more details, refer to *Configuring a PG Node in a Local CUDB Node for Backup Notification* described in *CUDB System Administrator Guide*.

EDA/PG nodes use Java Management Extensions (JMX) and Java Naming and Directory Interface (JNDI) for receiving CUDB notifications and must follow the specific order outlined below.

The following input is required to configure the CUDB Blocking for Backup Notifications class, CudbProvisioningGatewayConfig:

- The pgUserName is set to cudb.
- The pgPassword for the cudb user.
- The pgNodeIpAddresses lists the VIP OAM addresses for the primary and standby EDA/PG.



- The JMX port is : 8994
- The JNDI port is: 8099

The format of the pgNodeIpAddresses is: <OAM EDA/PG VIP>:8994:8099.  
Nodes are separated with "," and addresses for each node are separated with ";".

The following is an example of the pgNodeIpAddresses parameter with one node with two IP addresses:

```
"[ 10.1.33.141:8994:8099;10.1.33.142:8994:8099 ]"
```

The following is an example of the pgNodeIpAddresses parameter with two nodes with two IP addresses each:

```
"[ 10.1.33.141:8994:8099;10.1.33.142:8994:8099, 10.1.33.143:8994:8099;10.1.33.144:8994:8099 ]" →
```

For more details, refer to the section *Class CudbProvisioningGatewayConfig in CUDB Node Configuration Data Model Description*.

---



---

## Do!

Obtain the EDA/PG VIP OAM address and the pgPassword for the pgUserName:cudb.

---



---

### 3.2.11

#### Provisioning Assurance Configuration in CUDB

Provisioning Assurance (Data Durability) preserves the provisioning data durability after an unexpected and unplanned mastership change, in order to ensure correct service availability for end-users.

The following inputs are required to configure the Provisioning Assurance notification:

Refer to the following documents for more information:

- *CUDB System Administrator Guide*
- *Configuration Manual UDC Data Durability*

The following inputs are required to configure the Provisioning Assurance notification:

- HTTP/REST used to notify EDA/PG to start provisioning assurance (data durability).
  - EDA/PG OAM VIP address



- EDA/PG Replay Http port: 8282 or Https port: 8383
  - Provisioning gateway endpoint identifier:  
Cudb\_Prov\_Gateway\_End\_Point\_Id
  - Replay userid set in attribute pg\_Http\_user
  - Replay user password set in attribute pg\_Http\_password
  - EDA/PG Replay request URL set in attribute pgReplayRequestURL
  - EDA/PG Replay status URL set in attribute pgReplayStatusURL
- LDAP user for provisioning assurance (data durability) between CUDB and EDA/PG.
- EDA/PG Provisioning VIP IP address
  - EDA/PG Ports: LDAP: 389 or LDAPS: 636
  - EDA/PG replay LDAP userid
  - EDA/PG replay LDAP user password

---



---

### Do!

Obtain the end point identifier, VIP addresses, ports, replay userid and password to be set in CUDB.

---



---

## 3.2.12

### SAPC Application Counters

The following files are needed during the application counter installation:

- *UDC SAPC Application Counters Installation*

**Note:** Download and rename app\_counters\_sapc.pl.

- *SAPC Application Counters for CUDB*
- 
- 

### Do!

Refer to the appropriate SAPC software level Release Information to download the latest version of these documents and files.

---



---

For a detailed procedure explanation, refer to the section *Configuring SAPC Application Counters in External Database (CUDB)* in the document *Configuration Guide for SAPC Application in UDC*.



## 3.3 Prepare EDA/PG

When preparing the EDA/PG in a UDC deployment, consider the planning and preparations in this section along with those in *Software Installation for Virtual and Cloud Deployment* for cloud environment, or *Software Installation for Native Deployment* for native environment.

### 3.3.1 Customer Questionnaire

The customer questionnaire includes questions about the site and customer-specific parameters required to configure the EDA/PG. To note this information, choose from the following documents according to the deployment type.

For native deployments, use the following documents:

- *Customer Questionnaire for Native Deployment*
- *Parameter List for Native Deployment*

For virtual and cloud deployments, use the following documents:

- *Customer Questionnaire for Virtual and Cloud Deployment*
- *Parameter List for CEE Deployment*
- *Parameter List for Openstack Deployment*
- *Parameter List for Virtual Deployment*

EDA/PG access user:

- EDA/PG username and password
- User authority level and role
- Configuration management authority
- Provisioning authority

---

---

### Do!

Complete the questionnaire before starting the installation of EDA/PG.

---

---

### 3.3.2 EDA/PG License

License keys grant the usage of purchased functionality or capacity.





---

---

### Do!

Secure the license files are generated and available at installation time.

---

---

## 3.3.3 EDA/PG Templates

Installation templates are required as an input to the installation and configuration activities. Network information regarding remote CUDB nodes, EDA/PG, and FE applications are referenced in these templates.

Use the following documents to fill out the templates, as appropriate for the deployment.

- *Network Description and Configuration for Native Deployment*
  - *Network Description and Configuration for Virtual and Cloud Deployment*
- 
- 

### Do!

Ensure all templates are updated to reflect the site-specific network plan of the customer.

---

---

## 3.3.4 EDA/PG Router Redundancy Mechanism

Bidirectional Forwarding Detection (BFD) and Virtual Router Redundancy Protocol (VRRP) are the supported router protocols used to provide a redundancy mechanism towards the customer network.

The protocol selected is site-specific and serves as an input to the customer questionnaire. For more information, refer to:

- *Network Description and Configuration for Native Deployment*
  - *Network Description and Configuration for Virtual and Cloud Deployment*
- 
- 

### Do!

Prepare the customer questionnaire using the site-specific router protocol.

---

---

## 3.3.5 CUDB Provisioning Network Elements, Groups and Routing

A provisioning Network Element (NE) should be defined and configured for each CUDB node to which an EDA/PG is connected. The configured primary,



secondary and tertiary NEs are grouped in a provisioning NE Group. The NE Group is used as a logical NE.

The CUDB provisioning network groups are found in section *CUDB Configuration* in *Configuration Manual for Resource Activation*.

The following inputs are required to configure EDA/PG:

- Heartbeat DN, that is `rootdn`
- CUDB VIP address and port for each primary, secondary and tertiary CUDB to be connected to the EDA/PG for each Network Group. The default port is 389. For LDAPS, the port is 636.

**Note:** Be sure the CUDB IPs addresses correspond to a PL-DS node, that is, CUDBs with both PLDB and DSG clusters.

---

### Do!

Obtain the `rootdn`. Also note the primary, secondary and tertiary CUDB VIP addresses and ports per network group in the *Customer Questionnaire*.

---

## 3.3.6 Data Durability Function in EDA/PG

As part of the UDC Data Durability solution, EDA/PG enables the automatic replay of LDAP operations in the event of a temporary outage in CUDB. In CUDB, this function is called Provisioning Assurance.

The following input is required:

- A replay user name and password
- CUDB VIP address and port for each primary, secondary and tertiary CUDB to be connected to the EDA/PG. The default port is 389. For LDAPS, the port is 636.

For more details refer to section *Network Element - Network Element Group Configuration* in *Configuration Manual UDC Data Durability*.




---

---

## Do!

Obtain the replay user name and password as well as the primary, secondary and tertiary CUDB VIP addresses and ports per network group.

---

---

### 3.3.7 CUDB Blocking for Backup

The EDA/PG can receive a notification from CUDB to block certain provisioning towards CUDB during a CUDB backup to preserve the consistency of the data.

CUDB blocking for Backup must always be enabled in the UDC solutions.

The following input is required to install and configure EDA/PG:

- The username (cudb) and a password used when configuring EDA/PG notifications in CUDB.
  - JMX port: 8994
  - JDNI port: 8099
- 
- 

## Do!

Obtain the password valid for the username cudb above.

---

---

## 3.4 Prepare SAPC

When preparing the SAPC in a UDC deployment, consider the planning and preparations in this section along with those in the appropriate deployment document below:

- Physical Node Function (PNF).  
*SAPC PNF Deployment Instruction.*
- Virtualized Network Function deployment on OpenStack.  
*SAPC VNF Deployment Instruction for OpenStack.*
- Virtualized Network Function deployment on VMware.  
*SAPC VNF Deployment Instruction for VMware.*

### 3.4.1 SAPC License

License keys grant the usage of purchased functionality or capacity.



---

---

## Do!

Secure the license files are generated and available at installation time.

---

---

### 3.4.2 SAPC Entities

After successful SAPC SW installation, SAPC uses a mechanism based on configuration entities to know the CUDB nodes to connect and the data to retrieve to map each attribute to its internal data model. Entity Data Sources (EDSs) configure the data to retrieve from CUDB and Entity Data Targets (EDTs) configure data to update in CUDB. The examples provided in the *Configure Database Access in the SAPC* section in *Integration in User Data Consolidation* must be modified to include customer-specific information. See [Configure SAPC Entities](#) on page 23.

### 3.4.3 SAPC VNF Descriptor

The VNF Descriptor for the SAPC can be written in the Open Virtualization Format (OVF), generating an OVF package, or in Heat Orchestration Template (HOT), generating a HOT package.

The *SAPC VNF Descriptor Generator Tool* describes how to generate SAPC Virtual Network Function (VNF) Descriptor for the cloud environment.

---

---

## Do!

Generate the SAPC VNF Descriptor following the procedures in the *SAPC VNF Descriptor Generator Tool*.

---

---

## 3.5 Install CUDB

Perform the installation procedure described in *CUDB Installation Instruction* for native environment, or *Virtualized CUDB Installation Instruction* for cloud environment.

## 3.6 Install EDA/PG

Perform installation procedures as described in the document *Software Installation for Virtual and Cloud Deployment* for cloud environment, or *Software Installation for Native Deployment* for native environment.



## 3.7 Install SAPC

The following are the deployments scenarios of SAPC in UDC:

- Physical Node Function (PNF).

The installation of SAPC as PNF is described in the *SAPC PNF Deployment Instruction*.

- Virtualized Network Function deployment on OpenStack.

The installation of SAPC on CEE is described in the *SAPC VNF Deployment Instruction for OpenStack*.

- Virtualized Network Function deployment on VMware.

The installation of SAPC on VMware is described in the *SAPC VNF Deployment Instruction for VMware*.

---



---

### Do!

Choose the appropriate installation scenario from the list above.

Perform the SAPC installation following the procedure in the selected deployment instruction.

---



---

## 3.8 Configure CUDB for UDC

### 3.8.1 Create and Configure LDAP Users

The creation of LDAP application users in the CUDB is mandatory. UDC applications use these unique user identities for communicating with the CUDB over LDAP protocol. A password for the LDAP user is prepared according to the restrictions in the *CUDB Security and Privacy Management* document.

All security related configuration is captured in the `.cudbSystemSecurity` object class. Refer to the *Configuration Manual for Resource Activation*.

#### Prerequisites

The `ac1s.conf` file is prepared and available for direct LDAP access to UDC data.

The `cudbUserGroup` attribute is mandatory, and the `cudbLdapUserId` value is set to `cudbUserGroup=""` unless CUDB LDAP user groups are activated. This indicates that the LDAP user does not belong to any group. For more



information, refer to *CUDB Node Configuration Data Model*. The creation of LDAP application users in the CUDB is mandatory.

Use the following documents in this task:

- *CUDB System Administrator Guide*
- *CUDB Security and Privacy Management*
- *CUDB Node Configuration Data Model Description*

### Steps

1. Create an EDA/PG LDAP application user by following the procedure *Adding a New CUDB LDAP User to a Local CUDB Node* described in the *CUDB System Administrator Guide*.
2. Ensure that the following attributes and values are defined:
  - `isProvisioningUser=true`
  - `readModeInPL=MA`
  - `readModeInDS=MA`
  - `cudbUserGroup=" "`
3. Create an EDA/PG LDAP replay user.
4. Ensure that the following attributes and values are defined:
  - `isProvisioningUser=true`
  - `isReProvisioningUser=true`
  - `readModeInPL=MA`
  - `readModeInDS=MA`
  - `cudbUserGroup=" "`
5. Create an Application Front End LDAP user.
6. Ensure that the following attributes and values are defined:
  - `isProvisioningUser=false`
  - `readModeInPL=LP`
  - `readModeInDS=MP`
  - `cudbUserGroup=" "`



7. From each remote CUDB node, pull the LDAP user information by executing the `updateUserInfo` command. Refer to the *Updating CUDB LDAP User Information in a CUDB Node* procedure described in the *CUDB System Administrator Guide*.

### 3.8.2 Configure EDA/PG Backup Notifications in CUDB

Configuration of EDA/PG nodes as a destination for CUDB backup notifications is mandatory.

#### Prerequisites

- The EDA/PG `userid` , `pgUserName`, is set to `cudb`
- The password, `pgUserPassword`, is known.
- VIP OAM addresses for the primary and standby EDA/PG are known.
- JMX port: 8994
- JNDI port: 8099

Use the following document in this task:

- *CUDB Node Configuration Data Model Description*

#### Steps

1. Create the `CudbProvisioningGatewayConfig` class.

Refer to the section *Class CudbProvisioningGatewayConfig* in *CUDB Node Configuration Data Model Description*.

The full path to the instance of this class is as follows:

```
ManagedElement=1,CudbSystem=1,CudbLocalNode=<CUDB_Local_Node_Id>,CudbProvisioningGatewayConfig=1
```

2. Set the EDA/PG VIP OAM addresses and ports.

The ports must be written in this specific order: <OAM EDA/PG VIP> : 8994:8099 .

#### Example

```
pgNodeIpAddresses="[ 10.1.33.141:8994:8099;10.1.33.142:8994:8099, 10.1.33.143:8994:8099;10.1.33.144:8994:8099 ]"
```

3. Set the `pgUserName` and `pgUserPassword`.



4. Execute the applyConfig action to distribute the configuration to all CUDB nodes.

### 3.8.3 Configure CUDB for Provisioning Assurance

#### Prerequisites

An EDA/PG replay LDAP user is defined in the CUDB.

- Provisioning gateway end point identifier in the CUDB
- EDA/PG OAM VIP address and port
- The replay user name set in attribute pg\_Http\_User
- The replay users password set in attribute pg\_Http\_Password
- EDA/PG Replay request URL set in attribute pgReplayRequestURL
- EDA/PG Replay status URL set in attribute pgReplayStatusURL

Use the following documents for this task:

- *CUDB System Administrator Guide*
- *Configuration Manual UDC Data Durability*

#### Steps

1. Disable log obfuscation.
2. Enable Provisioning Assurance in the data model: > ManagedElement=1, CudbSystem=1, CudbNotifications=1, provisioningAssurance=true
3. Configure EDA/PG endpoints in the CUDB following the procedure *Configuring PG Endpoints in a Local CUDB Node for the Provisioning Assurance Function* described in *CUDB System Administrator Guide*.

#### Example

```
ManagedElement=1, CudbSystem=1, cudbProvisioningGatewayMgmt=1  
CudbProvGatewayEndPoint=<Cudb_Prov_Gateway_End_Point_Id>
```

```
pgHttpUser="<pg_Http_User>"
```

```
pg_Http_Password="<pg_Http_Password>"
```

```
pgReplayRequestURL="http://<EDA/PG_OAM_VIP>:8282/replayer/execute"
```





```
pgReplayStatusURL="http://<EDA/PG_OAM_VIP>:8282/replayer/state"
```

**Note:** If HTTPS is used, change the port to 8383.

### 3.8.4 Configure SAPC Application Counters

The configuration of the application counters on the CUDB is mandatory.

#### Prerequisites

Use the following document in this task:

— *Configuration Guide for SAPC Application in UDC*

#### Steps

1. Install SAPC application counters using section *Configuring SAPC Application Counters in External Database (CUDB) of Configuration Guide for SAPC Application in UDC*.

**Note:** If integrating CUDB with OSS-RC or a node that provides its own PM jobs, do not initiate the PM jobs in CUDB.

### 3.8.5 Configure SAPC SOAP Notifications

Notifications are used for notifying applications after specific attributes are modified in CUDB.

The procedure to configure the SAPC SOAP notifications is described in the document *Configuration Guide for SAPC Application in UDC*.

#### Prerequisites

The following inputs and files are required:

- `sapc_notifications.txt`
- SAPC Node VIP address for SOAP.
- Port number for SOAP (default 8080).
- `sapc_notifications_gen.sh`
- `sapc_notifications_conf.conf`



### Steps

1. Configure the SAPC notifications in CUDB by following the procedure in section *UDC Maiden Installation* in the *Configuration Guide for SAPC Application in UDC*.

## 3.9 Configure EDA/PG for UDC

### 3.9.1 Configure EDA/PG for SAPC

This section outlines the EDA/PG configuration steps required to integrate the UDC components. These steps are to be executed in the redundant EDA/PG system.

**Note:** After a successful execution of EDA/PG SW installation, it is mandatory to configure the EDA/PG node for UDC provisioning.

#### Prerequisites

The following documents are needed to configure EDA/PG for UDC with SAPC.

- *Customer Questionnaire for Native Deployment*
- or
- *Customer Questionnaire for Virtual and Cloud Deployment*
- *Configuration Manual for Resource Activation*
- *Configuration Manual UDC Data Durability*

#### Prerequisites

- The EDA/PG username and password exist on the CUDB.
- The licenses for administration domains are active.
- JMX ports 8994 and 8099 are available for CUDB Blocking for Backup.
- An operator-specific `<rootdn>` is defined in the recommended `dc=<operator_id>` structure. The `<rootdn>` cannot be changed once the installation is completed and the database is initialized.

If the automatic replay operation (Provisioning Assurance) is used, the following input must be available:

- CUDB provisioning VIP address and port (Default port is 389).



- Replay userid and password.
- Other protocol parameters listed in the section: *Network Element - Network Element Group Configuration* in *Configuration Manual UDC Data Durability*.

### Steps

1. Follow the steps in section *Configuration for SAPC Provisioning* in *Configuration Manual for Resource Activation* to configure EDA/PG for SAPC
2. Configure the EDA/PG with a CUDB user and password for the CUDB network element as indicated in the section *CUDB Blocking for Backup* in *Configuration Manual for Resource Activation*, using as input the *Network Element for CUDB Blocking for Backup* document..
 

**Note:** UDC recommends to enable the CUDB Blocking for Backup feature in EDA/PG even though it does not support the provisioning orders of some front ends.
3. Update all configurable activation logic components such that value of the <rootdn> is the same value as the <rootdn> defined in the CUDB.
4. Configure EDA/PG for Data Durability (Provisioning Assurance in CUDB) as described in the *Configuration Manual UDC Data Durability*.

## 3.10 Configure SAPC

### 3.10.1 Configure SAPC Entities

After successful SAPC SW installation, SAPC needs to know the CUDB nodes to connect and the data to retrieve to map each attribute to its internal data model. SAPC provides a mechanism based on configuration entities for this purpose. There are Entity Data Sources (EDSs) to configure the data to retrieve from CUDB and Entity Data Targets (EDTs) to configure data to update in CUDB.

The examples must be modified to include customer-specific information.

### Steps

1. Configure the EDSs and EDTs in SAPC according to the details in *Configure Database Access in the SAPC* section in *Integration in User Data Consolidation*.



## 4 Introduction of SAPC into an Existing UDC

The introduction of the SAPC into an existing UDC system describes how to install and configure a SAPC in a UDC system which does not contain any SAPCs.

### 4.1 Introduction of SAPC into UDC Workflow

The complete Introduction of SAPC to UDC workflow instruction is outlined below.

---

---

#### Stop!

This installation scenario requires configuration on a live UDC system and all activities on the deployed system must be performed during the maintenance window to avoid potential traffic impacts.

---

---

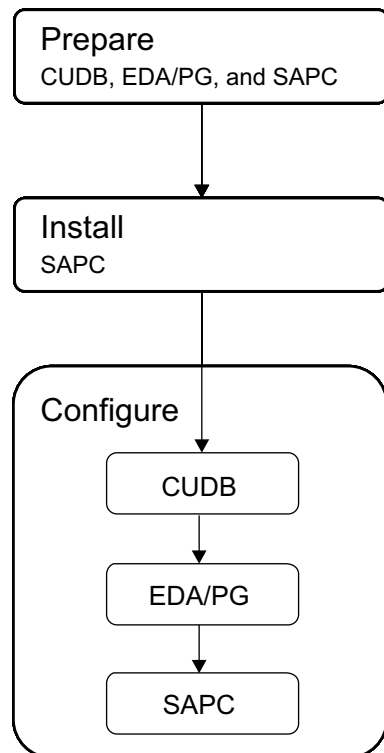


Figure 2 Introduction of SAPC to UDC Workflow

It is recommended to perform the procedure in the order of the sections appear in this chapter.



## 4.2 Prepare CUDB

When preparing the CUDB in a UDC deployment, consider the planning and preparations in this section along with those in [CUDB Installation Instruction](#) for native environment, or [Virtualized CUDB Installation Instruction](#) for cloud environment.

### 4.2.1 SAPC LDAP User

The LDAP user is required for both CUDB and FE configuration to establish an LDAP session between them.

CUDB imposes restrictions on the minimum password length. All security-related configuration is captured in the `CudbSystemSecurity` object class. Refer to the *CUDB Security and Privacy Management* for information about password restrictions.

The LDAP user information such as authentication credentials and configuration parameters are stored in the CUDB administrative branch `ou=admin, <rootdn>`.

The LDAP authentication bind DN request is presented in the following format:  
`cudbUser=<LDAP_user_name>,ou=admin,<rootdn>`

---

---

#### Do!

Select the SAPC LDAP `userid` and password.

---

---

### 4.2.2 CUDB Network Routing Update

The following input is required:

- FE traffic network address or VIP
- FE subnet mask

For BSP8100 HW

- IP address of the Site Router gateway for VRRP towards the Front End, used to send traffic back to the application FE `<vrrpGatewayToNewFE>`
- IP address of the Site Router 1 (left) gateway for BFD towards the Front End, used to send traffic back to the application FE `<BFDGateway1ToNewFE>`
- IP address of the Site Router 2 (right) gateway for BFD towards the Front End, used to send traffic back to the application FE `<BFDGateway2ToNewFE>`

For additional network configuration information, refer to:



- *CUDB Node Network Configuration*
- *Virtualized CUDB Node Network Configuration*

---

---

### Do!

Obtain the IP addresses for the site routers as well as the IP address and subnet mask of the application FE.

---

---

## 4.2.3

### Prepare New Schema and SQL Files

Introducing a new FE into an existing UDC system requires an update to the CUDB configuration model. The procedure relies on the *CUDB Schema Conversion Tool* to translate the new LDAP schema files into corresponding PL and DS SQL files.

#### Prerequisites

The following SAPC-specific files are required:

- *SAPC LDAP schema for UDC*

**Note:** Download and rename `sapc.schema`.

---

---

### Do!

Refer to the Release Information applicable to the SAPC software level to be installed for the specific revisions of the SAPC documents to use. Release Information is available through SAPC PLM.

---

---

The following common files are required:

- *UDC Identities (openLDAP loadable) schema file, see Common Schema Files for SAPC.*

Use the original `identities.schema`.

- *UDC MultiService Consumer Identities (openLDAP loadable) schema file, see Common Schema Files for SAPC.*

Use the original `mscIdentities.schema`.

- *UDC Association Administrative Data (openLDAP loadable) schema file, 2/155 64-HSC 113 08/5.*

Download and rename `assoc.schema`.




---

## Do!

Refer to the section *Identities Schema Files* in *UDC Product Revision Information* to download the appropriate revision of these files. Names of the files with .schema extension are case-sensitive.

---

### Steps

1. Perform the procedure in section *Adding New Schemas* described in *CUDB Application Schema Update* up to the point where the necessary new schema and SQL files are generated.

## 4.2.4

### SAPC Application Counters

The following files are needed during the application counter installation:

- *UDC SAPC Application Counters Installation*

**Note:** Download and rename app\_counters\_sapc.pl.

- *SAPC Application Counters for CUDB*
- 

## Do!

Refer to the appropriate SAPC software level Release Information to download the latest version of these documents and files.

---

For a detailed procedure explanation, refer to the section *Configuring SAPC Application Counters in External Database (CUDB)* in the document *Configuration Guide for SAPC Application in UDC*.

---

## 4.2.5

### SAPC SOAP Notifications

Notifications are used for notifying applications after specific attributes are modified in CUDB.

SAPC notifications configuration requires update of the CUDB configuration model with a new instance of the CudbNotificationEndPoint class for the SAPC that is added in the UDC system. This class defines an endpoint receiving the notification event.

The procedure how to configure the SAPC SOAP notifications are described in the document *Configuration Guide for SAPC Application in UDC*.

The following inputs are required:



- The document *Configuration Guide for SAPC Application in UDC*.
  - SAPC Node VIP address of the SAPCs available in the UDC system
- Note:** SAPC uses the same VIP address for LDAP traffic and SOAP traffic.
- Port number for SOAP over HTTP, in this case port:8080
  - *SOAP notifications configuration in UDC* file.
  - *SAPC SOAP notifications installation in UDC* script.
  - *SAPC input for SOAP notifications installation in UDC* file.

---

## Do!

Download the *SOAP notifications configuration in UDC* file and rename to `sapc_notifications.txt`.

Download the *SAPC SOAP notifications installation in UDC* file and rename to `sapc_notifications_gen.sh`.

Download the *SAPC input for SOAP notifications installation in UDC* file and rename to `sapc_notifications_conf.conf`.

---

## 4.3 Prepare EDA/PG

When preparing the EDA/PG in a UDC deployment, consider the planning and preparations in this section along with those in *Software Installation for Virtual and Cloud Deployment* for cloud environment, or *Software Installation for Native Deployment* for native environment.

### 4.3.1 SAPC Provisioning

The SAPC provisioning configuration activities are described in the section *Configuration for SAPC Provisioning* in the document *Configuration Manual for Resource Activation*.






---

---

## Do!

Obtain the input needed for SAPC provisioning, following section *Layered SAPC Provisioning Configuration* in the document *Configuration Manual for Resource Activation*.

---

---

## 4.4 Prepare SAPC

When preparing the SAPC in a UDC deployment, consider the planning and preparations in this section along with those in the appropriate deployment document below:

- Physical Node Function (PNF).  
*SAPC PNF Deployment Instruction.*
- Virtualized Network Function deployment on OpenStack.  
*SAPC VNF Deployment Instruction for OpenStack.*
- Virtualized Network Function deployment on VMware.  
*SAPC VNF Deployment Instruction for VMware.*

### 4.4.1 SAPC License

License keys grant the usage of purchased functionality or capacity.

---

---

## Do!

Secure the license files are generated and available at installation time.

---

---

### 4.4.2 SAPC Entities

After successful SAPC SW installation, SAPC uses a mechanism based on configuration entities to know the CUDB nodes to connect and the data to retrieve to map each attribute to its internal data model. Entity Data Sources (EDSs) configure the data to retrieve from CUDB and Entity Data Targets (EDTs) configure data to update in CUDB. The examples provided in the *Configure Database Access in the SAPC* section in *Integration in User Data Consolidation* must be modified to include customer-specific information. See [Configure SAPC Entities](#) on page 23.



### 4.4.3 SAPC VNF Descriptor

The VNF Descriptor for the SAPC can be written in the Open Virtualization Format (OVF), generating an OVF package, or in Heat Orchestration Template (HOT), generating a HOT package.

The *SAPC VNF Descriptor Generator Tool* describes how to generate SAPC Virtual Network Function (VNF) Descriptor for the cloud environment.

---

---

#### Do!

Generate the SAPC VNF Descriptor following the procedures in the *SAPC VNF Descriptor Generator Tool*.

---

---

## 4.5 Install SAPC

The following are the deployments scenarios of SAPC in UDC:

- Physical Node Function (PNF).

The installation of SAPC as PNF is described in the *SAPC PNF Deployment Instruction*.

- Virtualized Network Function deployment on OpenStack.

The installation of SAPC on CEE is described in the *SAPC VNF Deployment Instruction for OpenStack*.

- Virtualized Network Function deployment on VMware.

The installation of SAPC on VMware is described in the *SAPC VNF Deployment Instruction for VMware*.




---

---

## Do!

Choose the appropriate installation scenario from the list above.

Perform the SAPC installation following the procedure in the selected deployment instruction.

---

---

## 4.6 Configure CUDB for UDC

### 4.6.1 Create and Configure LDAP User for SAPC

The creation of LDAP application users in the CUDB is mandatory. UDC applications use these unique user identities for communicating with the CUDB over LDAP protocol. A password for the LDAP user is prepared according to the restrictions in the *CUDB Security and Password Management*.

All security related configuration is captured in the `cudbSystemSecurity` object class. Refer to the *CUDB Node Configuration Data Model Description* for more information

#### Prerequisites

Use the following documents in this task:

- • *CUDB System Administrator Guide*
- *CUDB Security and Password Management*
- *CUDB Node Configuration Data Model Description*

**Note:** Perform this procedure during the maintenance window if you are introducing or adding SAPC to UDC.

#### Steps

1. Create an LDAP application user by following the procedure *Adding a New CUDB LDAP User to a Local CUDB Node* described in the *CUDB System Administrator Guide*.
2. Populate the following attributes and values:
  - `isProvisioningUser=false`
  - `readModeInPL=LP`
  - `readModeInDS=MP`
  - `cudbUserGroup="<cudbLdapUserId>"`



**Note:** The `cudbUserGroup` attribute is mandatory and if this functionality is not used, the `<cudbLdapUserId>` value must be left empty indicating the LDAP user does not belong to any group, that is `cudbUserGroup=""`. For more information, refer to *CUDB Node Configuration Data Model Description*.

3. Propagate the LDAP user information to all remote CUDB nodes by performing the *Updating CUDB LDAP User Information in a CUDB Node* procedure in the *CUDB System Administrator Guide*.

## 4.6.2 Configure CUDB Network Routing

Before updating the eVIP configuration, the added FE VIP needs to be added to the BSP virtual router `sig_data_sp` in the CUDB on BSP 8100, in native environment. When in virtual environment it impacts the cloud network infrastructure.

### 4.6.2.1 Configure BSP Virtual Routers

**Note:** This procedure needs to be performed on every CUDB BSP8100 node.

#### Prerequisites

The following FE input is required:

- FE traffic network address or VIP
- FE subnet mask

The following Site Router input is required:

- IP address of the Site Router gateway for VRRP towards the Front End, used to send traffic back to the application FE `<vrrpGatewayToNewFE>`
- IP address of the Site Router 1 (left) gateway for BFD towards the Front End, used to send traffic back to the application FE `<BFDGateway1ToNewFE>`
- IP address of the Site Router 2 (right) gateway for BFD towards the Front End, used to send traffic back to the application FE `<BFDGateway2ToNewFE>`

#### Steps

1. Enter `cliss` in the CUDBs BSP.
2. Go to the MOM `ManagedElement=1, Transport=1, Router=0-26-sig_data_sp, RouteTableIPv4Static=1`



3. Print the data for one of the FEs defined there (other than 0.0.0.0/0): show all Dst=xxxx
4. Create a new element for the destination in both sig\_data\_sp virtual routers

In this case the destination is the new FE LDAP VIP.

- a. Check the elements that are already defined in the virtual routers.

```
show all ManagedElement=1,Transport=1,Router=0-26-
sig_data_sp,RouteTableIPv4Static=1
```

```
show all ManagedElement=1,Transport=1,Router=0-28-
sig_data_sp,RouteTableIPv4Static=1
```

Example

```
RouteTableIPv4Static=1
  Dst=0.0.0.0/0-Default
    dst="0.0.0.0/0"
    NextHop=blackhole
      adminDistance=1
      nexthop
        discard
  Dst=10.120.174.230/32-HLR_LDAP_FE-InterCMX
    dst="10.120.174.230/32"
    NextHop=sig_data_sp_nlc1
      adminDistance=120
      bfdEnable
      nexthop
        address="192.168.208.10"
```

- b. In the case where VRRP is used between BSP and the site routers (infrastructure):

Example

```
ManagedElement=1,Transport=1,Router=0-26-sig_data_sp,
RouteTableIPv4Static=1
  configure
    Dst=<dst_IP_or_nw_name>_LDAP_FE
    dst="<dst_IP_or_nw/mask>"
    NextHop=fe_gw_vrrp
      adminDistance=5
      nexthop
        address="<vrrpGatewayToNewFE>"
  commit
ManagedElement=1,Transport=1,Router=0-28-sig_data_sp,
RouteTableIPv4Static=1
  configure
    Dst=<dst_IP_or_nw_name>_LDAP_FE
    dst="<dst_IP_or_nw/mask>"
    NextHop=fe_gw_vrrp
      adminDistance=5
```



```

        nexthop
        address="<vrrpGatewayToNewFE>"
    commit

```

- c. In the case where BFD is used between BSP and the site routers (infrastructure):

#### Example

```

ManagedElement=1,Transport=1,Router=0-26-sig_data_sp,
RouteTableIPv4Static=1
configure
Dst=<dst_IP_or_nw_name>_LDAP_FE
dst="<dst_IP_or_nw/mask>"
    NextHop=fe_bfd_gw_A1
    adminDistance=5
    bfdEnable
    nexthop
        address="<BFDGateway1ToNewFE>"
    commit

```

```

ManagedElement=1,Transport=1,Router=0-28-sig_data_sp,
RouteTableIPv4Static=1
configure
Dst=<dst_IP_or_nw_name>_LDAP_FE
dst="<dst_IP_or_nw/mask>"
    NextHop=fe_bfd_gw_B1
    adminDistance=5
    bfdEnable
    nexthop
        address="<BFDGateway2ToNewFE>"
    commit

```

- d. Check that the new entries have been successfully committed in the virtual router:

#### Example

```

show all ManagedElement=1,Transport=1,Router=0-26-
sig_data_sp,RouteTableIPv4Static=1

```

```

show all ManagedElement=1,Transport=1,Router=0-28-
sig_data_sp,RouteTableIPv4Static=1

```

5. Repeat the steps in this task in Router=0-28-sig\_data\_sp.

### 4.6.2.2 Configure eVIP for SAPC

The eVIP configuration must be updated with a route to the SAPC traffic network. This affects every CUDB node in the system.



For general information on the eVIP, refer to *eVIP Management Guide*. The commands used during the procedure are subject to certain eVIP limitations. These limitations are as follows:

- Note:**
- The maximum length of a command name is limited to 50 characters.
  - The maximum length of the sum of all command names for a blade are limited to 4040 characters.

This section describes how to add new routes for the new remote node. Refer to section *eVIP Static, Routes Configuration in an Installed System* in *CUDB System Administrator Guide*.

### Steps

1. Establish a new administrative CUDB CLI session towards one of the SC blades of the target CUDB node with the following command:

```
ssh <admin_user>@<CUDB_Node_OAM_VIP_Address>
```

2. Define a new startup command by doing the following steps:

- a. List all commands on the blades with the following command:

```
cudbEvipEncapsulator --show --blade <number_of_blade>|all
```

#### Example

Example

```
#cudbEvipEncapsulator --show --blade 4
Showing commands for blade PL_2_4:
flush_route_cache
set_site_120
set_site_130
set_provisioning_PG
set_provisioning_120
set_provisioning_130
set_HSS_FE6106
set_HSS_FE6124
set_HLR_FE02
set_HLR_BS01
```

- b. Add the new startup command in the eVIP configuration command section. Select the ALB number where routes have to go ("alb\_0", "alb\_1" or "alb\_2"):

```
cudbEvipEncapsulator --new-command --name <command_name>
--definition <command_definition>
```

where <command\_definition> is the Linux command for route definition towards the new node.



### Example

#### Example

```
# cudbEvipEncapsulator --new-command --name
"set_SAPC01" --definition "ip route add
10.1.0.212/32 dev alb_1"
Config file saved
Added a new command with name "set_SAPC01"
```

3. Add the new startup command to every blade except the system controllers in the node as follows:

```
cudbEvipEncapsulator --add --name <command_name> --blade
<number_of_blade>
```

**Note:** The <number\_of\_blade> value depends on the number of blades in the system. For instance: values range from 3 to 10 for a 10-blade system, 3–22 for 22-blade and 3–34 for a 34-blade system.

Below is an example on using the command:

#### Example

```
# cudbEvipEncapsulator --add --name "set_SAPC01" --blade 4
```

4. The newly added startup commands are applied by running the cudbEvipEncapsulator script on all the blades.

```
cudbEvipEncapsulator --blade <number_of_blade>
```

**Note:** The <number\_of\_blade> value depends on the number of blades in the system. For instance: values range from 3 to 10 for a 10-blade system, 3–22 for 22-blade and 3–34 for a 34-blade system.

#### Example

```
#cudbEvipEncapsulator --blade 4
```

5. Check that the new startup commands are added:

```
cudbEvipEncapsulator --show --blade <number_of_blade>|all
```

#### Example

```
#cudbEvipEncapsulator --show --blade 4
Showing commands for blade PL_2_4:
flush_route_cache
set_site_120
set_site_130
set_provisioning_PG
set_provisioning_120
set_provisioning_130
set_HSS_FE6106
set_HSS_FE6124
set_HLR_FE02
```





```
set_HLR_BS01  
set_SAPC01
```

6. This procedure must be performed for all remaining CUDB nodes.

### 4.6.3 Configure SAPC Application Counters

The configuration of the application counters on the CUDB is mandatory. When this activity is performed as part of a SAPC application installation on a live deployed UDC system, it must be done during a maintenance window to minimize potential traffic impacts.

#### Prerequisites

**Note:** Perform this procedure during the maintenance window when introducing SAPC to a live UDC network.

Use the following document in this task:

- Configuration Guide for SAPC Application in UDC

#### Steps

1. Install SAPC application counters using section *Configuring SAPC Application Counters in External Database (CUDB)* of *Configuration Guide for SAPC Application in UDC*.

**Note:** If integrating CUDB with OSS-RC or a node that provides its own PM jobs, do not initiate the PM jobs in CUDB.

### 4.6.4 Configure SAPC SOAP Notifications

Notifications are used for notifying applications after specific attributes are modified in CUDB.

The procedure to configure the SAPC SOAP notifications is described in the document *Configuration Guide for SAPC Application in UDC*.

#### Prerequisites

The following inputs and files are required:

- `sapc_notifications.txt`
- SAPC Node VIP address for SOAP.
- Port number for SOAP (default 8080).



- `sapc_notifications_gen.sh`
- `sapc_notifications_conf.conf`

### Steps

1. Configure the SAPC notifications in CUDB by following the procedure in section *UDC Maiden Installation* in the *Configuration Guide for SAPC Application in UDC*.

## 4.6.5 Add Schemas and Application Services

A new `cudbAppService` instance must be created for each new LDAP schema generated from the *CUDB Schema Conversion Tool*

### Prerequisites

The following input is required for each application service instance:

- `<appName>-pl.sql` and `<appName>-ds.sql`, where `<appName>` is the prefix of the object classes present in the new LDAP schemas

### Steps

1. Perform the procedure in section *Adding New Schemas* described in *CUDB Application Schema Update* starting from the point after the new schema and SQL files were generated.

---

---

### Do!

Perform this task during the maintenance window. Schema updates trigger the restart of the LDAP FE.

---

---

2. In case UPG is part of the UDC deployment and User.360 feature (User Profile Analytics and Reports) is active, online schema update may need to be done in UPG, depending on the customer requirements to support SAPC profile/data in User.360. Follow the procedure in section *UPG Schema Change for Adding New Schemas of CUDB* described in *UPG Schema Change for CUDB*.



## 4.7 Configure EDA/PG for UDC

### 4.7.1 Update EDA/PG Configuration for SAPC

#### Prerequisites

The following documents are needed to configure EDA/PG for SAPC.

— *Configuration Manual for Resource Activation*

#### Steps

1. Follow the steps in section *Configuration for SAPC Provisioning* in *Configuration Manual for Resource Activation* to configure EDA/PG for SAPC

## 4.8 Configure SAPC

### 4.8.1 Configure SAPC Entities

After successful SAPC SW installation, SAPC needs to know the CUDB nodes to connect and the data to retrieve to map each attribute to its internal data model. SAPC provides a mechanism based on configuration entities for this purpose. There are Entity Data Sources (EDSs) to configure the data to retrieve from CUDB and Entity Data Targets (EDTs) to configure data to update in CUDB.

The examples must be modified to include customer-specific information.

#### Steps

1. Configure the EDSs and EDTs in SAPC according to the details in *Configure Database Access in the SAPC* section in *Integration in User Data Consolidation*.



## 5 Addition of SAPC in UDC

The addition of SAPC in UDC describes how to install and configure an additional SAPC into a UDC system which already includes at least one SAPC

### 5.1 Adding a New SAPC in UDC Workflow

Addition of a new SAPC workflow is outlined below.

**Note:** Since this installation scenario requires configuration on a live UDC system, all activities on the deployed system must be performed during the maintenance window to avoid potential traffic impacts.

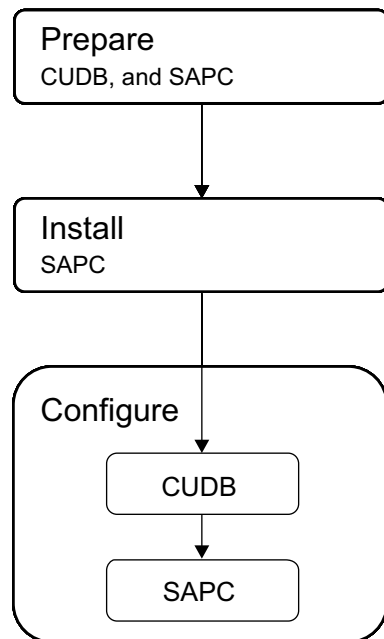


Figure 3 Adding New SAPC Workflow

It is recommended to perform the procedure in the order of the sections appear in this chapter.

### 5.2 Prepare CUDB

When preparing the CUDB in a UDC deployment, consider the planning and preparations in this section along with those in [CUDB Installation Instruction for native environment](#), or [Virtualized CUDB Installation Instruction for cloud environment](#).



## 5.2.1 CUDB Network Routing Update

The following input is required:

- FE traffic network address or VIP
- FE subnet mask

For BSP8100 HW

- IP address of the Site Router gateway for VRRP towards the Front End, used to send traffic back to the application FE <vrrpGatewayToNewFE>
- IP address of the Site Router 1 (left) gateway for BFD towards the Front End, used to send traffic back to the application FE <BFDGateway1ToNewFE>
- IP address of the Site Router 2 (right) gateway for BFD towards the Front End, used to send traffic back to the application FE <BFDGateway2ToNewFE>

For additional network configuration information, refer to:

- *CUDB Node Network Configuration*
- *Virtualized CUDB Node Network Configuration*

---

### Do!

Obtain the IP addresses for the site routers as well as the IP address and subnet mask of the application FE.

---

## 5.2.2 SAPC SOAP Notifications

Notifications are used for notifying applications after specific attributes are modified in CUDB.

SAPC notifications configuration requires update of the CUDB configuration model with a new instance of the CudbNotificationEndPoint class for the SAPC that is added in the UDC system. This class defines an endpoint receiving the notification event.

Refer to *CUDB Node Configuration Data Model Description* for CudbNotificationEndPoint attribute details.

The procedure how to configure the SAPC SOAP notifications are described in the document *Configuration Guide for SAPC Application in UDC*.

The following inputs are required:

- The document *Configuration Guide for SAPC Application in UDC*.



- The name of the added SAPC node to be used in the network.  
SAPC\_Node\_VIP\_Address is the IP of the new SAPC
- SAPC Node VIP address of the SAPCs available in the UDC system.  
**Note:** SAPC uses the same VIP address for LDAP traffic and SOAP traffic.
- Port number for SOAP over HTTP, in this case port:8080

---

---

### Do!

- Obtain the network name and SAPC Node VIP address of the added SAPC.
  - Obtain the names and SAPC Node VIP addresses of the SAPCs available in the UDC system
- 
- 

## 5.3 Prepare SAPC

When preparing the SAPC in a UDC deployment, consider the planning and preparations in this section along with those in the appropriate deployment document below:

- Physical Node Function (PNF).  
*SAPC PNF Deployment Instruction.*
- Virtualized Network Function deployment on OpenStack.  
*SAPC VNF Deployment Instruction for OpenStack.*
- Virtualized Network Function deployment on VMware.  
*SAPC VNF Deployment Instruction for VMware.*

### 5.3.1 SAPC License

License keys grant the usage of purchased functionality or capacity.




---

---

## Do!

Secure the license files are generated and available at installation time.

---

---

### 5.3.2 SAPC Entities

After successful SAPC SW installation, SAPC uses a mechanism based on configuration entities to know the CUDB nodes to connect and the data to retrieve to map each attribute to its internal data model. Entity Data Sources (EDSs) configure the data to retrieve from CUDB and Entity Data Targets (EDTs) configure data to update in CUDB. The examples provided in the *Configure Database Access in the SAPC* section in *Integration in User Data Consolidation* must be modified to include customer-specific information. See [Configure SAPC Entities](#) on page 23.

### 5.3.3 SAPC VNF Descriptor

The VNF Descriptor for the SAPC can be written in the Open Virtualization Format (OVF), generating an OVF package, or in Heat Orchestration Template (HOT), generating a HOT package.

The *SAPC VNF Descriptor Generator Tool* describes how to generate SAPC Virtual Network Function (VNF) Descriptor for the cloud environment.

---

---

## Do!

Generate the SAPC VNF Descriptor following the procedures in the *SAPC VNF Descriptor Generator Tool*.

---

---

## 5.4 Install SAPC

The following are the deployments scenarios of SAPC in UDC:

- Physical Node Function (PNF).

The installation of SAPC as PNF is described in the *SAPC PNF Deployment Instruction*.

- Virtualized Network Function deployment on OpenStack.

The installation of SAPC on CEE is described in the *SAPC VNF Deployment Instruction for OpenStack*.

- Virtualized Network Function deployment on VMware.



The installation of SAPC on VMware is described in the *SAPC VNF Deployment Instruction for VMware*.

---

---

## Do!

Choose the appropriate installation scenario from the list above.

Perform the SAPC installation following the procedure in the selected deployment instruction.

---

---

## 5.5 Configure CUDB for UDC

### 5.5.1 Configure CUDB Network Routing

Before updating the eVIP configuration, the added FE VIP needs to be added to the BSP virtual router sig\_data\_sp in the CUDB on BSP 8100, in native environment. When in virtual environment it impacts the cloud network infrastructure.

#### 5.5.1.1 Configure BSP Virtual Routers

**Note:** This procedure needs to be performed on every CUDB BSP8100 node.

#### Prerequisites

The following FE input is required:

- FE traffic network address or VIP
- FE subnet mask

The following Site Router input is required:

- IP address of the Site Router gateway for VRRP towards the Front End, used to send traffic back to the application FE <vrrpGatewayToNewFE>
- IP address of the Site Router 1 (left) gateway for BFD towards the Front End, used to send traffic back to the application FE <BFDGateway1ToNewFE>
- IP address of the Site Router 2 (right) gateway for BFD towards the Front End, used to send traffic back to the application FE <BFDGateway2ToNewFE>

#### Steps

1. Enter cliss in the CUDBs BSP.





2. Go to the MOM ManagedElement=1,Transport=1,Router=0-26-sig\_data\_sp,RouteTableIPv4Static=1
3. Print the data for one of the FEs defined there (other than 0.0.0.0/0): show all Dst=xxxx
4. Create a new element for the destination in both sig\_data\_sp virtual routers

In this case the destination is the new FE LDAP VIP.

- a. Check the elements that are already defined in the virtual routers.

```
show all ManagedElement=1,Transport=1,Router=0-26-
sig_data_sp,RouteTableIPv4Static=1
```

```
show all ManagedElement=1,Transport=1,Router=0-28-
sig_data_sp,RouteTableIPv4Static=1
```

Example

```
RouteTableIPv4Static=1
  Dst=0.0.0.0/0-Default
    dst="0.0.0.0/0"
    NextHop=blackhole
      adminDistance=1
      nexthop
        discard
  Dst=10.120.174.230/32-HLR_LDAP_FE-InterCMX
    dst="10.120.174.230/32"
    NextHop=sig_data_sp_nlc1
      adminDistance=120
      bfdEnable
      nexthop
        address="192.168.208.10"
```

- b. In the case where VRRP is used between BSP and the site routers (infrastructure):

Example

```
ManagedElement=1,Transport=1,Router=0-26-sig_data_sp,
RouteTableIPv4Static=1
  configure
    Dst=<dst_IP_or_nw_name>_LDAP_FE
    dst="<dst_IP_or_nw/mask>"
    NextHop=fe_gw_vrrp
      adminDistance=5
      nexthop
        address="<vrrpGatewayToNewFE>"
  commit
ManagedElement=1,Transport=1,Router=0-28-sig_data_sp,
RouteTableIPv4Static=1
  configure
    Dst=<dst_IP_or_nw_name>_LDAP_FE
```



```
dst="<dst_IP_or_nw/mask>"
NextHop=fe_gw_vrrp
adminDistance=5
nexthop
address="<vrrpGatewayToNewFE>"
commit
```

- c. In the case where BFD is used between BSP and the site routers (infrastructure):

Example

```
ManagedElement=1,Transport=1,Router=0-26-sig_data_sp,
RouteTableIPv4Static=1
configure
Dst=<dst_IP_or_nw_name>_LDAP_FE
dst="<dst_IP_or_nw/mask>"
NextHop=fe_bfd_gw_A1
adminDistance=5
bfdEnable
nexthop
address="<BFDGateway1ToNewFE>"
commit
```

```
ManagedElement=1,Transport=1,Router=0-28-sig_data_sp,
RouteTableIPv4Static=1
configure
Dst=<dst_IP_or_nw_name>_LDAP_FE
dst="<dst_IP_or_nw/mask>"
NextHop=fe_bfd_gw_B1
adminDistance=5
bfdEnable
nexthop
address="<BFDGateway2ToNewFE>"
commit
```

- d. Check that the new entries have been successfully committed in the virtual router:

Example

```
show all ManagedElement=1,Transport=1,Router=0-26-
sig_data_sp,RouteTableIPv4Static=1
```

```
show all ManagedElement=1,Transport=1,Router=0-28-
sig_data_sp,RouteTableIPv4Static=1
```

5. Repeat the steps in this task in Router=0-28-sig\_data\_sp.



### 5.5.1.2 Configure eVIP for SAPC

The eVIP configuration must be updated with a route to the SAPC traffic network. This affects every CUDB node in the system.

For general information on the eVIP, refer to *eVIP Management Guide*. The commands used during the procedure are subject to certain eVIP limitations. These limitations are as follows:

- Note:**
- The maximum length of a command name is limited to 50 characters.
  - The maximum length of the sum of all command names for a blade are limited to 4040 characters.

This section describes how to add new routes for the new remote node. Refer to section *eVIP Static, Routes Configuration in an Installed System* in *CUDB System Administrator Guide*.

#### Steps

1. Establish a new administrative CUDB CLI session towards one of the SC blades of the target CUDB node with the following command:

```
ssh <admin_user>@<CUDB_Node_OAM_VIP_Address>
```

2. Define a new startup command by doing the following steps:

- a. List all commands on the blades with the following command:

```
cudbEvipEncapsulator --show --blade <number_of_blade>|all
```

#### Example

Example

```
#cudbEvipEncapsulator --show --blade 4
Showing commands for blade PL_2_4:
flush_route_cache
set_site_120
set_site_130
set_provisioning_PG
set_provisioning_120
set_provisioning_130
set_HSS_FE6106
set_HSS_FE6124
set_HLR_FE02
set_HLR_BS01
```

- b. Add the new startup command in the eVIP configuration command section. Select the ALB number where routes have to go ("alb\_0", "alb\_1" or "alb\_2"):



```
cudbEvipEncapsulator --new-command --name <command_name>
--definition <command_definition>
```

where <command\_definition> is the Linux command for route definition towards the new node.

#### Example

##### Example

```
# cudbEvipEncapsulator --new-command --name
"set_SAPC01" --definition "ip route add
10.1.0.212/32 dev alb_1"
Config file saved
Added a new command with name "set_SAPC01"
```

3. Add the new startup command to every blade except the system controllers in the node as follows:

```
cudbEvipEncapsulator --add --name <command_name> --blade
<number_of_blade>
```

**Note:** The <number\_of\_blade> value depends on the number of blades in the system. For instance: values range from 3 to 10 for a 10-blade system, 3–22 for 22-blade and 3–34 for a 34-blade system.

Below is an example on using the command:

#### Example

```
# cudbEvipEncapsulator --add --name "set_SAPC01" --blade 4
```

4. The newly added startup commands are applied by running the cudbEvipEncapsulator script on all the blades.

```
cudbEvipEncapsulator --blade <number_of_blade>
```

**Note:** The <number\_of\_blade> value depends on the number of blades in the system. For instance: values range from 3 to 10 for a 10-blade system, 3–22 for 22-blade and 3–34 for a 34-blade system.

#### Example

```
#cudbEvipEncapsulator --blade 4
```

5. Check that the new startup commands are added:

```
cudbEvipEncapsulator --show --blade <number_of_blade>|all
```

#### Example

```
#cudbEvipEncapsulator --show --blade 4
Showing commands for blade PL_2_4:
flush_route_cache
set_site_120
set_site_130
```



```
set_provisioning_PG
set_provisioning_120
set_provisioning_130
set_HSS_FE6106
set_HSS_FE6124
set_HLR_FE02
set_HLR_BS01
set_SAPC01
```

6. This procedure must be performed for all remaining CUDB nodes.

## 5.5.2 Configure SAPC SOAP Notifications

Notifications are used for notifying applications after specific attributes are modified in CUDB.

The procedure how to configure the SAPC SOAP notifications are described in the document *Configuration Guide for SAPC Application in UDC*.

### Prerequisites

The following inputs and files are required:

- Network name and SAPC Node VIP address for SOAP for the new SAPC.
- Network names and SAPC Node VIP addresses for all the existing SAPCs nodes in the network.
- Port number for SOAP (default 8080).

### Steps

1. Configure the SAPC notifications in CUDB by following the procedure in section *Adding New SAPC* in the *Configuration Guide for SAPC Application in UDC*.

## 5.6 Configure SAPC

### 5.6.1 Configure SAPC Entities

After successful SAPC SW installation, SAPC needs to know the CUDB nodes to connect and the data to retrieve to map each attribute to its internal data model. SAPC provides a mechanism based on configuration entities for this purpose. There are Entity Data Sources (EDSs) to configure the data to retrieve from CUDB and Entity Data Targets (EDTs) to configure data to update in CUDB.



The examples must be modified to include customer-specific information.

### Steps

1. Configure the EDSs and EDTs in SAPC according to the details in *Configure Database Access in the SAPC* section in *Integration in User Data Consolidation*.



# Installation Instruction for SAPC Application in UDC Reference List

## UDC

Typographic Conventions

Glossary of Terms and Acronyms

Trademark Information

UDC CN Connectivity and Traffic Distribution Guideline

UDC System Description

[EIN – UDC](#)

[EIN – vUDC](#)

## CUDB

CUDB Installation Instruction

Virtualized CUDB Installation Instruction

CUDB Import and Export Procedures

CUDB Node Configuration Data Model Description

CUDB Node Network Configuration

Virtualized CUDB Node Network Configuration

CUDB Application Schema Update

CUDB Notifications

CUDB Schema Conversion Tool

CUDB System Administrator Guide

eVIP Management Guide

CUDB Security and Privacy Management

OpenLDAP, Idapadd Tool Manual

OpenLDAP, slapadd Tool Manual

## EDA/PG

Software Installation for Virtual and Cloud Deployment

Software Installation for Native Deployment



Network Description and Configuration for Native Deployment  
Network Description and Configuration for Virtual and Cloud Deployment  
Parameter List for Native Deployment  
Parameter List for Virtual Deployment  
Parameter List for CEE Deployment  
Parameter List for Openstack Deployment  
Configuration Manual for Resource Activation  
Configuration Manual UDC Data Durability  
Customer Questionnaire for Virtual and Cloud Deployment  
Customer Questionnaire for Native Deployment

### **SAPC References**

*SAPC PNF Deployment Instruction*, 8/1531-CSH 109 215/7  
*SAPC VNF Deployment Instruction for OpenStack*, 3/1531-CSH 109 215/7  
*SAPC VNF Deployment Instruction for VMware*, 4/1531-CSH 109 215/7  
*Integration in User Data Consolidation*, 11/1551-CSH 109 215/7-V1  
*Configuration Guide for SAPC Application in UDC*, 31/1553-CSH 109 215/7  
*SAPC VNF Descriptor Generator Tool*, 30/1553-CSH 109 215/7

### **SAPC Non-Document Reference**

*UDC SAPC Application Counters Installation*, 1/190 55-CXP 904 0293/4  
*SAPC Application Counters for CUDB*, 19089-CXC1735720/2  
*SOAP notifications configuration in UDC*, 1/1553-CXP 904 0613/3  
*SAPC SOAP notifications installation in UDC*, 1/190 89-CXP 904 0613/3.  
*SAPC input for SOAP notifications installation in UDC*, 1/1531-CXP 904 0613/3.

### **Schema Files**

*UDC Identities (openLDAP loadable) schema file*, 155 64-HSC 113 08/5  
*UDC MultiService Consumer Identities (openLDAP loadable) schema file*, 1/155 64-HSC 113 08/8  
*UDC Association Administrative Data (openLDAP loadable) schema file*, 2/155 64-HSC 113 08/5.  
*SAPC LDAP schema for UDC*, 2/1531-CXP 904 0613/3





## UPG

UPG Schema Change for CUDB, 6/198 17-AVA 901 38/3
---