



INSTALLATION GUIDE | PUBLIC

Document Version: 1.0 – 2019-05-16

Installation Guide

Content

- 1 Document History. 5**
- 2 Before You Start. 6**
 - 2.1 About This Document. 6
 - 2.2 Target Audience. 7
 - 2.3 What's New in This Document. 7
 - 2.4 Additional Information. 9
 - 2.5 Document Abbreviations. 9
 - 2.6 Document Definitions. 10
- 3 Installing SAP Convergent Charging. 12**
 - 3.1 SAP CC Software Components. 12
 - 3.2 Installing a mono-host landscape. 13
 - 3.3 Installing a multi-hosts landscape. 14
 - 3.4 Adding elements to your landscape. 15
 - 3.5 Post-installation operations. 16
- 4 Uninstalling SAP Convergent Charging. 17**
 - 4.1 Uninstalling an instance of a given host. 17
 - 4.2 Uninstalling a back-end database. 17
 - 4.3 Uninstalling a user interface. 18
- 5 Procedures. 19**
 - 5.1 Defining your landscape. 20
 - 5.2 Choosing System IDs. 21
 - 5.3 Downloading the Installation DVD. 22
 - 5.4 Downloading the JCE Jurisdiction Policy Files Archive. 25
 - 5.5 Downloading the SAP JVM. 26
 - 5.6 Downloading the SAPCAR Utility. 27
 - 5.7 Downloading the SAP Cryptographic Library. 27
 - 5.8 Downloading the Oracle JDBC driver. 28
 - 5.9 Checking free space. 29
 - 5.10 Creating required directories. 30
 - 5.11 Setting up the system encoding. 31
 - 5.12 Installing C Shell. 32
 - 5.13 Setting up the system time zone. 33
 - 5.14 Setting up the system environment variables. 35
 - 5.15 Preparing the Oracle Core Database. 36

5.16	Preparing the SQL Server Core Database.	40
5.17	Preparing the SAP ASE Core Database.	43
5.18	Preparing the SAP HANA Core Database.	48
5.19	Preparing the IBM DB2 Core Database (w/o pureScale Feature).	50
5.20	Installing a Core Server on a mono-host landscape.	54
5.21	Installing a Core Server on a multi-hosts landscape.	61
5.22	Testing a landscape basically.	67
5.23	Setting up a new host for a landscape.	70
5.24	Adding Core Server instances in a multi-hosts landscape.	70
5.25	Starting and stopping the servers.	73
5.26	Installing a BART Server in an existing landscape.	78
5.27	Preparing the Oracle BART Database.	85
5.28	Preparing the SQL Server BART Database.	87
5.29	Preparing the SAP ASE BART Database.	90
5.30	Preparing the SAP HANA BART Database.	94
5.31	Preparing the IBM DB2 BART Database (w/o pureScale Feature).	96
5.32	Installing a Diameter Server in an existing landscape.	99
5.33	Preparing the Oracle IEC Database.	103
5.34	Preparing the SQL Server IEC Database.	105
5.35	Preparing the SAP HANA IEC Database.	107
5.36	Preparing the Oracle Session Database.	109
5.37	Installing an IEC (Import Export Connector) in an existing landscape.	112
5.38	Launching the SAPinst tool.	115
5.39	Launching Core Tool.	117
5.40	Launching BART Tool.	119
5.41	Launching CAT Tool.	122
5.42	Launching Cockpit.	125
5.43	Launching Admin+.	130
5.44	Launching BART+.	131
5.45	Launching Setup Tool.	133
5.46	Launching BART Setup Tool.	135
5.47	Launching Config Tool.	136
5.48	Securing a landscape.	138
5.49	Securing communications with the Core Server system.	142
5.50	Securing communications with the BART Server system.	155
5.51	Securing communications with the Diameter Server system.	162
5.52	Securing communications with Cockpit and Tomcat Server.	165
5.53	Installing a permanent license.	170
5.54	Removing system(s) or instance(s) from a given host.	171
5.55	Integrating SAP CC with CA APM.	172
5.56	Integrating SAP CC with SAP CTS+.	175

5.57 Integrating SAP CC with SAP Convergent Invoicing178

5.58 Copying an SAP CC Core Server. 182

1 Document History

Version	Date	Description
1.0	May 2019	First Version

2 Before You Start

Related Information

[About This Document \[page 6\]](#)

[Target Audience \[page 7\]](#)

[What's New in This Document \[page 7\]](#)

[Additional Information \[page 9\]](#)

[Document Abbreviations \[page 9\]](#)

[Document Definitions \[page 10\]](#)

2.1 About This Document

The **Installation Guide** is an *SAP Product Document* that explains how to install an SAP Convergent Charging 5.0 system landscape, including the necessary components such as:

- Server systems
- User interfaces
- Additional components

This guide provides installation guidance for setting up system landscapes from development to production, grouped among 2 different installation scenarios:

- [Installing a mono-host landscape \[page 13\]](#), which corresponds to landscapes hosting the minimum required software components on a single Windows host
- [Installing a multi-hosts landscape \[page 14\]](#), which corresponds to landscapes hosting a more realistic set of software components on multiple Linux hosts that are configured and sized according to the business requirements

These 2 installation scenarios are described afterwards in this guide, and represent specific sets of installation steps that correspond to procedures available in the [Procedures](#) section. You can adapt each installation scenario to fit specific needs by using different or additional procedures, and thus create specific scenario such as:

- A mono-host landscape running on a Linux host
- A multi-hosts landscape running on Windows hosts and using an Oracle Core Database
- And so on

Caution

This guide does not provide any guidance for installing the following elements:

- HTTP Client and Message Client user interfaces
- IBM DB2 pureScale databases

This guide does not provide any guidance for integrating SAP CC with the following systems:

- SAP System Landscape Directory
- SAP Solution Manager
- SAP Convergent Invoicing

For further information about these elements, refer to the SAP CC 4.0 Installation Guide documentation.

2.2 Target Audience

This guide is intended for the following audience:

- Solution and Technology Consultants
- Application and System Administrators

2.3 What's New in This Document

What's New in SP 4 ?

As of SP 4, SAP Convergent Charging 5.0 provides you with the following modifications of this documentation:

- New [Downloading the Oracle JDBC driver \[page 28\]](#) procedure, that you must use before installing your landscape
- New [Upgrading Cockpit \[page 128\]](#) procedure, that you must know before upgrading Cockpit

What's New in SP 3 ?

As of SP 3, SAP Convergent Charging 5.0 provides you with the following modifications of this documentation:

- Minor corrections of the overall document
- Modification of the [architecture overview \[page 12\]](#) that now emphasis Cockpit communication channels
- New [Preparing the Oracle Session Database \[page 109\]](#) procedure, that you can use when implementing the optional Dual Database feature

What's New in SP 2 ?

As of SP 2, SAP Convergent Charging 5.0 provides you with the following modifications of this documentation:

- Minor corrections within the following procedures:
 - [Launching Core Tool \[page 117\]](#)
 - [Launching BART Tool \[page 119\]](#)
 - [Launching CAT Tool \[page 122\]](#)
 - [Preparing the IBM DB2 Core Database \(w/o pureScale Feature\) \[page 50\]](#)
 - [Preparing the IBM DB2 BART Database \(w/o pureScale Feature\) \[page 96\]](#)
 - [Securing the RFC over TCP/IP communications \[page 149\]](#)
- Simplification of the [Launching Cockpit \[page 125\]](#) procedure
- Modification of the [Preparing the SAP HANA Core Database \[page 48\]](#), [Preparing the SAP HANA BART Database \[page 94\]](#) and [Preparing the SAP HANA IEC Database \[page 107\]](#) procedures to take into account the MDC¹ mode and the high-availability capabilities of SAP HANA databases
- Modification of the [Installing a Core Server on a mono-host landscape \[page 54\]](#) and [Installing a Core Server on a multi-hosts landscape \[page 61\]](#) procedures to take into account the MDC mode and the high-availability capabilities of SAP HANA databases
- New [Integrating SAP CC with SAP Convergent Invoicing \[page 178\]](#) procedure that you can use during post-installation operations

What's New in SP 1 ?

As of SP 1, SAP Convergent Charging 5.0 provides you with the following modifications of this documentation:

- Modification of the mono-host and multi-hosts installation scenarios to take into account the integration with SAP Convergent Invoicing systems
- Minor corrections within the following procedures:
 - [Preparing the SAP ASE Core Database \[page 43\]](#)
 - [Preparing the SAP ASE BART Database \[page 90\]](#)
- Modification of the [Launching Cockpit \[page 125\]](#) procedure to take new configuration parameters into account
- Modifications within the following procedures to take new tablespaces/filegroups/segments into account:
 - [Preparing the Oracle Core Database \[page 36\]](#)
 - [Preparing the SQL Server Core Database \[page 40\]](#)
 - [Preparing the SAP ASE Core Database \[page 43\]](#)
 - [Preparing the IBM DB2 Core Database \(w/o pureScale Feature\) \[page 50\]](#)
- Modification of the [Launching Cockpit \[page 125\]](#) procedure to take new configuration parameters into account

¹ Multiple Data Container

2.4 Additional Information

For more information about specific topics, see the quick links as shown in the table below:

Content	Quick Link
SAP CC documentation	http://help.sap.com/cc50
<div style="border: 1px solid #ccc; padding: 10px; background-color: #f9f9f9;"> <p>i Note</p> <p>SAP CC is part of the SAP solution SAP Billing based on SAP Business Suite or SAP S/4 HANA. Consult the central solution information at the following address: https://cx.sap.com/fr/products/billing</p> </div>	
Related SAP notes	http://support.sap.com/notes
Related release notes	https://support.sap.com/en/my-support/knowledge-base.html
SAP Solution Manager	http://support.sap.com/solutionmanager

2.5 Document Abbreviations

Abbreviation	Meaning
BART	Batch Acquisition and Rating Toolset
CAT	Connector Administration Tool
CIF	Charging output Integration Framework
CMA	Customer Management Area
DBA	DataBase Administrator
HA	High Availability
HCI	Http Communication Interface
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secured
IEC	Import Export Connector
JDBC	Java Database Connectivity
JRE	Java Runtime Environment
JVM	Java Virtual Machine
MDC	Multiple Data Container
NFS	Network File system

Abbreviation	Meaning
PAM	Product Availability Matrix
PKCS	Public-Key Cryptography Standards

2.6 Document Definitions

SAP Global Host

The SAP Global Host corresponds to the first physical host on which an instance of an SAP CC system is installed. According to your installation scenario, your landscape may thus contain multiple SAP Global Hosts.

❁ Example

Considering a landscape containing 3 physical hosts:

- 1 H1 host dedicated to the installation of a Dispatcher and an Updater instances of the Core Server system
- 1 H2 host dedicated to the installation of additional instances of the Core Server system
- 1 H3 host dedicated to the installation of the BART Server and Diameter Server systems

Then:

- H1 is considered as the SAP Global Host for the Core Server system
- H3 is considered as the SAP Global Host for the BART Server system
- H3 is considered as the SAP Global Host for the Diameter Server system

SAP Central Repository

The SAP Central Repository is a concept related to SAP systems that are made up with instances distributed over multiple physical hosts, and that need to have a central location containing the executable programs and profiles of all these instances. This repository is located on the SAP Global Host of each SAP system, and is shared to the different hosts that make up this system.

On Microsoft Windows operating systems, the SAPinst tool:

- Automatically creates the SAP Central Repository using the `<DRIVE>:\usr\sap\<SID>\SYS` directory
- Shares the `<DRIVE>:\usr\sap` directory using the `sapmnt` and `saploc` share names

On UNIX and Linux operating systems:

- The SAP Central Repository must be manually created using the `/sapmnt` directory
- The SAP Central Repository must be manually shared to the other hosts using the `sapmnt` share name, and mounted on each host different than the SAP Global Host

- The SAPinst tool automatically creates the `/usr/sap/<SID>` directory and some associated symbolic links

i Note

As far as SAP Convergent Charging is concerned, only the Core Server system can be distributed over multiple hosts. The concept of SAP Central Repository is thus only relevant for the Core Server system.

The following table contains information about the content of the SAP Central Repository:

Subfolder	Description	Location									
		Global Host	Host								
exe	The exe folder is a physical folder that is located on each host of your landscape but contains subfolders mapped onto the Global Host of your system. Considering <code><OS></code> as the operating system of the host, the <code>uc/<OS></code> subfolder contains global executable programs and SAP CC programs that are located into different subfolders according to your SAP CC system:	P	P								
	<table border="1"> <thead> <tr> <th>System</th> <th>Folder Structure</th> </tr> </thead> <tbody> <tr> <td>Core Server</td> <td> <ul style="list-style-type: none"> • <code>exe/uc/<OS>/CC_CORE_SERVER/</code> • <code>exe/uc/<OS>/CC_CORE_SERVER/config/</code> • <code>exe/uc/<OS>/CC_CORE_SERVER/core_sql/</code> • <code>exe/uc/<OS>/CC_CORE_SERVER/session_sql/</code> • <code>exe/uc/<OS>/CC_CORE_SERVER/jars/</code> • <code>exe/uc/<OS>/CC_CORE_SERVER/licenses/</code> • <code>exe/uc/<OS>/CC_CORE_SERVER/tax/</code> </td> </tr> <tr> <td>BART Server</td> <td> <ul style="list-style-type: none"> • <code>exe/uc/<OS>/CC_BART_SERVER/</code> • <code>exe/uc/<OS>/CC_BART_SERVER/bart_sql/</code> • <code>exe/uc/<OS>/CC_BART_SERVER/config/</code> • <code>exe/uc/<OS>/CC_BART_SERVER/examples/</code> • <code>exe/uc/<OS>/CC_BART_SERVER/jars/</code> </td> </tr> <tr> <td>Diameter Server</td> <td> <ul style="list-style-type: none"> • <code>exe/uc/<OS>/CC_DIAMETER_SERVER/</code> • <code>exe/uc/<OS>/CC_DIAMETER_SERVER/config/</code> • <code>exe/uc/<OS>/CC_DIAMETER_SERVER/jars/</code> </td> </tr> </tbody> </table>	System	Folder Structure	Core Server	<ul style="list-style-type: none"> • <code>exe/uc/<OS>/CC_CORE_SERVER/</code> • <code>exe/uc/<OS>/CC_CORE_SERVER/config/</code> • <code>exe/uc/<OS>/CC_CORE_SERVER/core_sql/</code> • <code>exe/uc/<OS>/CC_CORE_SERVER/session_sql/</code> • <code>exe/uc/<OS>/CC_CORE_SERVER/jars/</code> • <code>exe/uc/<OS>/CC_CORE_SERVER/licenses/</code> • <code>exe/uc/<OS>/CC_CORE_SERVER/tax/</code> 	BART Server	<ul style="list-style-type: none"> • <code>exe/uc/<OS>/CC_BART_SERVER/</code> • <code>exe/uc/<OS>/CC_BART_SERVER/bart_sql/</code> • <code>exe/uc/<OS>/CC_BART_SERVER/config/</code> • <code>exe/uc/<OS>/CC_BART_SERVER/examples/</code> • <code>exe/uc/<OS>/CC_BART_SERVER/jars/</code> 	Diameter Server	<ul style="list-style-type: none"> • <code>exe/uc/<OS>/CC_DIAMETER_SERVER/</code> • <code>exe/uc/<OS>/CC_DIAMETER_SERVER/config/</code> • <code>exe/uc/<OS>/CC_DIAMETER_SERVER/jars/</code> 		
System	Folder Structure										
Core Server	<ul style="list-style-type: none"> • <code>exe/uc/<OS>/CC_CORE_SERVER/</code> • <code>exe/uc/<OS>/CC_CORE_SERVER/config/</code> • <code>exe/uc/<OS>/CC_CORE_SERVER/core_sql/</code> • <code>exe/uc/<OS>/CC_CORE_SERVER/session_sql/</code> • <code>exe/uc/<OS>/CC_CORE_SERVER/jars/</code> • <code>exe/uc/<OS>/CC_CORE_SERVER/licenses/</code> • <code>exe/uc/<OS>/CC_CORE_SERVER/tax/</code> 										
BART Server	<ul style="list-style-type: none"> • <code>exe/uc/<OS>/CC_BART_SERVER/</code> • <code>exe/uc/<OS>/CC_BART_SERVER/bart_sql/</code> • <code>exe/uc/<OS>/CC_BART_SERVER/config/</code> • <code>exe/uc/<OS>/CC_BART_SERVER/examples/</code> • <code>exe/uc/<OS>/CC_BART_SERVER/jars/</code> 										
Diameter Server	<ul style="list-style-type: none"> • <code>exe/uc/<OS>/CC_DIAMETER_SERVER/</code> • <code>exe/uc/<OS>/CC_DIAMETER_SERVER/config/</code> • <code>exe/uc/<OS>/CC_DIAMETER_SERVER/jars/</code> 										
profile	Also called SAP Profile Folder , the profile directory contains the configuration files related to boot and startup operations of all the instances (<code>jstart.config</code> , <code>boot.config</code>), available in the following subfolders: <ul style="list-style-type: none"> • <code>profile/boot</code>, within which the <code>boot.config</code> file is present • <code>profile/jstart</code>, which contains a subfolder for each installed instance, each subfolder containing the adequate <code>jstart.config</code> file 	P	S								

(P: Physical folder, S: Shared folder)

3 Installing SAP Convergent Charging

Related Information

- [SAP CC Software Components \[page 12\]](#)
- [Installing a mono-host landscape \[page 13\]](#)
- [Installing a multi-hosts landscape \[page 14\]](#)
- [Adding elements to your landscape \[page 15\]](#)
- [Post-installation operations \[page 16\]](#)

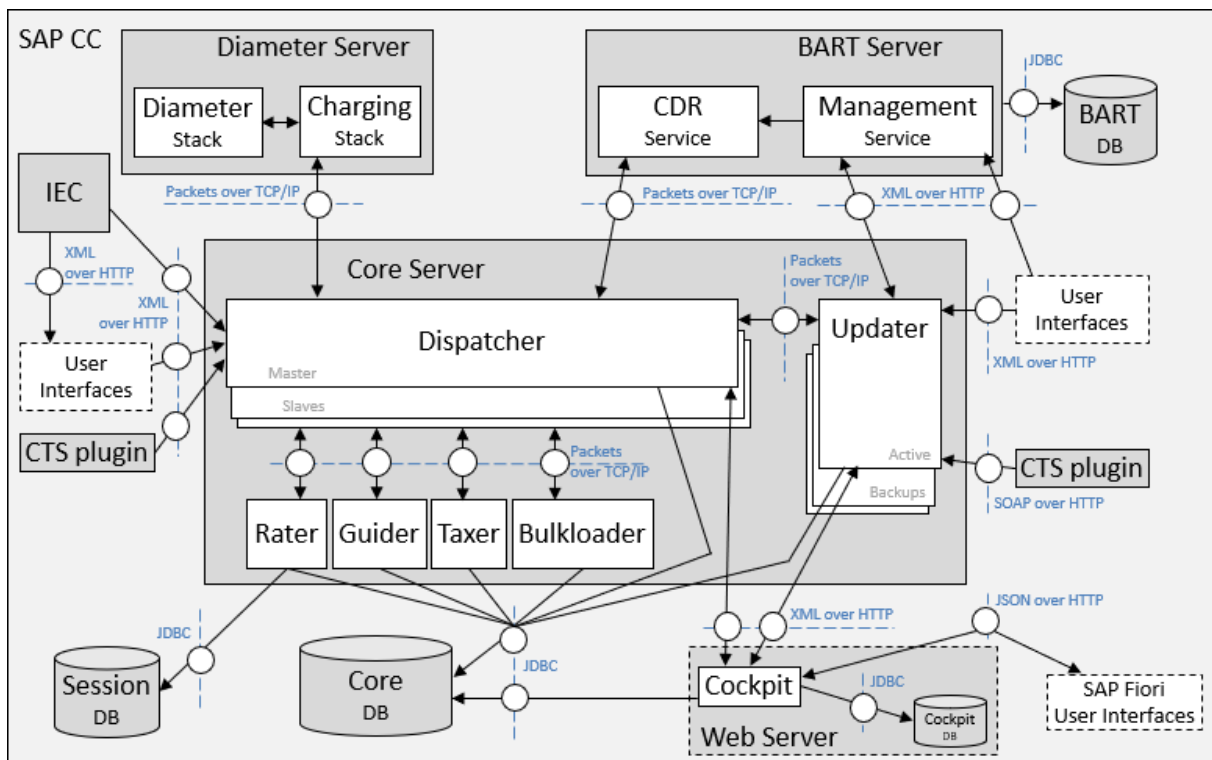
3.1 SAP CC Software Components

SAP Convergent Charging is made up with the following set of Java-based software components that you can install to perform your business operations. For further information about the different software components, refer to the PAM ² available at the following location: <https://support.sap.com/pam>, or to the *Architecture* section of the [SAP CC 5.0 Application Help](#) documentation.

Server systems	User interfaces	Databases
<ul style="list-style-type: none">• Core Server• BART Server• Diameter Server• Import/Export Connector	<ul style="list-style-type: none">• Core Tool, BART Tool, CAT Tool• Cockpit• Admin+, BART+• Setup Tool, BART Setup Tool• Config Tool• HTTP Client, Message Client	<ul style="list-style-type: none">• Core Database• BART Database• IEC Database• Session Database• Cockpit Database

The following schema provides you with an overview of the interactions between the different software components of SAP CC:

² Product Availability Matrix



Each software element is available in the installation DVD of SAP Convergent Charging, that you can download using the [Downloading the Installation DVD \[page 22\]](#) procedure available in this guide.

3.2 Installing a mono-host landscape

This installation scenario corresponds to landscapes containing the minimum set of software components, all installed on the same physical host (acting as the SAP Global Host) using a temporary license. This scenario consists in deploying on a Microsoft Windows host 4 instances of the Core Server (1 Dispatcher, 1 Guider, 1 Rater and 1 Updater):

- Working in conjunction with a pre-installed SQL Server database
- Without any encryption of the communication channels

The first step of this installation scenario consists in retrieving the different materials that are necessary to deploy the expected SAP CC elements. Execute the following common procedures, taking into account the associated recommendations:

- [Defining your landscape \[page 20\]](#)
- [Choosing System IDs \[page 21\]](#)
- [Downloading the Installation DVD \[page 22\]](#)
- [Downloading the JCE Jurisdiction Policy Files Archive \[page 25\]](#)

The second step of this installation scenario consists in using the [Setting up a new host for a landscape \[page 70\]](#) procedure to set up the system of the SAP Global Host before deploying the 4 instances of the Core Server system.

The third step of this installation scenario consists in preparing the database using the dedicated [Preparing the SQL Server Core Database \[page 40\]](#) procedure.

The last step of this installation scenario consists in deploying the expected SAP CC elements using the [Installing a Core Server on a mono-host landscape \[page 54\]](#) procedure that you can consider as an entry point for installing:

- A stand-alone landscape, that is not integrated with any third-party system and does not give the possibility to work with billable items or consumption items
- A landscape that is integrated with the SAP Convergent Invoicing system and gives the possibility to work with billable items and/or consumption items

When these 3 steps have been successfully executed, you can use the following procedures:

- [Starting and stopping the servers \[page 73\]](#), to manage your installed instances
- [Testing a landscape basically \[page 67\]](#), to ensure that your landscape is properly working

Even if your landscape only concerns development or test operations, you might need to tune it to get better performances. For further information about the tuning possibilities, refer to the [SAP CC 5.0 Tuning Guide](#) documentation.

3.3 Installing a multi-hosts landscape

This installation scenario corresponds to landscapes containing a more realistic set of software components used for production purpose. This scenario consists in deploying on different physical hosts 4 instances of the Core Server (1 Dispatcher, 1 Guider, 1 Rater and 1 Updater):

- Working in conjunction with an Oracle database pre-installed on a dedicated host
- Using a temporary license
- Without any encryption of the communication channels
- Every physical host running under a Linux operating system

i Note

For scalability purpose, you can extend your landscape by installing additional instances, respecting the following basic rules:

- For performance reasons, every Rater/Bulkloader couple shall be deployed on a dedicated host, and every Dispatcher/Guider couple shall be associated to 2 Rater/Bulkloader couples
- High availability for charging operations is available when the landscape contains either:
 - 3 hosts each containing a Dispatcher/Guider couple + 3 hosts each containing a Rater/Bulkloader couple
 - or 3 hosts each containing 1 Dispatcher, 1 Guider, 1 Rater and 1 Bulkloader instances
- Every Updater instance shall be deployed on a dedicated host, to avoid latencies during charging or refilling operations. High availability for provisioning operations is available when 2 Updaters are deployed within your landscape. Deploying more than 2 Updaters is possible but not necessary to ensure high availability

The first step of this installation scenario consists in retrieving the different materials that are necessary to deploy the expected SAP CC elements. Execute the following common procedures, taking into account the associated recommendations:

- [Defining your landscape \[page 20\]](#) considering:
 - 1 host (the SAP Global Host) containing 1 Dispatcher and 1 Guider
 - 1 host containing 1 Rater
 - 1 host containing 1 Updater
 - 1 host containing the Core Database
- [Choosing System IDs \[page 21\]](#)
- [Downloading the Installation DVD \[page 22\]](#)
- [Downloading the JCE Jurisdiction Policy Files Archive \[page 25\]](#)

The second step of this installation scenario consists in using the [Setting up a new host for a landscape \[page 70\]](#) procedure to set up the system of the following physical hosts before deploying the expected SAP CC elements :

- The SAP Global Host, that will contain the installation DVD and the following 2 instances of the Core Server:
 - 1 Dispatcher
 - 1 Guider
- The host dedicated to provisioning operations, containing 1 Updater
- The host dedicated to operations such as charging, refilling, and so on, containing 1 Rater

The third step of this installation scenario consists in preparing the database using the dedicated [Preparing the Oracle Core Database \[page 36\]](#) procedure.

The last step of this installation scenario consists in deploying the expected SAP CC elements using:

- The [Installing a Core Server on a multi-hosts landscape \[page 61\]](#) procedure, that you can consider as an entry point for managing the SAP Global Host and installing:
 - A stand-alone landscape, that is not integrated with any third-party system and does not give the possibility to work with billable items or consumption items
 - A landscape that is integrated with the SAP Convergent Invoicing system and gives the possibility to work with billable items and/or consumption items
- The [Adding Core Server instances in a multi-hosts landscape \[page 70\]](#) procedure to manage the other hosts of the landscape

When these 4 steps have been successfully executed, you can use the following procedures:

- [Starting and stopping the servers \[page 73\]](#), to manage your installed instances
- [Testing a landscape basically \[page 67\]](#), to ensure that your landscape is properly working

3.4 Adding elements to your landscape

After the installation of the Core Server system, you can extend your landscape by:

- Installing the following SAP CC systems:
 - BART Server, using the dedicated [Installing a BART Server in an existing landscape \[page 78\]](#) procedure

- Diameter Server, using the dedicated [Installing a Diameter Server in an existing landscape \[page 99\]](#) procedure
- Import/Export Connector, using the dedicated [Installing an IEC \(Import Export Connector\) in an existing landscape \[page 112\]](#) procedure
- Deploying the following user interfaces to interact with the installed systems:
 - Core Tool, using the dedicated [Launching Core Tool \[page 117\]](#) procedure
 - BART Tool, using the dedicated [Launching BART Tool \[page 119\]](#) procedure
 - CAT Tool, using the dedicated [Launching CAT Tool \[page 122\]](#) procedure
 - Cockpit, using the dedicated [Launching Cockpit \[page 125\]](#) procedure
 - Admin+, using the dedicated [Launching Admin+ \[page 130\]](#) procedure
 - BART+, using the dedicated [Launching BART+ \[page 131\]](#) procedure
 - Setup Tool, using the dedicated [Launching Setup Tool \[page 133\]](#) procedure
 - BART Setup Tool, using the dedicated [Launching BART Setup Tool \[page 135\]](#) procedure
 - Config Tool, using the dedicated [Launching Config Tool \[page 136\]](#) procedure

3.5 Post-installation operations

Once your landscape is installed, you may need to perform post-installations operations such as:

- Administrating your landscape (permanent license installation, instances management, and so on)
- Configuring elements to fit your business requirements (VAT³ rules and rates, public holidays, and so on)
- Integrating your SAP CC landscape with other systems available within a global infrastructure, such as SAP System Landscape Directory, SAP Solution Manager, SAP CI, SAP CRM, and so on
- Copying a Core Server system from one host to another

You can use the following list to perform post-installation operations:

- Administrating your landscape:
 - [Installing a permanent license \[page 170\]](#)
 - [Starting and stopping the servers \[page 73\]](#), to manage the instances deployed within your landscape
 - [Securing a landscape \[page 138\]](#)
- Integrating your landscape with other systems:
 - [Integrating SAP CC with CA APM \[page 172\]](#)
 - [Integrating SAP CC with SAP CTS+ \[page 175\]](#)
 - [Integrating SAP CC with SAP Convergent Invoicing \[page 178\]](#)
- Managing your landscape:
 - [Copying an SAP CC Core Server \[page 182\]](#)

³ Value Added Tax

4 Uninstalling SAP Convergent Charging

For any reason, you can modify your SAP CC system landscape by uninstalling :

- One or multiple instances of a given host
- A back-end database
- A user interface

Related Information

[Uninstalling an instance of a given host \[page 17\]](#)

[Uninstalling a back-end database \[page 17\]](#)

[Uninstalling a user interface \[page 18\]](#)

4.1 Uninstalling an instance of a given host

The SAPinst tool used to install instances within your SAP CC landscape also gives the possibility to uninstall instances. To remove one or multiple instances of a given host within an existing landscape, refer to the [Removing system\(s\) or instance\(s\) from a given host \[page 171\]](#) dedicated procedure.

⚠ Caution

If your landscape is a multi-hosts landscape, you must first uninstall instances deployed on hosts different than the [SAP Global Host \[page 10\]](#). The SAP Global Host of every installed SAP CC system must be the last host you uninstall elements from.

4.2 Uninstalling a back-end database

SAP Convergent Charging does not provide any mechanism to uninstall a backend database from a landscape.

Refer to your DBA⁴ to get the relevant procedure.

⁴ DataBase Administrator

4.3 Uninstalling a user interface

SAP Convergent Charging provides a set of user interfaces that are either automatically deployed by the SAPinst tool during the installation process, or manually deployed when necessary.

To uninstall a given user interface, execute the following procedure:

1. Open the procedure dedicated to the launching of the concerned user interface
2. Open the folder that contains the script used to launch the user interface
3. Remove the launch script from this folder to avoid any further use

5 Procedures

Related Information

- [Defining your landscape \[page 20\]](#)
- [Choosing System IDs \[page 21\]](#)
- [Downloading the Installation DVD \[page 22\]](#)
- [Downloading the JCE Jurisdiction Policy Files Archive \[page 25\]](#)
- [Downloading the SAP JVM \[page 26\]](#)
- [Downloading the SAPCAR Utility \[page 27\]](#)
- [Downloading the SAP Cryptographic Library \[page 27\]](#)
- [Downloading the Oracle JDBC driver \[page 28\]](#)
- [Checking free space \[page 29\]](#)
- [Creating required directories \[page 30\]](#)
- [Setting up the system encoding \[page 31\]](#)
- [Installing C Shell \[page 32\]](#)
- [Setting up the system time zone \[page 33\]](#)
- [Setting up the system environment variables \[page 35\]](#)
- [Preparing the Oracle Core Database \[page 36\]](#)
- [Preparing the SQL Server Core Database \[page 40\]](#)
- [Preparing the SAP ASE Core Database \[page 43\]](#)
- [Preparing the SAP HANA Core Database \[page 48\]](#)
- [Preparing the IBM DB2 Core Database \(w/o pureScale Feature\) \[page 50\]](#)
- [Installing a Core Server on a mono-host landscape \[page 54\]](#)
- [Installing a Core Server on a multi-hosts landscape \[page 61\]](#)
- [Testing a landscape basically \[page 67\]](#)
- [Setting up a new host for a landscape \[page 70\]](#)
- [Adding Core Server instances in a multi-hosts landscape \[page 70\]](#)
- [Starting and stopping the servers \[page 73\]](#)
- [Installing a BART Server in an existing landscape \[page 78\]](#)
- [Preparing the Oracle BART Database \[page 85\]](#)
- [Preparing the SQL Server BART Database \[page 87\]](#)
- [Preparing the SAP ASE BART Database \[page 90\]](#)
- [Preparing the SAP HANA BART Database \[page 94\]](#)
- [Preparing the IBM DB2 BART Database \(w/o pureScale Feature\) \[page 96\]](#)
- [Installing a Diameter Server in an existing landscape \[page 99\]](#)
- [Preparing the Oracle IEC Database \[page 103\]](#)
- [Preparing the SQL Server IEC Database \[page 105\]](#)

[Preparing the SAP HANA IEC Database \[page 107\]](#)
[Preparing the Oracle Session Database \[page 109\]](#)
[Installing an IEC \(Import Export Connector\) in an existing landscape \[page 112\]](#)
[Launching the SAPinst tool \[page 115\]](#)
[Launching Core Tool \[page 117\]](#)
[Launching BART Tool \[page 119\]](#)
[Launching CAT Tool \[page 122\]](#)
[Launching Cockpit \[page 125\]](#)
[Launching Admin+ \[page 130\]](#)
[Launching BART+ \[page 131\]](#)
[Launching Setup Tool \[page 133\]](#)
[Launching BART Setup Tool \[page 135\]](#)
[Launching Config Tool \[page 136\]](#)
[Securing a landscape \[page 138\]](#)
[Securing communications with the Core Server system \[page 142\]](#)
[Securing communications with the BART Server system \[page 155\]](#)
[Securing communications with the Diameter Server system \[page 162\]](#)
[Securing communications with Cockpit and Tomcat Server \[page 165\]](#)
[Installing a permanent license \[page 170\]](#)
[Removing system\(s\) or instance\(s\) from a given host \[page 171\]](#)
[Integrating SAP CC with CA APM \[page 172\]](#)
[Integrating SAP CC with SAP CTS+ \[page 175\]](#)
[Integrating SAP CC with SAP Convergent Invoicing \[page 178\]](#)
[Copying an SAP CC Core Server \[page 182\]](#)

5.1 Defining your landscape

Description

During the installation of your SAP Convergent Charging landscape, you will have to perform manual operations and checks on the different software components concerned by the installation. This procedure summarizes the information relating to the different hosts that make up this landscape, such as hostnames, IP addresses, Operating Systems, software components to install, individual and service users (and associated passwords), and so on.

Prerequisites

For more information about naming rules for SAP Servers, refer to [611361](#) 

Procedure

Fill the following table with the information related to your landscape:

Useful information (Friendly name, O.S, ...)	Hostname + IP address	Software Components	User + Password

5.2 Choosing System IDs

Description

The SAP System ID (or SID) corresponds to the identifier for an SAP system. This procedure provides you with information related to the selection of the SIDs of each SAP CC system you want to install on your landscape (Core Server, Core Server or Diameter Server).

Prerequisites

Before choosing your SIDs, please take into account the following rules:

- The SID must be unique throughout your organization and consistent throughout your system installation landscape. If you want to install an additional instance, make sure that no gateway instance with the same SID already exists in your SAP system landscape
- The SID must consist of **exactly** three alphanumeric characters
- Only uppercase letters are allowed
- The first character must be a letter (not a digit)
- The following SIDs are reserved and cannot be used:

ADD	ALL	AMD	AND	ANY	ASC	AUX	COM	CON
DBA	END	EPS	FOR	GID	IBM	INT	KEY	LOG
LPT	MON	NIX	NOT	NUL	OFF	OMS	PRN	RAW
ROW	SAP	SET	SGA	SHG	SID	SQL	SYS	TMP

Procedure

Caution

Choose your SID carefully. Renaming is complicated and requires that you re-install your system.

Write down in the following table the different SIDs you have chosen for your SAP CC systems:


Software Component	System ID
Core Server	
BART Server	
Diameter Server	

5.3 Downloading the Installation DVD

Description

The installation DVD of SAP Convergent Charging 5.0 contains all the SAP CC software components and units relating to a given Support Package (SP) and required for either an initial installation or an update of an existing SAP CC system. You normally obtain this installation DVD as part of the installation package provided by SAP SE. In case you did not receive this DVD, you can use this procedure to download it from SAP ONE Support Launchpad and possibly customize its content to fit your installation scenario.

Preliminary Notes

The installation DVD of SAP CC 5.0 is available as a multispanning archive made up with multiple files. For more information about multispanning archives, refer to [886535](#) 

Procedure

To download the SAP Convergent Charging 5.0 DVD, execute the following procedure:

1. Go to SAP ONE Support Launchpad at the following address: <https://launchpad.support.sap.com/>
2. Click the *Software Downloads* launch tile of the *System Operations and Maintenance* section
3. Expand the *By Alphabetical Index (A-Z)* section
4. Click the *C* letter
5. Click the *SAP Convergent Charging* element of the list
6. Click the *SAP Convergent Charging 5.0* element to open the information page dedicated to SAP CC5.0

Note

Previous versions of SAP CC are also available but this procedure only concerns the 5.0 release

7. Click the *Installation* link available in the upper part of the screen in order to open the *Downloads* section
8. Click on each element of the table to download it

Once downloaded, use the following procedure to unpack the multispanning archive and get the content of the installation DVD:

1. Double-click the `EXE` file, which corresponds to a self-extracting archive, and specify a destination folder for the extracted files
2. Click *Install* to unpack the content
3. Check that you get the following unpacked content in the specified destination folder:

DVD Directory	Content Description
/	The root directory corresponds to the SAP material number of the installation DVD. In addition to the directories listed afterwards, it contains the following files: <ul style="list-style-type: none"> ◦ CDLABEL.ASC ◦ CDLABEL.EBC ◦ COPY_TM.HTM ◦ COPY_TM.TXT ◦ LABEL.ASC ◦ LABEL.EBC ◦ LABELIDX.ASC ◦ MD5FILE.DAT ◦ MID.XML ◦ SHAFILE.DAT ◦ VERSION.ASC ◦ VERSION.EBC
/DATA_UNITS/	The DATA_UNITS directory contains a list of subdirectories that correspond to each data unit available in the installation DVD.
/DATA_UNITS/ CC50_<su>_CON- TENT_UC_OSIND	These directories corresponds to the different SAP CC systems that are available in the installation DVD. Available directories are: <ul style="list-style-type: none"> ◦ CC50_CORE_CONTENT_UC_OSIND for the Core Server ◦ CC50_BART_CONTENT_UC_OSIND for the BART Server ◦ CC50_DIAMETER_CONTENT_UC_OSIND for the Diameter Server

DVD Directory	Content Description
/DATA_UNITS/ CC50_IM_<os> and / DATA_UNITS/ INST_CC50_UC_<os>	<p>These directories contain the installation materials. Available directories are:</p> <ul style="list-style-type: none"> CC50_IM_<os> for the SAPinst tool INST_CC50_UC_<os> for the installation framework, that contains a version of the SAP JVM⁵ (available as a SAR⁶ file) <p>Where <os> corresponds to the supported operating systems, listed in the preliminary notes.</p>
/DATA_UNITS/ CC50_TOOLS_CON- TENT_UC_OSIND	This directory contains the different user interfaces and documentation of the development libraries provided with SAP CC 5.0, available as ZIP archive files.

Once unpacked, you can customize the installation DVD for optimization purpose. Use the following procedure to remove the non-relevant content and only keep the LABELIDX.ASC file plus the different directories that are necessary to install the relevant software components.

⚠ Caution

Be careful when removing the non-relevant content. In case you remove a content that is required for your landscape, you will have to unpack the installation DVD again to recover this content.

1. Remove all data units directories that do not refer to the operating systems of your landscape (except the operating system of the machine you are using for installation purpose)
2. Remove all data units directories that are not relevant for your landscape, according to the following table:

Data Unit	Core Server	BART Server	Diameter Server
CC50_CORE_CONTENT_UC_OSIND	Required	-	-
CC50_BART_CONTENT_UC_OSIND	-	Required	-
CC50_DIAMETER_CONTENT_UC_OSIND	-	-	Required
CC50_IM_<os>	Required	Required	Required
INST_CC50_UC_<os>	Required	Required	Required
CC50_TOOLS_CONTENT_UC_OSIND	Required	Required	-

3. Remove all **files** located in the root directory, except the LABELIDX.ASC file that must be kept. You now have a customized version of the SAP Convergent Charging 5.0 installation DVD, whose content can be copied or shared within your landscape.

⁵ Java Virtual Machine

⁶ SAP Archive

5.4 Downloading the JCE Jurisdiction Policy Files Archive

Description


As an application based on Java technologies, SAP Convergent Charging 5.0 works in conjunction with the SAP JVM⁷. The SAP JVM is not delivered with Java Cryptography Extension (JCE) Jurisdiction Policy files, which are required within secured landscapes and must thus be available for the SAPinst program. This procedure explains you how to get the adequate JCE Jurisdiction Policy files.

Preliminary Notes

For more information about JCE Jurisdiction Policy Files, refer to [1240081](#) 

Procedure

To download the JCE Jurisdiction Policy Files Archive, execute the following procedure:

1. Go to the Oracle website at the following address: <http://www.oracle.com> 
2. Click the *Downloads* menu
3. Click the *Java* icon
4. Click the *Java SE* link
5. Browse the page and click the *Download* button of the *Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files for JDK/JRE 8* element of the *Additional Resources* section
6. Select the *Accept License Agreement* radio button
7. Click the *jce_policy-8.zip* link to start the download
8. Save this file into the directory containing the customized version of the installation DVD


⁷ Java Virtual Machine

5.5 Downloading the SAP JVM

Description

SAP Convergent Charging 5.0 is a set of java-based applications that require the SAP JVM 8.1. A version of this SAP JVM is included within the installation DVD as a SAR file, but you can also download the latest available version if necessary.


Preliminary Notes

For more information about the SAP JVM installation prerequisites, refer to [1367498](#)

Procedure

If you want to get the SAP JVM from the installation DVD, take it from the following folder of the DVD: /
DATA_UNITS/INST_CC50_UC_<OS>⁸/DBINDEP

If you want to download the SAP JVM, execute the following procedure:

1. Go to SAP ONE Support Launchpad at the following address: <https://launchpad.support.sap.com>
2. Click the *Software Downloads* launch tile of the *System Operations and Maintenance* section
3. Search for the *SAP JVM 8.1* element
4. Click the *SAP JVM 8.1* category within the list of search results in order to open the *Downloads* section
5. Select your operating system
6. Browse the list of available SAP archives and click the one that corresponds to the highest patch level in order to download it

Once you retrieved the SAR file relating to the SAP JVM, you have to use the SAPCAR utility to uncompress it. For further information about the SAPCAR utility, refer to the [Downloading the SAPCAR Utility \[page 27\]](#) procedure. Then, execute the following procedure:

1. Copy the SAPCAR utility into the folder containing the SAP JVM SAR file you retrieved
2. Execute the following command into a command line prompt:

```
<SAPCAR_FILENAME> -xvf <SAR_FILENAME> -R ./SAPJVM
```

The newly created `SAPJVM` folder contains the uncompressed version of the SAP JVM.

⁸ Operating System

5.6 Downloading the SAPCAR Utility

Description


SAPCAR is a utility used by SAP to compress and/or uncompress SAP archive files (SAR: SAP Archive). You can use this procedure to download the latest available version of SAPCAR for your operating system.

Preliminary Notes

For more information about the SAPCAR utility, refer to [212876](#) 

Procedure

To download the SAPCAR utility, execute the following procedure:

1. Go to SAP ONE Support Launchpad at the following address: <https://launchpad.support.sap.com> 
2. Click the *Software Downloads* launch tile of the *System Operations and Maintenance* section
3. Click the *Support Packages and Patches* section
4. Expand the *By Alphabetical Index (A-Z)* section
5. Click the *S* letter
6. Click the *SAPCAR* element of the list
7. Select the highest available version of SAPCAR in order to open the *Downloads* section
8. Select your operating system
9. Click the element you want to download

Once downloaded, execute the downloaded EXE file to use the SAPCAR utility (setting appropriate execution rights when necessary) to compress or uncompress SAR files.

5.7 Downloading the SAP Cryptographic Library

Description

The SAP Cryptographic Library represents the security product provided by SAP for encryption with SAP Systems. In an SAP Convergent Charging landscape, this library is required in case of secured communications

performed using the RFC⁹ over TCP/IP¹⁰ communication channel. You can use this procedure to download the relevant version of the SAP Cryptographic Library for your operating system.

Preliminary Notes

You have identified the version of the SAP Cryptographic Library you want to use for securing communications performed using the RFC over TCP/IP communication channel.

Procedure

To download the SAP Cryptographic Library, execute the following procedure:

1. Go to SAP ONE Support Launchpad at the following address: <https://launchpad.support.sap.com>
2. Click the *Software Downloads* launch tile of the *System Operations and Maintenance* section
3. Click the *Support Packages and Patches* section
4. On the top of the screen, select the *Downloads* element of the list, and type **cryptolib** in the search field
5. Click the *Search* button
6. Select the relevant version of the library in order to open the *Downloads* section
7. Select your operating system
8. Click the element you want to download

Once downloaded, refer to [2471232](#) for further information about the installation of the SAP Cryptographic Library.

5.8 Downloading the Oracle JDBC driver

Description

According to your business requirements, your SAP Convergent Charging landscape can contain Oracle databases. This procedure explains you how to download the relevant JDBC¹¹ driver that is required at installation time.

⁹ Remote Function Call

¹⁰ Transmission Control Protocol / Internet Protocol

¹¹ Java Database Connectivity

Procedure

To download the Oracle JDBC driver, execute the following procedure:

1. Go to the Oracle website at the following address: <http://www.oracle.com>
2. Click the ► *Products* ► *Databases* ► *Application Development* ▾ menu
3. Click the *Java* icon of the *Database Languages and Tools* section
4. Browse the page and click the *JDBC Download* button
5. Click the *Oracle Database 12c Release 1 (12.1.0.2) drivers* link to access to the download list
6. Read the *Oracle Technology Network License Agreement* and Select the *Accept License Agreement* radio button if you agree with the terms and conditions
7. Click the *ojdbc6.jar* link
8. Sign-in to your Oracle account to start the download
9. Save this file

5.9 Checking free space

Description

Every host on which you install software components of SAP Convergent Charging must have enough free space, either for installation materials, or for running tasks (log files, temporary files, and so on). You can use this procedure to check if your hosts have enough free space.

Procedure

The following table contains the list of required free space that your host must have:

Elements	Required Space
Installation DVD	4.1 GB max.
SAPinst depot (*)	1 GB
SAP CC Core Server instances	1 GB per instance
SAP CC BART Server	1 GB
SAP CC Diameter Server	1 GB

(*) The SAPinst depot corresponds to a directory created and used by the SAPinst tool during the installation process to create temporary files. Each time you launch SAPinst, the following directories are automatically created:

- <DRIVE>:\Program Files\sapinst_instdir for *MS Windows* hosts
- /tmp/sapinst_instdir and /tmp/sapinst_exe* for *UNIX and Linux* hosts

i Note

Once the installation with SAPinst is completed, you can delete the content of the `SAPInst_exe*` directory to get free space. On the contrary, it is recommended to keep the `sapinst_instdir` directory because it contains log files related to the installation process, that can be useful in case an issue occurs during later installations.

5.10 Creating required directories

Description

Some directories must be created on each host on which you install software components of SAP Convergent Charging, either for installation materials, or for running tasks (such as data files generated during charging operations). You can use this procedure to create the following directories:

- `sapmnt`, which corresponds to the SAP Central Repository of each installed SAP CC system and contains the different programs and profiles related to the different software components to install. This directory must be created **on every Global Host** running on a Linux or UNIX operating system. If your landscape is a multi-hosts landscape, you must also share this directory so that the other hosts related to the same SAP CC system can access it
- `workingDirectory`, which corresponds to a directory used by the instances of the Core Server system to store data files resulting from business operations

Procedure Linux and UNIX operating systems

1. To create the SAP Central Repository and share it with the adequate permissions, execute the following commands as the root user **on the SAP Global Host** of your SAP CC system:

```
mkdir /sapmnt
/etc/init.d/nfs start
/sbin/chkconfig nfs on
chmod -R 766 /sapmnt
echo "/sapmnt *(rw, sync, no_root_squash)" >> /etc/exports
/usr/sbin/exportfs -ra
/etc/init.d/nfs restart
```

2. If your landscape is a multi-hosts landscape, you must mount the SAP Central Repository created on the SAP Global Host on every other host related to your SAP CC system. Execute the following procedure

(adapting the IP address of the SAP Global Host) as the root user **on every host different than the Global Host** of your SAP CC system in order to access the sapmnt directory:

```
mkdir /sapmnt
chmod 766 /sapmnt
echo "<IP_GLOBAL_HOST>:/sapmnt /sapmnt nfs defaults 0 0" >> /etc/fstab
mount /sapmnt
```

3. To create the SAP CC Working Directory on a host where you want to install instances of a Core Server system, execute the following commands as the root user **on each concerned host of your landscape**:

```
mkdir /workingDirectory
chmod 777 /workingDirectory
```

And in case you need to share the SAP CC Working Directory, execute the following additional commands:

```
echo "/workingDirectory *(rw, sync, no_root_squash)" >> /etc/exports
/usr/sbin/exportfs -ra
/etc/init.d/nfs restart
```

Procedure Microsoft Windows operating system

1. To create the SAP CC Working Directory on a host where you want to install instances of a Core Server system, execute the following command as a member of the Administrators group **on each concerned host of your landscape**:

```
mkdir C:\workingDirectory
```

And in case you need to share the SAP CC Working Directory, execute the following additional command:

```
net share workingDirectory=C:\workingDirectory /grant:Everyone, FULL
```

5.11 Setting up the system encoding

Description

To install a software component of SAP Convergent Charging on a *Linux or UNIX* host, SAPinst requires to use the UTF-8 encoding. Use this procedure to set the UTF-8 encoding on your *Linux or UNIX* hosts.

Preliminary Notes

MS Windows does not allow modifying the default encoding of the whole system. As a consequence, this procedure only concerns hosts running Linux operating systems.

Procedure

To set up the system encoding on a given *Linux or UNIX* host, execute the following procedure as the root user:

1. Edit the `/etc/sysconfig/i18n` file
2. Modify or create the `LANG` property with the `en_US.UTF-8` value
3. Save your modifications and exit your text editor. This encoding value will be available at next logon, and can be checked using the following command:

```
echo $LANG
```

5.12 Installing C Shell

Description

Every host running the SAPinst tool requires the presence of the C Shell command language interpreter. To ensure that C Shell is already installed on the host before running SAPinst, verify the existence of the `/bin/csh` script file. When not existing, use this procedure to install C Shell on your Linux host.

Preliminary Notes

- This procedure only concerns hosts running *Linux or UNIX* operating systems
- For further information about the Yum installer, refer to its [dedicated documentation](#) ➡
- For further information about the Zypper installer, refer to its [dedicated documentation](#) ➡

Procedure Linux and UNIX operating systems

To set up the system encoding on a given *Linux or UNIX* host, execute the following procedure as the root user:

1. Execute the following command to install the adequate packages:

- For Red Hat distributions:

```
yum install csh
```

- For SuSe distributions:

```
sudo zypper install csh
```

2. Check that the `/bin/csh` script file exists using the following command:

```
ls -al /bin/csh
```

5.13 Setting up the system time zone

Description

For both business and technical reasons, it is necessary to ensure that the *time zone* is correctly configured on each host containing software components of SAP Convergent Charging. Furthermore, in a multi-hosts landscape, this *time zone* must be similar for each host. Ideally, it is recommended to use a NTP¹² server to synchronize the clocks of your hosts. This procedure explains you how to set up the time zone of a given SAP CC host.

⚠ Caution

Do not modify the time zones of your hosts after the installation of SAP CC.

Procedure Linux and UNIX operating systems

To set up the *time zone* on a given *Linux or UNIX* host, execute the following procedure as the *root* user:

1. Execute the following command to open a graphical user interface dedicated to the management of time zones:

- For Red Hat distributions:

```
system-config-date (or system-config-time)
```

- For SuSe distributions:

```
yast timezone
```

- For AIX:

```
smit chtz
```

¹² Network Time Protocol

- For Solaris:

```
sysconfig configure
```

2. Select your *time zone* and validate the modification
3. Finally, test that your modification has been taken into account by executing the following command to display the current time of your system:

- For Red Hat distributions:

```
date
```

- For SuSe distributions:

```
date
```

- For AIX:

```
grep TZ /etc/environment
```

- For Solaris:

```
date
```

Procedure Microsoft Windows operating system

To set up the *time zone* on a given *MS Windows* host, use the *Date and Time* menu of the *Control Panel*, or execute the following procedure as a member of the *Administrators* group:

1. Execute the following command (or refer to *Microsoft MSDN online documentation*) to get the list of time zones supported by Microsoft:

```
tzutil /l
```

2. Execute the following command to modify the current time zone of your host, considering that `<TIME_ZONE>` corresponds to the name of the time zone:

```
tzutil /s <TIME_ZONE>
```

3. Finally, test that your modification has been taken into account by executing the following command to display the current time of your system:

```
tzutil /g
```

5.14 Setting up the system environment variables

Description

SAP Convergent Charging requires to set up some environment variables, either used by the SAPinst tool during the installation process, or used by some user interfaces. Use this procedure to set up the following environment variables for each host of your SAP CC landscape:

- `SAPCC_JAVA_HOME`, used by SAP CC GUIs¹³
- `SAP_IPv6_ACTIVE`, used for JCo¹⁴ communications
- `NI_USEIPv6`, used for communication with SAP MMC¹⁵

Procedure Linux and UNIX operating systems

The `SAP_IPv6_ACTIVE` and `NI_USEIPv6` environment variables only concern hosts that use *IPv6* addresses. To check whether your host uses *IPv4* or *IPv6* addresses, execute the following procedure:

1. Connect as the `root` user to the host, and execute the following command to display information about the network configuration of your host:

```
ifconfig
```

2. Locate the section dedicated to the Ethernet connection:
 - The `inet` string means that your host uses *IPv4* addresses
 - The `inet6` string means that your host uses *IPv6* addresses

To set up the environment variables, execute the following procedure as the `root` user:

1. Execute the following command to edit the configuration file containing the environment variables:

```
vi /etc/environment
```

2. Assuming that they do not already exist, add the following lines at the end of the file:
 - `SAPCC_JAVA_HOME=<SAP_JVM_PATH>`, where `<SAP_JVM_PATH>` corresponds to the path of the folder that contains the SAP JVM 8.1. This environment variable is only relevant if a GUI must be installed on this host
 - `NI_USEIPv6=1`, if this host uses *IPv6* addresses
 - `SAP_IPv6_ACTIVE=1`, if this host uses *IPv6* addresses
3. Save the file. These environment variables will be available when reconnecting to the host

¹³ Graphical User Interface

¹⁴ Java Connector

¹⁵ SAP Microsoft Management Console

Procedure Microsoft Windows operating system

The `SAP_IPv6_ACTIVE` and `NI_USEIPv6` environment variables only concern hosts that use *IPv6* addresses. To check whether your host uses *IPv4* or *IPv6* addresses, execute the following procedure:

1. Open a command line prompt and execute the following command to display information about the network configuration of your host:

```
ipconfig
```

2. Locate the section dedicated to the Ethernet connection. If an *IPv6* address is displayed, it means that your host uses *IPv6* addresses

To create the environment variables, use the *System* menu of the *Control Panel* and execute the following procedure:

1. Click on *Advanced system settings* to open the *System Properties* dialog
2. Select the *Advanced* tab, and click the *Environment Variables* button to open the dialog dedicated to the management of user and system variables
3. If a GUI must be installed on this host, click the *New* button of the *System variables* section in order to open the *New System Variable* dialog. If you are not granted adequate rights to create system variables, click the *New...* button of the *User variables for xxx* section in order to open the *New User Variable* dialog
4. Enter `SAPCC_JAVA_HOME` as the *variable name*, and specify the path of the folder that contains the SAP JVM 8.1 as the *value*
5. Click *OK* to create the new variable
6. If this host uses *IPv6* addresses, click again the *New...* button to open the *New System Variable* dialog. If you are not granted adequate rights to create system variables, click the *New...* button of the *User variables for xxx* section in order to open the *New User Variable* dialog
7. Enter `NI_USEIPv6` as the *variable name*, and `1` as the *value*
8. Click *OK* to create the new variable
9. If this host uses *IPv6* addresses, click again the *New...* button to open the *New System Variable* dialog. If you are not granted adequate rights to create system variables, click the *New...* button of the *User variables for xxx* section in order to open the *New User Variable* dialog
10. Enter `SAP_IPv6_ACTIVE` as the *variable name*, and `1` as the *value*
11. Click *OK* to create the new variable
12. Close the dialog windows

5.15 Preparing the Oracle Core Database

Description

According to your business requirements, your SAP Convergent Charging landscape can contain from 1 (the Core Database) to 4 databases (the Core Database, Session Database, BART Database and IEC Database).

This procedure explains you how to prepare your Core Database running under an Oracle RDBMS¹⁶ (Standard or Enterprise edition).

Preliminary Notes

- In a development landscape, you can install all the SAP CC databases on the same physical host, but using different schemas. Nevertheless, SAP SE highly recommends that you install the different databases on separated hosts, in order to ease administration tasks and improve performances
- For further information about the installation of Oracle, refer to the following pages available on SAP Community:
 - <http://scn.sap.com/community/oracle>
 - <http://scn.sap.com/docs/DOC-7888>

Prerequisites

An instance of an Oracle RDBMS must be installed and available in your landscape. This database instance must use the UTF-8 character encoding to work in conjunction with the different SAP CC software components, and the *Oracle SQL*plus* tool must be installed to execute this procedure. Refer to your system administrator to get information about these prerequisites relating to the SAP CC Core Database.

Procedure

The preparation of your SAP CC Core Database consists in the following operations:

- Setting up some initialization parameters
 - Creating a user account and granting the adequate roles and privileges to this user
 - Creating the different tablespaces
1. SAP Convergent Charging requires to modify some initialization parameters of the Oracle database, located in the `init.ora` file which contains the persistent parameters used during database startup. You can use the following procedure to:
 - Set the `_optim_peek_user_binds` parameter to `FALSE` in order to disable the bind peeking feature, which is not compatible with SAP CC
 - Increase the maximum number of processes and sessions by setting the `processes` and `sessions` parameters to 300 multiplied by the number of databases installed on this Oracle instance, i.e. 1 (as only the Core Database is installed on this instance)

To correctly set up the initialization parameters of your Core Database, execute the following commands:

```
sqlplus / as sysdba
alter system set "_optim_peek_user_binds"=false scope=spfile;
alter system set processes=300 scope=spfile;
alter system set sessions=300 scope=spfile;
```

¹⁶ Relational Database Management System

```
shutdown immediate
startup
```

- An Oracle user must be created and granted the adequate roles and privileges to administrate the Core Database. Execute the following commands by replacing <DB_USER> by the name of the Core Database administrator and <DB_PASSWORD> by its password:

```
sqlplus / as sysdba
define dbuser=<DB_USER>;
define dbpwd="<DB_PASSWORD>";
create user &dbuser identified by &dbpwd;
grant CONNECT, RESOURCE TO &dbuser;
grant EXECUTE_CATALOG_ROLE to &dbuser;
grant EXP_FULL_DATABASE, IMP_FULL_DATABASE to &dbuser;
grant CREATE_PROCEDURE to &dbuser;
grant CREATE_SESSION to &dbuser;
grant CREATE_TABLESPACE, DROP_TABLESPACE to &dbuser;
grant ALTER_TABLESPACE to &dbuser;
grant CREATE_ANY_DIRECTORY to &dbuser;
grant DROP_ANY_DIRECTORY to &dbuser;
grant EXECUTE ON dbms_lock TO &dbuser;
```

- The data storage of your SAP CC Core Database must be optimized by creating the following mandatory tablespaces, whose size depends on the edition of your RDBMS (Standard or Enterprise edition):

Tablespace name	Description	Minimal Size (MB)	
		SE	EE
CATALOG_DATA	Tables used to store the objects belonging to the catalog, and the operations audit.	180	180
CATALOG_DATA	Tables used to store the objects belonging to the catalog, and the operations audit.	180	180
CATALOG_INDX	Indexes used for the objects belonging to the catalog, and the operations audit	220	220
SUBSCRIBER_DATA	Tables containing objects belonging to provider contracts and subscriptions	100	20000
SUBSCRIBER_INDX	Indexes used for the objects belonging to provider contracts and subscriptions	200	20000
ACCESS_DATA	Tables used to store chronologies of mappings between technical identifiers and corresponding contract or subscription	10	1000
ACCESS_INDX	Indexes used for chronologies of mappings between technical identifiers and corresponding contract or subscription	20	250
PRERATING_DATA	Tables used to store prerating data	10	2000
PRERATING_INDX	Indexes used for prerating data	10	3000
COUNTER_DATA	Tables used to store the counters declared in subscriptions and provider contracts	20	1000
COUNTER_INDX	Indexes used for counters	10	10
C_SNAPSHOT_DATA	Tables used to store snapshots of counter values for subscriptions and provider contracts	20	1000
C_SNAPSHOT_INDX	Indexes used for snapshots of counter values	10	10

Tablespace name	Description	Minimal Size (MB)	
		SE	EE
SESSION_RATING_DATA	Tables used to store session-based charging events and charging session histories for failover purposes	1500	7000
SESSION_RATING_INDX	Indexes used for session-based charging events and charging session histories for failover purposes	500	500
OBJECT_CHANGE_DATA	Tables used to store data related to the object change log for audited operations	100	2000
OBJECT_CHANGE_INDX	Indexes used for object change log for audited operations	100	1000
ALLOWANCE_DATA	Tables used to store allowances	20	1500
ALLOWANCE_INDX	Indexes used for allowances	15	500
MONITORING_DATA	Tables used to store the objects used for monitoring purpose, such as data files metadata	10	1000
MONITORING_INDX	Indexes used for the objects used for monitoring purpose, such as data files metadata	5	500

To create the mandatory tablespaces, execute the following command by replacing:

- `<TABLESPACE_NAME>` by the name of the tablespace to create
- `<FILE_LOCATION>` by the full path of the file that will contain the tablespace, located in the `oradata` directory
- `<SIZE>` by the recommended value associated to the tablespace, listed in the above table and using the `AUTO_EXTEND` option

```
sqlplus / as sysdba
```

And then, for each tablespace listed in the above table:

```
CREATE BIGFILE TABLESPACE <TABLESPACE_NAME> DATAFILE '<FILE_LOCATION>' SIZE
<SIZE> AUTOEXTEND ON MAXSIZE UNLIMITED UNIFORM SIZE 1M LOGGING EXTENT
MANAGEMENT LOCAL SEGMENT SPACE MANAGEMENT AUTO;
```

Followed by this command **for Oracle 12c databases**:

```
ALTER USER <DB_USER> QUOTA UNLIMITED ON <TABLESPACE_NAME>;
```

❁ Example

For an Oracle 12c Standard Edition RDBMS installed on a Linux host, you can use the following statement:

- To create the "SUBSCRIBER_DATA" tablespace
- To give the "sapcc" user the possibility to access this tablespace

```
CREATE BIGFILE TABLESPACE SUBSCRIBER_DATA DATAFILE '/oradata/vol1/
SUBSCRIBER_DATA.dbf' SIZE 100M AUTOEXTEND ON MAXSIZE UNLIMITED UNIFORM
SIZE 1M LOGGING EXTENT MANAGEMENT LOCAL SEGMENT SPACE MANAGEMENT AUTO;
ALTER USER sapcc QUOTA UNLIMITED ON SUBSCRIBER_DATA;
```

5.16 Preparing the SQL Server Core Database

Description

According to your business requirements, your SAP Convergent Charging landscape can contain from 1 (the Core Database) to 4 databases (the Core Database, Session Database, BART Database and Import/Export Connector database). This procedure explains you how to prepare your Core Database running under a Microsoft SQL Server RDBMS¹⁷ (Standard or Enterprise edition).

Preliminary Notes

- In a development landscape, you can install all the SAP CC databases on the same physical host, but using different schemas. Nevertheless, SAP SE highly recommends that you install the different databases on separated hosts, in order to ease administration tasks and improve performances
- For further information about the installation of Microsoft SQL Server, refer to the following pages available on SAP Community:
 - <http://scn.sap.com/community/sqlserver>
 - <http://scn.sap.com/docs/DOC-8286>

Prerequisites

An instance of a SQL Server RDBMS must be installed and available in your landscape. The *SQL Server Management Studio* application must be installed to execute this procedure. Refer to your System Administrator to get information about these prerequisites relating to the SAP CC Core Database.

Procedure

The preparation of your SAP CC Core Database consists in the following operations:

- Creating a SQL Server user account and granting the adequate roles to this user on the adequate server
 - Creating the Core database with the user as the owner
 - Creating the different filegroups within this database
1. An SQL Server user must be created for your SAP CC Core Database, and granted the adequate roles and privileges. Execute the following procedure to create this SAP CC user:
 - Open the *SQL Server Management Studio* application

¹⁷ Relational Database Management System

- The *Connect to Server* dialog window opens. Use the following settings:
 - *Server Name*: Select *(local)*
 - *Authentication*: Select *Windows Authentication*, in order to use your operating system user
 - Click the *Connect* button
 - Open the **View** > *Object Explorer* menu to display the *Object Explorer* and expand the *(local)* server
 - Right-click the *Security* element of the tree and open the *New / Login...* menu to display the **Login** screen
 - Fill the *General* tab with the following information:
 - *Login name*: Fill with the name of the Core Database administrator
 - Select the *SQL Server authentication* option
 - *Password*: Fill with a password respecting the SAP password policy
 - *Confirm password*: Re-type the chosen password
 - *User must change password at next login*: Untick the checkbox
 - *Default database*: Select the *master* database
 - In the *Server Roles* tab, select the following roles:
 - *dbcreator*
 - *diskadmin*
 - *serveradmin*
 - Click the *OK* button
 - Right-click the *(local)* server and click *Disconnect*
2. Once the SQL Server user dedicated to the Core Database has been created, it is necessary to reconnect to the server using the previously created user in order to create the Core Database. Execute the following procedure:
- Open the **File** > *Connect Object Explorer...* menu or click the *Connect Object Explorer* button to re-open the *Connect to Server* dialog window. Use the following settings:
 - *Server Name*: Specify the full name of the machine hosting the database
 - *Authentication*: Select *SQL Server authentication*
 - *Login*: Fill with the previously created user
 - *Password*: Fill with the password of the previously created user
 - Click the *Connect* button
 - Right-click the *Databases* element of the tree and open the *New Database...* menu to display the **New Database** screen
 - Fill the *General* tab with the following information:
 - *Database name*: Fill with the name of the Core Database
 - *Owner*: Fill with the name of the previously created user
 - Fill the *Options* tab with the following information:
 - *Collation*: Collation defines the way strings are managed in SQL Server databases. The Core Database must be case-sensitive (CS) and compatible with ASCII Unicode (AS). Thus select the element that corresponds to the appropriate language, ending by the *CS_AS* string (e.g. *Latin1_General_CS_AS*)
 - *Recovery model*: Select *Full*
 - *Compatibility level*: Ensure that *SQL Server 2008 (100)* is selected
 - Click the *OK* button
3. The data storage of your SAP CC Core Database must then be optimized by creating the following mandatory filegroups:

Filegroup name	Description
CATALOG_DATA	Tables used to store the objects belonging to the catalog, and the operations audit.
CATALOG_DATA	Tables used to store the objects belonging to the catalog, and the operations audit.
CATALOG_INDX	Indexes used for the objects belonging to the catalog, and the operations audit
SUBSCRIBER_DATA	Tables containing objects belonging to provider contracts and subscriptions
SUBSCRIBER_INDX	Indexes used for the objects belonging to provider contracts and subscriptions
ACCESS_DATA	Tables used to store chronologies of mappings between technical identifiers and corresponding contract or subscription
ACCESS_INDX	Indexes used for chronologies of mappings between technical identifiers and corresponding contract or subscription
PRERATING_DATA	Tables used to store prerating data
PRERATING_INDX	Indexes used for prerating data
COUNTER_DATA	Tables used to store the counters declared in subscriptions and provider contracts
COUNTER_INDX	Indexes used for counters
C_SNAPSHOT_DATA	Tables used to store snapshots of counter values for subscriptions and provider contracts
C_SNAPSHOT_INDX	Indexes used for snapshots of counter values
SESSION_RATING_DATA	Tables used to store session-based charging events and charging session histories for failover purposes
SESSION_RATING_INDX	Indexes used for session-based charging events and charging session histories for failover purposes
OBJECT_CHANGE_DATA	Tables used to store data related to the object change log for audited operations
OBJECT_CHANGE_INDX	Indexes used for object change log for audited operations
ALLOWANCE_DATA	Tables used to store allowances
ALLOWANCE_INDX	Indexes used for allowances
MONITORING_DATA	Tables used to store the objects used for monitoring purpose, such as data files metadata
MONITORING_INDX	Indexes used for the objects used for monitoring purpose, such as data files metadata

To create the mandatory filegroups, execute the following procedure by replacing `<DATABASE_NAME>` by the name of the Core Database, `<FILEGROUP_NAME>` by the name of the filegroup to create, and `<FILE_LOCATION>` by the full path of the file that will contain the filegroup directory:

- Right-click your server and open the *New Query* menu
- For each filegroup listed in the above table, type the following query and execute it:

```
ALTER DATABASE "<DATABASE_NAME>" ADD FILEGROUP <FILEGROUP_NAME>;
ALTER DATABASE "<DATABASE_NAME>" ADD FILE
(
  NAME = <FILEGROUP_NAME>,
  FILENAME = '<FILE_LOCATION>',
  SIZE = 1MB,
  MAXSIZE = 1000MB,
  FILEGROWTH = 5MB
)
```

```
TO FILEGROUP <FILEGROUP_NAME>;
```

❖ Example

To create the "SUBSCRIBER_DATA" filegroup in the "SAP CC" Core Database of an SQL Server RDBMS, you can use the following query:

```
ALTER DATABASE "SAPCC" ADD FILEGROUP SUBSCRIBER_DATA;  
ALTER DATABASE "SAPCC" ADD FILE  
(  
  NAME = SUBSCRIBER_DATA,  
  FILENAME = 'c:\tmp\SUBSCRIBER_DATA.ndf',  
  SIZE = 1MB,  
  MAXSIZE = 1000MB,  
  FILEGROWTH = 5MB  
)  
TO FILEGROUP SUBSCRIBER_DATA;
```

5.17 Preparing the SAP ASE Core Database

Description

According to your business requirements, your SAP Convergent Charging landscape can contain from 1 (the Core Database) to 4 databases (the Core Database, Session Database, BART Database and Import/Export Connector database). This procedure explains you how to prepare your Core Database running under an SAP Adaptive Server Enterprise RDBMS¹⁸.

Preliminary Notes

- In a development landscape, you can install all the SAP CC databases on the same physical host, but using different schemas. Nevertheless, SAP SE highly recommends that you install the different databases on separated hosts, in order to ease administration tasks and improve performances
- For further information about the installation of SAP ASE, refer to the following pages:
 - <http://infocenter.sybase.com>
 - <http://scn.sap.com/community/developer-center/oltp-db>
 - <http://scn.sap.com/docs/DOC-34995>
 - <http://scn.sap.com/docs/DOC-34996>

¹⁸ Relational Database Management System

Prerequisites

An instance of an SAP ASE RDBMS must be installed and available in your landscape. This instance must be:

- Correctly licensed in order to fit specific needs such as data partitioning, communication securing, system high-availability, and so on
- Installed with the following configuration:
 - **Application Type:** Mixed (OLTP/DSS)
 - **Page Size:** 8k. Note that this value cannot be modified after the installation. The modification of the value leads to a warning message informing that the newly specified page size must be similar between databases used for import purposes
 - **Default Character Set:** utf-8 : Unicode 3.1 for UTF-8 Character Set
 - **Default Sort Order:** altdict : Alternate (lower-case first) dictionary ordering

In addition, the *Interactive SQL tool* must be installed to execute the different steps of this procedure. For further information about this tool, refer afterwards. To get information about these prerequisites relating to the SAP CC Core Database, refer to your System Administrator.

⚠ Caution

Free Developer Edition or Small Business Edition of SAP ASE are not supported by SAP CC. You must install a licensed copy of the Sybase Adaptive Enterprise Suite.

Using the Interactive SQL tool

Interactive SQL is a command-line tool provided by SAP ASE to execute SQL statements:

- Interactively, to execute individual commands
- In a batch mode, to execute script files that contain multiple commands

To use the interactive mode, you have to:

- Launch isql using the following synopsis, providing the username and password specified at installation time:

```
isql -U <USERNAME> -P <PASSWORD>
```

- Type the command to execute, followed by the "go" statement:

```
<command to execute>  
go
```

To use the batch mode, you have to:

- Create a text file containing the list of commands to execute, each command being followed by the "go" statement:

```
<command to execute>  
go  
<command to execute>  
go
```

and so on

- Launch isql using the following synopsis, providing the username and password specified at installation time, and specifying the previously created script file:

```
isql -U <username> -P <password> -i <script file>
```

i Note

- Whatever the execution mode is, you can use the `quit` command to exit the isql tool.
- For further information about the isql tool, refer to its [dedicated documentation](#).

Procedure

The preparation of your SAP CC Core Database consists in the following operations:

- Setting up some parameters of the SAP ASE Server
 - Creating the devices for data and logs, and the database relying on these devices
 - Setting up some database options
 - Creating a user account and granting the adequate roles and privileges to this user
 - Creating the different segments
1. Some parameters of the SAP ASE Server must be modified in order to fit specific needs of SAP Convergent Charging. Use the following list of commands to modify the configuration of the ASE Server accordingly:

```
use master
GO
sp_configure "number of open objects", 10000
GO
sp_configure "number of open indexes", 2000
GO
sp_configure "max network packet size", 16384
GO
sp_configure "default network packet size", 16384
GO
sp_configure "optimization goal", 0, 'allows_mix'
GO
sp_configure "disable varbinary truncation", 1
GO
sp_configure "number of user connections", 200
GO
sp_configure "number of locks", 1000000
GO
sp_configure "deadlock checking period", 800
GO
sp_configure "lock hashtable size", 16384
GO
sp_configure "row lock promotion HWM", 214748364
GO
sp_configure "row lock promotion LWM", 214748364
GO
sp_configure "SQL batch capture", 1
GO
sp_configure "kernel resource memory", 12000
GO
sp_configure "enable monitoring", 1
GO
sp_configure "sql text pipe active", 1
GO
sp_configure "sql text pipe max messages", 2000
```

```

GO
sp_configure "plan text pipe active", 1
GO
sp_configure "plan text pipe max messages", 2000
GO
sp_configure "statement pipe active", 1
GO
sp_configure "statement pipe max messages", 2000
GO
sp_configure "errorlog pipe active", 1
GO
sp_configure "errorlog pipe max messages", 2000
GO
sp_configure "deadlock pipe active", 1
GO
sp_configure "deadlock pipe max messages", 2000
GO
sp_configure "lock timeout pipe max messages", 2000
GO
sp_configure "lock timeout pipe active", 1
GO
sp_configure "wait event timing", 1
GO
sp_configure "process wait events", 1
GO
sp_configure "object lockwait timing", 1
GO
sp_configure "statement statistics active", 1
GO
sp_configure "per object statistics active", 1
GO
sp_configure "max SQL text monitored", 512
GO
sp_configure "enable stmt cache monitoring", 1
GO
sp_configure "aux scan descriptors", 1000
GO
sp_configure "select for update", 1
GO

```

If you use the database partitioning function for your database, execute the following commands:

```

sp_configure "enable semantic partitioning", 1
GO
sp_configure "number of open partitions", 100000
GO

```

If you use secured communications with your database, execute the following command:

```

sp_configure "enable SSL", 1
GO

```

2. To create the devices for data and logs, and then the database that relies on these devices, use the following list of commands considering that:
 - `<DB_NAME>` corresponds to the name of your database
 - `<DEVICE_PATH>` corresponds to the path of the device
 - `<DEVICE_SIZE>` corresponds to the amount of space to allocate to the device, made up with a quantity followed by one of these supported unit specifiers:
 - k or K (kilobytes)
 - m or M (megabytes)
 - g or G (gigabytes)

- o t or T (terabytes)

```
disk init name="<DB_NAME>_data", physname="<DEVICE_PATH>\<DB_NAME>_data",
size=<DEVICE_SIZE>, dsync = true
GO
disk init name="<DB_NAME>_log", physname="<DEVICE_PATH>\<DB_NAME>_log",
size=<DEVICE_SIZE>, dsync = true
GO
create database <DB_NAME> on <DB_NAME>_data=2000000 log on
<DB_NAME>_log=2000000
GO
```

3. Some options of the previously created database must be modified. Use the following list of commands, considering that <DB_NAME> corresponds to the name of your database:

```
sp_dboption <DB_NAME>,"ddl in tran", true
GO
sp_dboption <DB_NAME>, "select into", true
GO
```

4. A dedicated user must be created to administrate the Core Database, and must be declared as the owner of the Core Database. Use the following list of commands considering that:
 - o <DB_USER> corresponds to the name of the Core Database administrator
 - o <DB_PASSWORD> corresponds to the password of the Core Database administrator, that respects the SAP password policy
 - o <DB_NAME> corresponds to the name of the Core Database

```
create login <DB_USER> with password <DB_PASSWORD>
GO
use <DB_NAME>
GO
sp_changedbowner <DB_USER>
GO
```

5. To optimize the storage of your data, you need to create mandatory segments within your database. Use the following list of commands, considering that <DB_NAME> corresponds to the name of your Core Database:

```
use <DB_NAME>
GO
sp_addsegment 'ACCESS_DATA', '<DB_NAME>', '<DB_NAME>_data'
GO
sp_addsegment 'ACCESS_INDX', '<DB_NAME>', '<DB_NAME>_data'
GO
sp_addsegment 'ALLOWANCE_DATA', '<DB_NAME>', '<DB_NAME>_data'
GO
sp_addsegment 'ALLOWANCE_INDX', '<DB_NAME>', '<DB_NAME>_data'
GO
sp_addsegment 'C_SNAPSHOT_DATA', '<DB_NAME>', '<DB_NAME>_data'
GO
sp_addsegment 'C_SNAPSHOT_INDX', '<DB_NAME>', '<DB_NAME>_data'
GO
sp_addsegment 'CATALOG_DATA', '<DB_NAME>', '<DB_NAME>_data'
GO
sp_addsegment 'CATALOG_INDX', '<DB_NAME>', '<DB_NAME>_data'
GO
sp_addsegment 'COUNTER_DATA', '<DB_NAME>', '<DB_NAME>_data'
GO
sp_addsegment 'COUNTER_INDX', '<DB_NAME>', '<DB_NAME>_data'
GO
sp_addsegment 'OBJECT_CHANGE_DATA', '<DB_NAME>', '<DB_NAME>_data'
GO
sp_addsegment 'OBJECT_CHANGE_INDX', '<DB_NAME>', '<DB_NAME>_data'
```

```

GO
sp_addsegment 'PRERATING_DATA', '<DB_NAME>', '<DB_NAME>_data'
GO
sp_addsegment 'PRERATING_INDX', '<DB_NAME>', '<DB_NAME>_data'
GO
sp_addsegment 'SESSION_RATING_DATA', '<DB_NAME>', '<DB_NAME>_data'
GO
sp_addsegment 'SESSION_RATING_INDX', '<DB_NAME>', '<DB_NAME>_data'
GO
sp_addsegment 'SUBSCRIBER_DATA', '<DB_NAME>', '<DB_NAME>_data'
GO
sp_addsegment 'SUBSCRIBER_INDX', '<DB_NAME>', '<DB_NAME>_data'
GO
sp_addsegment 'MONITORING_DATA', '<DB_NAME>', '<DB_NAME>_data'
GO
sp_addsegment 'MONITORING_INDX', '<DB_NAME>', '<DB_NAME>_data'
GO

```

5.18 Preparing the SAP HANA Core Database

Description

According to your business requirements, your SAP Convergent Charging landscape can contain from 1 (the Core Database) to 4 databases (the Core Database, the Session Database, the BART Database and the IEC Database). This procedure explains you how to prepare your Core Database running under an SAP HANA in-memory database system using a single container or a multiple containers mode.

Preliminary Notes

- In a development landscape, you can install all the SAP CC databases on the same physical host, but using different schemas. Nevertheless, SAP SE highly recommends that you install the different databases on separated hosts, in order to ease administration tasks and improve performances
- For further information about the installation of SAP HANA, refer to the following pages available on SAP Community:
 - <http://scn.sap.com/community/developer-center/hana>
 - <http://scn.sap.com/docs/DOC-53955>

For further information about data types, operators, functions, statements, and so on, refer to the SAP HANA SQL and System Views Reference documentation available on SAP Help Portal:<http://help.sap.com>.

Prerequisites

An SAP HANA database system must be installed and available in your landscape. The *SAP HANA Studio* application must be installed to execute this procedure. Refer to your System Administrator to get information about these prerequisites relating to the SAP CC Core Database.

Procedure

The preparation of your SAP CC Core Database consists in the following operations:

- Declaring your system within the SAP HANA Administration Console of the *SAP HANA Studio* application
 - Creating a user account and granting the adequate roles and privileges to this user on this system
 - Disabling the expiration of the user's password
1. An SAP HANA system must be created to administrate your SAP CC Core Database. Execute the following procedure to create this system:
 - Open the *SAP HANA Studio* application
 - Open the **▶ Window ▶ Perspective ▶ Open Perspective ▶ SAP HANA Administration Console ▶** menu to display the perspective dedicated to the management of SAP HANA systems
 - Open the **▶ Window ▶ Show View ▶ Systems ▶** menu to display the view containing the list of SAP HANA systems
 - Click the *Add System* icon to open the *System* dialog window
 - Use the following settings to fill the *Specify System* screen:
 - *Host Name*: Fill with the master host name
 - *Instance Number*: Fill with the instance number of your SAP HANA system
 - *Mode*: Select *Single Container* or *Multiple containers*, according to your needs
 - *Description*: Fill with a text that describes your system
 - Click the *Next* button
 - The *Connection Properties* screen opens. Select the *Authentication by database user* option and use the following settings:
 - *User Name*: Fill with the name of the SAP HANA system administrator
 - *Password*: Fill with a password respecting the SAP password policy
 - Click the *Finish* button to log on the newly declared SAP HANA system
 2. Once you are connected to the relevant SAP HANA system, it is necessary to create a user account and grant the adequate roles and privileges to this user in order to administrate the Core Database. Execute the following procedure to create this user:
 - Expand the *Security* folder, and right-click the *Users* element to display the context menu corresponds to the name of your database
 - Right-click the *Users* element of the tree and open the *New User* menu to display the screen dedicated to the creation of new users
 - Fill the *User* tab with the following information:
 - *User Name*: Fill with the name of the Core Database administrator
 - Select the *Password* option in the *Authentication* fieldset
 - *Password*: Fill with a password respecting the SAP password policy
 - *Confirm password*: Re-type the chosen password

- In the *Granted Roles* subtab, click the + button to add the following roles to the user:
 - *CONTENT_ADMIN*
 - *MODELING*
 - In the *System Privileges* subtab, click the + button to add the following privileges to the user:
 - *EXPORT*
 - *IMPORT*
 - Click the *Deploy* button to finalize the creation of the user
3. Once the user has been created and deployed on your SAP HANA system, it is necessary to disable the expiration of its password. Execute the following procedure:
- Right-click the previously created SAP HANA system and open the *Open SQL Console* menu to display the screen dedicated to the execution of SQL statements
 - Type the following SQL statement within the editor, considering that `<USERNAME>` corresponds to the name of your previously created user. For further information, refer to the documentation of the `ALTER USER` command available in the SAP HANA documentation:

```
ALTER USER <USERNAME> DISABLE PASSWORD LIFETIME;
```


- Click the *Execute* button to execute the SQL statement

5.19 Preparing the IBM DB2 Core Database (w/o pureScale Feature)

Description

According to your business requirements, your SAP Convergent Charging landscape can contain from 1 (the Core Database) to 4 databases (the Core Database, Session Database, BART Database and Import/Export Connector database). This procedure explains you how to prepare your Core Database running under an IBM DB2 RDBMS¹⁹ without the pureScale feature.

Preliminary Notes

- In a development landscape, you can install all the SAP CC databases on the same physical host, but using different schemas. Nevertheless, SAP SE highly recommends that you install the different databases on separated hosts, in order to ease administration tasks and improve performances
- For further information about the installation of IBM DB2, refer to the following pages available on SAP Community:
 - <http://scn.sap.com/community/db2-for-linux-unix-windows>

¹⁹ Relational Database Management System

- <http://scn.sap.com/docs/DOC-8211>
- This procedure uses the following variables:
 - <DB_GROUP>, which corresponds to the name of the group containing the DB2 administrators, specified at DB2 installation time
 - <DB_NAME>, which corresponds to the name of the Core Database
 - <DB_USER>, which corresponds to the name of the Core Database administrator, which corresponds to a user granted adequate roles and privileges
 - <DB_PASSWORD,> which corresponds to the password of the Core Database administrator, respecting the SAP password policy but without any expiration date
 - <TABLESPACE_NAME>, which corresponds to the name of the tablespace to create
 - <FILE_LOCATION>, which corresponds to the full path of the directory that will contain the tablespaces

Prerequisites

An instance of an IBM DB2 database must be installed and available in your landscape. The *IBM DB2 db2cmd tool* must be installed to execute this procedure. Refer to your Application and System Administrators to get information about these prerequisites relating to the SAP CC Core Database.

Procedure

The preparation of your SAP CC Core Database consists in the following operations:

- Creating a user account and adding this user to the relevant group
 - Creating the Core Database and setting up some configuration parameters
 - Granting the newly created user the adequate roles and privileges
 - Creating a user account and granting the adequate roles and privileges to this user
 - Creating the different tablespaces within this database
1. SAP Convergent Charging requires to create a dedicated user for your SAP CC Core Database, and add this user to the group containing the DB2 administrators. Execute the following procedure:
 - For a Microsoft Windows operating system, execute the following commands into a command line prompt:


```
net user <DB_USER> "<DB_PASSWORD>" /ADD /PASSWORDCHG:NO /EXPIRES:never
```

```
wmic UserAccount where Name="<DB_USER>" set PasswordExpires=False
```

```
net localgroup <DB_GROUP> <DB_USER> /add
```
 - For Linux and UNIX operating systems, execute the following command:


```
cat /etc/group | grep -i <DB_GROUP> | cut -d':' -f3
```
 2. SAP Convergent Charging requires to modify some configuration parameters when creating the DB2 database. You can use the following procedure to:

- Create the database
- Set the default page size of the database to 16K
- Specify an amount of storage for recovery log files by pre-allocating a number of 50 primary log files
- Set the amount of the database heap memory to use as a buffer for recording logs before writing these records to disk to 1024 4KB pages
- Set the size of each primary and secondary log file to 16K 4KB pages. This size limits the number of records that can be written in these files before they become full and require the creation of new ones
- Specify the percentage of changed pages at which the asynchronous page cleaners will be started (if they are not currently active)
- Activate the dynamically distribution of the available memory resources between the memory consumers
- Activate the automatic sampling rate determination, based on table size
- Set the default prefetch size of tablespaces to 960 pages
- Set an automatic percentage for the lock list held by an application that must be filled before performing lock escalation
- Set an automatic amount of 4K pages to store the lock list

To create the SAP CC Core Database, execute the following procedure:

```
db2cmd
db2
create database <DB_NAME> pagesize 16384
update database configuration for <DB_NAME> using LOGPRIMARY 50
update database configuration for <DB_NAME> using DECFLT_ROUNDING
ROUND_CEILING
update database configuration for <DB_NAME> using LOGBUFSZ 1024
update database configuration for <DB_NAME> using LOGFILSIZ 16384
update database configuration for <DB_NAME> using CHNGPGS_THRES 40
update database configuration for <DB_NAME> using SELF_TUNING_MEM ON
update database configuration for <DB_NAME> using AUTO_SAMPLING ON
update database configuration for <DB_NAME> using DFT_PREFETCH_SZ 960
update database configuration for <DB_NAME> using MAXLOCKS AUTOMATIC
update database configuration for <DB_NAME> using LOCKLIST AUTOMATIC
db2set DB2_COMPATIBILITY_VECTOR=MYS
```

3. The user created in Step1 must then be granted the adequate roles and privileges on the SAP CC Core Database. Execute the following procedure:

```
db2cmd
db2
connect to <DB_NAME>
grant dbadm on database to <DB_USER>
connect reset
```

4. The data storage of your SAP CC Core Database must then be optimized by creating the following mandatory tablespaces:

Tablespace name	Description
CATALOG_DATA	Tables used to store the objects belonging to the catalog, and the operations audit
CATALOG_INDX	Indexes used for the objects belonging to the catalog, and the operations audit
SUBSCRIBER_DATA	Tables containing objects belonging to provider contracts and subscriptions
SUBSCRIBER_INDX	Indexes used for the objects belonging to provider contracts and subscriptions

Tablespace name	Description
ACCESS_DATA	Tables used to store chronologies of mappings between technical identifiers and corresponding contract or subscription
ACCESS_INDX	Indexes used for chronologies of mappings between technical identifiers and corresponding contract or subscription
PRERATING_DATA	Tables used to store prerating data
PRERATING_INDX	Indexes used for prerating data
COUNTER_DATA	Tables used to store the counters declared in subscriptions and provider contracts
COUNTER_INDX	Indexes used for counters
C_SNAPSHOT_DATA	Tables used to store snapshots of counter values for subscriptions and provider contracts.
C_SNAPSHOT_INDX	Indexes used for snapshots of counter values.
SESSION_DATA	Tables used to store session-based charging events and charging session histories for failover purposes
SESSION_INDX	Indexes used for session-based charging events and charging session histories for failover purposes
OBJECT_CHANGE_DATA	Tables used to store data related to the object change log for audited operations
OBJECT_CHANGE_INDX	Indexes used for object change log for audited operations
ALLOWANCE_DATA	Tables used to store allowances
ALLOWANCE_INDX	Indexes used for allowances
MONITORING_DATA	Tables used to store the objects used for monitoring purpose, such as data files metadata
MONITORING_INDX	Indexes used for the objects used for monitoring purpose, such as data files metadata

To create the mandatory tablespaces, execute the following procedure:

```
db2cmd
db2
connect to <DB_NAME>
```

And then, for each tablespace listed in the above table:

```
create tablespace <TABLESPACE_NAME> MANAGED BY DATABASE USING (file
'<FILE_LOCATION><TABLESPACE_NAME>' 256000) EXTENTSIZE 2 DROPPED TABLE
RECOVERY OFF AUTORESIZE YES
```

❖ Example

For an IBM DB2 RDBMS installed on a Microsoft Windows host, you can use the following statement to create the CATALOG_DATA tablespace:

```
create tablespace CATALOG_DATA MANAGED BY DATABASE USING (file 'C:
\DB2\tablespaces\CATALOG_DATA' 256000) EXTENTSIZE 2 DROPPED TABLE RECOVERY
OFF AUTORESIZE YES
```

5.20 Installing a Core Server on a mono-host landscape

Description

The installation of a Core Server system on a mono-host landscape is performed using the SAPinst tool. This procedure explains you how to configure the different steps of the installation scenario handled by SAPinst in order to install:

- A stand-alone landscape that is not integrated with any third-party system
- A landscape that is integrated with the SAP Convergent Invoicing system

Preliminary Notes

For more information about license keys, refer to SAP Notes [197623](#) and [94998](#).

Prerequisites

- The Installation DVD of SAP Convergent Charging 5.0 must be downloaded and available on the host. Refer to the [Downloading the Installation DVD \[page 22\]](#) procedure if necessary
- On Linux and UNIX hosts, a shell script must be installed and available. Refer to the [Installing C Shell \[page 32\]](#) procedure if necessary
- On Microsoft Windows hosts, the “Microsoft Visual C++ 2013 runtime” libraries must be installed and available. For further information, refer to SAP Note [2676219](#).
- A SID²⁰ must be chosen for the Core Server system. Refer to the [Choosing System IDs \[page 21\]](#) procedure if necessary
- The JCE Jurisdiction Policy Files archive must be downloaded and available on the host. Refer to the [Downloading the JCE Jurisdiction Policy Files Archive \[page 25\]](#) procedure if necessary
- The SAP CC Working Directory must be created on the host. Refer to the [Creating required directories \[page 30\]](#) procedure if necessary
- A database must be prepared and available. Depending of your landscape, refer if necessary to one of the following procedures:
 - [Preparing the Oracle Core Database \[page 36\]](#)
 - [Preparing the SQL Server Core Database \[page 40\]](#)
 - [Preparing the SAP ASE Core Database \[page 43\]](#)
 - [Preparing the SAP HANA Core Database \[page 48\]](#)
 - [Preparing the IBM DB2 Core Database \(w/o pureScale Feature\) \[page 50\]](#)

²⁰ SAP System Identifier

- If your Core Database is running under an Oracle RDBMS²¹, the dedicated JDBC²² driver must be downloaded and available on the host. Refer to the [Downloading the Oracle JDBC driver \[page 28\]](#) procedure if necessary

Procedure


As this procedure relies on the SAPinst tool, you first need to launch it using the [Launching the SAPinst tool \[page 115\]](#) dedicated procedure.

Once opened, the SAPinst tool displays a succession of screens that give you the possibility to configure your installation scenario. Use the following recommendations to fill the different screens:

1. **Welcome to SAP Convergent Charging** screen
 - Click ► *SAP Convergent Charging* ► *Install* ► *Standard System Installation* ► *Core Server - First Steps* ►
 - Click the *Next* button
2. **Parameter Settings** screen
 - *Parameter Mode*: Select *Custom*
 - Click the *Next* button
 - You will be prompted to log off in order to let SAPinst grant you the authorizations that are required to perform the installation. Click the *OK* button to log off, and reconnect to the host. SAPinst automatically restarts to continue the installation from there
3. **General SAP System Parameters** screen
 - *SAP System ID (SAPSID)*: Fill with the chosen SID
 - Click the *Next* button
4. **Master Password** screen
 - *Password for All Users*: Fill with a password respecting the SAP password policy
 - *Confirm*: Re-type the chosen password
 - Click the *Next* button
5. **Windows Domain** screen
 - *Domain Model*: Select *Local Domain*
 - Click the *Next* button
6. **Operating System Users** screen
 - *Password of SAP System Administrator*: Filled by default with the password you specified in the **Master Password** screen, you can specify a different password
 - *Confirm*: Re-type the chosen password
 - *Password of SAP Service User*: Filled by default with the password you specified in the **Master Password** screen, you can specify a different password
 - *Confirm*: Re-type the chosen password
 - Click the *Next* button
7. **Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files** screen
 - *JCE Unlimited Strength Jurisdiction Policy Files*: Click the *Browse* button and select the ZIP archive you downloaded using the [dedicated procedure \[page 25\]](#)

²¹ Relational Database Management System

²² Java Database Connectivity

- Click the *Next* button
- 8. **SAP Convergent Charging Host License** screen
 - Tick the *Generate a temporary license* checkbox
 - Click the *Next* button
- 9. **Database Type** screen
 - *Database Type*: Select the adequate RDBMS
 - Click the *Next* button
- 10. **SAP HANA, Sybase ASE, Oracle, Oracle RAC, MS SQL Server, DB2, or DB2 pureScale** screen
 - **SAP HANA** screen
(*Database Connection*)
 - *Primary Host*: Fill with the IP address of the machine hosting the primary node
 - *Secondary Host*: Fill with the IP address of the machine hosting the secondary node
 - *User*: Fill with the name of the Core Database administrator you specified during the preparation of your Core Database
 - *Password*: Fill with the password of the Core Database administrator you specified during the preparation of your Core Database
 - *Mode*: Select the mode that corresponds to the installation scenario of your SAP HANA database
 - *Single Container Mode*
 - *Port*: Fill with the relevant port of the system database of your SAP HANA system. For further information about the default ports of SAP products, refer to the dedicated section on SAP Help Portal: <https://help.sap.com/viewer/ports>
 - *Multiple Containers Mode*
 - *Tenant Name*: Fill with the name of the tenant database to connect to
 - *Port*: Fill with the relevant port of the tenant database of your SAP HANA system you want to connect to. Typical assignment rule for port number are:
 - 3<INSTANCE_NUMBER>15 for a single-container system
 - Between 3<INSTANCE_NUMBER>41 and 3<INSTANCE_NUMBER>98 for a multitenant system
 For further information about the value of such port, refer to the SAP Note [2365930](https://help.sap.com/viewer/ports)  or to the section dedicated to the default ports on SAP Help Portal: <https://help.sap.com/viewer/ports>
 - **Sybase ASE** screen
(*Primary Database Connection*)
 - *Host*: Fill with the IP address of the machine hosting the database
 - *Port*: Fill with the port specified during the installation of the database
 - *Name*: Fill with the unique name of the database instance within which the content of the Core Database will be installed
 - *User*: Fill with the name of the Core Database administrator you specified during the preparation of your Core Database
 - *Password*: Fill with the password of the Core Database administrator you specified during the preparation of your Core Database
 - *Use Partitioning*: Tick the checkbox if your RDBMS supports the partitioning feature. Refer to your database administrator if necessary
 - (*Backup Database Connection*)
Tick the *Use backup database connection* checkbox if you want to use a backup database pour high availability purpose. If you tick this checkbox, specify the following information:

- *Host*: Fill with the IP address of the machine hosting the backup database
- *Port*: Fill with the port used to connect to the backup database
- **Oracle** screen
(*JDBC Driver*)
 - *JDBC Driver JAR Archive*: Click the *Browse* button and select the JAR archive you downloaded using the [dedicated procedure \[page 28\]](#)
 (*Database Authentication*)
 - *Host*: Fill with the IP address of the machine hosting the database
 - *Port*: Fill with the port specified during the installation of the database
 - *Instance Id*: Fill with the unique name of the database instance within which the content of the Core Database will be installed

i Note

For an Oracle database, you can use the following command to fill the *Instance Id* field:

```
sqlplus / as sysdba
SELECT sys_context('USERENV', 'DB_NAME') FROM DUAL;
```

- *User*: Fill with the name of the Core Database administrator you specified during the preparation of your Core Database
- *Password*: Fill with the password of the Core Database administrator you specified during the preparation of your Core Database
- *Use Partitioning*: Tick the checkbox if your RDBMS supports the partitioning feature. Refer to your database administrator if necessary
- **Oracle RAC** screen
(*JDBC Driver*)
 - *JDBC Driver JAR Archive*: Click the *Browse* button and select the JAR archive you downloaded using the [dedicated procedure \[page 28\]](#)
 (*Database Authentication*)
 - *User*: Fill with the name of the Core Database administrator you specified during the preparation of your Core Database
 - *Password*: Fill with the password of the Core Database administrator you specified during the preparation of your Core Database
 (*Database Instances*)

Click the *Add* button to add instances according to your needs, each instance containing the following information:

 - *Host*: Fill with the IP address of the machine hosting the database instance
 - *Port*: Fill with the port specified during the installation of the database instance
 - *Instance Id*: Fill with the unique name of the database instance
- **MS SQL Server** screen
(*Database Connection*)
 - *Host*: Fill with the IP address of the machine hosting the database
 - *Port*: Fill with the port specified during the installation of the database
 - *Name*: Fill with the unique name of the database instance within which the content of the Core Database will be installed
 - *User*: Fill with the name of the Core Database administrator you specified during the preparation of your Core Database

- *Password*: Fill with the password of the Core Database administrator you specified during the preparation of your Core Database
- *Use Partitioning*: Tick the checkbox if your RDBMS supports the partitioning feature. Refer to your database administrator if necessary
- **DB2** screen
(*Database Connection*)
 - *Host*: Fill with the IP address of the machine hosting the database
 - *Port*: Fill with the port specified during the installation of the database
 - *Database Name*: Fill with the unique name of the database instance within which the content of the Core Database will be installed
 - *Schema Name*: Fill with the name of the database schema you want to create within the Core Database
 - *User*: Fill with the name of the Core Database administrator you specified during the preparation of your Core Database
 - *Password*: Fill with the password of the Core Database administrator you specified during the preparation of your Core Database
 - *Use Partitioning*: Tick the checkbox if your RDBMS supports the partitioning feature. Refer to your database administrator if necessary
- **DB2 pureScale** screen
(*Database Parameters*)
 - *Database Name*: Fill with the unique name of the database instance within which the content of the Core Database will be installed
 - *Schema Name*: Fill with the name of the database schema you want to create within the Core Database
 - *User*: Fill with the name of the Core Database administrator you specified during the preparation of your Core Database
 - *Password*: Fill with the password of the Core Database administrator you specified during the preparation of your Core Database
 (*Database Instances*)
 Click the *Add* button to add instances according to your needs, each instance containing the following information:
 - *Host*: Fill with the IP address of the machine hosting the database instance
 - *Port*: Fill with the port specified during the installation of the database instance
 - Click the *Next* button
- 11. **Tablespaces / Filegroups / Segments** screen
 - Ensure that each table or index is associated to the correct filegroup, tablespace or segment created during the preparation of your Core Database. When necessary, modify the associations accordingly
 - Click the *Next* button
- 12. **SAP Convergent Charging Working Directory** screen
 - *Working Directory*: Click the *Browse* button and select the directory you specified during the [creation of the required directories \[page 30\]](#)
 - Click the *Next* button
- 13. **CA Introscope Java Agent** screen
 - *Use monitoring with CA Introscope*: Untick the checkbox
 - Click the *Next* button
- 14. **System Landscape Directory** screen
 - *Configure System Landscape Directory*: Untick the checkbox

- Click the *Next* button
- 15. **SAP Convergent Charging Security** screen
 - *Security*: Select the *Disabled* option
 - Click the *Next* button
- 16. **SAP Convergent Charging Administrator User** screen
 - *Password*: Fill with a password respecting the SAP password policy
 - *Confirm*: Re-type the chosen password
 - Click the *Next* button
- 17. **SAP Convergent Charging Tax** screen
 - Only tick the *VAT* taxation framework
 - Click the *Next* button
- 18. **SAP Convergent Charging Integration Scenario** screen
 - *Scenario*: Select the scenario that corresponds to your landscape:
 - If you select the *Stand-alone* integration scenario, no dedicated intermediate screen needs to be filled
 - If you select the *Billing and Invoicing in SAP Convergent Invoicing* or *Billing, Invoicing, and Storage of Consumption Data in SAP Convergent Invoicing* integration scenario, use the following recommendations to fill these dedicated intermediate screens:
 - **JCo Connection Configuration** screen
 - Click the *Add* button to add the adequate JCo destination(s)
 - *Name*: Fill with the name of the JCo destination
 - *SAP Application*: Select the relevant type of targeted SAP Application
 - *Application Server Host*: Specify the full name of the machine hosting the SAP Application
 - *SAP System Number*: Specify the relevant SAP system number
 - *SAP Client*: Specify the relevant SAP client number
 - *Logon User*: Specify the name of the SAP user you want to use for connecting to the SAP Application
 - *Logon Password*: Specify the password of the previously specified user
 - *Install SAP Cryptographic Library*: Untick the checkbox
 - Click the *Next* button
 - **Customer Management Area and ERP Reference System** screen
 - *Default Customer Management Area*: Specify a name for the default CMA
 - *JCo Destination for ERP*: Select the JCo destination to use for the default CMA
 - *JCo Destination for CRM*: Select the JCo destination to use for the default CMA
 - *JCo Destination*: Select the JCo destination to use for connecting to the ERP reference system
 - Click the *Next* button
 - Click the *Next* button
- 19. **SAP Convergent Charging Instances** screen
 - Click the *Add* button to add the following instances to your landscape:
 - *Dispatcher*
 - *Guider*
 - *Rater*
 - *Taxer*
 - *Bulkloader* (not available if you selected the *Stand-alone* integration scenario)

- Click the *Next* button

20. SAP Convergent Charging Dispatcher Instance screen

- *<SERVICE> Port*: Keep the default configuration, or set specific values for each configurable port
- *<SERVICE> Host*: Specify the full name of the machine hosting the dispatcher instance. If this host has several network interfaces and thus different IP addresses, tick the *Bind on a specific interface* checkbox and specify one of these IP addresses
- Click the *Next* button

21. SAP Convergent Charging Updater Instance screen

- *<SERVICE> Port*: Keep the default configuration, or set specific values for each configurable port
- *<SERVICE> Host*: Specify the full name of the machine hosting the updater instance. If this host has several network interfaces and thus different IP addresses, tick the *Bind on a specific interface* checkbox and specify one of these IP addresses
- Click the *Next* button

22. Start Instances after Installation screen

- *Start SAP Convergent Charging instances after installation*: Tick the checkbox to automatically start the instances at the end of the installation process

i Note

The SAP Management Console is deployed during the installation process and gives you the possibility to manage each instance of your landscape

- Click the *Next* button

23. Prerequisites Checker screen

- Click the *Next* button

24. Host Agent and SAPOSCOL Log Directory screen

- Click the *Next* button

25. Windows Domain for Host Agent screen

- *Domain Model*: Select the *Local Domain* option
- Click the *Next* button

26. Unpack Archives screen

- Click the *Next* button

27. Parameter Summary screen

- Carefully check that all your settings have been taken into account before starting the installation. In case you need to correct one or multiple settings, tick the corresponding checkboxes and click the *Revise* button
- If all your settings are correctly taken into account, click the *Next* button to start the installation

28. Task Progress screen

- This screen contains the different steps of your installation scenario, whose advancement can be followed

5.21 Installing a Core Server on a multi-hosts landscape

Description

The installation of a Core Server system on a multi-hosts landscape is performed using the SAPinst tool. This procedure explains you how to configure the different steps of the installation scenario handled by SAPinst in order to install:

- A stand-alone landscape that is not integrated with any third-party system
- A landscape that is integrated with the SAP Convergent Invoicing system

Preliminary Notes

For more information about license keys, refer to SAP Notes [197623](#) and [94998](#).

Prerequisites

- The Installation DVD of SAP Convergent Charging 5.0 must be downloaded and available on the host. Refer to the [Downloading the Installation DVD \[page 22\]](#) procedure if necessary
- On Linux and UNIX hosts, a shell script must be installed and available. Refer to the [Installing C Shell \[page 32\]](#) procedure if necessary
- On Microsoft Windows hosts, the “Microsoft Visual C++ 2013 runtime” libraries must be installed and available. For further information, refer to SAP Note [2676219](#).
- A SID²³ must be chosen for the Core Server system. Refer to the [Choosing System IDs \[page 21\]](#) procedure if necessary
- The JCE Jurisdiction Policy Files archive must be downloaded and available on the host. Refer to the [Downloading the JCE Jurisdiction Policy Files Archive \[page 25\]](#) procedure if necessary
- The adequate directories must be created. Refer to the [Creating required directories \[page 30\]](#) procedure if necessary
- A database must be prepared and available. Depending of your landscape, refer if necessary to one of the following procedures:
 - [Preparing the Oracle Core Database \[page 36\]](#)
 - [Preparing the SQL Server Core Database \[page 40\]](#)
 - [Preparing the SAP ASE Core Database \[page 43\]](#)
 - [Preparing the SAP HANA Core Database \[page 48\]](#)
 - [Preparing the IBM DB2 Core Database \(w/o pureScale Feature\) \[page 50\]](#)

²³ SAP System Identifier

- If your Core Database is running under an Oracle RDBMS²⁴, the dedicated JDBC²⁵ driver must be downloaded and available on the host. Refer to the [Downloading the Oracle JDBC driver \[page 28\]](#) procedure if necessary

Procedure


As this procedure relies on the SAPinst tool, you first need to launch it using the [Launching the SAPinst tool \[page 115\]](#) dedicated procedure.

Once opened, the SAPinst tool displays a succession of screens that give you the possibility to configure your installation scenario. Use the following recommendations to fill the different screens:

1. **Welcome to SAP Convergent Charging** screen
 - Click ► *SAP Convergent Charging* ► *Install* ► *Standard System Installation* ► *Core Server - First Steps* ►
 - Click the *Next* button
2. **Parameter Settings** screen
 - *Parameter Mode*: Select *Custom*
 - Click the *Next* button
3. **General SAP System Parameters** screen
 - *SAP System ID (SAPSID)*: Fill with the chosen SID
 - Click the *Next* button
4. **Master Password** screen
 - *Password for All Users*: Fill with a password respecting the SAP password policy
 - *Confirm*: Re-type the chosen password
 - Click the *Next* button
5. **SAP System Administrator** screen (related to the SAP CC system)
 - *Password of SAP System Administrator*: Filled by default with the password you specified in the **Master Password** screen, you can specify a different password
 - *User ID*: left empty
 - *Group ID of sapsys*: left empty
 - Click the *Next* button
6. **Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files** screen
 - *JCE Unlimited Strength Jurisdiction Policy Files*: Click the *Browse* button and select the ZIP archive you downloaded using the [dedicated procedure \[page 25\]](#)
 - Click the *Next* button
7. **SAP Convergent Charging Host Licenses** screen
 - Tick the *Generate a temporary license* checkbox
 - Click the *Next* button
8. **Database Type** screen
 - *Database Type*: Select the adequate RDBMS
 - Click the *Next* button
9. **SAP HANA, Sybase ASE, Oracle, Oracle RAC, MS SQL Server, DB2, or DB2 pureScale** screen

²⁴ Relational Database Management System

²⁵ Java Database Connectivity

- **SAP HANA** screen
(*Database Connection*)
 - *Primary Host*: Fill with the IP address of the machine hosting the primary node
 - *Secondary Host*: Fill with the IP address of the machine hosting the secondary node
 - *User*: Fill with the name of the Core Database administrator you specified during the preparation of your Core Database
 - *Password*: Fill with the password of the Core Database administrator you specified during the preparation of your Core Database
 - *Mode*: Select the mode that corresponds to the installation scenario of your SAP HANA database
 - *Single Container Mode*
 - *Port*: Fill with the relevant port of the system database of your SAP HANA system. For further information about the default ports of SAP products, refer to the dedicated section on SAP Help Portal: <https://help.sap.com/viewer/ports>
 - *Multiple Containers Mode*
 - *Tenant Name*: Fill with the name of the tenant database to connect to
 - *Port*: Fill with the relevant port of the tenant database of your SAP HANA system you want to connect to. Typical assignment rule for port number are:
 - 3<INSTANCE_NUMBER>15 for a single-container system
 - Between 3<INSTANCE_NUMBER>41 and 3<INSTANCE_NUMBER>98 for a multitenant system
 For further information about the value of such port, refer to the SAP Note [2365930](https://help.sap.com/viewer/ports)  or to the section dedicated to the default ports on SAP Help Portal: <https://help.sap.com/viewer/ports>
- **Sybase ASE** screen
(*Primary Database Connection*)
 - *Host*: Fill with the IP address of the machine hosting the database
 - *Port*: Fill with the port specified during the installation of the database
 - *Name*: Fill with the unique name of the database instance within which the content of the Core Database will be installed
 - *User*: Fill with the name of the Core Database administrator you specified during the preparation of your Core Database
 - *Password*: Fill with the password of the Core Database administrator you specified during the preparation of your Core Database
 - *Use Partitioning*: Tick the checkbox if your RDBMS supports the partitioning feature. Refer to your database administrator if necessary

(*Backup Database Connection*)

Tick the *Use backup database connection* checkbox if you want to use a backup database pour high availability purpose. If you tick this checkbox, specify the following information:

 - *Host*: Fill with the IP address of the machine hosting the backup database
 - *Port*: Fill with the port used to connect to the backup database
- **Oracle** screen
(*JDBC Driver*)
 - *JDBC Driver JAR Archive*: Click the *Browse* button and select the JAR archive you downloaded using the [dedicated procedure \[page 28\]](#)

(*Database Authentication*)

 - *Host*: Fill with the IP address of the machine hosting the database
 - *Port*: Fill with the port specified during the installation of the database

- *Instance Id*: Fill with the unique name of the database instance within which the content of the Core Database will be installed

i Note

For an Oracle database, you can use the following command to fill the *Instance Id* field:

```
sqlplus / as sysdba
SELECT sys_context('USERENV', 'DB_NAME') FROM DUAL;
```

- *User*: Fill with the name of the Core Database administrator you specified during the preparation of your Core Database
- *Password*: Fill with the password of the Core Database administrator you specified during the preparation of your Core Database
- *Use Partitioning*: Tick the checkbox if your RDBMS supports the partitioning feature. Refer to your database administrator if necessary
- **Oracle RAC** screen
(*JDBC Driver*)
 - *JDBC Driver JAR Archive*: Click the *Browse* button and select the JAR archive you downloaded using the [dedicated procedure \[page 28\]](#)
 (*Database Authentication*)
 - *User*: Fill with the name of the Core Database administrator you specified during the preparation of your Core Database
 - *Password*: Fill with the password of the Core Database administrator you specified during the preparation of your Core Database
 (*Database Instances*)
 Click the *Add* button to add instances according to your needs, each instance containing the following information:
 - *Host*: Fill with the IP address of the machine hosting the database instance
 - *Port*: Fill with the port specified during the installation of the database instance
 - *Instance Id*: Fill with the unique name of the database instance
- **MS SQL Server** screen
(*Database Connection*)
 - *Host*: Fill with the IP address of the machine hosting the database
 - *Port*: Fill with the port specified during the installation of the database
 - *Name*: Fill with the unique name of the database instance within which the content of the Core Database will be installed
 - *User*: Fill with the name of the Core Database administrator you specified during the preparation of your Core Database
 - *Password*: Fill with the password of the Core Database administrator you specified during the preparation of your Core Database
 - *Use Partitioning*: Tick the checkbox if your RDBMS supports the partitioning feature. Refer to your database administrator if necessary
- **DB2** screen
(*Database Connection*)
 - *Host*: Fill with the IP address of the machine hosting the database
 - *Port*: Fill with the port specified during the installation of the database
 - *Database Name*: Fill with the unique name of the database instance within which the content of the Core Database will be installed

- *Schema Name*: Fill with the name of the database schema you want to create within the Core Database
 - *User*: Fill with the name of the Core Database administrator you specified during the preparation of your Core Database
 - *Password*: Fill with the password of the Core Database administrator you specified during the preparation of your Core Database
 - *Use Partitioning*: Tick the checkbox if your RDBMS supports the partitioning feature. Refer to your database administrator if necessary
- **DB2 pureScale** screen
(*Database Parameters*)
- *Database Name*: Fill with the unique name of the database instance within which the content of the Core Database will be installed
 - *Schema Name*: Fill with the name of the database schema you want to create within the Core Database
 - *User*: Fill with the name of the Core Database administrator you specified during the preparation of your Core Database
 - *Password*: Fill with the password of the Core Database administrator you specified during the preparation of your Core Database
- (*Database Instances*)
Click the *Add* button to add instances according to your needs, each instance containing the following information:
- *Host*: Fill with the IP address of the machine hosting the database instance
 - *Port*: Fill with the port specified during the installation of the database instance
- Click the *Next* button
10. **Tablespaces / Filegroups / Segments** screen
- Ensure that each table or index is associated to the correct filegroup, tablespace or segment created during the preparation of your Core Database. When necessary, modify the associations accordingly
 - Click the *Next* button
11. **SAP Convergent Charging Working Directory** screen
- *Working Directory*: Click the *Browse* button and select the directory you specified during the [creation of the required directories \[page 30\]](#)
 - Click the *Next* button
12. **CA Introscope Java Agent** screen
- *Use monitoring with CA Introscope*: Untick the checkbox
 - Click the *Next* button
13. **System Landscape Directory** screen
- *Configure System Landscape Directory*: Untick the checkbox
 - Click the *Next* button
14. **SAP Convergent Charging Security** screen
- *Security*: Select the *Disabled* option
 - Click the *Next* button
15. **SAP Convergent Charging Administrator User** screen
- *Password*: Fill with a password respecting the SAP password policy
 - *Confirm*: Re-type the chosen password
 - Click the *Next* button
16. **SAP Convergent Charging Tax** screen

- Only tick the *VAT* taxation framework
- Click the *Next* button

17. SAP Convergent Charging Integration Scenario screen

- *Scenario*: Select the scenario that corresponds to your landscape:
 - If you select the *Stand-alone* integration scenario, no dedicated intermediate screen needs to be filled
 - If you select the *Billing and Invoicing in SAP Convergent Invoicing* or *Billing, Invoicing, and Storage of Consumption Data in SAP Convergent Invoicing* integration scenario, use the following recommendations to fill these dedicated intermediate screens:
 - **JCo Connection Configuration** screen
 - Click the *Add* button to add the adequate JCo²⁶ destination(s)
 - *Name*: Fill with the name of the JCo destination
 - *SAP Application*: Select the relevant type of targeted SAP Application
 - *Application Server Host*: Specify the full name of the machine hosting the SAP Application
 - *SAP System Number*: Specify the relevant SAP system number
 - *SAP Client*: Specify the relevant SAP client number
 - *Logon User*: Specify the name of the SAP user you want to use for connecting to the SAP Application
 - *Logon Password*: Specify the password of the previously specified user
 - *Install SAP Cryptographic Library*: Untick the checkbox
 - Click the *Next* button
 - **Customer Management Area and ERP Reference System** screen
 - *Default Customer Management Area*: Specify a name for the default CMA²⁷
 - *JCo Destination for ERP*: Select the JCo destination to use for the default CMA
 - *JCo Destination for CRM*: Select the JCo destination to use for the default CMA
 - *JCo Destination*: Select the JCo destination to use for connecting to the ERP reference system
 - Click the *Next* button
- Click the *Next* button

18. SAP Convergent Charging Instances screen

- Click the *Add* button to add the following instances to your landscape:
 - *Dispatcher*
 - *Guider*
- Click the *Next* button

19. SAP Convergent Charging Dispatcher Instance screen

- *<SERVICE> Port*: Keep the default configuration, or set specific values for each configurable port
- *<SERVICE> Host*: Specify the full name of the machine hosting the dispatcher instance. If this host has several network interfaces and thus different IP addresses, tick the *Bind on a specific interface* checkbox and specify one of these IP addresses
- Click the *Next* button

20. Start Instances after Installation screen

- *Start SAP Convergent Charging instances after installation*: Tick the checkbox to automatically start the instances at the end of the installation process

²⁶ Java Connector

²⁷ Customer Management Area

i Note

The SAP Management Console is deployed during the installation process and gives you the possibility to manage each instance of your landscape

- Click the *Next* button
- 21. **Prerequisites Checker** screen
 - Click the *Next* button
- 22. **SAP System Administrator** screen (global user for all SAP systems)
 - *Password of SAP System Administrator*: Filled by default with the password you specified in the **Master Password** screen, you can specify a different password
 - *User ID*: left empty
 - *Group ID of sapsys*: left empty
 - Click the *Next* button
- 23. **Unpack Archives** screen
 - Click the *Next* button
- 24. **Parameter Summary** screen
 - Carefully check that all your settings have been taken into account before starting the installation. In case you need to correct one or multiple settings, tick the corresponding checkboxes and click the *Revise* button
 - If all your settings are correctly taken into account, click the *Next* button to start the installation
- 25. **Task Progress** screen
 - This screen contains the different steps of your installation scenario, whose advancement can be followed

5.22 Testing a landscape basically

Description

Once an SAP CC Core Server system has been installed, you can use this procedure to perform some basic checks of your landscape relating to:

- The SAP Central Repository of the Global Host
- The Working Directory of each host
- The log files related to the installation process
- The status of the instances of your Core Server system

Preliminary Notes

- For more information about the Admin+ user interface, refer to its dedicated documentation: [SAP CC 5.0 Primary Help for Admin+](#)
- This procedure uses the following variables:
 - `<DRIVE>`, which corresponds to the drive of the Microsoft Windows host on which the system is installed
 - `<SYSTEM_ID>`, which corresponds to the identifier of your system
 - `<INSTANCE_NAME>`, which corresponds to the name of the concerned instance
 - `<SAPCC_SYSADM_USERNAME>`, which corresponds to the name of the administrator of your Core Server system (`<admin>` by default)
 - `<SAPCC_SYSADM_PASSWORD>`, which corresponds to the password of the administrator of your Core Server system, that you specified at installation time in the "SAP Convergent Charging *Administrator User*" screen of the SAPinst tool

Checking the SAP Central Repository and the Working Directory

As described in the [Document Definitions \[page 10\]](#) section, the SAP Central Repository is used to centralize the configuration of each installed system within the following directory:

- `/sapmnt/<SYSTEM_ID>/SYS` for Linux and UNIX operating systems
- `<DRIVE>:\usr\sap\<SYSTEM_ID>\SYS` for a Microsoft Windows operating system

You can browse this directory to get information about your installed system(s). In addition to the SAP Central Repository, the SAPinst tool creates a working directory for each deployed instance, in order to centralize elements such as configuration files, works logs, and so on. You can browse the following directories:

- `/usr/sap/<SYSTEM_ID>/<INSTANCE_NAME>` for Linux and UNIX operating systems
- `<DRIVE>:\usr\sap\<SYSTEM_ID>\<INSTANCE_NAME>` for a Microsoft Windows operating system

Checking the installation logs

When an SAP CC system has been installed, you can check some log files to get detailed information about:

- The execution of the different installation steps performed by the SAPinst tool
- The status of the installed elements

The following table contains information about folders containing log files that you can get information from:

SAPinst installation steps Depending whether your host is the Global Host of your system or not, you can browse the FIRST or the ADDITIONAL folders of the following directory:

Linux and UNIX operating systems

`/tmp/sapinst_instdir/CC50/INSTALL/STANDARD/`

Microsoft Windows operating system

`<DRIVE>:\Program Files\sapinst_instdir\CC50\INSTALL\STANDARD\`

Instances status The log files relating to a given instance are available within the following directories:

Linux and UNIX operating systems

`/usr/sap/<SYSTEM_ID>/<INSTANCE_NAME>/work`

`/usr/sap/<SYSTEM_ID>/<INSTANCE_NAME>/work/log`

Microsoft Windows operating system

`<DRIVE>:\usr\sap<SYSTEM_ID>\<INSTANCE_NAME>\work`

`<DRIVE>:\usr\sap<SYSTEM_ID>\<INSTANCE_NAME>\work\log`

Checking the instances status using

Checking the status of the different instances available within your landscape consists in the following operations:

- Launching the Admin+ user interface
- Identifying as the administrator of the Core Server system and displaying the following table filled with the status of the different instances:

```
+-----+-----+-----+-----+-----+-----+-----+-----+
| ID   | HOSTNAME | HTTP | EXTERNAL | INTERNAL | CURRENT DATE | START DATE | STATUS |
+-----+-----+-----+-----+-----+-----+-----+-----+
:     | :       | :   | :       | :       | :           | :         | :     |
+-----+-----+-----+-----+-----+-----+-----+-----+
```

As this procedure relies on the Admin+ user interface, you first need to launch it using the [Launching Admin+ \[page 130\]](#) dedicated procedure.

Once launched, execute the following commands within Admin+ in order to identify as the administrator of the Core Server system and display the status of the instances (that should be ON for alive instances):

```
user <SAPCC_SYSADM_USERNAME> <SAPCC_SYSADM_PASSWORD>
list
```

5.23 Setting up a new host for a landscape

Description

For many reasons such as business growth, performances improvement, and so on, it might be necessary to extend your landscape to add new system(s) or instance(s) of an existing system. This procedure explains you how to set up a new host within an existing landscape.

Procedure

To set up a new physical host, execute the following procedures:

- [Checking free space \[page 29\]](#), considering the installation DVD and the system(s) to install
- [Creating required directories \[page 30\]](#), with the adequate permissions
- [Installing C Shell \[page 32\]](#), required by the SAPinst tool for Linux and UNIX operating systems
- [Setting up the system encoding \[page 31\]](#), because the SAPinst tool requires an UTF-8 character encoding for Linux and UNIX operating systems
- [Setting up the system time zone \[page 33\]](#), to ensure that the time zone is correctly configured
- [Setting up the system environment variables \[page 35\]](#)

5.24 Adding Core Server instances in a multi-hosts landscape

Description

For many reasons such as business growth, performances improvement, and so on, it might be necessary to extend your Core Server system. This procedure explains you how to add new instance(s) on a given host of an existing Core Server system, using the SAPinst tool.

i Note

The new instances can be deployed:

- On an existing host of your landscape, that already contains instances of a Core Server system
- On a new host, that must be set up before launching the SAPinst tool. Refer to the [Setting up a new host for a landscape \[page 70\]](#) procedure if necessary

Preliminary Notes

For more information about license keys, refer to SAP Notes [197623](#) and [94998](#).

Prerequisites

The Global Host must be installed before executing this procedure. Refer to the [Installing a Core Server on a multi-hosts landscape \[page 61\]](#) procedure if necessary

Procedure

As this procedure relies on the SAPinst tool, you first need to launch it using the [Launching the SAPinst tool \[page 115\]](#) dedicated procedure.

Once opened, the SAPinst tool displays a succession of screens that give you the possibility to configure your installation scenario. Use the following recommendations to fill the different screens:

1. **Welcome to SAP Convergent Charging** screen
 - Click **SAP Convergent Charging > Install > Standard System Installation > Core Server - Add Instances**
 - Click the *Next* button
2. **Parameter Settings** screen
 - *Parameter Mode*: Select *Custom*
 - Click the *Next* button
3. **General SAP System Parameters** screen
 - *Profile Directory*: Filled by default with the location of the SAP system profile directory. Ensure that this location is correct
 - Click the *Next* button
4. **Master Password** screen
 - *Password for All Users*: Fill with a password respecting the SAP password policy
 - *Confirm*: Re-type the chosen password
 - Click the *Next* button
5. **SAP System Administrator** screen (related to the SAP CC system)
 - *Password of SAP System Administrator*: Filled by default with the password you specified in the **Master Password** screen, you can specify a different password
 - *User ID*: Fill with the identifier of the user that corresponds to the same user as for the Global Host

i Note

You can use the following command on a Linux host:

```
cat /etc/passwd | grep -i <SAP_System_ID>adm | cut -d':' -f3
```

- *Group ID of sapsys*: left empty

- Click the *Next* button
- 6. **Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files** screen
 - *JCE Unlimited Strength Jurisdiction Policy Files*: Click the *Browse* button and select the ZIP archive you downloaded using the [dedicated procedure \[page 25\]](#)
 - Click the *Next* button
- 7. **SAP Convergent Charging Host License** screen
 - Tick the *Generate a temporary license* checkbox
 - Click the *Next* button
- 8. **SAP Convergent Charging Instances** screen
 - Click the *Add* button to add the adequate instance(s) to your landscape
 - Click the *Next* button
- 9. **SAP Convergent Charging Updater Instance** screen
 - *<SERVICE> Port*: Keep the default configuration, or set specific values for each configurable port
 - *<SERVICE> Host*: Specify the full name of the machine hosting the dispatcher instance. If this host has several network interfaces and thus different IP addresses, tick the *Bind on a specific interface* checkbox and specify one of these IP addresses
 - Click the *Next* button
- 10. **Start Instances after Installation** screen
 - *Start SAP Convergent Charging instances after installation*: Tick the checkbox to automatically start the instances at the end of the installation process

i Note

The SAP Management Console is deployed during the installation process and gives you the possibility to manage each instance of your landscape

- Click the *Next* button
- 11. **Prerequisites Checker** screen
 - Click the *Next* button
- 12. **SAP System Administrator** screen (global user for all SAP systems)
 - *Password of SAP System Administrator*: Filled by default with the password you specified in the **Master Password** screen, you can specify a different password
 - *User ID*: left empty
 - *Group ID of sapsys*: left empty
 - Click the *Next* button
- 13. **Unpack Archives** screen
 - Click the *Next* button
- 14. **Parameter Summary** screen
 - Carefully check that all your settings have been taken into account before starting the installation. In case you need to correct one or multiple settings, tick the corresponding checkboxes and click the *Revise* button
 - If all your settings are correctly taken into account, click the *Next* button to start the installation
- 15. **Task Progress** screen
 - This screen contains the different steps of your installation scenario, whose advancement can be followed

5.25 Starting and stopping the servers

Description

During the installation of an SAP CC system, the following applications are automatically deployed to manage your SAP Convergent Charging landscape:

- SAP Management Console (SAP MC)
- SAP Microsoft Management Console (SAP MMC)
- SAPControl

The following table shows the availability of each application according to the operating system of your host:

Application	Application Type		OS Availability	
	GUI	Command-line	Windows	Linux/Unix
SAP Management Console (SAP MC)	■		■	■
SAP Microsoft Management Console (SAP MMC)	■		■	
SAPControl		■	■	■

You can use this procedure to get information about the use of each application.

Preliminary Notes

- It is recommended to respect the following sequence when starting the SAP systems you installed within your landscape:
 - Core Server instances, respecting the following recommendations:

→ Recommendation

- Start or restart one instance at a time: one after the other. Wait for an instance to be fully (re)started before (re)starting another one.
- Always first (re)start the Dispatcher instances.
- SAP SE recommends this specific order for (re)starting:
 1. Dispatcher
 2. Updater
 3. Guider
 4. Rater
 5. Bulkloader

- Diameter Server
- BART Server
- Import/Export Connector
- For more information about the SAP Management Console, refer to its dedicated documentation: <https://help.sap.com/34212da60ac54baebaf71b03fd0ac16d>
- For more information about the SAP Microsoft Management Console, refer to its dedicated documentation: <https://help.sap.com/db29f6d5eb9a49598b378c923bd9c894>
- For more information about SAPControl, refer to its dedicated documentation: <https://help.sap.com/viewer/ff18034f08af4d7bb33894c2047c3b71/latest/en-US/471d6feeff6e0d46e1000000a155369.html>

Java Startup Framework

All the applications mentioned in this procedure rely on the Java Startup Framework, which provides centralized management of the Java server processes and gives the possibility to monitor their life cycle. This framework handles the following shutdown modes that can be used to stop or restart an instance of a system:

- **Hard shutdown**, which consists in waiting for a given period during which the instance is supposed to stop properly by itself. This period is defined via a timeout specified in the `shutdownTimeout` property of the `jstart.config` configuration file (set by default to 150 seconds but capped by the operating system to 180 seconds on Windows and 300 on Linux and UNIX). When this timeout is reached, the Startup Framework stops the java process. SAP SE or an SAP affiliate company recommends that you avoid using this shutdown mode, as the timeout may be too small to let instances stop properly
- **Soft shutdown with timeout**, which consists in waiting for a given period during which the instance is supposed to stop properly by itself. When this timeout is reached, the Startup Framework tries additional internal methods to stop the instance, which means that the instance may be definitively stopped only few minutes after the timeout has been reached
- **Soft shutdown without timeout**, which consists in waiting for the instance to stop, whatever the time it will take. In case of unexpected situation, the result of these shutdown operations cannot be ensured. When such a situation occurs, or when the instance takes too much time to stop, it is possible to stop the instance by executing a Hard shutdown operation or by killing the process.

i Note

An instance can also stop due to the following reasons:

- A signal has been sent by the operating system:
 - `SIGKILL`, which corresponds to an immediate shutdown
 - `SIGTERM`, which uses an internal timeout before shutting down the process
- An individual user executed a dedicated command of a user interface (such as the `server stop` command of the Admin+ tool or the `sapcontrol stop` command of SAPControl)
- An applicative shutdown has been triggered, due to internal reasons such as bad startup configuration, invalid license, starting request refused by a dispatcher, conflict between dispatchers, and so on
- An unrecoverable error occurred:
 - `java.lang.VirtualMachineError`, coming from the Java Virtual Machine and leading to an immediate shutdown
 - `java.lang.Error` and `java.lang.Throwable`, which both lead to a shutdown after an internal timeout

Using the SAP Management Console (SAP MC)

If you have installed a Java Runtime Environment (JRE, version 5.0 and higher) and if you use a Web browser that is able to run Java applets, then you can launch the SAP Management Console as a Java applet in your Web browser using the following procedure:

- Open the `http://<HOST>:5<INSTANCE_NUMBER>13` URL within your Web browser, where:
 - `<HOST>` corresponds to the name or IP address of a host of your landscape
 - `<INSTANCE_NUMBER>` corresponds to the number of the instance

❖ Example

Considering a landscape containing a host:

- Whose hostname is **SAPCCHOST1** and IP address is 192.168.1.1
- That contains an instance whose name is **CCD02**

You can launch the SAP Management Console using the following URLs: `http://192.168.1.1:50213` or `http://SAPCCHOST1:50213`

i Note

If your Web browser display a security warning message, configure the options in order to trust the Java applets and reopen the URL.

To manage an instance of an SAP CC system using the SAP Management Console application, use the following procedure:

1. Open the SAP Management Console using the procedures described above
2. Expand the *SAP Systems* node and expand the system which contains the instance you want to manage
3. To manage instances, you must identify with the login information you provided at installation time. Click the instance you want to manage and fill the *Logon* screen with the information relating to the `<SID>adm` user
4. Right-click the instance you want to manage, and select the action you want to perform:
 - *Start*, which directly starts the process without any intermediate action
 - *Stop*, which opens a dialog window that gives you the possibility to specify which kind of shutdown mode you want to use and tune the associated timeouts
 - *Restart*, which indeed corresponds to a *Stop* action followed by a *Start* action, and thus opens the related dialog window

Using the SAP Microsoft Management Console (SAP MMC)

Microsoft Windows operating system

To launch the SAP Microsoft Management Console, connect to the host of your landscape that contains the SAP CC system you want to manage, and open the SAP Management Console program either from the shortcut available on the desktop or from the *Windows Start* menu.

To manage an instance of an SAP CC system using the SAP Microsoft Management Console application, use the following procedure:

1. Open the SAP Microsoft Management Console using the procedures described above
2. Expand the *SAP Systems* node and expand the system which contains the instance you want to manage
3. To manage instances, you must identify with the login information you provided at installation time. Click the instance you want to manage and fill the *Logon* screen with the information relating to the `<SID>adm` user
4. Right-click the instance you want to manage, and select the action you want to perform:
 - *Start*, which directly starts the process without any intermediate action
 - *Stop*, which opens a dialog window that gives you the possibility to specify which kind of shutdown mode you want to use and tune the associated timeouts
 - *Restart*, which indeed corresponds to a *Stop* action followed by a *Start* action, and thus opens the related dialog window

Using SAPControl

You can use SAPControl to start or stop an SAP Convergent Charging System Instance from the command line. You need to be logged on to the SAP Convergent Charging System host as user `<sid>adm` where `<SID>` is the SAP System ID of your SAP Convergent Charging System.

i Note

`<sid>adm` user comes with direct access to SAPControl (SAPControl is available in the PATH of this user). The following table contains the list of installation locations for SAPControl :

OS	Location
Linux/UNIX	<code>/usr/sap/hostctrl/exe/sapcontrol</code>
Microsoft Windows	<code>%ProgramFiles%\SAP\hostctrl\exe\sapcontrol.exe</code>

The SAPControl command-line application has the following partial synopsis:

```
sapcontrol [-trace <filename>]
           [-debug]
           [-user <user> <password>]
           -host <hostname>]
           -nr <instance number>
           -function <webmethod> [parameter list]
```

Where:

- The `-trace` option can be used to write SOAP request and/or response information into the specified file
- The `-debug` option can be used to write local trace to the `stderr` writing channel
- The `-user` option gives the possibility to execute the operation using a specific user, such as an SAP CC individual or service user granted the Administrator role
- The `-host` option gives the possibility to specify the host concerned by the operation
- The `-nr` parameter is used to specify the number of the instance concerned by the operation
- The `-function` parameter is used to specify the operation to perform on the target instance, such as:
 - **Start**, which directly starts the process

- **Stop**, which corresponds to:
 - A **hard shutdown** when no timeout is specified
 - A **soft shutdown with timeout** when a timeout is specified
- **Shutdown**, which corresponds to a **soft shutdown without timeout** (that SAP SE or an SAP affiliate company recommends you to avoid)
- **RestartInstance**, which indeed corresponds to:
 - A **hard shutdown** when no timeout is specified
 - A **soft shutdown with timeout** when a timeout is specified
 followed by a **Start** action
- And so on

i Note

To get the whole synopsis of the SAPControl application (particularly the list of supported functions), consult its documentation: <https://help.sap.com/viewer/ff18034f08af4d7bb33894c2047c3b71/7.31.24/en-US/471d6feeff6e0d46e1000000a155369.html>

🔗 Example

Considering a landscape containing a host:

- Whose hostname is **SAPCCHOST1** and IP address is 192.168.1.1
- That contains a rater instance whose name is **CCR04** and belonging to the **CCD** Core Server system whose administrator username is **CCDadm** and password is **CCDpwd**

You can use the following synopsis to execute a soft shutdown with a 10s timeout on this rater:

```
sapcontrol -host 192.168.1.1 -user CCDadm CCDpwd -nr 4 -function Stop 10
```

Linux and UNIX operating systems

• Starting an SAP Convergent Charging System Instance

You can start an SAP Convergent Charging system instance by executing the following command from the command line (<instance_number> can be the number of any instance of the pname conkeyref="loio03e69dcde4b54cd6bf4c127d2027be24/PRODUCT_NAME"/> system with SAP system ID <SID>):

```
sapcontrol -nr <instance_number> -function Start
```

For remote instances, the syntax is slightly different, because the `-host` and `-user` parameters also have to be specified:

```
sapcontrol -nr <instance_number> -host <remote_host> -user <sid>adm <password> -function Start
```

• Stopping an SAP Convergent Charging System Instance

You can stop an SAP Convergent Charging system instance by executing the following command from the command line (<instance_number> can be the number of any instance of the SAP Convergent Charging system with SAP system ID <SID>):

```
sapcontrol -nr <instance_number> -function Stop
```

For remote instances, the syntax is slightly different, because the `-host` and `-user` parameters also have to be specified:

```
sapcontrol -nr <instance_number> -host <remote_host> -user <sid>adm  
<password> -function Stop
```

Microsoft Windows operating system

- **Starting an SAP Convergent Charging System Instance**

You can start an SAP Convergent Charging system instance by executing the following command from the command line (<instance_number> can be the number of any instance of the SAP Convergent Charging system with SAP system ID <SID>):

```
sapcontrol.exe -nr <instance_number> -function Start
```

For remote instances, the syntax is slightly different, because the `-host` and `-user` parameters also have to be specified:

```
sapcontrol.exe -nr <instance_number> -host <remote_host> -user <sid>adm  
<password> -function Start
```

- **Stopping an SAP Convergent Charging System Instance**

You can stop an SAP Convergent Charging system instance by executing the following command from the command line (<instance_number> can be the number of any instance of the SAP Convergent Charging system with SAP system ID <SID>):

```
sapcontrol.exe -nr <instance_number> -function Stop
```

For remote instances, the syntax is slightly different, because the `-host` and `-user` parameters also have to be specified:

```
sapcontrol.exe -nr <instance_number> -host <remote_host> -user <sid>adm  
<password> -function Stop
```

5.26 Installing a BART Server in an existing landscape

Description

The BART Server is an SAP CC system that is dedicated to operations on Chargeable Items such as acquisition, consolidation, charging or rerating operations, all performed using a batch execution mode.

i Note

The BART Server can be deployed:

- On an existing host of your landscape, that already contains other systems
- On a new host within your landscape, that is dedicated to the BART Server system

This procedure explains you how to configure the different steps of the installation of the BART Server handled by SAPinst, on a dedicated host.

Prerequisites

- A Core Server system must be available within your landscape. According to your installation scenario, refer to the [Installing a Core Server on a mono-host landscape \[page 54\]](#) or the [Installing a Core Server on a multi-hosts landscape \[page 61\]](#) procedure if necessary. A dispatcher of this Core Server system must be available, and at least 1 instance must be connected to this dispatcher
- A dedicated host must be set up and available within your landscape. Refer to the [Setting up a new host for a landscape \[page 70\]](#) procedure if necessary
- On Microsoft Windows hosts, the “Microsoft Visual C++ 2013 runtime” libraries must be installed and available. For further information, refer to SAP Note [2676219](#)
- A database must be prepared and available. Depending of your landscape, refer if necessary to one of the following procedures:
 - [Preparing the Oracle Core Database \[page 36\]](#)
 - [Preparing the SQL Server Core Database \[page 40\]](#)
 - [Preparing the SAP ASE Core Database \[page 43\]](#)
 - [Preparing the SAP HANA Core Database \[page 48\]](#)
 - [Preparing the IBM DB2 Core Database \(w/o pureScale Feature\) \[page 50\]](#)
- If your BART Database is running under an Oracle RDBMS²⁸, the dedicated JDBC²⁹ driver must be downloaded and available on the host. Refer to the [Downloading the Oracle JDBC driver \[page 28\]](#) procedure if necessary
- A SID³⁰ must be chosen for the BART Server system. Refer to the [Choosing System IDs \[page 21\]](#) procedure if necessary

Procedure

The installation of the BART Server system consists in the following operations:

- Creating an SAP CC service user and granting the adequate roles and privileges to this user. To avoid runtime problems such as password expiration or user locking, the password management policy does not apply to this service user
- Launching the SAPinst tool to install the system

As described in the [SAP CC 5.0 Security Guide](#) documentation, you must create a service user for the BART Server system and grant the *Process Manager* and *Message Charging Client* roles to this user. Execute the following procedure to create this service user:

1. Launch the Core Tool using the [Launching Core Tool](#) dedicated procedure
2. Connect to the host that contains the Core Server system for communicating with your BART Server system. To connect to the host, use an SAP CC user that is granted the adequate authorizations for creating new users

²⁸ Relational Database Management System

²⁹ Java Database Connectivity

³⁰ SAP System Identifier

3. Create and set up a new user with the following information:
 - *Log on*: Fill with the name of the BART Server service user you want to create
 - *Password*: Fill with a password respecting the SAP password policy
 - *Security Profile*: Select *Service User*
 - *Roles*: Tick the *Process Manager* and *Message Charging Client* roles
 - Save your modifications

Once the adequate service user has been created, you can use the [Launching the SAPinst tool \[page 115\]](#) dedicated procedure to launch the installation of the BART Server system. Once opened, the SAPinst tool displays a succession of screens that give you the possibility to configure your installation scenario. Use the following recommendations to fill the different screens:

1. **Welcome to SAP Convergent Charging** screen
 - Click ► *SAP Convergent Charging* ► *Install* ► *Standard System Installation* ► *BART Server* ►
 - Click the *Next* button
2. **Parameter Settings** screen
 - *Parameter Mode*: Select *Custom*
 - Click the *Next* button
 - You will be prompted to log off in order to let SAPinst grant you the authorizations that are required to perform the installation. Click the *OK* button to log off, and reconnect to the host. SAPinst automatically restarts to continue the installation from there
3. **General SAP System Parameters** screen
 - *SAP System ID (SAPSID)*: Fill with the chosen SID for the BART Server
 - *Destination Drive or SAP Mount Directory*: Keep the default configuration
 - Click the *Next* button
4. **Master Password** screen
 - *Password for All Users*: Fill with a password respecting the SAP password policy
 - *Confirm*: Re-type the chosen password
 - Click the *Next* button
5. **Windows Domain** screen
 - *Domain Model*: Select *Local Domain*
 - Click the *Next* button
6. **Operating System Users** screen
 - *Password of SAP System Administrator*: Filled by default with the password you specified in the **Master Password** screen, you can specify a different password
 - *Confirm*: Re-type the chosen password
 - *Password of SAP System Service User*: Filled by default with the password you specified in the **Master Password** screen, you can specify a different password
 - *Confirm*: Re-type the chosen password
 - Click the *Next* button
7. **Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files** screen
 - *JCE Unlimited Strength Jurisdiction Policy Files*: Click the *Browse* button and select the ZIP archive you can find within the SAP Central Repository on the Global Host that you have mounted when executing the [dedicated procedure \[page 25\]](#)
 - Click the *Next* button
8. **Prerequisites Checker** screen
 - Click the *Next* button

9. **Database Type** screen
 - *Database Type*: Select the adequate RDBMS
 - Click the *Next* button
10. **SAP HANA, Sybase ASE, Oracle, Oracle RAC, MS SQL Server, DB2, or DB2 pureScale** screen
 - **SAP HANA** screen
(*Database Connection*)
 - *Primary Host*: Fill with the IP address of the machine hosting the primary node
 - *Secondary Host*: Fill with the IP address of the machine hosting the secondary node
 - *User*: Fill with the name of the BART Database administrator you specified during the preparation of your BART Database
 - *Password*: Fill with the password of the BART Database administrator you specified during the preparation of your BART Database
 - *Mode*: Select the mode that corresponds to the installation scenario of your SAP HANA database
 - *Single Container Mode*
 - *Port*: Fill with the relevant port of the system database of your SAP HANA system. For further information about the default ports of SAP products, refer to the dedicated section on SAP Help Portal: <https://help.sap.com/viewer/ports>
 - *Multiple Containers Mode*
 - *Tenant Name*: Fill with the name of the tenant database to connect to
 - *Port*: Fill with the relevant port of the tenant database of your SAP HANA system you want to connect to. For further information about the value of such port, refer to the SAP Note [2365930](https://help.sap.com/viewer/ports) or to the section dedicated to the default ports on SAP Help Portal: <https://help.sap.com/viewer/ports>
 - **Sybase ASE** screen
(*Primary Database Connection*)
 - *Host*: Fill with the IP address of the machine hosting the database
 - *Port*: Fill with the port specified during the installation of the database
 - *Name*: Fill with the unique name of the database instance within which the content of the BART Database will be installed
 - *User*: Fill with the name of the BART Database administrator you specified during the preparation of your BART Database
 - *Password*: Fill with the password of the BART Database administrator you specified during the preparation of your BART Database
 - *Use Partitioning*: Tick the checkbox if your RDBMS supports the partitioning feature. Refer to your database administrator if necessary

(*Backup Database Connection*)

Tick the *Use backup database connection* checkbox if you want to use a backup database pour high availability purpose. If you tick this checkbox, specify the following information:

 - *Host*: Fill with the IP address of the machine hosting the backup database
 - *Port*: Fill with the port used to connect to the backup database
 - **Oracle** screen
(*JDBC Driver*)
 - *JDBC Driver JAR Archive*: Click the *Browse* button and select the JAR archive you downloaded using the [dedicated procedure \[page 28\]](#)

(*Database Authentication*)

 - *Host*: Fill with the IP address of the machine hosting the database
 - *Port*: Fill with the port specified during the installation of the database

- *Instance Id*: Fill with the unique name of the database instance within which the content of the BART Database will be installed

i Note

For an Oracle database, you can use the following command to fill the *Instance Id* field:

```
sqlplus / as sysdba
SELECT sys_context('USERENV', 'DB_NAME') FROM DUAL;
```

- *User*: Fill with the name of the BART Database administrator you specified during the preparation of your BART Database
- *Password*: Fill with the password of the BART Database administrator you specified during the preparation of your BART Database
- *Use Partitioning*: Tick the checkbox if your RDBMS supports the partitioning feature. Refer to your database administrator if necessary
- **Oracle RAC** screen
(*JDBC Driver*)
 - *JDBC Driver JAR Archive*: Click the *Browse* button and select the JAR archive you downloaded using the [dedicated procedure \[page 28\]](#)
 (*Database Authentication*)
 - *User*: Fill with the name of the BART Database administrator you specified during the preparation of your BART Database
 - *Password*: Fill with the password of the BART Database administrator you specified during the preparation of your BART Database
 (*Database Instances*)
 Click the *Add* button to add instances according to your needs, each instance containing the following information:
 - *Host*: Fill with the IP address of the machine hosting the database instance
 - *Port*: Fill with the port specified during the installation of the database instance
 - *Instance Id*: Fill with the unique name of the database instance
- **MS SQL Server** screen
(*Database Connection*)
 - *Host*: Fill with the IP address of the machine hosting the database
 - *Port*: Fill with the port specified during the installation of the database
 - *Name*: Fill with the unique name of the database instance within which the content of the BART Database will be installed
 - *User*: Fill with the name of the BART Database administrator you specified during the preparation of your BART Database
 - *Password*: Fill with the password of the BART Database administrator you specified during the preparation of your BART Database
 - *Use Partitioning*: Tick the checkbox if your RDBMS supports the partitioning feature. Refer to your database administrator if necessary
- **DB2** screen
(*Database Connection*)
 - *Host*: Fill with the IP address of the machine hosting the database
 - *Port*: Fill with the port specified during the installation of the database
 - *Database Name*: Fill with the unique name of the database instance within which the content of the BART Database will be installed

- *Schema Name*: Fill with the name of the database schema you want to create within the BART Database
 - *User*: Fill with the name of the BART Database administrator you specified during the preparation of your BART Database
 - *Password*: Fill with the password of the BART Database administrator you specified during the preparation of your BART Database
 - *Use Partitioning*: Tick the checkbox if your RDBMS supports the partitioning feature. Refer to your database administrator if necessary
- **DB2 pureScale** screen
(*Database Parameters*)
- *Database Name*: Fill with the unique name of the database instance within which the content of the BART Database will be installed
 - *Schema Name*: Fill with the name of the database schema you want to create within the BART Database
 - *User*: Fill with the name of the BART Database administrator you specified during the preparation of your BART Database
 - *Password*: Fill with the password of the BART Database administrator you specified during the preparation of your BART Database
- (*Database Instances*)
Click the *Add* button to add instances according to your needs, each instance containing the following information:
- *Host*: Fill with the IP address of the machine hosting the database instance
 - *Port*: Fill with the port specified during the installation of the database instance
- Click the *Next* button
11. **Tablespaces / Filegroups / Segments** screen
- Ensure that each table or index is associated to the correct filegroup, tablespace or segment created during the preparation of your BART Database. When necessary, modify the associations accordingly
 - Click the *Next* button
12. **CA Introscope Java Agent** screen
- *Use monitoring with CA Introscope*: Untick the checkbox
 - Click the *Next* button
13. **System Landscape Directory** screen
- *Configure System Landscape Directory*: Untick the checkbox
 - Click the *Next* button
14. **SAP Convergent Charging Security** screen
- *Security*: Select the *Disabled* option
 - Click the *Next* button
15. **BART Server Settings** screen BART Database
- *<SERVICE> Port*: Keep the default configuration, or set specific values for each configurable port
 - *Message Host*: Specify the full name of the machine hosting the BART Server. If this host has several network interfaces and thus different IP addresses, tick the *Bind on a specific interface* checkbox and specify one of these IP addresses.
 - Click the *Next* button
16. **SAP Convergent Charging Core Server Connection Security** screen
- *Security*: Select the *None* option
 - Click the *Next* button

17. **SAP Convergent Charging Core Server Connection** screen

- Click the *Add* button to add a new line in the table containing the list of dispatchers available within your landscape
- Click the *Dispatcher HTTP Host* column of the newly inserted row, and fill with the IP address of an available dispatcher
- Click the *Dispatcher HTTP Port* column of the newly inserted row, and fill with the port number of this available dispatcher
- *Login*: Fill with the name of the service user for the BART Server, created previously
- *Password*: Fill with the password of the service user for the BART Server
- Click the *Next* button

18. **Start Instances after Installation** screen

- *Start SAP Convergent Charging instances after installation*: Tick the checkbox to automatically start the instances at the end of the installation process

i Note

The SAP Management Console is deployed during the installation process and gives you the possibility to manage each instance of your landscape

- Click the *Next* button

19. **Host Agent and SAPOSCOL Log Directory** screen

- Click the *Next* button

20. **Windows Domain for Host Agent** screen

- *Domain Model*: Select the *Local Domain* option
- Click the *Next* button

21. **Operating System Users** screen

- *Password of SAP System Administrator*: Filled by default with the password you specified in the *Master Password* screen, you can specify a different password
- *Confirm*: Re-type the chosen password
- Click the *Next* button

22. **Unpack Archives** screen

- Click the *Next* button

23. **Parameter Summary** screen

- Carefully check that all your settings have been taken into account before starting the installation. In case you need to correct one or multiple settings, tick the corresponding checkboxes and click the *Revise* button
- If all your settings are correctly taken into account, click the *Next* button to start the installation

24. **Task Progress** screen

- This screen contains the different steps of your installation scenario, whose advancement can be followed

5.27 Preparing the Oracle BART Database

Description

According to your business requirements, your SAP Convergent Charging landscape can contain from 1 (the Core Database) to 4 databases (the Core Database, the Session Database, the BART Database and the IEC Database). This procedure explains you how to prepare your BART Database running under an Oracle RDBMS³¹ (Standard or Enterprise edition).

Preliminary Notes

- In a development landscape, you can install all the SAP CC databases on the same physical host, but using different schemas. Nevertheless, SAP SE highly recommends that you install the different databases on separated hosts, in order to ease administration tasks and improve performances
- For further information about the installation of Oracle, refer to the following pages available on SAP Community:
 - <http://scn.sap.com/community/oracle>
 - <http://scn.sap.com/docs/DOC-7888>

Prerequisites

An instance of an Oracle RDBMS must be installed and available in your landscape. This database instance must use the UTF-8 character encoding to work in conjunction with the different SAP CC software components, and the *Oracle SQL*plus* tool must be installed to execute this procedure. Refer to your System Administrator to get information about these prerequisites relating to the SAP CC BART Database.

Procedure

The preparation of your SAP CC BART Database consists in the following operations:

- Setting up some initialization parameters
 - Creating a user account and granting the adequate roles and privileges to this user
 - Creating the different tablespaces
1. SAP Convergent Charging requires to modify some initialization parameters of the Oracle database, located in the `init.ora` file which contains the persistent parameters used during database startup. You can use the following procedure to:

³¹ Relational Database Management System

- Set the `_optim_peek_user_binds` parameter to **FALSE** in order to disable the bind peeking feature, which is not compatible with SAP CC
- Increase the maximum number of processes and sessions by setting the `processes` and `sessions` parameters to 300 multiplied by the number of databases installed on this Oracle instance, i.e. 1 (as only the BART Database is installed on this instance)

To correctly set up the initialization parameters of your BART Database, execute the following procedure:

```
sqlplus / as sysdba
alter system set "_optim_peek_user_binds"=false scope=spfile;
alter system set processes=300 scope=spfile;
alter system set sessions=300 scope=spfile;
shutdown immediate
startup
```

2. An Oracle user must be created and granted the adequate roles and privileges to administrate the BART Database. Execute the following procedure by replacing `<DB_USER>` by the name of the BART Database administrator and `<DB_PASSWORD>` by its password:

```
sqlplus / as sysdba
define dbuser="<DB_USER>"
define dbpwd="<DB_PASSWORD>"
create user &dbuser identified by &dbpwd;
grant CONNECT, RESOURCE TO &dbuser;
grant EXECUTE CATALOG_ROLE to &dbuser;
grant EXP_FULL_DATABASE, IMP_FULL_DATABASE to &dbuser;
grant CREATE PROCEDURE to &dbuser;
grant CREATE SESSION to &dbuser;
grant CREATE TABLESPACE, DROP TABLESPACE to &dbuser;
grant ALTER TABLESPACE to &dbuser;
grant CREATE ANY DIRECTORY to &dbuser;
grant DROP ANY DIRECTORY to &dbuser;
grant EXECUTE ON dbms_lock TO &dbuser;
```

3. The data storage of your SAP CC BART Database must be optimized by creating the following mandatory tablespaces, whose size depends on the edition of your RDBMS (Standard or Enterprise edition):

Tablespace name	Description	Minimal Size (MB)	
		SE	EE
BART_DATA	Tables used to store the BART data which are not related to CDRs	50	50
BART_INDX	Indexes used for the BART data which are not related to CDRs	10	10
CDR_DATA	Tables containing data related to CDRs	100	2000
CDR_INDX	Indexes used for the data related to CDRs	600	10000

To create the mandatory tablespaces, execute the following procedure by replacing:

- `<tablespace_name>` by the name of the tablespace to create
- `<file_location>` by the full path of the file that will contain the tablespace, located in the `oradata` directory
- `<size>` by the recommended value associated to the tablespace, listed in the above table and using the `AUTO_EXTEND` option

```
sqlplus / as sysdba
```

And then, for each tablespace listed in the above table:

```
CREATE BIGFILE TABLESPACE <tablespace_name> DATAFILE '<file_location>' SIZE
<size> AUTOEXTEND ON MAXSIZE UNLIMITED UNIFORM SIZE 1M LOGGING EXTENT MANAGEMENT
LOCAL SEGMENT SPACE MANAGEMENT AUTO;
```

Followed by this command for Oracle 12c databases:

```
ALTER USER <dbuser> QUOTA UNLIMITED ON <tablespace_name>;
```

❁ Example

For an Oracle 12c Standard Edition RDBMS installed on a Linux host, you can use the following statement:

- To create the **BART_DATA** tablespace
- To give the **sapccbart** user the possibility to access this tablespace

```
CREATE BIGFILE TABLESPACE BART_DATA DATAFILE '/oradata/vol1/BART_DATA.dbf'
SIZE 100M AUTOEXTEND ON MAXSIZE UNLIMITED UNIFORM SIZE 1M LOGGING EXTENT
MANAGEMENT LOCAL SEGMENT SPACE MANAGEMENT AUTO;
ALTER USER sapccbart QUOTA UNLIMITED ON BART_DATA;
```

5.28 Preparing the SQL Server BART Database

Description

According to your business requirements, your SAP Convergent Charging landscape can contain from 1 (the Core Database) to 4 databases (the Core Database, the Session Database, the BART Database and the IEC Database). This procedure explains you how to prepare your BART Database running under a Microsoft SQL Server RDBMS³² (Standard or Enterprise edition).

Preliminary Notes

- In a development landscape, you can install all the SAP CC databases on the same physical host, but using different schemas. Nevertheless, SAP SE highly recommends that you install the different databases on separated hosts, in order to ease administration tasks and improve performances
- For further information about the installation of Microsoft SQL Server, refer to the following pages available on the SAP Community:
 - <http://scn.sap.com/community/sqlserver>
 - <http://scn.sap.com/docs/DOC-8286>

³² Relational Database Management System

Prerequisites

An instance of a SQL Server RDBMS must be installed and available in your landscape. The *SQL Server Management Studio* application must be installed to execute this procedure. Refer to your System Administrator to get information about these prerequisites relating to the SAP CC BART Database.

Procedure

The preparation of your SAP CC BART Database consists in the following operations:

- Creating a SQL Server user account and granting the adequate roles on the adequate server to this user
 - Creating the BART Database with the user as the owner
 - Creating the different filegroups within this database
1. An SQL Server user must be created for your SAP CC BART Database, and granted the adequate roles and privileges. Execute the following procedure to create this SAP CC user:
 - Open the *SQL Server Management Studio* application
 - The *Connect to Server* dialog window opens. Use the following settings:
 - *Server Name*: Select *(local)*
 - *Authentication*: Select *Windows Authentication*, in order to use your operating system user
 - Click the *Connect* button
 - Open the *View / Object Explorer* menu to display the *Object Explorer* and expand the *(local)* server
 - Right-click the *Security* element of the tree and open the *New / Login...* menu to display the *Login* screen
 - Fill the *General* tab with the following information:
 - *Login name*: Fill with the name of the BART Database administrator
 - Select the *SQL Server authentication* option
 - *Password*: Fill with a password respecting the SAP password policy
 - *Confirm password*: Re-type the chosen password
 - *User must change password at next login*: Untick the checkbox
 - *Default database*: Select the *master* database
 - In the *Server Roles* tab, select the following roles:
 - *dbcreator*
 - *diskadmin*
 - *serveradmin*
 - Click the *OK* button
 - Right-click the *(local)* server and click *Disconnect*
 2. Once the SQL Server user dedicated to the BART Database has been created, it is necessary to reconnect to the server in order to create the BART Database. Execute the following procedure:
 - Open the *File / Connect Object Explorer...* menu or click the *Connect Object Explorer* button to re-open the *Connect to Server* dialog window. Use the following settings:
 - *Server Name*: Specify the full name of the machine hosting the database
 - *Authentication*: Select *SQL Server authentication*
 - *Login*: Fill with the previously created user
 - *Password*: Fill with the password of the previously created user

- Click the *Connect* button
 - Right-click the *Databases* element of the tree and open the *New Database...* menu to display the *New Database* screen
 - Fill the *General* tab with the following information:
 - *Database name*: Fill with the name of the BART Database
 - *Owner*: Fill with the name of the previously created user
 - Fill the *Options* tab with the following information:
 - *Collation*: Collation defines the way strings are managed in SQL Server databases. The BART Database must be case-sensitive (CS) and compatible with ASCII Unicode (AS). Thus select the element that corresponds to the appropriate language, ending by the *CS_AS* string (e.g. *Latin1_General_CS_AS*)
 - *Recovery model*: Select *Full*
 - *Compatibility level*: Ensure that *SQL Server 2008 (100)* is selected
 - Click the *OK* button
3. The data storage of your SAP CC BART Database must then be optimized by creating the following mandatory filegroups:

Tablespace name	Description
BART_DATA	Tables used to store the BART data which are not related to CDRs
BART_INDX	Indexes used for the BART data which are not related to CDRs
CDR_DATA	Tables containing data related to CDRs
CDR_INDX	Indexes used for the data related to CDRs

To create the mandatory filegroups, execute the following procedure by replacing `<DATABASE_NAME>` by the name of the BART Database `<FILEGROUP_NAME>` by the name of the filegroup to create, and `<FILE_LOCATION>` by the full path of the file that will contain the filegroup directory:

- Right-click your server and open the *New Query* menu
- For each filegroup listed in the above table, type the following query and execute it:

```
ALTER DATABASE "<DATABASE_NAME>" ADD FILEGROUP <FILEGROUP_NAME>;
ALTER DATABASE "<DATABASE_NAME>" ADD FILE
(
  NAME = <FILEGROUP_NAME>,
  FILENAME = '<FILE_LOCATION>',
  SIZE = 1MB,
  MAXSIZE = 1000MB,
  FILEGROWTH = 5MB
)
TO FILEGROUP <FILEGROUP_NAME>;
```

❁ Example

To create the **BART_DATA** filegroup in the **SAPCCBART** BART Database of an SQL Server RDBMS, you can use the following query:

```
ALTER DATABASE "SAPCCBART" ADD FILEGROUP BART_DATA;
ALTER DATABASE "SAPCCBART" ADD FILE
(
  NAME = BART_DATA,
  FILENAME = 'c:\tmp\BART_DATA.ndf',
  SIZE = 1MB,
  MAXSIZE = 1000MB,
```

```
FILEGROWTH = 5MB
)
TO FILEGROUP BART_DATA;
```

5.29 Preparing the SAP ASE BART Database

Description

According to your business requirements, your SAP Convergent Charging landscape can contain from 1 (the Core Database) to 4 databases (the Core Database, the Session Database, the BART Database and the IEC Database). This procedure explains you how to prepare your BART Database running under an SAP Adaptive Server Enterprise RDBMS³³.

Preliminary Notes

- In a development landscape, you can install all the SAP CC databases on the same physical host, but using different schemas. Nevertheless, SAP SE highly recommends that you install the different databases on separated hosts, in order to ease administration tasks and improve performances
- For further information about the installation of Microsoft SQL Server, refer to the following pages available on the SAP Community:
 - <http://infocenter.sybase.com/>
 - <http://scn.sap.com/community/developer-center/oltp-db>
 - <http://scn.sap.com/docs/DOC-34995>
 - <http://scn.sap.com/docs/DOC-34996>

Prerequisites

An instance of an SAP ASE RDBMS must be installed and available in your landscape. This instance must be:

- Correctly licensed in order to fit specific needs such as data partitioning, communication securing, system high-availability, and so on
- Installed with the following configuration:
 - *Application Type*: Mixed (OLTP/DSS)
 - *Page Size*: 8k. Note that this value cannot be modified after the installation. The modification of the value leads to a warning message informing that the newly specified page size must be similar between databases used for import purposes

³³ Relational Database Management System

- *Default Character Set*: utf-8 : Unicode 3.1 for UTF-8 Character Set
- *Default Sort Order*: altdict : Alternate (lower-case first) dictionary ordering

In addition, the *Interactive SQL* tool must be installed to execute the different steps of this procedure. For further information about this tool, refer afterwards.

To get information about these prerequisites relating to the SAP CC BART Database, refer to your System Administrator.

⚠ Caution

Free Developer Edition or Small Business Edition of SAP ASE are not supported by SAP CC. You must install a licensed copy of the Sybase Adaptive Enterprise Suite

Using the Interactive SQL tool

Interactive SQL is a command-line tool provided by SAP ASE to execute SQL statements:

- Interactively, to execute individual commands
- In a batch mode, to execute script files that contain multiple commands

To use the interactive mode, you have to:

- Launch isql using the following synopsis, providing the username and password specified at installation time:

```
isql -U <USERNAME> -P <PASSWORD>
```

- Type the command to execute, followed by the `go` statement:

```
<command to execute>
go
```

To use the batch mode, you have to:


- Create a text file containing the list of commands to execute, each command being followed by the `go` statement:

```
<command to execute>
go
<command to execute>
go
<command to execute>
go
and so on
```

- Launch isql using the following synopsis, providing the username and password specified at installation time, and specifying the previously created script file:

```
isql -U <username> -P <password> -i <script file>
```

i Note

- Whatever the execution mode is, you can use the `quit` command to exit the isql tool
- For further information about the isql tool, refer to the [dedicated documentation](#) 

Procedure

The preparation of your SAP CC BART Database consists in the following operations:

- Setting up some parameters of the SAP ASE Server
 - Creating the devices for data and logs, and the database relying on these devices
 - Setting up some database options
 - Creating a user account and granting the adequate roles and privileges to this user
 - Creating the different segments
1. Some parameters of the SAP ASE Server must be modified in order to fit specific needs of SAP Convergent Charging. Use the following list of commands to modify the configuration of the ASE Server accordingly:

```
use master
GO
sp_configure "number of open objects", 10000
GO
sp_configure "number of open indexes", 2000
GO
sp_configure "max network packet size", 16384
GO
sp_configure "default network packet size", 16384
GO
sp_configure "optimization goal", 0, 'allows_mix'
GO
sp_configure "disable varbinary truncation", 1
GO
sp_configure "number of user connections", 200
GO
sp_configure "number of locks", 1000000
GO
sp_configure "deadlock checking period", 800
GO
sp_configure "lock hashtable size", 16384
GO
sp_configure "row lock promotion HWM", 214748364
GO
sp_configure "row lock promotion LWM", 214748364
GO
sp_configure "SQL batch capture", 1
GO
sp_configure "kernel resource memory", 12000
GO
sp_configure "enable monitoring", 1
GO
sp_configure "sql text pipe active", 1
GO
sp_configure "sql text pipe max messages", 2000
GO
sp_configure "plan text pipe active", 1
GO
sp_configure "plan text pipe max messages", 2000
GO
sp_configure "statement pipe active", 1
GO
sp_configure "statement pipe max messages", 2000
GO
sp_configure "errorlog pipe active", 1
GO
sp_configure "errorlog pipe max messages", 2000
GO
sp_configure "deadlock pipe active", 1
GO
sp_configure "deadlock pipe max messages", 2000
```

```

GO
sp_configure "lock timeout pipe max messages", 2000
GO
sp_configure "lock timeout pipe active", 1
GO
sp_configure "wait event timing", 1
GO
sp_configure "process wait events", 1
GO
sp_configure "object lockwait timing", 1
GO
sp_configure "statement statistics active", 1
GO
sp_configure "per object statistics active", 1
GO
sp_configure "max SQL text monitored", 512
GO
sp_configure "enable stmt cache monitoring", 1
GO
sp_configure "aux scan descriptors", 1000
GO
sp_configure "select for update", 1
GO

```

If you use the database partitioning function for your database, execute the following commands:

```

sp_configure "enable semantic partitioning", 1
GO
sp_configure "number of open partitions", 100000
GO

```

If you use secured communications with your database, execute the following command:

```

sp_configure "enable SSL", 1
GO

```

2. To create the devices for data and logs, and then the database that relies on these devices, use the following list of commands considering that:
 - `<DB_NAME>` corresponds to the name of your database
 - `<DEVICE_PATH>` corresponds to the path of the device
 - `<DEVICE_SIZE>` corresponds to the amount of space to allocate to the device, made up with a quantity followed by one of these supported unit specifiers:
 - k or K (kilobytes)
 - m or M (megabytes)
 - g or G (gigabytes)
 - t or T (terabytes)

```

disk init name="<DB_NAME>_data", physname="<DEVICE_PATH>\<DB_NAME>_data",
size=<DEVICE_SIZE>, dsync = true
GO
disk init name="<DB_NAME>_log", physname="<DEVICE_PATH>\<DB_NAME>_log",
size=<DEVICE_SIZE>, dsync = true
GO
create database <DB_NAME> on <DB_NAME>_data=2000000 log on
<DB_NAME>_log=2000000
GO

```

3. Some options of the previously created database must be modified. Use the following list of commands, considering that `<DB_NAME>` corresponds to the name of your database:

```

sp_dboption <DB_NAME>,"ddl in tran", true

```

```
GO
sp_dboption <DB_NAME>, "select into", true
GO
```

4. A dedicated user must be created to administrate the BART Database, and must be declared as the owner of the BART Database. Use the following list of commands considering that:
 - <DB_USER> corresponds to the name of the BART Database administrator
 - <DB_PASSWORD> corresponds to the password of the BART Database administrator, that respects the SAP password policy
 - <DB_NAME> corresponds to the name of the BART Database

```
create login <DB_USER> with password <DB_PASSWORD>
GO
use <DB_NAME>
GO
sp_cangedbowner <DB_USER>
GO
```

5. To optimize the storage of your data, you need to create mandatory segments within your database. Use the following list of commands, considering that <DB_NAME> corresponds to the name of your BART Database:

```
use <DB_NAME>
GO
sp_addsegment 'BART_DATA', '<DB_NAME>', '<DB_NAME>_data'
GO
sp_addsegment 'BART_INDX', '<DB_NAME>', '<DB_NAME>_data'
GO
sp_addsegment 'CDR_DATA', '<DB_NAME>', '<DB_NAME>_data'
GO
sp_addsegment 'CDR_INDX', '<DB_NAME>', '<DB_NAME>_data'
GO
```

5.30 Preparing the SAP HANA BART Database

Description

According to your business requirements, your SAP Convergent Charging landscape can contain from 1 (the Core Database) to 4 databases (the Core Database, the Session Database, the BART Database and the IEC Database). This procedure explains you how to prepare your BART Database running under an SAP HANA in-memory database system using a single container or a multiple containers mode.

Preliminary Notes

- In a development landscape, you can install all the SAP CC databases on the same physical host, but using different schemas. Nevertheless, SAP SE highly recommends that you install the different databases on separated hosts, in order to ease administration tasks and improve performances
- For further information about the installation of SAP HANA, refer to the following pages available on SAP Community:
 - <http://scn.sap.com/community/developer-center/hana>
 - <http://scn.sap.com/docs/DOC-53955>

For further information about data types, operators, functions, statements, and so on, refer to the SAP HANA SQL and System Views Reference documentation available on SAP Help Portal:<http://help.sap.com>

Prerequisites

An SAP HANA database system must be installed and available in your landscape. The SAP HANA Studio application must be installed to execute this procedure. Refer to your System Administrator to get information about these prerequisites relating to the SAP CC BART Database.

Procedure

The preparation of your SAP CC BART Database consists in the following operations:

- Declaring your system within the SAP HANA Administration Console of the *SAP HANA Studio* application
 - Creating a user account and granting the adequate roles and privileges to this user on this system
 - Disabling the expiration of the user's password
1. An SAP HANA system must be created to administrate your SAP CC BART Database. Execute the following procedure to create this system:
 - Open the *SAP HANA Studio* application
 - Open the **Window > Perspective > Open Perspective > SAP HANA Administration Console** menu to display the perspective dedicated to the management of SAP HANA systems
 - Open the **Window > Show View > Systems** menu to display the view containing the list of SAP HANA systems
 - Click the *Add System* icon to open the *System* dialog window
 - Use the following settings to fill the *Specify System* screen:
 - *Host Name*: Fill with the master host name
 - *Instance Number*: Fill with the instance number of your SAP HANA system
 - *Mode*: Select *Single Container* or *Multiple containers*, according to your needs
 - *Description*: Fill with a text that describes your system
 - Click the *Next* button
 - The *Connection Properties* screen opens. Select the *Authentication by database user* option and use the following settings:

- *User Name*: Fill with the name of the SAP HANA system administrator
 - *Password*: Fill with a password respecting the SAP password policy
 - Click the *Finish* button to log on the newly declared SAP HANA system
2. Once you are connected to the relevant SAP HANA system, it is necessary to create a user account and grant the adequate roles and privileges to this user in order to administrate the BART Database. Execute the following procedure to create this user:
- Expand the *Security* folder, and right-click the *Users* element to display the context menu corresponds to the name of your database
 - Right-click the *Users* element of the tree and open the *New User* menu to display the screen dedicated to the creation of new users
 - Fill the *User* tab with the following information:
 - *User Name*: Fill with the name of the BART Database administrator
 - Select the *Password* option in the *Authentication* fieldset
 - *Password*: Fill with a password respecting the SAP password policy
 - *Confirm password*: Re-type the chosen password
 - In the *Granted Roles* subtab, click the + button to add the following roles to the user:
 - *CONTENT_ADMIN*
 - *MODELING*
 - In the *System Privileges* subtab, click the + button to add the following privileges to the user:
 - *EXPORT*
 - *IMPORT*
 - Click the *Deploy* button to finalize the creation of the user
3. Once the user has been created and deployed on your SAP HANA system, it is necessary to disable the expiration of its password. Execute the following procedure:
- Right-click the previously created SAP HANA system and open the *Open SQL Console* menu to display the screen dedicated to the execution of SQL statements
 - Type the following SQL statement within the editor, considering that `<USERNAME>` corresponds to the name of your previously created user. For further information, refer to the documentation of the `ALTER USER` command available in the SAP HANA documentation:
- ```
ALTER USER <USERNAME> DISABLE PASSWORD LIFETIME;
```
- Click the *Execute* button to execute the SQL statement

## 5.31 Preparing the IBM DB2 BART Database (w/o pureScale Feature)

### Description

According to your business requirements, your SAP Convergent Charging landscape can contain from 1 (the Core Database) to 4 databases (the Core Database, the Session Database, the BART Database and the IEC



Database). This procedure explains you how to prepare your BART Database running under an IBM DB2 RDBMS<sup>34</sup> without the pureScale feature.

## Preliminary Notes

- In a development landscape, you can install all the SAP CC databases on the same physical host, but using different schemas. Nevertheless, SAP SE highly recommends that you install the different databases on separated hosts, in order to ease administration tasks and improve performances
- For further information about the installation of Microsoft SQL Server, refer to the following pages available on the SAP Community:
  - <http://scn.sap.com/community/db2-for-linux-unix-windows>
  - <http://scn.sap.com/docs/DOC-8211>

This procedure uses the following variables:

- `<DB_GROUP>`, which corresponds to the name of the group containing the DB2 administrators, specified at DB2 installation time
- `<DB_NAME>`, which corresponds to the name of the BART Database
- `<DB_USER>`, which corresponds to the name of the BART Database administrator, which corresponds to a user granted adequate roles and privileges
- `<DB_PASSWORD>`, which corresponds to the password of the BART Database administrator, respecting the SAP password policy but without any expiration date
- `<TABLESPACE_NAME>`, which corresponds to the name of the tablespace to create
- `<FILE_LOCATION>`, which corresponds to the full path of the directory that will contain the tablespaces

## Prerequisites

An instance of an IBM DB2 database must be installed and available in your landscape. The *IBM DB2 db2cmd* tool must be installed to execute this procedure. Refer to your System Administrator to get information about these prerequisites relating to the SAP CC BART Database.

## Procedure

The preparation of your SAP CC BART Database consists in the following operations:

- Creating a user account and adding this user to the relevant group
  - Creating the BART Database and setting up some configuration parameters
  - Granting the newly created user the adequate roles and privileges
  - Creating the different tablespaces within this database
1. SAP Convergent Charging requires to create a dedicated user for your SAP CCBART Database, and add this user to the group containing the DB2 administrators. Execute the following procedure:

---

<sup>34</sup> Relational Database Management System

- For a Microsoft Windows operating system, execute the following commands into a command line prompt:

```
net user <DB_USER> "<DB_PASSWORD>" /ADD /PASSWORDCHG:NO /EXPIRES:never
wmic UserAccount where Name="<DB_USER>" set PasswordExpires=False
net localgroup <DB_GROUP> <DB_USER> /add
```

- For Linux and UNIX operating systems, execute the following commands in order to retrieve the identifier of the group containing the DB2 administrators, create the user within the adequate group and set a password for this user:

```
cat /etc/group | grep -i <DB_GROUP> | cut -d':' -f3
useradd -g <GROUP_ID> <DB_USER>
passwd <DB_USER>
```

2. SAP Convergent Charging requires to modify some configuration parameters when creating the DB2 database. You can use the following procedure to:

- Create the database
- Set the default page size of the database to 16K
- Specify an amount of storage for recovery log files by pre-allocating a number of 50 primary log files
- Set the amount of the database heap memory to use as a buffer for recording logs before writing these records to disk to 1024 4KB pages
- Set the size of each primary and secondary log file to 16K 4KB pages. This size limits the number of records that can be written in these files before they become full and require the creation of new ones
- Specify the percentage of changed pages at which the asynchronous page cleaners will be started (if they are not currently active)
- Activate the dynamically distribution of the available memory resources between the memory consumers
- Activate the automatic sampling rate determination, based on table size
- Set the default prefetch size of tablespaces to 960 pages
- Set an automatic percentage for the lock list held by an application that must be filled before performing lock escalation
- Set an automatic amount of 4K pages to store the lock list

To create the SAP CC BART Database, execute the following procedure:

```
db2cmd
db2
create database <DB_NAME> pagesize 16384
update database configuration for <DB_NAME> using LOGPRIMARY 50
update database configuration for <DB_NAME> using DECFLT_ROUNDING
ROUND_CEILING
update database configuration for <DB_NAME> using LOGBUFSZ 1024
update database configuration for <DB_NAME> using LOGFILSIZ 16384
update database configuration for <DB_NAME> using CHNGPGS_THRES 40
update database configuration for <DB_NAME> using SELF_TUNING_MEM ON
update database configuration for <DB_NAME> using AUTO_SAMPLING ON
update database configuration for <DB_NAME> using DFT_PREFETCH_SZ 960
update database configuration for <DB_NAME> using MAXLOCKS AUTOMATIC
update database configuration for <DB_NAME> using LOCKLIST AUTOMATIC
```

3. The user created in Step1 must then be granted the adequate roles and privileges on the SAP CC BART Database. Execute the following procedure:

```
db2cmd
db2
connect to <DB_NAME>
grant dbadm on database to <DB_USER>
```

```
connect reset
```

4. The data storage of your SAP CC BART Database must then be optimized by creating the following mandatory tablespaces:

| Tablespace name | Description                                                      |
|-----------------|------------------------------------------------------------------|
| BART_DATA       | Tables used to store the BART data which are not related to CDRs |
| BART_INDX       | Indexes used for the BART data which are not related to CDRs     |
| CDR_DATA        | Tables containing data related to CDRs                           |
| CDR_INDX        | Indexes used for the data related to CDRs                        |

To create the mandatory tablespaces, execute the following procedure:

```
db2cmd
db2
connect to <DB_NAME>
```

And then, for each tablespace listed in the above table:

```
create tablespace <TABLESPACE_NAME> MANAGED BY DATABASE USING (file
'<FILE_LOCATION><TABLESPACE_NAME>' 256000) EXTENTSIZE 2 DROPPED TABLE
RECOVERY OFF AUTORESIZE YES
```

#### ❁ Example

For an IBM DB2 RDBMS installed on a Microsoft Windows host, you can use the following statement to create the **BART\_DATA** tablespace:

```
create tablespace BART_DATA MANAGED BY DATABASE USING (file 'C:
\DB2\tbspaces\BART_DATA' 256000) EXTENTSIZE 2 DROPPED TABLE RECOVERY
OFF AUTORESIZE YES
```

## 5.32 Installing a Diameter Server in an existing landscape

### Description

The Diameter Server component represents a message translator which is used to convert credit-control messages coming from a Diameter client application into charging messages that the Core Server system is able to handle. It behaves as an online mediation system providing credit-control capabilities such as real-time services control, prepaid balances management, customers notification, sessions termination, and so on.

#### i Note

The Diameter Server can be deployed:

- On an existing host of your landscape, that already contains other systems
- On a new host within your landscape, that is dedicated to the Diameter Server system

This procedure explains you how to configure the different steps of the installation of the Diameter Server handled by SAPinst, on a dedicated host.

## Prerequisites

- A Core Server system must be available within your landscape. According to your installation scenario, refer to the [Installing a Core Server on a mono-host landscape \[page 54\]](#) or the [Installing a Core Server on a multi-hosts landscape \[page 61\]](#) procedure if necessary. A dispatcher of this Core Server system must be available, and at least 1 instance must be connected to this dispatcher
- A dedicated host must be set up and available within your landscape. Refer to the [Setting up a new host for a landscape \[page 70\]](#) procedure if necessary
- On Microsoft Windows hosts, the "Microsoft Visual C++ 2013 runtime" libraries must be installed and available. For further information, refer to SAP Note [2676219](#)
- A SID must be chosen for the Diameter Server system. Refer to the [Choosing System IDs \[page 21\]](#) procedure if necessary

## Procedure

The installation of the Diameter Server system consists in the following operations:

- Creating an SAP CC service user and granting the adequate roles and privileges to this user. To avoid runtime problems such as password expiration or user locking, the password management policy does not apply to this service user
- Launching the SAPinst tool to install the system

As described in the [SAP CC 5.0 Security Guide](#) documentation, you must create a service user for the Diameter Server system and grant the *Message Charging Client* role to this user. Execute the following procedure to create this service user:

1. Launch the Core Tool using the [Launching Core Tool](#) dedicated procedure
2. Connect to the host that contains the Core Server system for communicating with your Diameter Server system. To connect to the host, use an SAP CC user that is granted the adequate authorizations for creating new users
3. Create and set up a new user with the following information:
  - *Log on*: Fill with the name of the Diameter Server service user you want to create
  - *Password*: Fill with a password respecting the SAP password policy
  - *Security Profile*: Select *Service User*
  - *Roles*: Tick the *Message Charging Client* role
  - Save your modifications

Once the adequate service user has been created, you can use the [Launching the SAPinst tool \[page 115\]](#) dedicated procedure to launch the installation of the Diameter Server system. Once opened, the SAPinst tool displays a succession of screens that give you the possibility to configure your installation scenario. Use the following recommendations to fill the different screens:

1. **Welcome to SAP Convergent Charging** screen
  - Click [SAP Convergent Charging](#) > [Install](#) > [Standard System Installation](#) > [Diameter Server](#) >
  - Click the [Next](#) button
2. **Parameter Settings** screen
  - [Parameter Mode](#): Select [Custom](#)
  - Click the [Next](#) button
  - You will be prompted to log off in order to let SAPinst grant you the authorizations that are required to perform the installation. Click the [OK](#) button to log off, and reconnect to the host. SAPinst automatically restarts to continue the installation from there
3. **General SAP System Parameters** screen
  - [SAP System ID \(SAPSID\)](#): Fill with the chosen SID for the Diameter Server
  - Click the [Next](#) button
4. **Master Password** screen
  - [Password for All Users](#): Fill with a password respecting the SAP password policy
  - [Confirm](#): Re-type the chosen password
  - Click the [Next](#) button
5. **Windows Domain** screen
  - [Domain Model](#): Select [Local Domain](#)
  - Click the [Next](#) button
6. **Operating System Users** screen
  - [Password of SAP System Administrator](#): Filled by default with the password you specified in the **Master Password** screen, you can specify a different password
  - [Confirm](#): Re-type the chosen password
  - [Password of SAP System Service User](#): Filled by default with the password you specified in the **Master Password** screen, you can specify a different password
  - [Confirm](#): Re-type the chosen password
  - Click the [Next](#) button
7. **Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files** screen
  - [JCE Unlimited Strength Jurisdiction Policy Files](#): Click the [Browse](#) button and select the ZIP archive you downloaded using the [Downloading the JCE Jurisdiction Policy Files Archive \[page 25\]](#) dedicated procedure
  - Click the [Next](#) button
8. **Prerequisites Checker** screen
  - Click the [Next](#) button
9. **OpenBlox License** screen
  - [License Key](#): Fill with your license key provided by the Traffix Systems company
  - Click the [Next](#) button
10. **CA Introscope Java Agent** screen
  - [Use monitoring with CA Introscope](#): Untick the checkbox
  - Click the [Next](#) button
11. **System Landscape Directory** screen
  - [Configure System Landscape Directory](#): Untick the checkbox
  - Click the [Next](#) button
12. **SAP Convergent Charging Security** screen
  - [Security](#): Select the [Disabled](#) option

- Click the *Next* button
13. **Diameter Server Settings** screen
- *Diameter Port*: Keep the default configuration, or set a specific value
  - *Diameter Host*: Specify the full name of the machine hosting the Diameter Server. If this host has several network interfaces and thus different IP addresses, tick the *Bind on a specific interface* checkbox and specify one of these IP addresses
  - Click the *Next* button
14. **SAP Convergent Charging Core Server Connection Security** screen
- *Security*: Select the *None* option
  - Click the *Next* button
15. **SAP Convergent Charging Core Server Connection** screen
- Click the *Add* button to add a new line in the table containing the list of dispatchers available within your landscape
  - Click the *Dispatcher Message Host* column of the newly inserted row, and fill with the IP address of an available dispatcher
  - Click the *Dispatcher Message Port* column of the newly inserted row, and fill with the port number of this available dispatcher
  - *Login*: Fill with the name of the service user for the Diameter Server, created previously
  - *Password*: Fill with the password of the service user for the Diameter Server
  - Click the *Next* button
16. **Start Instances after Installation** screen
- *Start SAP Convergent Charging instances after installation*: Tick the checkbox to automatically start the instances at the end of the installation process
- i Note**

The SAP Management Console is deployed during the installation process and gives you the possibility to manage each instance of your landscape
- Click the *Next* button
17. **Host Agent and SAPOSCOL Log Directory** screen
- Click the *Next* button
18. **Windows Domain for Host Agent** screen
- *Domain Model*: Select the *Local Domain* option
  - Click the *Next* button
19. **Unpack Archives** screen
- Click the *Next* button
20. **Parameter Summary** screen
- Carefully check that all your settings have been taken into account before starting the installation. In case you need to correct one or multiple settings, tick the corresponding checkboxes and click the *Revise* button
  - If all your settings are correctly taken into account, click the *Next* button to start the installation
21. **Task Progress** screen
- This screen contains the different steps of your installation scenario, whose advancement can be followed

## 5.33 Preparing the Oracle IEC Database

### Description

According to your business requirements, your SAP Convergent Charging landscape can contain from 1 (the Core Database) to 4 databases (the Core Database, the Session Database, the BART Database and the IEC Database). This procedure explains you how to prepare your IEC Database running under an Oracle RDBMS<sup>35</sup> (Standard or Enterprise edition).

### Preliminary Notes

- In a development landscape, you can install all the SAP CC databases on the same physical host, but using different schemas. Nevertheless, SAP SE highly recommends that you install the different databases on separated hosts, in order to ease administration tasks and improve performances
- For further information about the installation of Oracle, refer to the following pages available on SAP Community:
  - <http://scn.sap.com/community/oracle>
  - <http://scn.sap.com/docs/DOC-7888>

### Prerequisites

An instance of an Oracle RDBMS must be installed and available in your landscape. This database instance must use the UTF-8 character encoding to work in conjunction with the different SAP CC software components, and the *Oracle SQL\*plus* tool must be installed to execute this procedure. Refer to your System Administrator to get information about these prerequisites relating to the SAP CC IEC Database.

### Procedure

The preparation of your SAP CC IEC Database consists in the following operations:

- Setting up some initialization parameters
  - Creating a user account and granting the adequate roles and privileges to this user
  - Executing the SQL script to create the structure of the database
1. SAP Convergent Charging requires to modify some initialization parameters of the Oracle database, located in the `init.ora` file which contains the persistent parameters used during database startup. You can use the following procedure to:

---

<sup>35</sup> Relational Database Management System

- Set the `_optim_peek_user_binds` parameter to **FALSE** in order to disable the bind peeking feature, which is not compatible with SAP CC
- Increase the maximum number of processes and sessions by setting the `processes` and `sessions` parameters to 300 multiplied by the number of databases installed on this Oracle instance, i.e. 1 (as only the IEC Database is installed on this instance)

To correctly set up the initialization parameters of your IEC Database, execute the following procedure:

```
sqlplus / as sysdba
alter system set "_optim_peek_user_binds"=false scope=spfile;
alter system set processes=300 scope=spfile;
alter system set sessions=300 scope=spfile;
shutdown immediate
startup
```

2. An Oracle user must be created and granted the adequate roles and privileges to administrate the IEC Database. Execute the following procedure by replacing `<dbuser>` by the login of the IEC Database administrator and `<dbpwd>` by its password:

```
sqlplus / as sysdba
define dbuser="<dbuser>";
define dbpwd="<dbpwd>";
create user &dbuser identified by &dbpwd;
grant CONNECT, RESOURCE TO &dbuser;
grant EXECUTE CATALOG_ROLE to &dbuser;
grant EXP_FULL_DATABASE, IMP_FULL_DATABASE to &dbuser;
grant CREATE PROCEDURE to &dbuser;
grant CREATE SESSION to &dbuser;
grant CREATE TABLESPACE, DROP TABLESPACE to &dbuser;
grant ALTER TABLESPACE to &dbuser;
grant CREATE ANY DIRECTORY to &dbuser;
grant DROP ANY DIRECTORY to &dbuser;
grant EXECUTE ON dbms_lock TO &dbuser
```

3. To create the structure of the SAP CC IEC Database, execute the following procedure:
  - Open the following folder of the installation DVD: `/DATA_UNITS/CC50_TOOLS_CONTENT_UC_OSIND`
  - Uncompress the `iec.zip` archive using the following command:

```
unzip iec.zip -d iec
```

- Open the newly created `iec/iec_sql` directory, and locate the `oracle_iecdb_create.sql` file that corresponds to the SQL script to use for creating the structure of the IEC database
- Execute the following command, replacing `<dbuser>` by the login and `<dbpwd>` by the password of the previously created user:

```
sqlplus <dbuser>/<dbpwd> oracle_iecdb_create.sql
```



## 5.34 Preparing the SQL Server IEC Database

### Description

According to your business requirements, your SAP Convergent Charging landscape can contain from 1 (the Core Database) to 4 databases (the Core Database, the Session Database, the BART Database and the IEC Database). This procedure explains you how to prepare your IEC Database running under a Microsoft SQL Server RDBMS<sup>36</sup> (Standard or Enterprise edition).

### Preliminary Notes

- In a development landscape, you can install all the SAP CC databases on the same physical host, but using different schemas. Nevertheless, SAP SE highly recommends that you install the different databases on separated hosts, in order to ease administration tasks and improve performances
- For further information about the installation of Microsoft SQL Server, refer to the following pages available on the SAP Community:
  - <http://scn.sap.com/community/sqlserver>
  - <http://scn.sap.com/docs/DOC-8286>

### Prerequisites

An instance of a SQL Server RDBMS must be installed and available in your landscape. The *SQL Server Management Studio* application must be installed to execute this procedure. Refer to your System Administrator to get information about these prerequisites relating to the SAP CC IEC Database.

### Procedure

The preparation of your SAP CC IEC Database consists in the following operations:

- Creating a SQL Server user account and granting the adequate roles on the adequate server to this user
  - Creating the IEC Database with the user as the owner
  - Executing the SQL script to create the structure of the database
1. An SQL Server user must be created for your SAP CC IEC Database, and granted the adequate roles and privileges. Execute the following procedure to create this SAP CC user:
    - Open the *SQL Server Management Studio* application

---

<sup>36</sup> Relational Database Management System

- The *Connect to Server* dialog window opens. Use the following settings:
    - *Server Name*: Select *(local)*
    - *Authentication*: Select *Windows Authentication*, in order to use your operating system user
    - Click the *Connect* button
  - Open the **View** > *Object Explorer* menu to display the *Object Explorer* and expand the *(local)* server
  - Right-click the *Security* element of the tree and open the *New / Login...* menu to display the **Login** screen
  - Fill the *General* tab with the following information:
    - *Login name*: Fill with the name of the IEC Database administrator
    - Select the *SQL Server authentication* option
    - *Password*: Fill with a password respecting the SAP password policy
    - *Confirm password*: Re-type the chosen password
    - *User must change password at next login*: Untick the checkbox
    - *Default database*: Select the *master* database
  - In the *Server Roles* tab, select the following roles:
    - *dbcreator*
    - *diskadmin*
    - *serveradmin*
  - Click the *OK* button
  - Right-click the *(local)* server and click *Disconnect*
2. Once the SQL Server user dedicated to the IEC Database has been created, it is necessary to reconnect to the server in order to create the IEC Database. Execute the following procedure:
- Open the **File** > *Connect Object Explorer...* menu or click the *Connect Object Explorer* button to re-open the *Connect to Server* dialog window. Use the following settings:
    - *Server Name*: Specify the full name of the machine hosting the database
    - *Authentication*: Select *SQL Server authentication*
    - *Login*: Fill with the previously created user
    - *Password*: Fill with the password of the previously created user
    - Click the *Connect* button
  - Right-click the *Databases* element of the tree and open the *New Database...* menu to display the **New Database** screen
  - Fill the *General* tab with the following information:
    - *Database name*: Fill with the name of the IEC Database
    - *Owner*: Fill with the name of the previously created user
  - Fill the *Options* tab with the following information:
    - *Collation*: Collation defines the way strings are managed in SQL Server databases. The IEC Database must be case-sensitive (CS) and compatible with ASCII Unicode (AS). Thus select the element that corresponds to the appropriate language, ending by the *CS\_AS* string (e.g. *Latin1\_General\_CS\_AS*)
    - *Recovery model*: Select *Full*
    - *Compatibility level*: Ensure that *SQL Server 2008 (100)* is selected
    - Click the *OK* button
3. To create the structure of the SAP CC IEC Database, execute the following procedure:
- Open the following folder of the installation DVD: `/DATA_UNITS/CC50_TOOLS_CONTENT_UC_OSIND`

- Uncompress the iec.zip archive using the following command:

```
unzip iec.zip -d iec
```

- Right-click the previously created database, and open the *New Query* menu to display the SQLQuery screen
- Open the *Edit / Insert File As Text...* menu and browse the uncompressed `iec/iec_sql` directory to select the `sqlserver_iecdb_create.sql` file that corresponds to the SQL script to use for creating the structure of the IEC Database
- Open the **▶ Query ▶ Execute ▶** menu to create the structure of the database

## 5.35 Preparing the SAP HANA IEC Database

### Description

According to your business requirements, your SAP Convergent Charging landscape can contain from 1 (the Core Database) to 4 databases (the Core Database, the Session Database, the BART Database and the IEC Database). This procedure explains you how to prepare your IEC Database running under an SAP HANA in-memory database system using a single container or a multiple containers mode.

### Preliminary Notes

- In a development landscape, you can install all the SAP CC databases on the same physical host, but using different schemas. Nevertheless, SAP SE highly recommends that you install the different databases on separated hosts, in order to ease administration tasks and improve performances
- For further information about the installation of Microsoft SQL Server, refer to the following pages available on the SAP Community:
  - <http://scn.sap.com/community/developer-center/hana>
  - <http://scn.sap.com/docs/DOC-53955>

For further information about data types, operators, functions, statements, and so on, refer to the SAP HANA SQL and System Views Reference documentation available on SAP Help Portal:<http://help.sap.com>

### Prerequisites

An SAP HANA database system must be installed and available in your landscape. The SAP HANA Studio application must be installed to execute this procedure. Refer to your System Administrator to get information about these prerequisites relating to the SAP CC IEC Database.

## Procedure

The preparation of your SAP CC IEC Database consists in the following operations:

- Declaring your system within the SAP HANA Administration Console of the *SAP HANA Studio* application
  - Creating a user account and granting the adequate roles and privileges to this user on this system
  - Disabling the expiration of the user's password
  - Executing the SQL script to create the structure of the database
1. An SAP HANA system must be created to administrate your SAP CC IEC Database. Execute the following procedure to create this system:
    - Open the *SAP HANA Studio* application
    - Open the **▶ Window ▶ Perspective ▶ Open Perspective ▶ SAP HANA Administration Console ▶** menu to display the perspective dedicated to the management of SAP HANA systems
    - Open the **▶ Window ▶ Show View ▶ Systems ▶** menu to display the view containing the list of SAP HANA systems
    - Click the *Add System* icon to open the *System* dialog window
    - Use the following settings to fill the *Specify System* screen
      - *Host Name*: Fill with the master host name
      - *Instance Number*: Fill with the instance number of your SAP HANA system
      - *Mode*: Select *Single Container* or *Multiple containers*, according to your needs
      - *Description*: Fill with a text that describes your system
      - Click the *Next* button
    - The **Connection Properties** screen opens. Select the *Authentication by database user* option and use the following settings:
      - *User Name*: Fill with the name of the SAP HANA system administrator
      - *Password*: Fill with a password respecting the SAP password policy
      - Click the *Finish* button to log on the newly declared SAP HANA system
  2. Once you are connected to the relevant SAP HANA system, it is necessary to create a user account and grant the adequate roles and privileges to this user in order to administrate the IEC Database. Execute the following procedure to create this user:
    - Expand the *Security* folder, and right-click the *Users* element to display the context menu corresponds to the name of your database
    - Right-click the *Users* element of the tree and open the "New User" menu to display the screen dedicated to the creation of new users
    - Fill the *User* tab with the following information:
      - *User Name*: Fill with the name of the IEC Database administrator
      - Select the *Password* option in the *Authentication* fieldset
      - *Password*: Fill with a password respecting the SAP password policy
      - *Confirm password*: Re-type the chosen password
    - In the *Granted Roles* subtab, click the + button to add the following roles to the user:
      - *CONTENT\_ADMIN*
      - *MODELING*
    - In the *System Privileges* subtab, click the + button to add the following privileges to the user:
      - *EXPORT*
      - *IMPORT*

- Click the *Deploy* button to finalize the creation of the user
- 3. Once the user has been created and deployed on your SAP HANA system, it is necessary to disable the expiration of its password. Execute the following procedure:
  - Right-click the previously created SAP HANA system and open the *Open SQL Console* menu to display the screen dedicated to the execution of SQL statements
  - Type the following SQL statement within the editor, considering that `<USERNAME>` corresponds to the name of your previously created user. For further information, refer to the documentation of the `ALTER USER` command available in the SAP HANA documentation:

```
ALTER USER <USERNAME> DISABLE PASSWORD LIFETIME;
```

- Click the *Execute* button to execute the SQL statement
- 4. To create the structure of the SAP CC IEC Database, execute the following procedure:
  - Open the following folder of the installation DVD:  
/DATA\_UNITS/CC50\_TOOLS\_CONTENT\_UC\_OSIND
  - Uncompress the `iec.zip` archive using the following command:

```
unzip iec.zip -d iec
```

- Right-click the previously created SAP HANA system and click the *Add System with Different User...* menu to authenticate as the IEC Database administrator
- Select the *Authentication by database user* option, and specify the following information:
  - *User Name*: Fill with the name of the IEC Database administrator, specified in Step 2
  - *Password*: Fill with the password of the IEC Database administrator, specified in Step 2
- Click the *Finish* button to create the new system
- Right-click the newly created SAP HANA system and click the *Open SQL Console* menu to display the screen dedicated to the execution of SQL statements
- Right-click the opened SQL Console and click the *Open File...* menu to open the file dialog window
- Browse the uncompressed `iec/iec_sql` directory to select the `hdb_iecdb_create.sql` file that corresponds to the SQL script to use for creating the structure of the IEC Database
- Click the *Execute* button to execute the SQL statement

## 5.36 Preparing the Oracle Session Database

### Description

According to your business requirements, your SAP Convergent Charging landscape can contain from 1 (the Core Database) to 4 databases (the Core Database, the Session Database, the BART Database and the IEC Database). This procedure explains you how to prepare your Session Database running under an Oracle RDBMS<sup>37</sup> (Standard or Enterprise edition).

<sup>37</sup> Relational Database Management System

## Preliminary Notes

- In a development landscape, you can install all the SAP CC databases on the same physical host, but using different schemas. Nevertheless, SAP SE highly recommends that you install the different databases on separated hosts, in order to ease administration tasks and improve performances
- For further information about the installation of Oracle, refer to the following pages available on SAP Community:
  - <http://scn.sap.com/community/oracle>
  - <http://scn.sap.com/docs/DOC-7888>

## Prerequisites

An instance of an Oracle RDBMS must be installed and available in your landscape. This database instance must use the UTF-8 character encoding to work in conjunction with the different SAP CC software components, and the *Oracle SQL\*plus* tool must be installed to execute this procedure. Refer to your System Administrator to get information about these prerequisites relating to the SAP CC Session Database.

## Procedure

The preparation of your SAP CC Session Database consists in the following operations:

- Setting up some initialization parameters
  - Creating a user account and granting the adequate roles and privileges to this user
  - Creating the different tablespaces
  - Executing the SQL script to create the structure of the database
1. SAP Convergent Charging requires to modify some initialization parameters of the Oracle database, located in the `init.ora` file which contains the persistent parameters used during database startup. You can use the following procedure to:
    - Set the `_optim_peek_user_binds` parameter to **FALSE** in order to disable the bind peeking feature, which is not compatible with SAP CC
    - Increase the maximum number of processes and sessions by setting the `processes` and `sessions` parameters to 300 multiplied by the number of databases installed on this Oracle instance, i.e. 1 (as only the Session Database is installed on this instance)

To correctly set up the initialization parameters of your Session Database, execute the following procedure:

```
sqlplus / as sysdba
scope=spfile;
alter system set "_optim_peek_user_binds"=false;
alter system set processes=300 scope=spfile;
alter system set sessions=300 scope=spfile;
shutdown immediate
startup
```

- An Oracle user must be created and granted the adequate roles and privileges to administrate the Session Database. Execute the following procedure by replacing `<DB_USER>` by the login of the Session Database administrator and `<DB_PASSWORD>` by its password:

```
sqlplus / as sysdba

define dbuser="<DB_USER>";
define dbpwd="<DB_PASSWORD>";
create user &dbuser identified by &dbpwd;
grant CONNECT, RESOURCE TO &dbuser;
```

- The data storage of your SAP CC Session Database, must be optimized by creating the following mandatory tablespaces:

| Tablespace name     | Description                                                  | Size (MB) |
|---------------------|--------------------------------------------------------------|-----------|
| SESSION_RATING_DATA | Tables used to store the data related to the rating sessions | 7000      |
| SESSION_RATING_INDX | Indexes used for the data related to the rating sessions     | 500       |

To create the mandatory tablespaces, execute the following procedure by replacing:

- `<TABLESPACE_NAME>` by the name of the tablespace to create
- `<FILE_LOCATION>` by the full path of the file that will contain the tablespace, located in the oradata directory
- `<SIZE>` by the recommended value associated to the tablespace, listed in the above table and using the `AUTO_EXTEND` option

```
sqlplus / as sysdba
```

And then, for each tablespace listed in the above table:

```
CREATE BIGFILE TABLESPACE <TABLESPACE_NAME> DATAFILE '<FILE_LOCATION>' SIZE <SIZE> AUTOEXTEND ON MAXSIZE UNLIMITED UNIFORM SIZE 1M LOGGING EXTENT MANAGEMENT LOCAL SEGMENT SPACE MANAGEMENT AUTO;
```

Followed by this command for Oracle 12c databases:

```
ALTER USER <DB_USER> QUOTA UNLIMITED ON <TABLESPACE_NAME>;
```

### ❁ Example

For an Oracle 12c Standard Edition RDBMS installed on a Linux host, you can use the following statement:

- To create the `SESSION_RATING_DATA` tablespace
- To give the `sapccsession` user the possibility to access this tablespace

```
CREATE BIGFILE TABLESPACE SESSION_RATING_DATA DATAFILE '/oradata/vol1/SESSION_RATING_DATA.dbf' SIZE 100M AUTOEXTEND ON MAXSIZE UNLIMITED UNIFORM SIZE 1M LOGGING EXTENT MANAGEMENT LOCAL SEGMENT SPACE MANAGEMENT AUTO;
ALTER USER sapccsession QUOTA UNLIMITED ON SESSION_RATING_DATA;
```

- To create the structure of the SAP CC Session Database, execute the following procedure:

- Open the following folder of the SAP Central Repository directory (refer to the [Document Definitions \[page 10\]](#) section for further information):

```
exe/uc/<OS>/CC_CORE_SERVER/session_sql/
```

- Locate the `oracle_enterprise_sessiondb_create.sql` file that corresponds to the SQL script to use for creating the structure of the Session Database
- Execute the following command, replacing `<DB_USER>` by the login and `<DB_PASSWORD>` by the password of the previously created user:

```
sqlplus <DB_USER>/<DB_PASSWORD> oracle_enterprise_sessiondb_create.sql
```

## 5.37 Installing an IEC (Import Export Connector) in an existing landscape

### Description

The IEC (Import Export Connector) is an SAP CC system that is used to connect the SAP CC Core Server system to external systems such as back office, legacy applications, and so on, and perform operations such as data transfer, modification or consolidation. This procedure explains you how to install and start the IEC.

#### **i** Note

The IEC can be deployed:

- On an existing host of your landscape, that already contains other systems
- On a new host within your landscape, that is dedicated to the IEC

#### **⚠** Caution

The IEC must not be deployed in a system landscape used of production purpose. You can only deploy the IEC on a host of a landscape that is used for development or test purposes.

### Prerequisites

- A Core Server system must be available within your landscape. According to your installation scenario, refer to the [Installing a Core Server on a mono-host landscape \[page 54\]](#) or the [Installing a Core Server on a multi-hosts landscape \[page 61\]](#) procedure if necessary
- A dedicated host must be set up and available within your landscape. Refer to the [Setting up a new host for a landscape \[page 70\]](#) procedure if necessary
- If you plan to use the [Export to Database](#) or [Import XCI from Database](#) components within your scenario, the IEC Database must be prepared and available. Depending of your landscape, refer to the [Preparing the](#)



SAP HANA IEC Database [page 107], Preparing the Oracle IEC Database [page 103] or the Preparing the SQL Server IEC Database [page 105] procedure if necessary

- If your IEC Database is running under an Oracle RDBMS<sup>38</sup>, the dedicated JDBC<sup>39</sup> driver must be downloaded and available on the host. Refer to the [Downloading the Oracle JDBC driver \[page 28\]](#) procedure if necessary

## Installing IEC

The IEC is delivered within a dedicated archive that must be uncompressed using the following procedure:

- Open the following folder of the installation DVD: /DATA\_UNITS/CC50\_TOOLS\_CONTENT\_UC\_OSIND
- Uncompress the iec.zip archive using the following command:

```
unzip iec.zip -d iec
```

If your landscape contains Oracle databases, copy the JAR file of the downloaded Oracle JDBC driver into the `jars` subfolder of the newly created `iec` folder.

## Launching IEC in a standalone mode

To launch the IEC in a standalone mode, execute the following procedure:

- Open the previously uncompressed `iec/bin` directory, and locate the script file that corresponds to your operating system:
  - `iec.bat` for Microsoft Windows operating systems
  - `iec.sh` for Linux and UNIX operating systems, that needs to be:
    - Granted the executable right using the following command:

```
chmod a+x iec.sh
```

- Converted into the adequate format using the following command:

```
dos2unix iec.sh
```

- Execute the launch script, using the following synopsis:

```
iec <scenario_dir>
-login <user login>
-password <visible user password>
-uri <dispatchers list>
[-rootDir <log folder>]
[-scheduled]
```

Where:

- The `scenario_dir` parameter represents the path of the scenario file to execute
- The `-login` parameter is used to specify the service user to connect with (that must be granted the Connector Administrator role)

---

<sup>38</sup> Relational Database Management System

<sup>39</sup> Java Database Connectivity

- The `-password` parameter gives the possibility to specify the password of the provided user
- The `-uri` parameter is used to specify a comma-separated list of URIs relating to dispatcher instances, each URI using the following syntax: `<PROT>://<HOST_ADDRESS>:<MSG_TCP_PORT>`, where:
  - `<PROT>` corresponds to the tcp (or tcps) communication channel
  - `<HOST_ADDRESS>` corresponds to the name or IP address (IPv4 or IPv6) of the machine hosting the concerned dispatcher
  - `<MSG_TCP_PORT>` is the port number used by the dispatcher to communicate via the Message over TCP communication channel
- The `-rootDir` parameter is an optional parameter that can be used to specify a directory (`<log folder>`) to use for saving log files. When this parameter is not set, the working directory of the user is used by default
- The `-scheduled` parameter is an optional parameter that can be used to enable the scheduler configured within the scenario to execute. When this parameter is not set, the scenario is executed only once

## Launching IEC in a remote mode

To launch the IEC in a remote mode, execute the following procedure:

- Open the previously uncompressed `iec/bin` directory, and locate the script file that corresponds to your operating system:
  - `iec.remote.bat` for Microsoft Windows operating systems
  - `iec.remote.sh` for Linux and UNIX operating systems, that needs to be:
    - Granted the executable right using the following command:

```
chmod a+x iec_remote.sh
```

- Converted into the adequate format using the following command:

```
dos2unix iec_remote.sh
```

- Execute the launch script, using the following synopsis:

```
iec_remote -uri <dispatchers list>
 [-repositoryDir <repository folder>]
 [-port <listening port>]
 [-logDir <log folder>]
```

Where:

- The `-uri` parameter is used to specify a comma-separated list of URIs relating to dispatcher instances, each URI using the following syntax: `<PROT>://<HOST_ADDRESS>:<MSG_TCP_PORT>`, where:
  - `<PROT>` corresponds to the tcp (or tcps) communication channel
  - `<HOST_ADDRESS>` corresponds to the name or IP address (IPv4 or IPv6) of the machine hosting the concerned dispatcher
  - `<MSG_TCP_PORT>` is the port number used by the dispatcher to communicate via the Message over TCP communication channel

- The `-repositoryDir` parameter is an optional parameter that can be used to specify a folder containing scenario files. When this parameter is not set, the `iec-repository parent` folder is used by default
- The `-port` parameter is an optional parameter that can be used to specify a port for listening to connections from the CAT Tool user interface. When this parameter is not set, the 9002 port number is used by default
- The `-logDir` parameter is an optional parameter that can be used to specify a directory (`<log folder>`) to use for saving log files. When this parameter is not set, the `<repository folder>/log` subfolder is used by default

## 5.38 Launching the SAPinst tool

### Description

The installation of the different SAP Convergent Charging systems relies on a java-based GUI<sup>40</sup> named SAPinst. You can use this procedure to launch SAPinst and perform both local and remote installations.

#### i Note

Remote installations are used for hosts that do not have any graphical desktop environment. When such a situation occurs, you need to both execute SAPinst:

- In a server mode on this host
- In a client mode on a machine that has a graphical desktop environment

### Preliminary Notes

For more information about SAPinst launching modes, refer to SAP Note [1238121](#).

### Prerequisites

- SAPinst is available within the Installation DVD of SAP Convergent Charging 5.0. Refer to the [Downloading the Installation DVD \[page 22\]](#) procedure if necessary
- To perform remote installations, the JCE Jurisdiction Policy Files archive must be downloaded and available. Refer to the [Downloading the JCE Jurisdiction Policy Files Archive \[page 25\]](#) procedure if necessary

---

<sup>40</sup> Graphical User Interface

## Launching SAPinst locally

To launch SAPinst on a given host that has a graphical desktop environment, execute the following procedure:

### Linux and UNIX operating systems

- Open the `/DATA_UNITS/CC50_IM_<OS>` folder of the installation DVD of SAP Convergent Charging 5.0, where `<OS>` corresponds to the version of your Linux or UNIX operating system
- Execute the following command to update the access rights of the SAPinst launch script and make it executable:

```
chmod +x sapinst
```

- Open `./sapinst`

### Microsoft Windows operating system

- Open the `/DATA_UNITS/CC50_IM_WINDOWS_X86_64` folder of the installation DVD of SAP Convergent Charging 5.0
- Open `sapinst.exe`
- If a *User Account Control* dialog window opens, click the *Yes* button

## Launching SAPinst remotely

To perform remote installations on a given host that does not have any graphical desktop environment, you must both launch SAPinst:

- In a server mode on the remote host, using a given individual user
- In a client mode on a given machine that has a graphical desktop environment, using the same individual user

Execute the following procedure:

1. Connect to the host you want to install elements on
2. Using the [Launching SAPinst locally \[page 116\]](#) procedure described above, specify the `-nogui` argument to the SAPinst launch script in order to open SAPinst in a server mode listening for connections from the SAPinstGUI tool
3. Using the [Launching SAPinst locally \[page 116\]](#) procedure described above, open `sapinstgui` instead of `sapinst`
4. When SAPinstGUI starts, use the following recommendations to fill the **Connection to Server** screen:
  - *Host*: Specify the full name or IP address of the machine where SAPinst has been launched in a server mode
  - *Port*: Keep the default configuration
  - Click the *Log on* button
5. A *Server Authentication* dialog window opens. Click the *Accept* button
6. Use the following recommendations to fill the **Authentication** screen:
  - *User*: Fill with the name of the individual user you used to launch SAPinst on the remote host
  - *Password*: Fill with the password of the specified individual user

- Click the [Next](#) button
7. Once authenticated, the **Welcome to SAP Convergent Charging** screen of SAPinst appears

## 5.39 Launching Core Tool


### Description

The SAP CC Core Tool is the main user interface of an SAP Convergent Charging system landscape. This desktop application provides a Java-based GUI<sup>41</sup> that simplifies the management of a large number of processes or operations available in SAP CC, from implementation to production phases. You can use this procedure to launch the Core Tool from any host.

### Preliminary Notes

For more information about the Core Tool user interface, refer to its [dedicated documentation](#).

### Prerequisites

- An SAP Convergent Charging Core Server system, with at least one Dispatcher instance and one Updater instance up and running, is needed to work with Core Tool. Refer to the [Installing a Core Server on a mono-host landscape \[page 54\]](#) or to the [Installing a Core Server on a multi-hosts landscape \[page 61\]](#) procedures if necessary
- The SAP JVM 8.1 must be installed on the host, and the SAPCC\_JAVA\_HOME environment variable must be set to the path of the JVM<sup>42</sup>. Refer to the [Downloading the SAP JVM \[page 26\]](#) and [Setting up the system environment variables \[page 35\]](#) procedures if necessary
- On Microsoft Windows hosts, the "Microsoft Visual C++ 2013 runtime" libraries must be installed and available. For further information, refer to SAP Note [2676219](#)

### Getting Core Tool

The Core Tool user interface is available within a ZIP archive located:

- In the Installation DVD of SAP Convergent Charging 5.0

---

<sup>41</sup> Graphical User Interface

<sup>42</sup> Java Virtual Machine

- On SAP ONE Support Launchpad

If you want to get the Core Tool from the installation DVD, take it from the following folder of the DVD: /  
DATA\_UNITS/CC50\_TOOLS\_CONTENT\_UC\_OSIND

If you want to download the latest version compatible with your Core Server version, execute the following procedure:

### → Remember

Your Core Tool version must always match your Core Server version.

1. Go to SAP ONE Support Launchpad at the following address: <https://launchpad.support.sap.com/>
2. Click the *Software Downloads* launch tile of the *System Operations and Maintenance* section
3. Click the *Support Packages and Patches* section
4. Expand the *By Alphabetical Index (A-Z)* section
5. Click the *C* letter
6. Click the *SAP Convergent Charging* element of the list
7. Click the *SAP Convergent Charging 5.0* element of the list
8. Click the *CORE TOOL 5.0* element of the list to open the *Downloads* section
9. Choose the item matching your SAP Convergent Charging 5.0 Core Server system Support Package and Patch level: CCDESKTL<SP\_LEVEL>P\_<PATCH\_LEVEL>-XXXXXXXXX.ZIP

Where:

- <SP\_LEVEL> is the SAP Convergent Charging 5.0 Core Server Support Package level
- <PATCH\_LEVEL> is the SAP Convergent Charging 5.0 Core Server Patch level

## Starting Core Tool

Launching the SAP CC Core Tool user interface consists in the following operations:

- Checking the prerequisite related to the SAPCC\_JAVA\_HOME environment variable
- Unzipping the retrieved archive that contains the Core Tool
- Executing the launch script

### Linux and UNIX operating systems

- Execute the following command to check the existence of the SAPCC\_JAVA\_HOME environment variable:

```
echo $SAPCC_JAVA_HOME
```

If you get an empty result, it means that the variable is not set. To set this variable, refer to the [Setting up the system environment variables \[page 35\]](#) procedure

- Uncompress the `core_tool.zip` archive using the following command:

```
unzip core_tool.zip -d core_tool
```

- Open the newly created `core_tool/bin` directory
- Execute the following command to update the access rights of the Core Tool launch script and make it executable:

```
chmod +x core_tool.sh
```

- Open `./core_tool.sh` and log in:
  - With credentials relating to an SAP CC user granted the adequate role within SAP CC
  - Using the name and port of a dispatcher instance that will distribute the login request to the adequate updater that will interact with the Core Tool

### Microsoft Windows operating system

- Execute the following command into a command line prompt in order to check the existence of the `SAPCC_JAVA_HOME` environment variable:

```
echo %SAPCC_JAVA_HOME%
```

If you get an empty result, it means that the variable is not set. To set this variable, refer to the [Setting up the system environment variables \[page 35\]](#) procedure

- Uncompress the `core_tool.zip` archive using the following command:

```
unzip core_tool.zip -d core_tool
```

- Open the newly created `core_tool/bin` directory
- Open `core_tool.bat` and log in:
  - With credentials relating to an SAP CC user granted the adequate role within SAP CC
  - Using the name and port of a dispatcher instance that will distribute the login request to the adequate updater that will interact with the Core Tool

#### i Note

Once installed, you can use the following procedure to modify the configuration file of the Core Tool in order to specify the location of the dedicated online helps:

- Open the `core_tool/config` directory
- Copy the `core_tool.config.sk` to a new `core_tool.config` file
- Edit the `core_tool.config` file and uncomment the last 3 lines that contain the different links related to online helps

## 5.40 Launching BART Tool

### Description


The SAP CC BART Tool is a user interface of an SAP Convergent Charging system landscape which is dedicated to the supervision of a BART Server system. This desktop application provides a Java-based GUI<sup>43</sup> that can be used to monitor the BART Server system and ease operations such as CDR acquisition, jobs administration, and so on. You can use this procedure to launch the BART Tool from any host.

<sup>43</sup> Graphical User Interface

## Preliminary Notes

For more information about the BART Tool user interface, refer to its [dedicated documentation](#).

## Prerequisites


- A BART Server system must be available within your landscape. Refer to the [Installing a BART Server in an existing landscape \[page 78\]](#) procedure if necessary
- The SAP JVM 8.1 must be installed on the host, and the SAPCC\_JAVA\_HOME environment variable must be set to the path of the JVM. Refer to the [Downloading the SAP JVM \[page 26\]](#) and [Setting up the system environment variables \[page 35\]](#) appendices if necessary
- On Microsoft Windows hosts, the "Microsoft Visual C++ 2013 runtime" libraries must be installed and available. For further information, refer to SAP Note [2676219](#) 

## Getting BART Tool

The BART Tool user interface is available within a ZIP archive located:

- In the Installation DVD of SAP Convergent Charging 5.0
- On SAP ONE Support Launchpad

If you want to get the BART Tool from the installation DVD, take it from the following folder of the DVD: / DATA\_UNITS/CC50\_TOOLS\_CONTENT\_UC\_OSIND If you want to download the latest version, execute the following procedure:

1. Go to SAP ONE Support Launchpad at the following address: <https://launchpad.support.sap.com/> 
2. Click the *Software Downloads* launch tile of the *System Operations and Maintenance* section
3. Click the *Support Packages and Patches* section
4. Expand the *By Alphabetical Index (A-Z)* section
5. Click the *C* letter
6. Click the "*SAP Convergent Charging*" element of the list
7. Click the *SAP Convergent Charging 5.0* element of the list

### i Note

Previous versions are also available but this procedure only concerns the 5.0 release

8. Click the *BART TOOL 5.0* element of the list to open the *Downloads* section
9. Choose the item matching your SAP Convergent Charging 5.0 Core Server system Support Package and Patch level: CCBARTTL<SP\_LEVEL>P\_<PATCH\_LEVEL>-XXXXXXXXX.ZIP

Where:

- <SP\_LEVEL> is the SAP Convergent Charging 5.0 Core Server Support Package level
- <PATCH\_LEVEL> is the SAP Convergent Charging 5.0 Core Server Patch level



## Starting BART Tool

Launching the SAP CC BART Tool user interface consists in the following operations:

- Checking the prerequisite related to the SAPCC\_JAVA\_HOME environment variable
- Unzipping the archive that contains the BART Tool
- Modifying the default configuration to communicate with the BART Server system
- Executing the launch script

### Linux and UNIX operating systems

- Execute the following command to check the existence of the SAPCC\_JAVA\_HOME environment variable:

```
echo $SAPCC_JAVA_HOME
```

If you get an empty result, it means that the variable is not set. To set this variable, refer to the [Setting up the system environment variables \[page 35\]](#) procedure

- Uncompress the `bart_tool.zip` archive using the following command:

```
unzip bart_tool.zip -d bart_tool
```

- Open the newly created `bart_tool/config` directory, and copy the `bart_tool.config.sk` to a new `bart_tool.config` file
- Edit the `bart_tool.config` file and modify the `BARTServerURL` parameter with the URL<sup>44</sup> of the BART Server system you want to interact with, using the following syntax: `http(s)://<BART_SERVER_HOST>:<BART_SERVER_PORT>/`, where `<BART_SERVER_HOST>` corresponds to the name or IP address (IPv4 or IPv6) of a host of your landscape where a BART Server is installed and is running
- Open the `bart_tool/bin` directory
- Execute the following command to update the access rights of the BART Tool launch script and make it executable:

```
chmod +x bart_tool.sh
```

- Open `./bart_tool.sh` and log in with an SAP CC user granted the "**Batch Rating Administrator**" role within SAP CC

### Microsoft Windows operating system

- Execute the following command into a command line prompt in order to check the existence of the SAPCC\_JAVA\_HOME environment variable:

```
echo %SAPCC_JAVA_HOME%
```

If you get an empty result, it means that the variable is not set. To set this variable, refer to the [Setting up the system environment variables \[page 35\]](#) procedure

- Uncompress the `bart_tool.zip` archive using the following command:

```
unzip bart_tool.zip -d bart_tool
```

- Open the newly created `bart_tool/config` directory, and copy the `bart_tool.config.sk` to a new `bart_tool.config` file

---

<sup>44</sup> Uniform Resource Locator

- Edit the `bart_tool.config` file and modify the `BARTServerURL` parameter with the URL of the BART Server system you want to interact with, using the following syntax: `http(s)://<BART_SERVER_HOST>:<BART_SERVER_PORT>/`, where `<BART_SERVER_HOST>` corresponds to the name or IP address (IPv4 or IPv6) of a host of your landscape where a BART Server is installed and is running
- Open the `bart_tool/bin` directory
- Open `bart_tool.bat` and log in with an SAP CC user granted the "**Batch Rating Administrator**" role within SAP CC.

### i Note

Once installed, you can use the following procedure to modify the configuration file of the BART Tool in order to specify the location of the dedicated online helps:

- Open the `bart_tool.config` file located in the `bart_tool/config` directory
- Uncomment the 2 lines that contain the different links related to online helps

## 5.41 Launching CAT Tool

### Description

The SAP CC CAT Tool is a user interface of an SAP Convergent Charging system landscape which is dedicated to the definition and management of scenarios executed within an Import/Export Connector Server system. This desktop application provides a Java-based GUI<sup>45</sup> that can be used to perform operations such as data transfers between SAP CC and external systems, data modification, Java classes execution, and so on. You can use this procedure to launch the CAT Tool from any host.

### Preliminary Notes

For more information about the CAT Tool user interface, refer to its [dedicated documentation](#).

### Prerequisites

- An IEC system must be available within your landscape. Refer to the [Installing an IEC \(Import Export Connector\) in an existing landscape \[page 112\]](#) procedure if necessary. According to the components used within your scenarios, other systems might be available within your landscape. Refer to the adequate procedures if necessary

<sup>45</sup> Graphical User Interface

- The SAP JVM 8.1 must be installed on the host, and the SAPCC\_JAVA\_HOME environment variable must be set to the path of the JVM<sup>46</sup>. Refer to the [Downloading the SAP JVM \[page 26\]](#) and [Setting up the system environment variables \[page 35\]](#) appendices if necessary
- On Microsoft Windows hosts, the "Microsoft Visual C++ 2013 runtime" libraries must be installed and available. For further information, refer to SAP Note [2676219](#).

## Getting CAT Tool

The CAT Tool user interface is available within a ZIP archive located:

- In the Installation DVD of SAP Convergent Charging 5.0
- On SAP ONE Support Launchpad

If you want to get the CAT Tool from the installation DVD, take it from the following folder of the DVD: /  
DATA\_UNITS/CC50\_TOOLS\_CONTENT\_UC\_OSIND

If you want to download the latest version, execute the following procedure:

1. Go to SAP ONE Support Launchpad at the following address: <https://launchpad.support.sap.com/>
2. Click the *Software Downloads* launch tile of the *System Operations and Maintenance* section
3. Click the *Support Packages and Patches* section
4. Expand the *By Alphabetical Index (A-Z)* section
5. Click the *C* letter
6. Click the *SAP Convergent Charging* element of the list
7. Click the *SAP Convergent Charging 5.0* element of the list

### Note

Previous versions are also available but this procedure only concerns the 5.0 release

8. Click the *CAT TOOL 5.0* element of the list to open the *Downloads* section
9. Choose the item matching your SAP Convergent Charging 5.0 Core Server system Support Package and Patch level: `CCCAT<SP_LEVEL>P_<PATCH_LEVEL>-XXXXXXXX.ZIP`  
Where:
  - `<SP_LEVEL>` is the SAP Convergent Charging 5.0 Core Server Support Package level
  - `<PATCH_LEVEL>` is the SAP Convergent Charging 5.0 Core Server Patch level

## Starting CAT Tool

Launching the SAP CC CAT Tool user interface consists in the following operations:

- Checking the prerequisite related to the SAPCC\_JAVA\_HOME environment variable
- Unzipping the archive that contains the CAT Tool
- Initializing the configuration file from the provided default one
- Executing the launch script

<sup>46</sup> Java Virtual Machine

## Linux and UNIX operating systems

- Execute the following command to check the existence of the SAPCC\_JAVA\_HOME environment variable:

```
echo $SAPCC_JAVA_HOME
```

If you get an empty result, it means that the variable is not set. To set this variable, refer to the [Setting up the system environment variables \[page 35\]](#) procedure

- Uncompress the `cat_tool.zip` archive using the following command:

```
unzip cat_tool.zip -d cat_tool
```

- Open the newly created `cat_tool/config` directory, and copy the `cat_tool.config.sk` to a new `cat_tool.config` file
- Open the `cat_tool/bin` directory
- Execute the following command to update the access rights of the CAT Tool launch script and make it executable:

```
chmod +x cat_tool.sh
```

- Open `./cat_tool.sh` and log in with an SAP CC user granted the "**Connector Administrator**" role within SAP CC

## Microsoft Windows operating system

- Execute the following command into a command line prompt in order to check the existence of the SAPCC\_JAVA\_HOME environment variable:

```
echo %SAPCC_JAVA_HOME%
```

If you get an empty result, it means that the variable is not set. To set this variable, refer to the [Setting up the system environment variables \[page 35\]](#) procedure

- Uncompress the `cat_tool.zip` archive using the following command:

```
unzip cat_tool.zip -d cat_tool
```

- Open the newly created `cat_tool/config` directory, and copy the `cat_tool.config.sk` to a new `cat_tool.config` file
- Open the `cat_tool/bin` directory
- Open `cat_tool.bat` and log in with an SAP CC user granted the "**Connector Administrator**" role within SAP CC

### i Note

Once installed, you can use the following procedure to modify the configuration file of the CAT Tool in order to specify the location of the dedicated online helps:

- Open the `cat_tool.config` file located in the `cat_tool/config` directory
- Uncomment the 2 lines that contain the different links related to online helps

## 5.42 Launching Cockpit

### Description

SAP CC Cockpit is a user interface that provides a set of web applications dedicated to the administration and supervision of an SAP CC Core Server system. Deployed and run within a Java Web Server, the Cockpit application simplifies and empowers administrators' working tasks.

#### **i** Note

It is possible to install several Cockpit applications on a given Apache Tomcat server. If you want to secure your system landscape, SAP recommends that you install an Apache Tomcat server for each Cockpit application that must have secured communications with a Core Server system. Refer to the [Securing communications with Cockpit and Tomcat Server \[page 165\]](#) section in this document and to the [SAP CC 5.0 Security Guide](#) documentation.

### Preliminary Notes

#### Microsoft Windows operating system

The Cockpit application uses a configuration file that you must set up in the home directory of the operating system user of the Apache Tomcat server. When Tomcat is installed as a Windows service, the OS<sup>47</sup> user of Tomcat might be a special Windows user such as `LocalSystem` or `LocalService`. The home directory of these particular OS users is a special folder located within the Microsoft Windows administration folder.

If you install Tomcat as a Windows service, SAP recommends that you configure this Windows service to run the Tomcat process as a dedicated local OS user created for that purpose. This local user has a regular home directory that you can use to configure the different Cockpit applications.

For more information, refer to the Apache Tomcat server documentation.

#### Oracle RDBMS

If your landscape contains one or multiple Oracle databases, you need to execute the following procedure in order to update your Apache Tomcat server with the relevant Oracle JDBC<sup>48</sup> driver:

1. Execute the [Downloading the Oracle JDBC driver \[page 28\]](#) procedure to download the relevant JAR archive
2. Copy the downloaded JAR file into the lib subfolder that is available in the root directory of the Apache Tomcat server

---

<sup>47</sup> Operating System

<sup>48</sup> Java Database Connectivity

## Prerequisites

- The SAP CC Core Server system you want to administer with the Cockpit application must be available in your SAP system landscape. Refer to the [Installing a Core Server on a mono-host landscape \[page 54\]](#) or to the [Installing a Core Server on a multi-hosts landscape \[page 61\]](#) and procedures if necessary, and the Product Availability Matrix (PAM) here: <https://support.sap.com/pam>
- You have identified the SAP system ID (SID) of the targeted Core Server system and the list of HTTP<sup>49</sup> URLs of the dispatcher instances running in the system you want to connect to
- A Tomcat server using a Java 8 JVM<sup>50</sup> must be available. For further information, use the Tomcat documentation and recommendations.
  - In terms of security requirements, the installation must comply with the recommendations of the [SAP CC 5.0 Security Guide](#) documentation. As shown on the architecture schema available in the [SAP CC Software Components \[page 12\]](#) section, the Tomcat server must also be able to communicate with:
    - The Dispatcher and Updater instances running in the Core Server system
    - The Core Database
  - In terms of sizing requirements, SAP SE recommends that you increase the size of the Tomcat heap memory (Xmx option of the JVM) to 4096M in order to manage large objects within Cockpit
  - The time zone used by the Tomcat server must be the same as the system time zone of the connected Core Server system. Refer to the [Setting up the system time zone \[page 33\]](#) procedure to ensure that the time zone is correctly configured
- You install and maintain the same version for both the Core Server system and the Cockpit application

## Getting Cockpit

The SAP CC Cockpit application is delivered within a ZIP archive. The `cockpit.zip` file is available:

- In the Installation DVD of SAP Convergent Charging 5.0
- On SAP ONE Support Launchpad on SAP Support Portal

If you want to get the Cockpit software from the installation DVD, take it from the following folder of the DVD: /  
DATA\_UNITS/CC50\_TOOLS\_CONTENT\_UC\_OSIND

If you want to download the latest version, execute the following procedure:

1. Go to SAP ONE Support Launchpad at the following address: <https://launchpad.support.sap.com/>
2. Click the *Software Downloads* launch tile of the *System Operations and Maintenance* section
3. Click the *Support Packages and Patches* section
4. Expand the *By Alphabetical Index (A-Z)* section
5. Click the *C* letter
6. Click the “*SAP Convergent Charging*” element of the list
7. Click the *SAP Convergent Charging 5.0* element of the list

### i Note

Previous versions are also available but this procedure only concerns the 5.0 release

<sup>49</sup> HyperText Transfer Protocol

<sup>50</sup> Java Virtual Machine

8. Click the [CC COCKPIT 5.0](#) element of the list to open the [Downloads](#) section
9. Choose the item matching your SAP Convergent Charging 5.0 Core Server system Support Package and Patch level: `CCCOCKPIT<SP_LEVEL>P_<PATCH_LEVEL>-XXXXXXXXX.ZIP`

Where:

- `<SP_LEVEL>` is the SAP Convergent Charging 5.0 Core Server Support Package level
- `<PATCH_LEVEL>` is the SAP Convergent Charging 5.0 Core Server Patch level

## Installing Cockpit

The previously retrieved `cockpit.zip` file contains a `cccocockpit.war` file that represents the SAP CC Cockpit application. According to the configuration of the targeted Tomcat Server, this war file:

- Can be automatically deployed if the *Automatic Application Deployment* feature of Tomcat is **enabled** (which is the case for fresh installations of Tomcat servers)
- Must be specified as a dedicated Context within the configuration file of the Tomcat server if the *Automatic Application Deployment* feature of Tomcat is **disabled**

To install the SAP CC Cockpit application, execute the following procedure:

1. Uncompress the ZIP archive, that includes the `cccocockpit.war` file
2. Rename this WAR file if you want to customize the installation. The name of the file determines the URI that is used to access the Web application and the location of the Web application in the Tomcat Server.

### ❖ Example

- `cccocockpit_<SID>.war`, where `<SID>` corresponds to the identifier of the targeted Core Server system
- `mycccocockpit.war`

3. Copy the template file (delivered in the ZIP file) named `sap_cc_cockpit_[WEB_APP_NAME].properties.sk` to initialize a configuration file for the Cockpit application to deploy
4. Suppress the `.sk` extension of the copied file
5. Rename this `sap_cc_cockpit_[WEB_APP_NAME].properties` file to `sap_cc_cockpit_<war_file_name>.properties`, where `<war_file_name>` corresponds to the name of the deployed WAR file.

### ❖ Example

Considering the second example in step 2, the file name becomes:

`sap_cc_cockpit_mycccocockpit.properties`, where `mycccocockpit` is the name of the WAR file

6. Open the newly created configuration file and modify the different parameters that are either mandatory or that necessary to fit your specific needs. For further information and recommendations, refer to the [Configuring Cockpit](#) section available in the [SAP CC 5.0 Tuning Guide](#) documentation
7. Save your modifications.
8. Move this configuration file to the home directory of the OS user running the Tomcat Server as explained in the preliminary note. Enable the **read** access right to this file for this user account
9. If the *Automatic Application Deployment* feature of Tomcat is enabled, move the WAR file to `webapps` folder of the Tomcat Server. The Cockpit application will be automatically deployed by Tomcat while running.

If the *Automatic Application Deployment* feature of Tomcat is **disabled**, set up a dedicated Context in the configuration file of the Tomcat server. For further information about the creation of a Tomcat context, refer to its dedicated documentation.

10. Verify that the deployment is done by:
  - Launching the Web application in your favorite web browser. For further information, refer to the [Starting Cockpit \[page 128\]](#) dedicated procedure afterwards
  - Searching within the Tomcat log files the following log entry: `Deployment of web application archive ..\webapps\<war_file_name> has finished, where <war_file_name>` corresponds to the name of the deployed WAR file

When the installation process is completed, you can provide your Cockpit users with the relevant URLs of the deployed user interfaces.

## Starting Cockpit

To start an SAP CC Cockpit user interface to administer a Core Server system:

1. Open a web browser
2. Navigate to the deployed Web application by entering the URL that corresponds to the SAP CC Cockpit application you want to run, using the following syntax: `http(s)://<IP_OR_DNS_ADDRESS>:<PORT_NB>/<CCCOCKPIT_URI>/`  
Where:
  - `<IP_OR_DNS_ADDRESS>` corresponds to the IP address or DNS name of the Tomcat Server host
  - `<PORT_NB>` corresponds to the dedicated communication port
  - `<CCCOCKPIT_URI>` corresponds to the path to the Web application in the Tomcat Server or to the "Context Path" of the Cockpit application
3. A sign-in window appears
4. As an SAP CC user granted the adequate roles and privileges, log on to the SAP Convergent Charging Cockpit application to access the available apps

## Upgrading Cockpit

To upgrade the Cockpit application:

1. Stop the application in the Tomcat dashboard
2. Ensure that the database is not locked
3. Create a backup of the Cockpit properties file which is available at the location determined at the step **3** of the [Installing Cockpit \[page 127\]](#) section
4. Create a backup of the Cockpit Database, depending on its configuration:
  - **In-memory data storage:** no backup is needed as the whole database is re-created each time the Cockpit application is started
  - **File-based data storage:** A backup of the Cockpit Database must be performed before upgrading the Cockpit application. The location of this file is defined in the `datasource.jdbc.uri` property available in the configuration file of the Cockpit application



5. Replace the `.war` file of your current configuration by the previously retrieved one in the `cockpit.zip` archive, as described in the [Getting Cockpit \[page 126\]](#) section. The location of the current file depends on your original installation. For further information about this location, refer to the [Installing Cockpit \[page 127\]](#) dedicated section above
6. Start the Cockpit application using the [Starting Cockpit \[page 128\]](#) dedicated section above.

### Note

A refresh of the browser cache is necessary after the update, to get a correct display. To proceed, press `CTRL + F5`.

7. If the Cockpit application does not start, refer to the [Troubleshooting \[page 129\]](#) section below

## Troubleshooting



### "Cockpit does not start"

To prevent database corruption, the Cockpit application does not re-start. A possible solution consists in retrying the upgrade operation (**File-based** data storage).

To recover from an upgrade failure due to **a full disk storage**, the following steps can be executed:

1. Make space on the disk
2. Make sure the Cockpit application is not running
3. Replace the original database file with the backup file: restore the file previously created at step **3** of the main section. The location of this file is defined in the `datasource.jdbc.uri` property available in the configuration file of the Cockpit application
4. Start the Cockpit

To recover from an upgrade failure due to **corrupted data**, the following steps can be executed:

1. Check the logs and fix the issue
2. Make sure the Cockpit application is not running
3. Replace the original database file with the backup file: restore the file previously created at step **3** of the main section. The location of this file is defined in the `datasource.jdbc.uri` property available in the configuration file of the Cockpit application
4. Start the Cockpit



### "The second re-start fails again"

To prevent database corruption, the Cockpit application does not re-start. A possible solution consists in restoring a previous Cockpit application version (**File-based** data storage).

If the second upgrade attempt fails again, the previous version of the Cockpit application can be restored with the steps below:

1. Make sure the Cockpit application is not running
2. Replace the new Cockpit WAR file with the previous one
3. Replace the original database file with the backup file
4. Start the Cockpit application

In this case, contact the SAP Support Team to get help with the Cockpit application upgrade.

## 5.43 Launching Admin+

### Description

The SAP CC Admin+ user interface is dedicated to the administration operations relating to a Core Server system, such as getting and setting parameters' values, resetting data caches, managing batch groups, and so on. You can use this procedure to launch Admin+ from any host.

### Preliminary Notes

For more information about the Admin+ user interface, refer to its [dedicated documentation](#).

### Prerequisites

A Core Server system must be available within your landscape. Refer to the [Installing a Core Server on a mono-host landscape \[page 54\]](#) or to the [Installing a Core Server on a multi-hosts landscape \[page 61\]](#) procedures if necessary

### Getting Admin+

The Admin+ user interface is available:

- In the `script` folder of each installed Dispatcher
- In the `bin` folder of the Core Tool user interface. For further information, refer to the [Launching Core Tool \[page 117\]](#) procedure if necessary

### Starting Admin+

To launch Admin+, execute the following procedure considering that:

- `<SYSTEM_ID>` corresponds to the identifier of your Core Server system
- `<DISPATCHER_INSTANCE_NUMBER>` corresponds to the number of the Dispatcher instance
- `<DISPATCHER_HOST_ADDRESS>` corresponds to the name or IP address (IPv4 or IPv6) of a host of your landscape where a Dispatcher is installed and is running
- `<DISPATCHER_PORT>` corresponds to the port used by the targeted Dispatcher

- `<CORE_TOOL_INSTALLATION_PATH>` corresponds to the location of the Core Tool user interface

## Linux and UNIX operating systems

Connect to **a host of your landscape where a Dispatcher is installed and is running**, and execute the following commands:

```
cd /usr/sap/<SYSTEM_ID>/CCD<DISPATCHER_INSTANCE_NUMBER>/script
./admin+.sh
```

Or connect to **a host where a Core Tool is installed**, and execute the following commands:

```
cd <CORE_TOOL_INSTALLATION_PATH>/bin
./admin+ <DISPATCHER_HOST_ADDRESS> <DISPATCHER_PORT>
```

## Microsoft Windows operating system

Connect to **a host of your landscape where a Dispatcher is installed and is running**, and execute the following commands into a command line prompt:

```
cd C:\usr\sap\<SYSTEM_ID>\CCD<DISPATCHER_INSTANCE_NUMBER>\script
admin+
```

Or connect to **a host where a Core Tool is installed**, and execute the following commands into a command line prompt:

```
cd <CORE_TOOL_INSTALLATION_PATH>/bin
admin+ <DISPATCHER_HOST_ADDRESS> <DISPATCHER_PORT>
```

# 5.44 Launching BART+

## Description

The SAP CC BART+ user interface is dedicated to the administration operations relating to a BART Server system, such as getting and setting parameters' values, monitoring the batch acquisition sessions, and so on. You can use this procedure to launch BART+ from any host.

## Preliminary Notes

For more information about the BART+ user interface, refer to its [dedicated documentation](#).

## Prerequisites

A BART Server system must be available within your landscape. Refer to the [Installing a BART Server in an existing landscape \[page 78\]](#) procedure if necessary.

## Getting BART+

The BART+ user interface is available:

- In the `script` folder of each installed BART Server system
- In the `bin` folder of the BART Tool user interface. For further information, refer to the [Launching BART Tool \[page 119\]](#) procedure if necessary

## Starting BART+

To launch BART+, execute the following procedure considering that:

- `<SYSTEM_ID>` corresponds to the identifier of your BART Server system
- `<BART_INSTANCE_NUMBER>` corresponds to the number of the BART Server instance
- `<BART_SERVER_HOST_ADDRESS>` corresponds to the name or IP address (IPv4 or IPv6) of a host of your landscape where a BART Server system is installed and is running
- `<BART_SERVER_PORT>` corresponds to the port used by the targeted BART Server
- `<BART_TOOL_INSTALLATION_PATH>` corresponds to the location of the BART Tool user interface

### Linux and UNIX operating systems

Connect to **a host of your landscape where a BART Server is installed and is running**, and execute the following commands:

```
cd /usr/sap/<SYSTEM_ID>/CAB<BART_INSTANCE_NUMBER>/script
./bart+.sh
```

Or connect to **a host where a BART Tool is installed**, and execute the following commands:

```
cd <BART_TOOL_INSTALLATION_PATH>/bin
./bart+ <BART_SERVER_HOST_ADDRESS> <BART_SERVER_PORT>
```

### Microsoft Windows operating system

Connect to **a host of your landscape where a BART Server is installed and is running**, and execute the following commands into a command line prompt:

```
cd C:\usr\sap\<SYSTEM_ID>\CAB<BART_SERVER_INSTANCE_NUMBER>\script
bart+
```

Or connect to **a host where a BART Tool is installed**, and execute the following commands into a command line prompt:

```
cd <BART_TOOL_INSTALLATION_PATH>/bin
bart+ <BART_SERVER_HOST_ADDRESS> <BART_SERVER_PORT>
```

## 5.45 Launching Setup Tool

### Description

The SAP CC Setup Tool is a user interface of an SAP Convergent Charging system landscape which is dedicated to configuration and maintenance operations of a Core Server system. You can use this procedure to launch the Setup Tool from any host.

### Preliminary Notes

For more information about the Setup Tool user interface, refer to its [dedicated documentation](#).

### Prerequisites

A Core Server system must be available within your landscape. Refer to the [Installing a Core Server on a mono-host landscape \[page 54\]](#) or to the [Installing a Core Server on a multi-hosts landscape \[page 61\]](#) procedures if necessary.

### Getting Setup Tool

The Setup Tool user interface is available in the `script` folder of each installed Dispatcher.

### Starting Setup Tool

The Setup Tool user interface is a command-line application that has the following partial synopsis:

```
setup <command> [<arguments>]
[-login=<user login>]
[-password=<visible user password>]
```

Where:

- The `command` parameter is used to specify the operation to perform, such as:
  - `certentry list/import/export/...` that are used to manage client certificates for secured landscapes
  - `keyentry list/(un)link/import/export/...` that are used to manage key entries for secured landscapes
  - `cif delete/import/export`, that are used to manage the CIF configuration
  - `instancemap delete/import/export`, that are used to manage the instance map
  - `license import/export/...`, that are used to manage the licensing of your landscape
  - And so on
- The `-login` optional parameter is used to specify the individual user to connect with (that must be granted the Administrator role, except for the `help` and `about` commands). If you do not use the `-login` option, you will be prompted to enter this username
- The `-password` optional parameter gives the possibility to specify the password of the provided user. Please note that the specified password is displayed on your screen, and thus visible. If you do not use the `-password` option, you will be prompted to enter the password, which is a safer method to authenticate

### i Note

To get the whole synopsis of the Setup Tool user interface, consult [its documentation](#).

To launch Setup Tool, execute the following procedure considering that:

- `<SYSTEM_ID>` corresponds to the identifier of your Core Server system
- `<DISPATCHER_INSTANCE_NUMBER>` corresponds to the number of the dispatcher instance
- `<SYNOPSIS>` corresponds to the commands and options to execute

## Linux and UNIX operating systems

Connect to **a host of your landscape where a Dispatcher is installed and is running**, and execute the following commands:

```
cd /usr/sap/<SYSTEM_ID>/CCD<DISPATCHER_INSTANCE_NUMBER>/script
./setup.sh <SYNOPSIS>
```

## Microsoft Windows operating system

Connect to **a host of your landscape where a Dispatcher is installed and is running**, and execute the following commands into a command line prompt:

```
cd C:\usr\sap\<SYSTEM_ID>\CCD<DISPATCHER_INSTANCE_NUMBER>\script
setup <SYNOPSIS>
```

## 5.46 Launching BART Setup Tool

### Description

The SAP CC BART Setup Tool is a user interface of an SAP Convergent Charging system landscape which is dedicated to the management of security settings for securing the communication channels used by the BART Server system. You can use this procedure to launch the BART Setup Tool from any host.

### Preliminary Notes

For more information about the BART Setup Tool user interface, refer to its [dedicated documentation](#).

### Prerequisites

A BART Server system must be available within your landscape. Refer to the procedure [Installing a BART Server in an existing landscape \[page 78\]](#) if necessary.

### Getting BART Setup Tool

The BART Setup Tool user interface is available in the `script` folder of each installed BART Server.

### Starting BART Setup Tool

The BART Setup Tool user interface is a command-line application that has the following partial synopsis:

```
setup <command> [<arguments>]
[-login=<user login>]
[-password=<visible user password>]
```

Where:

- The `command` parameter is used to specify the operation to perform, such as:
  - `certentry list/import/export/...` that are used to manage client certificates for secured landscapes
  - `keyentry list/(un)link/import/export/...` that are used to manage key entries for secured landscapes
  - And so on

- The `-login` optional parameter is used to specify the individual user to connect with (that must be granted the Administrator role, except for the `help` and `about` commands). If you do not use the `-login` option, you will be prompted to enter this username
- The `-password` optional parameter gives the possibility to specify the password of the provided user. Please note that the specified password is displayed on your screen, and thus visible. If you do not use the `-password` option, you will be prompted to enter the password, which is a safer method to authenticate

### i Note

To get the whole synopsis of the BART Setup Tool user interface, consult its [documentation](#).

To launch BART Setup Tool, execute the following procedure considering that:

- `<SYSTEM_ID>` corresponds to the identifier of your BART Server system
- `<BART_INSTANCE_NUMBER>` corresponds to the number of the BART Server instance
- `<SYNOPSIS>` corresponds to the commands and options to execute

### Linux and UNIX operating systems

Connect to **a host of your landscape where a Dispatcher is installed and is running**, and execute the following commands:

```
cd /usr/sap/<SYSTEM_ID>/CAB<BART_INSTANCE_NUMBER>/script
./setup.sh <SYNOPSIS>
```

### Microsoft Windows operating system

Connect to **a host of your landscape where a BART Server is installed and is running**, and execute the following commands into a command line prompt:

```
cd C:\usr\sap\<SYSTEM_ID>\CAB<BART_INSTANCE_NUMBER>\script
setup <SYNOPSIS>
```

## 5.47 Launching Config Tool

### Description

The SAP CC Config Tool is a user interface of an SAP Convergent Charging system landscape which is dedicated to configuration operations of a Core Server system. You can use this procedure to launch the Config Tool from any host.

### Preliminary Notes

For more information about the Config Tool user interface, refer to its [dedicated documentation](#).



## Prerequisites

A Core Server system must be available within your landscape. Refer to the [Installing a Core Server on a mono-host landscape \[page 54\]](#) or to the [Installing a Core Server on a multi-hosts landscape \[page 61\]](#) procedures if necessary.

## Getting Config Tool

The Config Tool user interface is available in the `script` folder of each installed Dispatcher.

## Starting Config Tool

The Config Tool user interface is a command-line application that has the following partial synopsis:

```
config <command> [<arguments>]
[-login=<user login>]
[-password=<visible user password>]
```

Where:

- The `-login` optional parameter is used to specify the individual user to connect with (that must be granted the Administrator role, except for the `help` and `about` commands). If you do not use the `-login` option, you will be prompted to enter this username
- The `-password` optional parameter gives the possibility to specify the password of the provided user. Please note that the specified password is displayed on your screen, and thus visible. If you do not use the `-password` option, you will be prompted to enter the password, which is a safer method to authenticate
- The `command` parameter is used to specify the operation to perform

### i Note

To get the whole synopsis of the Config Tool user interface, consult its documentation.

To launch Config Tool, execute the following procedure considering that:

- `<SYSTEM_ID>` corresponds to the identifier of your Core Server system
- `<DISPATCHER_INSTANCE_NUMBER>` corresponds to the number of the dispatcher instance
- `<SYNOPSIS>` corresponds to the commands and options to execute

## Linux and UNIX operating systems

Connect to **a host of your landscape where a Dispatcher is installed and is running**, and execute the following commands:

```
cd /usr/sap/<SYSTEM_ID>/CCD<DISPATCHER_INSTANCE_NUMBER>/script
./config.sh <SYNOPSIS>
```

## Microsoft Windows operating system

Connect to **a host of your landscape where a Dispatcher is installed and is running**, and execute the following commands into a command line prompt:

```
cd C:\usr\sap\<SYSTEM_ID>\CCD<DISPATCHER_INSTANCE_NUMBER>\script
config <SYNOPSIS>
```

## 5.48 Securing a landscape

### Description


The communication between the different systems of an SAP Convergent Charging landscape relies on different communication channels that can be secured to fit security requirements. You can consider this procedure as an entry point for implementing a secured landscape, within which:

- Communications channels used by clients and servers can be secured using either a "dual" or a "oneway" mode
- SAP CC server systems can be configured to specify a list of protocols and cipher suites that can be enabled for encrypted communications using SSL/TLS

This procedure contains:

- A common procedure that you can use to generate the securing materials required within the different procedures relating to each SAP CC server system
- Cross-references to procedures dedicated to the securing of:
  - The Core Server system
  - The BART Server system
  - The Diameter Server system
  - The Cockpit application and its Tomcat Server system

### Preliminary Notes

- For more information about the different communication channels, refer to the [SAP CC 5.0 Security Guide](#) documentation
- The procedure used to secure your landscape can be adapted to fit specific security needs. In case you need to adapt the securing procedure and implement another securing policy for your landscape, SAP SE highly recommends that you to refer to your technology consultants and security experts
- This procedure contains commands which refer to command-line applications:
  - Delivered with the operating system
  - Provided within the SAP CC solution
  - Available for download on dedicated websites, where we invite you to get the latest version (such as the openssl tool, available at the following location: <http://www.openssl.org/> )

## Common procedure for generating the securing materials

The securing procedure relies on certificates and private keys, which are used to secure the different communication channels used by the different SAP CC systems. Execute the following procedure to create:

- A private key
- A X.509 v3 digital certificate, named `certificate.der` and DER encoded
- A keystore stored in a PKCS#12 archive file named `keystore.p12` and containing the created private certificate and private key

### 1. Generating a private key

To generate a private key named `key.pem`, use the following command:

```
openssl genrsa -out key.pem <KEY_SIZE>
```

Where the `<KEY_SIZE>` parameter represents the size (in bits) of the private key you want to generate.

Possible values are: 1024, 2048 or 4096

### 2. Creating a X.509 v3 digital certificate

#### Note

As far as certificates related to client applications are concerned, you can use X.509 v1 certificates, which do not require any configuration file. In this case, skip the `-config` argument of the `openssl` command below.

The creation of a X.509 v3 digital certificate is based upon a configuration file taken into account by the `openssl` command. This configuration file contains a property named `subjectAltName`, which gives the possibility to provide an exhaustive list of hostnames and/or IP addresses (IPv4 or IPv6) used to identify the host to trust and connect to. This property uses the following format:

```
IP:{$localHostAddress},DNS:{$localHostName},DNS:{$localCanonicalHostName}
```

You can use a generic domain name (e.g. `DNS:*.mydomain.com`) in order to easily add possible new hosts, but SAP SE highly recommends you to specify a list of IP addresses (IPv4 or IPv6) and/or hostnames (e.g. `IP:192.168.0.1, IP: fe80::192.168.0.2, DNS:host1`).

To create a configuration file named `openssl.config`, use the following text content (adapting the `subjectAltName` property to your own configuration):

```
[req]
distinguished_name = req_distinguished_name
x509_extensions = v3_req
[req_distinguished_name]
[v3_req]
subjectAltName = DNS:*.mydomain.com
```

#### Caution

When a condensed IPv6 address is used in the `subjectAltName` property, the `openssl` tool automatically records the complete address. This complete address corresponds to the address which must be provided when connecting to a given service secured with this certificate.

In addition, SAP SE also recommends you to use a pretty name when filling the common name, in order to distinguish each generated certificate. This common name contains information related to the trusting authority, i.e. the host to trust and connect to.

To generate the `certificate.pem` certificate, type the following command:

```
openssl req -new -x509 -key key.pem -out certificate.pem -days 365 -config
openssl.config -subj "/CN=<PRETTY_NAME>"
```

### 3. Creating the keystore used to store the certificate and its private key

To create a keystore named **keystore.p12**, secured with a passphrase and containing the previously created private key and certificate, type the following command:

```
openssl pkcs12 -export -in certificate.pem -inkey key.pem -out keystore.p12 -
passout pass:<KEYSTORE_PASSPHRASE>
```

### 4. Deleting the private key

For security reasons, delete the previously created private key using the following command:

- For Linux and UNIX OS:

```
rm key.pem
```

- For Microsoft Windows OS:

```
del key.pem
```

### 5. Modifying the certificate's format from PEM to DER

To convert the certificate from a PEM format to a DER one, type the following command:

```
openssl x509 -in certificate.pem -out certificate.der -outform der
```

## Securing communications with the Core Server system

Securing the Core Server system consists in the following operations:

- Specifying a list of protocols and cipher suites that can be enabled for encrypted communications using SSL/TLS
  - Securing the communications channels relating to the Core Server system
1. To specify a list of protocols and cipher suites that can be enabled for encrypted communications using SSL/TLS, you must modify the `TLS_PROTOCOLS` and `TLS_CIPHER_SUITES` parameters. Execute the following procedure to modify these system parameters:
    - Launch the Admin+ user interface using the [Launching Admin+ \[page 130\]](#) dedicated procedure
    - Execute the following commands within Admin+ in order to identify as the administrator of the Core Server system and modify the adequate parameters:

```
user <SAPCC_SYSADM_USERNAME> <SAPCC_SYSADM_PASSWORD>
set TLS_PROTOCOLS <TLS_PROTOCOLS> persistent <TARGET_INSTANCES>
set TLS_CIPHER_SUITES <TLS_TLS_CIPHER_SUITES> persistent <TARGET_INSTANCES>
```

Where:

- `<SAPCC_SYSADM_USERNAME>` and `<SAPCC_SYSADM_PASSWORD>` correspond to the name and password of the user granted with the Administrator role
- `<TLS_PROTOCOLS>` corresponds to the list of protocols to enable
- `<TLS_CIPHER_SUITES>` corresponds to the list of cipher suites to enable
- `<TARGET_INSTANCES>` corresponds to the concerned instances

## i Note

For further information about the `TLS_PROTOCOLS` and `TLS_CIPHER_SUITES` parameters, refer to the [SAP CC 5.0 System Parameter Reference](#) documentation.

2. To secure the communication channels relating to the Core Server system using a "dual" or a "oneway" mode, refer to the [Securing communications with the Core Server system \[page 142\]](#) dedicated procedure

## Securing communications with the BART Server system

Securing the BART Server system consists in the following operations:

- Specifying a list of protocols and cipher suites that can be enabled for encrypted communications using SSL/TLS
  - Securing the communications channels relating to the BART Server system
1. To specify a list of protocols and cipher suites that can be enabled for encrypted communications using SSL/TLS, you must modify the configuration file of the BART Server system. Execute the following procedure to modify these system parameters:
    - Open the `bart.config` file
    - Declare the protocols and cipher suites to enable by modifying the following parameters accordingly:

```
tls.protocols=<TLS_PROTOCOLS>
tls.cipher_suites=<TLS_CIPHER_SUITES>
```

Where:

- `<TLS_PROTOCOLS>` corresponds to the list of protocols to enable
  - `<TLS_CIPHER_SUITES>` corresponds to the list of cipher suites to enable
2. To secure the communication channels relating to the BART Server system using a "dual" or a "oneway" mode, refer to the [Securing communications with the BART Server system \[page 155\]](#) dedicated procedure

## Securing communications with the Diameter Server system

Securing the Diameter Server system consists in the following operations:

- Specifying a list of protocols and cipher suites that can be enabled for encrypted communications using SSL/TLS
  - Securing the communications channels relating to the Diameter Server system
1. To specify a list of protocols and cipher suites that can be enabled for encrypted communications using SSL/TLS, you must modify the configuration file of the Diameter Server system. Execute the following procedure to modify these system parameters:
    - Open the `serverConfig.xml` file
    - Declare the protocols and cipher suites to enable by modifying the following parameters accordingly:

```
<entry key="TLSEnabledProtocols" value="<TLS_PROTOCOLS>"/>
<entry key="TLSEnabledCipherSuites" value="<TLS_CIPHER_SUITES>"/>
```

Where:

- <TLS\_PROTOCOLS> corresponds to the list of protocols to enable
  - <TLS\_CIPHER\_SUITES> corresponds to the list of cipher suites to enable
2. To secure the communication channels relating to the Diameter Server system using a "dual" or a "oneway" mode, refer to the [Securing communications with the Diameter Server system \[page 162\]](#) dedicated procedure

## Securing communications with the Cockpit application and its Tomcat Server system

Securing the Cockpit application and its Apache Tomcat Server consists in:

- Securing the communications between the Web browsers and the Tomcat Server system that runs the Cockpit application
- Securing the communications between the Tomcat Server system and the Core Server system as an external client application

To secure the communication channels using a "dual" or a "oneway" mode, refer to the [Securing communications with Cockpit and Tomcat Server \[page 165\]](#) dedicated procedure.

## 5.49 Securing communications with the Core Server system

### Description

The communications relating to the Core Server system mostly concern the Core Server instances, which:

- Communicate together during internal operations
- Can be contacted by client applications such as SAP CC user interfaces or other systems (SAP CC systems and/or third-party systems)
- Are connected with the Core Database

Internal communications between the instances rely on the Packets over TCP/IP communication channel. The communication channels which are used for communications with clients applications depend on the concerned instance. The following table summarizes these interactions:

	(master) Dispatcher	(active) Updater	Guider/Rater	Bulkloader	Core Database
<b>Core Server</b>					
(master) Dispatcher	-	Packets over TCP/IP	Packets over TCP/IP	Packets over TCP/IP	JDBC

	<b>(master) Dispatcher</b>	<b>(active) Updater</b>	<b>Guider/Rater</b>	<b>Bulkloader</b>	<b>Core Database</b>
(slave) Dispatcher	Packets over TCP/IP	-	-	-	JDBC
(active) Updater	Packets over TCP/IP + XML over HTTP <sup>51</sup>	SOAP over HTTP <sup>52</sup>	-	-	JDBC
Guider/Rater	Packets over TCP/IP	-	-	-	JDBC
Bulkloader	Packets over TCP/IP	-	-	-	JDBC
<b>Client applications</b>					
Core Tool	XML over HTTP	XML over HTTP	-	-	-
Setup Tool	-	-	-	-	JDBC
Config Tool	-	-	-	-	JDBC
Admin+	XML over HTTP	-	-	-	-
Cockpit	XML over HTTP				
HTTP Client	XML over HTTP	XML over HTTP	-	-	-
<b>Third-party systems</b>					
Client application	Packets over TCP/IP	XML over HTTP	-	RFC over TCP/IP	-
Mediation	Packets over TCP/IP	-	-	-	-
SAP CI	SOAP over HTTP + RFC over TCP/IP	-	-	RFC over TCP/IP	-
SAP CRM	-	SOAP over HTTP	-	-	-
SAP SLD	XML over HTTP	-	-	-	-
SAP SMD	XML over HTTP	-	-	-	-
SAP CC CTS+ plugin	XML over HTTP	SOAP over HTTP	-	-	-

The securing of communications performed on the Packets over TCP/IP, XML over HTTP and SOAP over HTTP communications channels relies on dedicated properties located in the static instance map. Internal communications between instances can be secured using the `InternalSecure` property of the static instance map. The securing policy of external communications relies on different properties, according to the concerned communication channel. The following table displays the correspondence between communication channels and related securing properties, with the possible values for each concerned property:

<sup>51</sup>

<sup>52</sup>

When using the Catalog Transport feature of SAP Convergent Charging

When using the Catalog Transport feature of SAP Convergent Charging

Communication channel	Property	Dispatcher			Updater		
		off	oneway	dual	off	oneway	dual
Packets over TCP/IP	InternalSecure	■	□	■	□	□	□
	ExternalSecure	■	■	■	□	□	□
XML over HTTP	HttpSecure	■	■	■	■	■	■
SOAP over HTTP	WsSecure	■	■	■	■	■	■

■ Available, □ Not Available

The securing of communications performed on the RFC over TCP/IP communication channel and on the JDBC protocol relies on parameters set in associated parameters files or command-line arguments. For further information about these protocols, refer to the [SAP CC 5.0 Security Guide](#) documentation.

The securing procedure consists in securing both the Core Server system and its client applications, which corresponds to the "dual" mode. The operations described afterwards give you the possibility to:

- Secure the internal communications between the different instances, which consists in:
  - Generating a certificate related to the Core Server
  - Importing this certificate into the keystore of the Core Server
  - Linking this certificate to all the SAP CC instances, for the "internal" communication channel
- Secure the communications between the Core Server instances and a client application, considered as external communications and consisting in:
  - Generating a certificate related to the Core Server
  - Generating a certificate related to the client application
  - Importing the Core Server certificate into the keystore of the Core Server
  - Linking the Core Server certificate to all the concerned instances, for the adequate communication channels
  - Importing the Core Server certificate into the truststore of the JVM<sup>53</sup> used by the client application, so that this application can trust the Core Server
  - Updating the keystore of the client application, by declaring the client certificate towards the application
  - Importing the client certificate into the truststore of Core Server, so that the Core Server system can trust the client application
  - Linking the client certificate to all the concerned instances, for all the communication channels
- Secure the communications with the Core Database, that rely on the JDBC<sup>54</sup> protocol
- Secure the communications between the Core Server and other systems such as SAP CI or SAP CRM, that rely on the RFC over TCP/IP communication channel
- Enable this defined securing policy, which consists in:
  - Modifying the instance map
  - Restarting the Core Server, which finally runs in a dual authentication mode

<sup>53</sup> Java Virtual Machine

<sup>54</sup> Java Database Connectivity



## Preliminary Notes

- Some of the procedures described afterwards refer to the [Common procedure for generating the securing materials \[page 139\]](#) that is available in the [Securing a landscape \[page 138\]](#) procedure. Refer to it when necessary
- If your client application is not a java application, you must adapt some of the following procedures to fit the technology of your application

## Prerequisites

- The `setup` command specified in the following operations refers to the Setup Tool user interface. Refer to the [Launching Setup Tool \[page 133\]](#) procedure if necessary
- The `config` command specified in the following operations refers to the Config Tool user interface. Refer to the [Launching Config Tool \[page 136\]](#) procedure if necessary

## Securing the Core Server internal communications

Considering a keystore named `keystore.int.p12`, generated using the common procedure and containing a private certificate with its private key, use the following procedure to:

- Import the certificate and its private key into the keystore of Core Server
  - Configure all the instances of the Core Server system so that they use this private key when communicating one with another on the "internal" communication channel
- 1. Generating a certificate and its private key for the Core Server system**  
Use the common procedure to generate a keystore named `keystore.int.p12` and containing a certificate with its private key.
  - 2. Importing the certificate and its private key into the keystore of the Core Server system**  
To import the content of the `keystore.int.p12` keystore into the SAP CC keystore under the `InternalAlias` alias, type the following command:

```
setup keyentry import_p12 InternalAlias keystore.int.p12
```

### i Note

As far as certificates related to client applications are concerned, you can use X.509 v1 certificates, which do not require any configuration file. In this case, skip the `-config` argument of the `openssl` command below.

- 3. Linking the imported certificate**  
To specify that the Core Server system must use the imported certificate for internal communications between the different instances, type the following command:

```
setup keyentry link InternalAlias all internal
```

## Securing the Core Server external communications

To secure the communications between the Core Server system and a client application, execute the following operations in order to:

- Use the common procedure in order to generate a keystore:
  - Related to the Core Server
  - Named `keystore.ext.p12`
  - Containing a `certificate.ext.der` certificate and its private key
- Use the common procedure in order to generate a keystore:
  - Related to the client application
  - Named `keystore.cli.p12`
  - Containing a `certificate.cli.der` certificate and its private key
- Import the content of the `keystore.ext.p12` keystore into the keystore of the Core Server, using the `ExternalAlias` alias
- Link the `ExternalAlias` certificate to all the instances, for the "http", "ws" and "external" communication channels
- Import the `certificate.ext.der` certificate of the Core Server into the truststore of the client application
- Enable the `keystore.cli.p12` keystore on the client application side, by declaring this keystore on the client application side
- Import the `certificate.cli.der` certificate into the truststore of the Core Server, using the `ClientAlias` alias
- Link the `ClientAlias` certificate to all the instances, for all the communication channels

### 1. Generating a certificate and its private key for the Core Server

Use the common procedure to generate a keystore named `keystore.ext.p12` and containing a certificate with its private key.

### 2. Generating a certificate related to a client application

Use the common procedure to generate a keystore named `keystore.cli.p12` and containing a certificate with its private key.

#### i Note

It is necessary to remember the passphrase of the keystore file in order to execute the step 6 described below.

### 3. Importing the certificate of Core Server (and its private key) into the keystore of the Core Server system

To import the content of the `keystore.ext.p12` keystore into the keystore of the Core Server, under the `ExternalAlias` alias, type the following command:

```
setup keyentry import_p12 ExternalAlias keystore.ext.p12
```

#### i Note

You will be prompted to type the passphrase of the keystore file which contains the certificate and private key to import.

### 4. Linking the imported certificate

To specify that the Core Server must use the imported certificate for external communications relying on the "http", "ws" and "external" communication channels, type the following command:

```
setup keyentry link ExternalAlias all "http,ws,external"
```

#### 5. Importing the certificate of Core Server into the truststore of the client application

To give the possibility for a client application to trust the Core Server, it is necessary to import the certificate of the Core Server into the truststore used by this client application. To import the `certificate.ext.der` certificate into a java keystore named `keystore.cli.jks`, type the following command:

```
keytool -importcert -file certificate.ext.der -keystore keystore.cli.jks -
noprompt
```

#### i Note

You will be prompted to type a passphrase for the Java keystore file which will contain the certificate to import. It is necessary to remember this passphrase in order to execute the following command.

The client application must then be configured to use the above created keystore as a truststore. To make the client application use the `keystore.cli.jks` keystore as its default truststore, add the following options to the command-line of the application:

```
-Djavax.net.ssl.trustStore=<Path_of_the_java_keystore>
-Djavax.net.ssl.trustStorePassword=<Passphrase_of_the_java_keystore>
```

If your client application is not a Java application, you must adapt this step to fit the technology of your application.

#### 6. Enabling the client keystore on the client application side

The client application must take into account its certificate in order to use it when communicating in a secured mode. To enable this certificate, it is necessary to declare the related keystore in the command-line of the application. To declare the `keystore.cli.p12` client keystore, add the following options to the command-line of the application:

```
-Djavax.net.ssl.keyStoreType=pkcs12
-Djavax.net.ssl.keyStore=<Path_of_the_client_keystore>
-Djavax.net.ssl.keyStorePassword=<Passphrase_of_the_client_keystore>
```

#### 7. Importing the content of the client keystore into the truststore of the Core Server

To import the content of the `keystore.cli.p12` keystore into the SAP CC truststore under the `ClientAlias` alias, type the following command:

```
setup certentry import ClientAlias certificate.cli.der
```

#### 8. Linking the imported certificate

To specify that the Core Server must use the imported certificate when communicating with a client application, whatever the communication channel is, type the following command:

```
setup certentry link ClientAlias all all
```

## Securing the Core Server JDBC connections

To secure the communications between the Core Server and the Core Database, it is necessary to execute the following operations:

- Execute the securing procedures related to your database provider
- Update the configuration of the Core Server to modify the connection URL with the adequate parameters

### 1. Executing the securing procedures related to your database provider

Each database provider delivers specific procedures to encrypt communications with their databases management system. Refer to the documentation of your database provider to create the different materials secure the communications with the Core Database.

### 2. Updating the configuration of the Core Server

The Core Server supports the following parameters and associated values to secure the communications relying on the JDBC protocol:

Database Provider	Parameter	Value
SAP HANA	<code>encrypt</code>	True
	<code>validateCertificate</code>	False <sup>55</sup>
SAP ASE	<code>ENABLE_SSL</code>	True
Oracle	N/A	N/A
Microsoft SQL Server	<code>encrypt</code>	True
IBM DB2	<code>trustServerCertificate</code>	False

To secure the communications relying on the JDBC protocol, it is necessary to update the following parameters, both in the `boot.config` file (located in the `boot` directory of the SAP Profile Folder) and in the Core Database:

- `SQLHELPER_JDBC_URIx`, where `x` can be empty when no HA is required, or a value between 1 and 12 for the Oracle and DB2 database providers (depending on the HA configuration)
- `SQLHELPER_JDBC_PROPERTIES`, which corresponds to a CSV string used to specify the additional parameters to use when connecting to the database

To update the `SQLHELPER_JDBC_URIx` parameter into the `boot.config` file, open the configuration file and declare the adequate parameters to secure the communications with the Core Database, e.g.:

Database Provider	Value
SAP HANA	<code>jdbc:sap:&lt;server&gt;:&lt;port&gt;</code>
SAP ASE	<code>jdbc:sybase:Tds:&lt;server&gt;:&lt;port&gt;/&lt;database_name&gt;</code>
Oracle	<code>jdbc:oracle:thin:@//&lt;server&gt;:&lt;port&gt;/&lt;ServiceName&gt;</code>
	<code>jdbc:oracle:thin:@&lt;server&gt;:&lt;port&gt;:&lt;SID&gt;</code>

<sup>55</sup> When this value is set to **true**, it is necessary to specify additional parameters to the `SQLHELPER_JDBC_PROPERTIES` parameter, depending on the securing mode. See below for further information about these parameters.

Database Provider	Value
Microsoft SQL Server	<code>jdbc:sqlserver:// &lt;server&gt;:&lt;port&gt;;DatabaseName=&lt;database_ name&gt;</code>
IBM DB2	<code>jdbc:db2://&lt;server&gt;:&lt;port&gt;/ &lt;instance_name&gt;;currentSchema=&lt;schema_n ame&gt;;</code>

To update the `SQLHELPER_JDBC_PROPERTIES` parameter into the `boot.config` file, open it in a text editor and declare the adequate parameters and values corresponding to the database provider, e.g.:

Database Provider	Value
SAP HANA	<code>encrypt=true,validateCertificate=false</code> <sup>56</sup>
SAP ASE	<code>ENABLE_SSL=true</code>
IBM DB2	<code>sslConnection=true</code>

To update these parameters into the Core Database, first export the existing system configuration into an XML file, using the following command:

```
config configuration export parameters.xml all
```

Then, modify the values of the above modified parameters located in the XML file according to the database provider's format, and finally update the system configuration using the using the following command:

```
config configuration import parameters.xml
```

## Securing the RFC over TCP/IP communications

To secure the communications with other systems such as SAP CI, SAP ERP/FI-CA or SAP CRM, which all rely on the RFC over TCP/IP communication channel, it is necessary to execute the following operations:

- Download and install the SAP Cryptographic Library
- Setup a Personal Security Environment (PSE) for SNC, that contains information related to the SAP CC public-key which includes its private key, its certificate and the list of trusted certificates
- Create the credentials that are required at runtime by SAP CC for accessing its PSE
- Exchange public-key certificates between SAP CC and the Application Server
- Update the Core Server system configuration related to JCo<sup>57</sup> settings

<sup>56</sup> When the value of the `validateCertificate` parameter is set to `true`, it is necessary to specify the following additional parameters:

- `trustStore`, `trustStoreType` and `trustStorePassword` when using a "oneway" authentication mode
- `trustStore`, `trustStoreType`, `trustStorePassword`, `keyStore`, `keyStoreType` and `keyStorePassword` when using a "dual" authentication mode

<sup>57</sup> Java Connector

- Maintain System ACL<sup>58</sup> and Extended User ACL on the SAP Netweaver Application Server

### 1. Downloading and installing the SAP Cryptographic Library

To download and install the SAP Cryptographic Library, refer to the [Downloading the SAP Cryptographic Library \[page 27\]](#) dedicated procedure.

### 2. Setting up a Personal Security Environment (PSE) for SNC

To create the SNC PSE for SAP Convergent Charging, execute the following command:

```
sapgenpse4cc get_pse -p <PSE_NAME>> -x <PIN> <DISTINGUISHED_NAME>
```

Where:

- <PSE\_NAME> corresponds to the name of the PSE
- <PIN> corresponds to a PIN code
- <DISTINGUISHED\_NAME> corresponds to the absolute name of SAP Convergent Charging, made up with the following elements:
  - CN=<COMMON\_NAME>
  - OU=<ORGANIZATIONAL\_UNIT >
  - O=<ORGANIZATION>
  - C=<COUNTRY>

#### ❁ Example

The following command line creates a `SAP_CC.pse` file that is protected with the `ccpin` PIN code:

```
sapgenpse4cc get_pse -p SAP_CC.pse -x ccpin "CN=SAPCC, O=MyCompany, C=US"
```

When using this PSE, SAP Convergent Charging has the following distinguished name: CN=**SAPCC**, O=**MyCompany**, C=**US**

### 3. Creating credentials

The credentials required by SAP CC are located in the `/usr/sap/<SID>/sys/profile/sec/cred_v2` file, that must only be accessible by the OS user running the Core Server system. To create these credentials, execute the following command:

```
sapgenpse4cc seclogin -p <PSE_NAME> -x <PIN_CODE> -O <USER_ID>
```

Where:

- <PSE\_NAME> corresponds to the name of the PSE created in step 2
- <PIN\_CODE> corresponds to the PIN code provided at PSE creation time in step 2
- <USER\_ID> corresponds to name of the concerned user, including the domain name in case of Microsoft Windows operating system

#### ❁ Example

The following command line creates credentials for the `<SID>adm` user so that this user can access the previously created `SAP_CC.pse` file:

```
sapgenpse4cc seclogin -p SAP_CC.pse -x ccpin -O <SID>adm
```

Where <SID> corresponds to the system identifier of the concerned Core Server system.

<sup>58</sup> Access Control List

#### 4. Exchanging certificates

To communicate using SNC, SAP CC and the SAP Netweaver Application Server must identify and trust each other using their respective certificates available in the relevant PSEs (which means the PSE of Application Server is available). To exchange certificates between SAP CC and the Application Server, it is necessary to:

- Export the certificate of SAP CC, using the following command:

```
sapgenpse4cc export_own_cert -o <OUTPUT_FILE> -p <PSE_NAME> -x <PIN_CODE>
```

Where:

- <OUTPUT\_FILE> corresponds to the absolute path of the file containing the exported certificate
- <PSE\_NAME> corresponds to the name of the PSE related to SAP CC
- <PIN\_CODE> corresponds to the PIN code provided during the creation of the PSE related to SAP CC
- Import the certificate of SAP CC into the SNC PSE of the Application Server. If the Application Server is an SAP Web Application Server with release 6.20 or later, you can use the Trust Manager ("STRUST" transaction) to import the certificate. Otherwise, use the following command:

```
sapgenpse4cc maintain_pk -a <CERT_FILE> -p <PSE_NAME> -x <PIN_CODE>
```

Where:

- <CERT\_FILE> corresponds to the absolute path of the file containing the previously exported certificate
- <PSE\_NAME> corresponds to the name of the PSE related to SAP CC
- <PIN\_CODE> corresponds to the PIN code provided during the creation of the PSE related to SAP CC
- Export the certificate of the Application Server. If the Application Server is an SAP Web Application Server with release 6.20 or later, you can use the Trust Manager ("STRUST" transaction) to export the certificate. Otherwise, use the `export_own_cert` command of the `sapgenpse` tool installed on the Application Server
- Import the certificate of the Application Server in the SNC PSE of SAP CC

#### 5. Updating JCo settings of the Core Server system

To modify the configuration of the Core Server related to JCo settings, it is necessary to:

- Export the SAP CC configuration of the relevant SAP system.
  - If the concerned system is the SAP ERP/FI-CA system, execute the following command:

```
setup sapci exportConfiguration -login=<LOGIN> -password=<PASSWORD>
<OUTPUT_FILE>
```

Where:

- <LOGIN> corresponds to an SAP CC **individual** user granted the adequate role
- <PASSWORD> corresponds to the password of the specified user
- <OUTPUT\_FILE> corresponds to the absolute path of the file containing the exported settings
- If the concerned system is the SAP CRM system, execute the following command:

```
setup sapci jcoDestination export crm <OUTPUT_FILE>
```

Where <OUTPUT\_FILE> corresponds to the absolute path of the file containing the exported settings

- Edit the exported file and modify the values of the following parameters:

- `jco.client.snc_mode`
- `jco.client.snc_lib`
- `jco.client.snc_qop`
- `jco.client.snc_myname`
- `jco.client.snc_partnername`

For further information about these parameters, refer to the “JCo destinations / Configuration options” section of the [SAP CC 5.0 Tuning Guide](#) documentation.

- Import the modified configuration.
  - If the concerned system is the SAP ERP/FI-CA system, execute the following command:

```
setup sapci importConfiguration -login=<LOGIN> -password=<PASSWORD>
<INPUT_FILE>
```

Where:

- `<LOGIN>` corresponds to an SAP CC **individual** user granted the adequate role
- `<PASSWORD>` corresponds to the password of the specified user
- `<INPUT_FILE>` corresponds to the absolute path of the file containing the modified settings
- If the concerned system is the SAP CRM system, execute the following command:

```
setup sapci jcoDestination import crm <INPUT_FILE>
```

Where `<INPUT_FILE>` corresponds to the absolute path of the file containing the modified settings

- Restart all Dispatcher and Bulkloader instances

## 6. Maintaining system ACL and extended user ACL on the SAP Netweaver Application Server

In addition to being able to identify its communication partner using the SNC layer, SAP NetWeaver uses system Access Control Lists (ACLs) to make sure that it is communicating with the correct components. To maintain the SNC system ACL (table SNCSYSACL, view VSNCSYSACL, type=E), execute the following procedure:

- Use the "SM30" transaction used for table maintenance operations
  - Enter an asterisk (\*) as a wildcard in the *User* field
  - Use the sequence number if you have multiple entries with the same user
  - Enter SAP Convergent Charging's SNC name in the *SNC name* field. Make sure you enter the server's SNC name and not the Distinguished Name. The server's SNC name is the Distinguished Name prefixed with "p:"
- Save your modifications
- Use the "SM30" transaction used for table maintenance operations
- Confirm the warning
- Save your modifications

## Enabling the securing policy

To activate the securing policy which has been configured during the previous operations, it is necessary to execute the following operations:

- Update the instance map according to the defined securing policy



- Restart the Core Server instances, in order to get a secured system

### 1. Modifying the instance map

To modify the instance map, you need to:

- Export the instance map into a CSV file named `instanceMap.csv`, using the following command:

```
setup instancemap export instanceMap.csv
```

- Open this file with a text editor, and modify the values of the `InternalSecure`, `ExternalSecure`, `HttpSecure` and `WsSecure` properties with the "dual" value, according to the possibilities described above
- (Re)import the modified instance map in the system, using the following command:

```
setup instancemap import -clean instanceMap.csv
```

- The `BOOT_DISPATCHER_LIST` parameter located in the `boot.config` file is not compatible with secured landscapes. Open the `boot.config` file and remove this parameter when exists

### 2. Restarting the Core Server instances

To restart the Core Server instances, refer to the [Starting and stopping the servers \[page 73\]](#) procedure.

## Securing the communications with the SAP SLD system

To communicate with a secured version of the SAP SLD system, it is necessary to execute the following operations:

- Update the configuration of the Core Server regarding the connection to the SLD system
- Import the certificate of the SAP SLD system into the truststore of the JVM used by the Core Server, so that the Core Server can trust the SAP SLD system
- Restart the Core Server instances, in order to apply the new configuration

### 1. Updating the configuration of the Core Server

To configure the access to an SAP SLD system, refer to the "System settings for the System Landscape Directory" procedure described in the SAP Convergent Charging [SAP CC 5.0 Configuration Guide](#) documentation.

### 2. Importing the SAP SLD certificate into the truststore of the JVM used by the Core Server

To give the possibility to the Core Server to trust the SAP SLD system, it is necessary to import the certificate of the SAP SLD system into the truststore of the JVM used by the Core Server.

Once you retrieved the SLD certificate (X.509 v3 digital certificate, DER encoded), you need to import it into the truststore of the JVM used by the Core Server, using the following command:

```
keytool -importcert -file certificate.sld.der -keystore keystore.core.jks -noprompt
```

#### i Note

You will be prompted to type a passphrase for the java keystore file which will contain the certificate to import. It is necessary to remember this passphrase in order to execute the following command.

The Core Server must then be configured to use the above updated keystore as a truststore. To do this, open the `jstart.config` file of each dispatcher instance, located in the `jstart` directory of the SAP Profile Folder.

Then, update the `dispatcher-x.javaParameters` configuration parameter with the following information:

```
-Djavax.net.ssl.trustStore=<Path_of_the_Core_Server_java_keystore>
-Djavax.net.ssl.trustStorePassword=<Passphrase_of_the_keystore>
```

### 3. Restarting the Core Server instances

To restart the Core Server instances, refer to the [Starting and stopping the servers \[page 73\]](#) procedure.

## Securing communications with the SAP CC CTS+ plugin

To communicate with a secured version of Core Server, it is necessary to execute the following operations:

- Use the common procedure in order to generate a keystore:
  - Related to the SAP CC CTS+ plugin
  - Named `keystore.ctsplugin.p12`
  - Containing a `certificate.ctsplugin.der` certificate and its private key
- Update the configuration of the SAP CC CTS+ plugin to enable its keystore
- Import the certificate of the SAP CC CTS+ plugin into the truststore of the Core Server, so that the Core Server can trust the SAP CC CTS+ plugin
- Update SAP CTS system to enable secure connection

#### 1. Generating a certificate related to a client application

Use the [common procedure \[page 139\]](#) to generate a keystore named `keystore.ctsplugin.p12` and containing a certificate with its private key.

#### 2. Enabling the keystore of the SAP CC CTS+ plugin

The SAP CC CTS+ plugin must take into account its certificate in order to use it when communicating with the Core Server in a secured mode. To declare the `keystore.ctsplugin.p12` client keystore, uncomment the following lines in the SAP CC CTS+ plugin script file corresponding to your system and provide the missing information '<...>':

```
-Djavax.net.ssl.keyStoreType=pkcs12
-Djavax.net.ssl.keyStore=<Path_of_the_SAPCC_CTS_plugin_keystore>
-Djavax.net.ssl.keyStorePassword=<Passphrase_of_SAPCC_CTS_plugin_keystore>
```

#### 3. Importing the content of the SAP CC CTS+ plugin keystore into the truststore of the Core Server

To import the content of the `keystore.ctsplugin.p12` keystore into the SAP CC truststore under the "CTSAlias" alias, type the following command:

```
setup certentry import CTSAlias certificate.ctsplugin.der
```

#### **i** Note

The certificate must be imported in each SAP CC system that the SAP CC CTS+ plugin has to connect with.

#### 4. Linking the imported certificate

To specify that the Core Server must use the imported certificate when communicating with the SAP CC CTS+ plugin through the "transport" web service, type the following command:

```
setup certentry link CTSAlias all all
```

## 5. Update SAP CTS system to enable secure connection

Refer to the *Configuring the HTTP connection* section of the SAP CTS system documentation to get information about the configuration of transport landscapes: <https://help.sap.com/viewer/4a368c163b08418890a406d413933ba7/latest/en-US/2b326d6274134cea8b217f24889d19c1.html>.

# 5.50 Securing communications with the BART Server system

## Description

The communications with the BART Server system rely on:

- The Packets over TCP/IP communication channel to communicate with:
  - An offline mediation system
  - A Dispatcher instance of the Core Server
- The XML over HTTP communication channel to communicate with:
  - Client applications such as BART Tool
  - An Updater instance of the Core Server
  - The SLD system, at launch time
- The JDBC<sup>59</sup> protocol for interactions between the BART Setup Tool and the BART Database

The securing procedure consists in securing both the BART Server and its client applications. This procedure requires the use of the BART Setup Tool console application, which needs to communicate with the previously secured Core Server system for authentication purposes, and which must thus be first secured.

Once the BART Setup Tool has been secured, the following operations give you the possibility to:

- Secure the external communications of the BART Server, which concern:
  - The communications with the Core Server
  - The communications with a client application
- Secure the communications with the BART Database, relying on the JDBC protocol
- Enable this defined securing policy, which consists in:
  - Modifying the configuration of the BART Server
  - Restarting the BART Server, which finally runs in a secured mode

## Preliminary Notes

- Some of the procedures described afterwards refer to the [Common procedure for generating the securing materials \[page 139\]](#) that is available in the [Securing a landscape \[page 138\]](#) procedure. Refer to it when necessary

---

<sup>59</sup> Java Database Connectivity

- If your client application is not a java application, you must adapt some of the following procedures to fit the technology of your application

## Prerequisites

The `setup` command specified in the following operations refers to the BART Setup Tool user interface. Refer to the [Launching BART Setup Tool \[page 135\]](#) procedure if necessary

## Securing the BART Setup Tool console application

To secure the BART Setup Tool user interface, refer to the 5 to 8 steps of the [Securing the Core Server external communications \[page 146\]](#) section.

## Securing the BART Server external communications

External communications related to the BART Server system both concern:

- The Core Server system, with whom the BART Server system communicates
- Client applications, which can interact with BART Server to perform operations such as chargeable items batch charging or recharging

As far as communications with the Core Server system are concerned, execute the following operations:

- Use the `certificate.ext.der` certificate generated into the [Securing the Core Server external communications \[page 146\]](#) procedure, in order to give BART Server the possibility to trust Core Server:
  - Import this certificate into the truststore of the BART Server system, using the "CoreClientAlias" alias
  - Link this "CoreClientAlias" certificate to the Core Server system, for all the communication channels
- Use the `keystore.cli.p12` keystore generated into the [Securing the Core Server external communications \[page 146\]](#) procedure, so that the BART Server system can be trusted by the Core Server system (as BART Server can also be considered as a Java-based client application):
  - Import this keystore into the keystore of the BART Server system, using the "CoreClientAlias" alias
  - Link this "CoreClientAlias" certificate to the Core Server system, for all the communication channels
- Update the URLs of the Dispatcher instances declared in the configuration of the BART Server system

### 1. Trusting the Core Server

To trust the Core Server, use the certificate generated into the [Securing the Core Server external communications \[page 142\]](#) procedure and located in the `keystore.ext.p12` keystore.

Import the `certificate.ext.der` certificate into the truststore of the BART Server under the "CoreClientAlias" alias, using the following command:

```
setup certentry import CoreClientAlias certificate.ext.der
```

Specify that the BART Server must use the imported certificate for external communications, whatever the communication channel is, using the following command:

```
setup certentry link CoreClientAlias dispatcher all
```

## 2. Communicate with the Core Server as a trusted client application

To be considered by the Core Server as a trusted application, use the `keystore.cli.p12` keystore generated into the [Securing the Core Server external communications \[page 146\]](#) procedure.

Import the content of this keystore into the keystore of the BART Server, under the "CoreClientAlias" alias, using the following command:

```
setup keyentry import_p12 CoreClientAlias keystore.cli.p12
```

### Note

You will be prompted to type the passphrase of the keystore file which contains the certificate and private key to import.

Specify that the BART Server must use the imported certificate when communicating with the Core Server, whatever the used communication channel is, using the following command:

```
setup keyentry link CoreClientAlias dispatcher#1 all
```

## 3. Updating the configuration of the BART Server

Update the `CC.DISPATCHER.BOOT.HTTP.URL.LIST` parameter located in the `bart.config` file, in order to specify the list of dispatchers to contact in a secured mode, e.g.: `https://<host>:<port>`

To secure the communications between the BART Server and a client application, it is necessary to execute the following operations:

- Use the common procedure in order to generate a keystore:
  - Related to the BART Server
  - Named `keystore.bart.p12`
  - Containing a `certificate.bart.der` certificate and its private key
- Use the common procedure in order to generate a keystore:
  - Related to the client application
  - Named `keystore.bart.cli.p12`
  - Containing a `certificate.bart.cli.der` certificate and its private key
- Import the content of the `keystore.bart.p12` keystore into the keystore of the BART Server, using the "ExternalAlias" alias
- Link the "ExternalAlias" certificate to the BART Server, for all the communication channels
- Import the `certificate.bart.der` certificate of the BART Server into the truststore of the client application
- Enable the `keystore.bart.cli.p12` keystore on the client application side, by declaring this keystore in the Java command-line
- Import the `certificate.bart.cli.der` certificate into the truststore of the BART Server, using the "ClientAlias" alias
- Link the "ClientAlias" certificate to the BART Server, for all the communication channels

## i Note

If your client application is not a java application, you must adapt some of the following operations to fit the technology of your application.

### 1. **Generating a certificate and its private key for the BART Server**

Use the common procedure to generate a keystore named `keystore.bart.p12` and containing a certificate with its private key.

### 2. **Generating a certificate and its private key for a client application**

Use the common procedure to generate a keystore named `keystore.bart.cli.p12` and containing a `certificate.bart.cli.der` certificate with its private key.

## i Note

It is necessary to remember the passphrase of the keystore file in order to execute the step 5 described below.

### 3. **Importing the BART Server certificate into the keystore of the BART Server**

To import the content of the `keystore.bart.p12` keystore into the keystore of the BART Server, under the "ExternalAlias" alias, type the following command:

```
setup keyentry import_p12 ExternalAlias keystore.bart.p12
```

## i Note

You will be prompted to type the passphrase of the keystore file which contains the certificate and private key to import.

### 4. **Linking the imported certificate**

To specify that the BART Server must use the imported certificate for external communications, whatever the communication channel is, type the following command:

```
setup keyentry link ExternalAlias bart#1 all
```

### 5. **Importing the BART Server certificate into the truststore of the client application**

To give the possibility for a client application to trust the BART Server, it is necessary to import the certificate of the BART Server into the truststore used by this client application.

To import the `certificate.bart.der` certificate into a java keystore named `keystore.cli.jks`, type the following command:

```
keytool -importcert -file certificate.bart.der -keystore keystore.cli.jks -noprompt
```

## i Note

You will be prompted to type a passphrase for the java keystore file which will contain the certificate to import. It is necessary to remember this passphrase in order to execute the following command.

The client application must then be configured to use the above created keystore as a truststore. To make the client application use the `keystore.cli.jks` keystore as its default truststore, add the following options to the command-line of the application:

```
-Djavax.net.ssl.trustStore=<Path_of_the_java_keystore>
-Djavax.net.ssl.trustStorePassword=<Passphrase_of_the_java_keystore>
```

## 6. Enabling the `keystore.bart.cli.p12` keystore on the client application side

The client application must take into account its own certificate in order to use it when communicating in a secured mode with the BART Server. To enable this certificate, it is necessary to declare the related keystore in the command-line of the application. To declare the `keystore.bart.cli.p12` client keystore, add the following options to the command-line of the client application:

```
-Djavax.net.ssl.keyStoreType=pkcs12
-Djavax.net.ssl.keyStore=<Path_of_the_client_keystore>
-Djavax.net.ssl.keyStorePassword=<Passphrase_of_the_client_keystore>
```

## 7. Importing the client application's certificate into the truststore of the BART Server

To import the `certificate.bart.cli.der` client certificate into the truststore of the BART Server under the "ClientAlias" alias, type the following command:

```
setup certentry import ClientAlias certificate.bart.cli.der
```

## 8. Linking the imported certificate

To specify that the BART Server must use the imported certificate when communicating with a client application, whatever the communication channel is, type the following command:

```
setup certentry link ClientAlias bart all
```

# Securing the BART Server JDBC connections

To secure the communications with the BART Database, it is necessary to execute the following operations:

- Execute the securing procedures related to your database provider
- Update the configuration of the BART Server to modify the connection URL with the adequate parameters

### 1. Executing the securing procedures related to your database provider

Each database provider delivers specific procedures to encrypt communications with their databases management system. Refer to the documentation of your database provider to create the different materials secure the communications with the BART Database.

### 2. Updating the configuration of the BART Server

The BART Server supports the following parameters and associated values to secure the communications relying on the JDBC protocol:

Database Provider	Parameter	Value
SAP HANA	<code>encrypt</code>	True
	<code>validateCertificate</code>	False <sup>60</sup>
SAP ASE	<code>ENABLE_SSL</code>	True
Oracle	N/A	N/A
Microsoft SQL Server	<code>encrypt</code>	True
	<code>trustServerCertificate</code>	False

<sup>60</sup> When this value is set to **true**, it is necessary to specify additional parameters to the `SQLHELPER_JDBC_PROPERTIES` parameter, depending on the securing mode. See below for further information about these parameters.

Database Provider	Parameter	Value
IBM DB2	sslConnection	True

To secure the communications relying on the JDBC protocol, it is necessary to update the following parameters in the `bart.config` file (located in the `/usr/sap/<SYSTEM_ID>/<INSTANCE_NAME>/config` directory):

- `db.SQLHELPER_JDBC_URIx`, where `x` can be empty when no HA is required, or a value between 1 and 12 for the Oracle and DB2 database providers (depending on the HA configuration)
- `db.SQLHELPER_JDBC_PROPERTIES`, which corresponds to a CSV string used to specify the additional parameters to use when connecting to the database

To update the `db.SQLHELPER_JDBC_URIx` parameter into the `bart.config` file, open the configuration file and declare the adequate parameters to secure the communications with the BART Server, e.g.:

Database Provider	Value
SAP HANA	<code>jdbc:sap:&lt;server&gt;:&lt;port&gt;</code>
SAP ASE	<code>jdbc:sybase:Tds:&lt;server&gt;:&lt;port&gt;/&lt;database_name&gt;</code>
Oracle	<code>jdbc:oracle:thin:@//&lt;server&gt;:&lt;port&gt;/&lt;ServiceName&gt;</code>  <code>jdbc:oracle:thin:@&lt;server&gt;:&lt;port&gt;:&lt;SID&gt;</code>
Microsoft SQL Server	<code>jdbc:sqlserver://&lt;server&gt;:&lt;port&gt;;DatabaseName=&lt;database_name&gt;</code>
IBM DB2	<code>jdbc:db2://&lt;server&gt;:&lt;port&gt;/&lt;instance_name&gt;;currentSchema=&lt;schema_name&gt;;</code>

To update the `SQLHELPER_JDBC_PROPERTIES` parameter into the `bart.config` file, open it in a text editor and declare the adequate parameters and values corresponding to the database provider, e.g.:

Database Provider	Value
SAP HANA	<code>encrypt=true,validateCertificate=false</code> <sup>61</sup>
SAP ASE	<code>ENABLE_SSL=true</code>
IBM DB2	<code>sslConnection=true</code>

<sup>61</sup> When the value of the `validateCertificate` parameter is set to `true`, it is necessary to specify the following additional parameters:

- `trustStore`, `trustStoreType` and `trustStorePassword` when using a "oneway" authentication mode
- `trustStore`, `trustStoreType`, `trustStorePassword`, `keyStore`, `keyStoreType` and `keyStorePassword` when using a "dual" authentication mode



## Enabling the securing policy

To activate the securing policy which has been configured during the previous operations, it is necessary to execute the following operations:

- Update the configuration of the BART Server according to the defined securing policy
- Restart the BART Server, in order to get a secured system

### 1. Updating the configuration of the BART Server

Update the `BART.HTTP.SECURE` and `BART.COLLECTOR.SECURE` parameters located in the `bart.config` file, in order to declare the secured version, e.g.:

```
bart.http.secure=true
bart.http.secure.client_auth=true
bart.collector.secure=true
bart.collector.secure.client_auth=true
```

### 2. Restarting the BART Server

To restart the BART Server, refer to the [Starting and stopping the servers \[page 73\]](#) procedure.

## Securing the communications with the SAP SLD system

To communicate with a secured version of the SAP SLD system, it is necessary to execute the following operations:

- Update the configuration of the BART Server regarding the connection to the SLD system
- Import the certificate of the SAP SLD system into the truststore of the JVM used by the BART Server
- Restart the BART Server, in order to apply the new configuration

### 1. Updating the configuration of the BART Server

Update the following parameters located in the `bart.config` file, in order to configure the access to a secured SLD system:

```
bart.sld.url=<URL_of_the_secured_SLD_system>
bart.sld.user=<Username_used_to_connect_to_the_SLD_system>
bart.sld.password=<Password_used_to_connect_to_the_SLD_system>
```

### 2. Importing the SAP SLD certificate into the truststore of the JVM used by the BART Server

To give the possibility to the BART Server to trust the SAP SLD system, it is necessary to import the certificate of the SAP SLD system into the truststore of the JVM used by the BART Server.

Once you retrieved the SLD certificate (X.509 v3 digital certificate, DER encoded) you need to import it into the truststore of the JVM used by the BART Server, using the following command:

```
keytool -importcert -file certificate.sld.der -keystore keystore.bart.jks -
noprompt
```

#### **i** Note

You will be prompted to type a passphrase for the java keystore file which will contain the certificate to import. It is necessary to remember this passphrase in order to execute the following command.

The BART Server must then be configured to use the above updated keystore as a truststore. To do this, open the `jstart.config` file from the server's profile directory, located in the following folder: `<DRIVE>:\usr\sap\<SID>\SYS\profile\jstart\<SID>_<INSTANCE_NAME>_<HOST>`. Then, update the `BART.javaParameters` configuration parameter with the following information:

```
-Djavax.net.ssl.trustStore=<Path_of_the_BART_Server_java_keystore>
-Djavax.net.ssl.trustStorePassword=<Passphrase_of_the_keystore>
```

### 3. Restarting the BART Server

To restart the BART Server, refer to the [Starting and stopping the servers \[page 73\]](#) procedure.

## 5.51 Securing communications with the Diameter Server system

### Description

The communications with the Diameter Server system rely on:

- The Packets over TCP/IP communication channel to communicate with a Dispatcher instance of the Core Server
- The XML over HTTP communication channel to communicate with the SAP SLD system, at launch time
- The Diameter protocol for interactions with a network element

The securing procedure consists in:

- Configuring the Diameter Server as a client application of the Core Server
- Activating (when not already activated during the installation made with `SAPinst`) the secured version of the Diameter Stack in order to secure the communications with network elements
- Enabling this securing policy, which consists in:
  - Modifying the configuration file of the Diameter Server
  - Restarting the Diameter Server, which finally runs in a secured mode

### Preliminary Notes

- Some of the procedures described afterwards refer to the [Common procedure for generating the securing materials \[page 139\]](#) that is available in the [Securing a landscape \[page 138\]](#) procedure. Refer to it when necessary
- If your client application is not a java application, you must adapt some of the following procedures to fit the technology of your application

## Securing the communications between the Diameter Server and the Core Server

To configure the Diameter Server as a java client application, refer to the 5 to 8 steps of the [Securing the Core Server external communications \[page 142\]](#) section.

## Securing the communications with the network elements

To communicate with a network element using the Diameter protocol, the Diameter Server uses the OpenBlox Java Diameter Stack provided by the Tria Systems company. To use the secured version of this Diameter Stack, the configuration of the Diameter Server must contain the following information:

- A valid license key
- An adequate routing table used to handle the proxiable requests
- The TLS information used to secure the communication channel used by the network elements

### 1. Valid license key

Check (or specify) the `LicenseKey` parameter located in the `serverConfig.xml` file, to ensure that it contains a valid license key which must be used by the Diameter Server:

```
<entry key="LicenseKeys">
 <properties>
 <entry key="LicenseKey" value="<Valid_License_key>"/>
 </properties>
</entry>
```

#### i Note

To get a valid license key, contact the Tria Systems company, or refer to your technology consultants.

### 2. Routing table

Check (or specify) that the `RoutingTable` parameter located in the `serverConfig.xml` file refers to a realm-based routing table that the Diameter Server must use:

```
<entry key="RoutingTable">
 <properties>
 <entry key="RealmName" value="<Realm_name>"/>
 <entry key="RealmApplicationId" value="4"/>
 <entry key="RealmLocalAction" value="LOCAL"/>
 </properties>
</entry>
```

### 3. TLS information

To communicate in a secured mode with a network element using the Diameter protocol, it is necessary to:

- Generate a keystore:
    - Related to the Diameter Server
    - Named `keystore.diameter.p12`
    - Containing a `certificate.diameter.der` certificate and its private key
  - Update the configuration of the Diameter Server, in order to configure the necessary TLS parameters
1. To generate a keystore related to the Diameter Server, use the common procedure.

### Note

You will be prompted to type a passphrase for the java keystore file which will contain the certificate and its private key. It is necessary to remember this passphrase in order to update the configuration of the Diameter Server, as described below.

2. Once this keystore is created, update the `serverConfig.xml` file, in order to declare the TLS<sup>62</sup> parameters which must be used by the Diameter Server:

```
<entry key="InbandSecurityIds">
 <properties>
 <entry key="SecurityId" value="TLS"/>
 </properties>
</entry>
<entry key="TLSKeyStoreFile" value="<Path_of_the_server_keystore>"/>
<entry key="TLSTrustStoreFile" value="<Path_of_the_server_keystore>"/>
<entry key="TLSKeyStorePassword"
value="<Passphrase_of_the_server_keystore>"/>
<entry key="TLSTrustStorePassword"
value="<Passphrase_of_the_server_keystore>"/>
```

## Enabling the securing policy

To activate the securing policy which has been configured during the previous operations, it is necessary to execute the following operations:

- Update the configuration of the Diameter Server according to the defined securing policy
- Restart the Diameter Server, in order to get a fully secured system

### 1. Updating the configuration of the Diameter Server

Update the `OCS_SECURED` parameter located in the `serverConfig.xml` file, in order to declare the secured version:

```
<entry key="OCS_SECURED" value="true"/>
```

### 2. Restarting the Diameter Server

To restart the Diameter Server, refer to the [Starting and stopping the servers \[page 73\]](#) procedure.

## Securing the communications between the Diameter Server and the SAP SLD system

To communicate with a secured version of the SAP SLD system, it is necessary to execute the following operations:

- Update the configuration of the Diameter Server regarding the connection to the SLD system
- Import the certificate of the SAP SLD system into the truststore of the JVM used by the Diameter Server, so that the Diameter Server can trust the SAP SLD system
- Restart the Diameter Server, in order to apply the new configuration

<sup>62</sup> Transport Layer Security

### 1. Updating the configuration of the Diameter Server

Update the following parameters located in the `serverConfig.xml`, in order to configure the access to a secured SLD system:

```
<entry key="SLDURL" value="<URL_of_the_secured_SLD_system>"/>
<entry key="SLDUser" value="=<Username_used_to_connect_to_the_SLD_system>"/>
<entry key="SLDPassword"
value="<Password_used_to_connect_to_the_SLD_system>"/>
```

### 2. Importing the SAP SLD certificate into the truststore of the JVM used by the Diameter Server

To give the possibility to the Diameter Server to trust the SAP SLD system, it is necessary to import the certificate of the SAP SLD system into the truststore of the JVM used by the Diameter Server.

Once you retrieved the SLD certificate (X.509 v3 digital certificate, DER encoded) you need to import it into the truststore of the JVM used by the Diameter Server, using the following command:

```
keytool -importcert -file certificate.sld.der -keystore keystore.diameter.jks
-noprompt
```

#### i Note

You will be prompted to type a passphrase for the java keystore file which will contain the certificate to import. It is necessary to remember this passphrase in order to execute the following command.

The Diameter Server must then be configured to use the above updated keystore as a truststore. To do this, open the `jstart.config` file from the server's profile directory, located in the following folder:

```
<DRIVE>:\usr\sap\<SID>\SYS\profile\jstart\<SID>_<INSTANCE_NAME>_<HOST>
```

Then, update the `Diameter.javaParameters` configuration parameter with the following information:

```
-Djavax.net.ssl.trustStore=<Path_of_the_Diameter_Server_java_keystore>
-Djavax.net.ssl.trustStorePassword=<Passphrase_of_the_keystore>
```

### 3. Restarting the Diameter Server

To restart the Diameter Server, refer to the [Starting and stopping the servers \[page 73\]](#) procedure.

## 5.52 Securing communications with Cockpit and Tomcat Server

### Description

Cockpit is a Web application deployed on a Java Web Server such as Apache Tomcat Server. It includes two main components:

- A front-end component that corresponds to the user interface visible in the browser of the SAP power users
- A back-end component that is deployed on the Tomcat Server and communicates with the Core Server system

The communications with Cockpit rely on:

- The XML over HTTP communication channel, that is used by the back-end component of Cockpit to communicate with a running dispatcher of the Core Server system
- The HTTPS protocol, that is used for interactions between the browsers and the front-end component of Cockpit

SAP SE recommends that you configure your Tomcat Server with SSL/TLS to interact both with the user's browser and with the Core Server system.

To secure your SAP CC landscape, SAP SE recommends that you dedicate a Tomcat Server to each Cockpit application. If you need to secure several Cockpit applications, you need to install and secure several Tomcat Server systems. If you mix Cockpit applications that communicate with secured Core Server systems and non secured systems, you can deploy the non secured Cockpit applications on the same Apache Tomcat Server.

The securing procedure consists in:

- Securing the communications between the Apache Tomcat Server and the Core Server system by configuring the JVM of the Apache Tomcat Server as a client application of the Core Server system
- Securing the communications between web browsers and the Cockpit application by enabling SSL/TLS in the Apache Tomcat Server

Such securing mode corresponds to the "dual" mode. As a prerequisite, the Core Server system must already been secured as detailed in the [Securing the Core Server external communications \[page 146\]](#) procedure.

## Preliminary Notes

Some of the procedures described afterwards refer to the [Common procedure for generating the securing materials \[page 139\]](#) that is available in the [Securing a landscape \[page 138\]](#) procedure. Refer to it when necessary

## Prerequisites

- The Core Server system is already secured as detailed in the [Securing the Core Server external communications \[page 146\]](#) procedure
- You have generated a `keystore.ext.p12` keystore file. The keystore relates to the secured Core Server system. It includes the `certificate.ext.der` certificate and corresponding private key of the Core Server system
- You have imported the content of the `keystore.ext.p12` keystore into the keystore of the Core Server system, using the "ExternalAlias" alias

## Securing the Apache Tomcat Server

To implement your security policy, we recommend that you configure the Tomcat Server system to support the SSL/TLS technologies and important secured functions. Refer to the [SAP CC 5.0 Security Guide](#) documentation for more information about security recommendations such as:

- Implementing SSL
- Cross-Origin Resource Sharing (CORS)
- Cross-Site Request Forgery (CFRS)
- HTTP Header management
- Cookies management

## Securing the communications between the Cockpit and the Core Server system

To secure the communications between the Cockpit application and the Core Server system, you secure the JVM of the Apache Tomcat Server that runs the Web application.

To communicate with a secured version of the Core Server system in dual mode, it is necessary to execute the following operations:

- Use the common procedure to generate a keystore:
  - Related to the JVM of the Apache Tomcat Server that runs the Cockpit application
  - Named "keystore.cli.p12"
  - Containing a "certificate.cli.der" certificate and corresponding private key
- Import the `certificate.ext.der` certificate of Core Server into the truststore of the Tomcat JVM
- Enable the `keystore.cli.p12` keystore on the Tomcat JVM side, by declaring this keystore on the Tomcat JVM side
- Import the `certificate.cli.der` certificate into the truststore of the Core Server system, using the "ClientAlias" alias
- Link the "ClientAlias" certificate to all the instances, for all the communication channels
- Restart the Tomcat Server to apply the new configuration
- Update the configuration of the Cockpit application to use secured communications

### 1. Generating a certificate related to the Tomcat JVM as a client application of the Core Server system

Use the common procedure to generate a keystore named `keystore.cli.p12` and containing a `certificate.cli.der` certificate with its private key.

#### **i** Note

It is necessary to remember the passphrase of the keystore file in order to execute the steps described below.

### 2. Importing the certificate of the Core Server into the truststore of the JVM of the Apache Tomcat Server that runs the Cockpit application

To give the possibility for the Tomcat JVM to trust the Core Server system, it is necessary to import the certificate of the Core Server into the truststore used by the Tomcat JVM that runs the Cockpit application. Use the `certificate.ext.der` certificate generated into the [Securing the Core Server external communications \[page 146\]](#) procedure.

- To import the `certificate.ext.der` certificate into a Java keystore named `keystore.cli.jks`, type the following command:

```
keytool -importcert -file certificate.ext.der -keystore keystore.cli.jks -
noprompt
```

## i Note

You will be prompted to type a passphrase for the Java keystore file that will contain the certificate to import. It is necessary to remember this passphrase to execute the following command.

- The Tomcat JVM must then be configured to use the above created keystore as a truststore. To make the Tomcat JVM use the `keystore.cli.jks` keystore as its default truststore, you can customize a "setenv" or "setenv" script. This script file is in the `/bin` folder of the Tomcat installation. Create or change the appropriate Tomcat script file.

Operating system	Procedure
Linux and UNIX operating systems	Add the following lines in the <code>setenv.sh</code> file: <pre>export CATALINA_OPTS="\$CATALINA_OPTS - Djavax.net.ssl.trustStore=&lt;Path_of_ the_Java_keystore&gt;" export CATALINA_OPTS="\$CATALINA_OPTS - Djavax.net.ssl.trustStorePassword=&lt; Passphrase_of_the_Java_keystore&gt;"</pre>
Microsoft Windows operating system	Add the following lines in the <code>setenv.bat</code> file: <pre>set CATALINA_OPTS=%CATALINA_OPTS% - Djavax.net.ssl.trustStore=&lt;Path_of_ the_Java_keystore&gt; set CATALINA_OPTS=%CATALINA_OPTS% - Djavax.net.ssl.trustStorePassword=&lt; Passphrase_of_the_Java_keystore&gt;</pre>

### 3. Enabling the client keystore on the Apache Tomcat Server side

The Tomcat JVM that runs the Cockpit application must take into account its `certificate.cli.der` certificate to use it when communicating in a secured mode with the Core Server system.

To enable this certificate, declare the related `keystore.cli.p12` client keystore by customizing the "setenv" script. This script file is in the `/bin` folder of the Tomcat installation. Depending on the operating system, the Tomcat Server uses one of these script files automatically.

Operating system	Procedure
Linux and UNIX operating systems	Add the following lines in the <code>setenv.sh</code> file: <pre>export CATALINA_OPTS="\$CATALINA_OPTS -Djavax.net.ssl.keyStoreType=pkcs12" export CATALINA_OPTS="\$CATALINA_OPTS - Djavax.net.ssl.keyStore=&lt;Path_of_the_ client_keystore&gt;" export CATALINA_OPTS="\$CATALINA_OPTS - Djavax.net.ssl.keyStorePassword=&lt;Pass phrase_of_the_client_keystore&gt;"</pre>



## Operating system

## Procedure

Microsoft Windows operating system

Add the following lines in the `setenv.bat` file:

```
set CATALINA_OPTS=%CATALINA_OPTS% -
Djavax.net.ssl.keyStoreType=pkcs12
set CATALINA_OPTS=%CATALINA_OPTS% -
Djavax.net.ssl.keyStore=<Path_of_the_
client_keystore>
set CATALINA_OPTS=%CATALINA_OPTS% -
Djavax.net.ssl.keyStorePassword=<Pass
phrase_of_the_client_keystore>
```

### 4. Importing the content of the client keystore into the truststore of the Core Server system

To be considered by the Core Server system as a trusted client application, import the certificate of the Tomcat JVM to the truststore of the Core Server system.

To import the content of the `keystore.cli.p12` keystore into the SAP CC truststore under the "ClientAlias" alias, type the following command in SAP CC Setup Tool:

```
setup certentry import ClientAlias certificate.cli.der
```

### 5. Linking the imported certificate

To specify that the Core Server system must use the imported certificate when communicating with a client application, whatever the communication channel is, type the following command in SAP CC Setup Tool:

```
setup certentry link ClientAlias all all
```

### 6. Updating the configuration of the Cockpit application on Tomcat Server

In the configuration file of Cockpit, change the `hci.http.url` application parameter. The URLs must be based on the HTTPS protocol. Refer to the [Launching Cockpit \[page 125\]](#) procedure for more information on how and where to maintain the configuration settings for your installed Cockpit applications.

## Securing the communications between Web browsers and the Core Server system

To communicate with a Web browser, the Apache Tomcat Server that runs your Cockpit application must use the SSL/TLS technologies. To implement SSL, the Tomcat Server must have a certificate. To avoid warnings in your Web browsers, the certificate needs to be signed by your trusted certificate authority (CA).

Depending on the version of your installed Apache Tomcat Server, use its product documentation to perform the following steps:

- If needed, create a keystore to store the certificate
- Create a local Certificate Signing Request (CSR) and send it to your certificate authority
- Import the certificate into your keystore
- Activate the SSL support in Tomcat by uncommenting and completing the appropriate SSL connector in the `server.xml` file

### i Note

To facilitate the user experience of Cockpit users, you can use the redirect mechanism of Tomcat to redirect the HTTP port (8080 by default) to the HTTPS port (8443 by default). It enables you to manage simple URLs without the port number precision.

## Verify the technical implementation

To verify the technical implementation, launch the Cockpit application and log on to the user interface. For example, open your browser and use the following URL to check that there is no issue: `https://<TOMCAT_HOST>:8443/<WEB_APP_NAM>`.

## 5.53 Installing a permanent license

### Description

During the execution of your installation scenario, a temporary license has been installed for your SAP Convergent Charging system, that is only valid for a limited period of time. You can use this procedure remove this time limitation by installing a permanent license.

### Preliminary Notes

For more information about license keys, refer to SAP Notes [197623](#) and [94998](#).

### Prerequisites

- An SAP Convergent Charging 5.0 system must be installed and available before executing this procedure. Execute an installation scenario if necessary
- The `setup` command specified in the following operations refers to the Setup Tool user interface. Refer to the [Launching Setup Tool \[page 133\]](#) procedure if necessary

## Procedure

The installation of an SAP permanent license consists in the following operations:

- Applying for a permanent license
  - Installing the permanent license within your system landscape
  - Restarting the instances to take the permanent license into account
1. To obtain a permanent license key, open the "Keys, Systems & Installations" section of the SAP Support Portal available at <http://support.sap.com/licensekey>. You need to provide the hardware key of each host of your SAP Convergent Charging landscape. The different hardware keys are available in the hardware\_keys.txt file that is available in the SAP Central Repository directory (refer to the [Document Definitions \[page 10\]](#) section for further information)
  2. Copy the license file to a host of your landscape where a Dispatcher is installed
  3. Connect to this host and launch the Setup Tool user interface (refer to the [Launching Setup Tool \[page 133\]](#) procedure if necessary). Execute the following command as the administrator of your SAP CC system landscape, considering that <LICENSE\_FILE\_PATH> corresponds to the absolute path of the previously transferred file containing the permanent license:

```
setup license import <LICENSE_FILE_PATH>
```

4. Once the permanent license has been successfully installed within your SAP CC system, you need to restart the instances to take the new license into account. To restart the system, refer to the [Starting and stopping the servers \[page 73\]](#) procedure

## 5.54 Removing system(s) or instance(s) from a given host

### Description

This procedure explains you how to remove one or multiple systems or instances from a given host of an existing landscape, using the SAPinst tool.

### Procedure

As this procedure relies on the SAPinst tool, you first need to launch it using the [Launching the SAPinst tool \[page 115\]](#) dedicated procedure.

Once opened, the SAPinst tool displays a succession of screens that give you the possibility to configure your installation scenario. Use the following recommendations to fill the different screens:

1. **Welcome to SAP Convergent Charging** screen
  - Click ► *SAP Convergent Charging* ► *Software Life-Cycle Options* ► *Uninstall* ► *Uninstall - SAP Systems or Single Instances* ►


- Click the *Next* button
- 2. **General SAP System Parameter** screen
  - Tick the *Profiles Available* checkbox when not ticked by default
  - *Profile Directory*: Filled by default with the location of the SAP system profile directory. Ensure that this location is correct
  - Click the *Next* button
- 3. **Uninstall Instances** screen
  - Untick the *Uninstall all instances of the SAP system from this host* checkbox to unlock the table and select a list of instances to remove
- 4. **Parameter Summary** screen
  - Carefully check that all your settings have been taken into account before starting the installation. In case you need to correct one or multiple settings, tick the corresponding checkboxes and click the *Revise* button
  - If all your settings are correctly taken into account, click the *Next* button to uninstall the selected instances from your host
- 5. **Task Progress** screen
  - This screen contains the different steps of your installation scenario, whose advancement can be followed

## 5.55 Integrating SAP CC with CA APM

### Description

This procedure explains you how to configure your SAP CC Core Server system in order to communicate with CA Application Performance Management (CA APM) for monitoring purpose.

### Preliminary Notes

- For more information about CA APM, refer to SAP Note [1453216](#) 
- This procedure uses the following variables:
  - `<SYSTEM_ID>`, which corresponds to the identifier of your Core Server system
  - `<INSTANCE_NAME>`, which corresponds to the name of the concerned instance

### Prerequisites

- This procedure relies on the use of the Introscope Agent, that is automatically deployed when installing an instance of the Core Server system. Check that the following folder contains the `Agent.jar` file:

- /usr/sap/<SID>/<INSTANCE\_NAME>/exe/wily for Linux and UNIX operating systems
- \usr\sap\<SID>\<INSTANCE\_NAME>\exe\wily for a Microsoft Windows operating system
- To collect data using the Introscope Agent, an Introscope Enterprise Manager must be available within your overall landscape. This element is usually installed on the host used for SAP Solution Manager

## Procedure

The integration of an SAP Convergent Charging landscape with CA APM (formerly known as CA Wily Introscope) consists in the following operations:

- For each instance that is supposed to be monitored:
  - The Introscope Agent must be configured accordingly
  - The java configuration of the instance must be updated to take the Introscope Agent into account
  - The Introscope Agent must be activated
- The instances must be restarted
- The result of the integration must be checked

For each instance of your SAP CC system landscape that must be monitored via Introscope:

1. Configure the Introscope Agent, by retrieving the `IntroscopeAgent.profile` file located in the following subfolder of each instance working directory:
  - /usr/sap/<SID>/<INSTANCE\_NAME>/exe/wily/core/config for Linux and UNIX operating systems
  - \usr\sap\<SID>\<INSTANCE\_NAME>\exe\wily\core\config for a Microsoft Windows operating system
2. Copy this `IntroscopeAgent.profile` file into the following directory:
  - /usr/sap/<SID>/<INSTANCE\_NAME>/config for Linux and UNIX operating systems
  - \usr\sap\<SID>\<INSTANCE\_NAME>\config for a Microsoft Windows operating system
3. Edit the copied file and modify the following, uncommenting them when necessary:

Property name	Property value
<code>introscope.autoprobe.logfile</code>	<code>/usr/sap/&lt;SID&gt;/&lt;INSTANCE_NAME&gt;/work/introscope/IntroscopeAutoProbe.log</code>
<code>introscope.autoprobe.directivesFile</code>	<code>/usr/sap/&lt;SID&gt;/&lt;INSTANCE_NAME&gt;/exe/wily/core/config/sap_typical.jar,&lt;INSTANCE_WKG_DIRECTORY&gt;/exe/wily/core/config/sap_srm_crm.jar</code>
<code>log4j.appender.logfile.File</code>	<code>/usr/sap/&lt;SID&gt;/&lt;INSTANCE_NAME&gt;/work/introscope/IntroscopeAgent.log</code>
<code>introscope.agent.enterprise.manager.transport.tcp.host.DEFAULT</code>	<code>&lt;Enterprise Manager hostname or IP address&gt;</code>
<code>introscope.agent.enterprise.manager.transport.tcp.port.DEFAULT</code>	<code>&lt;Enterprise Manager port&gt;</code>

Property name	Property value
introscope.agent.customProcessName	<b>SAP Convergent Charging</b>
introscope.agent.defaultProcessName	<b>SAP Convergent Charging</b>
introscope.agent.extensions.directory	/usr/sap/<SID>/<INSTANCE_NAME>/exe/wily/core/extensions.directory
introscope.agent.jmx.enable	<b>true</b>
com.sap.introscope.agent.autojmx.enable	<false>
introscope.agent.jmx.globalfilter	<b>com.highdeal:*</b>
introscope.agent.jmx.name.primarykeys	<b>type,name</b>
introscope.agent.jmx.name.filter	<b>com.highdeal</b>
introscope.agent.hostName	<Instance hostname (in lower case)>

#### 4. Save changes

Introscope Agent must now be activated, according to the following procedure:

1. Edit the /usr/sap/<SID>/<INSTANCE\_NAME>/config/jstart.config file and add the following options to the javaParameters property:

```
-javaagent:/usr/sap/<SID>/<INSTANCE_NAME>/exe/wily/Agent.jar
-Dcom.wily.introscope.agent.Profile=/usr/sap/<SID>/<INSTANCE_NAME>/config/IntroscopeAgent.profile
-Dcom.wily.introscope.agent.agentName=<AGENT_NAME>
```

Where <AGENT\_NAME> represents a unique name used by every instance using Introscope, and whose value depends on the concerned system:

- **<AGENT\_NAME>=<SYSTEM\_ID>\_<INSTANCE\_TYPE>#<INSTANCE\_NUMBER>\_SCCCoreServer** for the Core Server system (e.g. <CCT\_dispatcher#1\_SCCCoreServer>)
  - **<AGENT\_NAME>=<SYSTEM\_ID>\_BART\_SCCServer** for the BART Server system
2. Save changes
  3. Once the java configuration of the concerned instances has been successfully updated, you need to restart these instances to take this new configuration into account. Refer to the [Starting and stopping the servers \[page 73\]](#) procedure if necessary.
  4. Once the instances successfully restarted, you can check the result of this integration procedure:
    - By checking the content of the following log file: /usr/sap/<SID>/<INSTANCE\_NAME>/work/IntroscopeAgent.<AGENT\_NAME>.log
    - By using an Introscope Workstation available in your overall landscape, and find your system within the list of connected agents

Once the java configuration of the concerned instances has been successfully updated, you need to restart these instances to take this new configuration into account. Refer to the [Starting and stopping the servers \[page 73\]](#) procedure if necessary.

## 5.56 Integrating SAP CC with SAP CTS+

### Description

This procedure explains you how to deploy and configure the SAP CC CTS+ plugin, that is necessary to integrate your SAP CC Core Server system with the SAP enhanced Change and Transport System (SAP CTS+).

### Preliminary Notes

- For more information about the enhanced Change and Transport System, refer to the following page available on the SAP Community Network: <http://scn.sap.com/docs/DOC-8576>
- This procedure only contains information about the SAP CTS+ plugin, and does not contain information about the configuration of the enhanced Change and Transport System. To get such information, refer to SAP Note [2156128](#)

### Prerequisites

- A Core Server system must be available within your landscape. Refer to the [Installing a Core Server on a mono-host landscape \[page 54\]](#) or to the [Installing a Core Server on a multi-hosts landscape \[page 61\]](#) procedures if necessary
- The SAP JVM 8.1 must be installed as standalone on the host where the SAP CC CTS+ plugin is planned to be deployed. This SAP JVM 8.1 must be accessible and executable by the OS user under which the AS JAVA (SAP CC CTS+ plugin `deploy_cc` script) runs. The `SAPCC_JAVA_HOME` environment variable must be set to the path of the JVM. Refer to the [Downloading the SAP JVM \[page 26\]](#) and [Setting up the system environment variables \[page 35\]](#) procedures if necessary

### Getting the SAP CC CTS+ plugin

The SAP CC CTS+ plugin is available within a ZIP archive located:

- In the Installation DVD of SAP Convergent Charging 5.0

- On SAP ONE Support Launchpad

If you want to get the Core Tool from the installation DVD, take it from the following folder of the DVD: /  
DATA\_UNITS/CC50\_TOOLS\_CONTENT\_UC\_OSIND

If you want to download the latest version, execute the following procedure:

1. Go to SAP ONE Support Launchpad at the following address: <https://launchpad.support.sap.com/>
2. Click the *Software Downloads* launch tile of the *System Operations and Maintenance* section
3. Click the *Support Packages and Patches* section
4. Expand the *By Alphabetical Index (A-Z)* section
5. Click the *C* letter
6. Click the “*SAP Convergent Charging*” element of the list
7. Click the *SAP Convergent Charging 5.0* element of the list

### i Note

Previous versions are also available but this procedure only concerns the 5.0 release

8. Click the *CTS+ PLUGIN 5.0* element of the list to open the *Downloads* section
9. Choose the item matching the level of the Support Package and Patch of your SAP Convergent Charging 5.0 Core Server system: CCCTSPLUGIN<SP\_LEVEL>P\_<PATCH\_LEVEL>-XXXXXXXXX.ZIP  
Where:
  - <SP\_LEVEL> is the SAP Convergent Charging 5.0 Core Server Support Package level
  - <PATCH\_LEVEL> is the SAP Convergent Charging 5.0 Core Server Patch level

## Deploying the SAP CC CTS+ plugin

Once downloaded, use the following procedure to deploy the SAP CC CTS+ plugin on the targeted SAP CTS system:

### Linux and UNIX operating systems

1. Copy the SAP CC CTS+ plugin ZIP archive on the targeted SAP CTS system. Refer to [Getting the SAP CC CTS+ plugin \[page 175\]](#) procedure if necessary.
2. Create an IS-CC folder within the /usr/sap/<CTS\_SYSTEM\_SID>/global/CtsScripts directory (the path will be /usr/sap/<CTS\_SYSTEM\_SID>/global/CtsScripts/IS-CC).

If this folder already exists, execute the following operations:

- Back-up the /usr/sap/<CTS\_SYSTEM\_SID>/global/CtsScripts/IS-CC/bin directory, that contains scripts files whose configuration might have been previously modified
  - Remove all elements of the /usr/sap/<CTS\_SYSTEM\_SID>/global/CtsScripts/IS-CC folder
3. Uncompress the SAP CC CTS+ plugin ZIP archive using the following command:

```
unzip <SAP_CC_CTS_PLUGIN_ZIP_ARCHIVE> -d /usr/sap/<CTS_SYSTEM_SID>/global/CtsScripts/IS-CC
```

4. Ensure security settings according to your needs and security policy:
  - The `deploy_cc.sh` script should have "execute" permissions for the user under which the AS JAVA runs.



- The `CtsScripts` directory should have restricted permissions for other users not involved into the deployment and setup process.
5. Apply SAP Note [2792507](#) to enable the script-based deployment of the SAP enhanced Change and Transport System (SAP CTS+)

## Microsoft Windows operating system

1. Copy the SAP CC CTS+ plugin ZIP archive on the targeted SAP CTS system. Refer to [Getting the SAP CC CTS+ plugin \[page 175\]](#) procedure if necessary.
2. Create an `IS-CC` folder within the `C:\usr\sap\<CTS_SYSTEM_SID>\global\CtsScripts` directory (the path will be `C:\usr\sap\<CTS_SYSTEM_SID>\global\CtsScripts\IS-CC`).  
If this folder already exists, execute the following operations:
  - Back-up the `C:\usr\sap\<CTS_SYSTEM_SID>\global\CtsScripts\IS-CC\bin` directory, that contains scripts files whose configuration might have been previously modified
  - Remove all elements of the `C:\usr\sap\<CTS_SYSTEM_SID>\global\CtsScripts\IS-CC` folder
3. Uncompress the SAP CC CTS+ plugin ZIP archive using the following command:
 

```
unzip <SAP_CC_CTS_PLUGIN_ZIP_ARCHIVE> -d C:\usr\sap\<CTS_SYSTEM_SID>\global\CtsScripts\IS-CC
```
4. Ensure security settings according to your needs and security policy:
  - The `deploy_CC.bat` script should have "execute" permissions for the user under which the AS JAVA runs.
  - The `CtsScripts` directory should have restricted permissions for other users not involved into the deployment and setup process.
5. Apply SAP Note [2792507](#) to enable the script-based deployment of the SAP enhanced Change and Transport System (SAP CTS+)

## Configuring the SAP CC CTS+ plugin

The SAP CC CTS+ plugin is delivered as a script file named:

- `deploy_CC.bat` for Microsoft Windows operating systems
- `deploy_CC.sh` for Linux and UNIX operating systems

To fit your environment, you can use the following procedure to modify the parameters used within the script file:

- `SAPCC_JAVA_HOME`, that corresponds to the home directory of the standalone SAP JVM 8.1
- `LIBRARY_PATH`, that corresponds to the folder containing the different libraries used by the plugin
- `LOG_SEVERITY`, that corresponds to the level of log messages received from the Core Server system, whose supported value can be:
  - `debug`, which is used to display all available information
  - `info`, which is used to display only relevant information
  - `warning`, which is used to display warnings and error messages
  - `error`, which is used to display only error messages

## Linux and UNIX operating systems

- Open the `/usr/sap/<CTS_SYSTEM_SID>/global/CtsScripts/IS-CC/bin/deploy_CC.sh` script file
- Uncomment and replace the `<JAVA_PATH>` string by the relevant value in the following line:

```
#SAPCC_JAVA_HOME=<JAVA_PATH>
```

- The default value of the `LIBRARY_PATH` parameter corresponds to the `/usr/sap/<CTS_SYSTEM_SID>/global/CtsScripts/IS-CC/jars` directory. In case you need to install these libraries in a different folder, modify the following line accordingly:

```
LIBRARY_PATH=./jars/
```

- The default value of the `LOG_SEVERITY` parameter corresponds to the info level. In case you need to modify this log level, modify the following line accordingly:

```
LOG_SEVERITY=info
```

- Save your modifications and exit your text editor

## Microsoft Windows operating system

- Open the `\usr\sap\<CTS_SYSTEM_SID>\global\CtsScripts\IS-CC\bin\deploy_CC.bat` script file
- Uncomment and replace the `<JAVA_PATH>` string by the relevant value in the following line:

```
::SET SAPCC_JAVA_HOME=<JAVA_PATH>
```

- The default value of the `LIBRARY_PATH` parameter corresponds to the `\usr\sap\<CTS_SYSTEM_SID>\global\CtsScripts\IS-CC\jars` directory. In case you need to install these libraries in a different folder, modify the following line accordingly:

```
SET LIBRARY_PATH=./jars\
```

- The default value of the `LOG_SEVERITY` parameter corresponds to the info level. In case you need to modify this log level, modify the following line accordingly:

```
SET LOG_SEVERITY=info
```

- Save your modifications and exit your text editor

# 5.57 Integrating SAP CC with SAP Convergent Invoicing

## Description

This procedure explains you how to configure an SAP CC stand-alone Core Server system in order to communicate with the SAP Convergent Invoicing system for billing and invoicing purposes.

## Preliminary Notes

- In case you have just installed your SAP CC Core Server system using a stand-alone scenario instead of an integrated one, SAP SE recommends that you reinstall your system instead of using this procedure, in order to avoid any possible manual error
- This procedure requires to restart your landscape. SAP SE thus recommends that you prepare and test this integration procedure within a validation landscape before executing it on your production landscape itself
- This procedure can be used to integrate with SAP CI and generate:
  - Charged items only (cit)
  - Charged items and consumptions items (cit\_ci)

According to your business, replace the <MODE> argument in the procedure with the relevant value.

## Prerequisites

- A Core Server system must be available within your landscape. Refer to the [Installing a Core Server on a mono-host landscape \[page 54\]](#) or to the [Installing a Core Server on a multi-hosts landscape \[page 61\]](#) procedures if necessary
- This procedure uses the Setup Tool, Config Tool and Core Tool user interfaces. For further information about these user interfaces, refer to the following procedures:
  - [Launching Setup Tool \[page 133\]](#)
  - [Launching Config Tool \[page 136\]](#)
  - [Launching Core Tool \[page 117\]](#)

## Procedure

The integration of an SAP Convergent Charging landscape with SAP Convergent Invoicing consists in the following operations:

- Installing Bulkloader instances
- Loading relevant information related to SAP CI in the Core Database:
  - JCo destination
  - Default mappings
  - CIF configuration
  - System parameters
- Restarting the Updater and Dispatcher instances
- Configuring the required master data:
  - Default CMA
  - External currencies
- Restarting the Rater instances
- Starting the Bulkloader instances

### 1. Installing the Bulkloader instances

To work in conjunction with SAP CI, each Rater of your landscape must be associated to a dedicated Bulkloader:

- Deployed on the same host as the Rater
- Sharing the same instance number

To install the relevant Bulkloaders within your landscape, execute the [Adding Core Server instances in a multi-hosts landscape \[page 70\]](#) procedure on each host where a Rater is currently deployed, taking into consideration the previously mentioned requirements and without restarting the instances at the end of the installation process.

## 2. Loading information related to SAP CI in the Core Database

Once Bulkloaders have been successfully installed, it is necessary to load the following information in the Core Database:

- The JCo destination used to connect to the relevant SAP CI system
  - The default mappings
  - The configuration of the CIF
  - Some additional system parameters
  - The configuration of the RIF
1. To create the relevant JCo destination, execute the following operations:
    - Connect to the host of your landscape where a Dispatcher is installed
    - Copy the `jco.destination.sk` file available in the `config/ci` folder of the Dispatcher instance in a new `jco.destination` file
    - Edit this newly created file and modify the following parameters to fit the targeted SAP CI system:
 

```
jco.client.ashost
jco.client.sysnr
jco.client.client
jco.client.user
jco.client.passwd
```
    - Execute the `jcodestination import` command of the Setup Tool user interface to import these parameters in the Core Database
    - Execute the `erpreferencesystem setJCoDestination` command of the Setup Tool user interface to link this JCo destination to the targeted SAP CI system
  2. To load the relevant default mappings related to charged items, execute the following operations:
    - Copy the `sapcc_ci_additionalFields.xml.sk` file available in the `config/standalone` folder of the Dispatcher instance in a new `sapcc_ci_additionalFields.xml` file
    - Execute the `sapci importDefaultMapping` command of the Setup Tool user interface (using the `chargeableItem` type) to import these parameters in the Core Database
    - Copy the `sapci_cit_defaultMapping.xml.sk` file available in the `config/sapci` folder of the Dispatcher instance in a new `sapci_cit_defaultMapping.xml` file
    - Execute the `sapci importDefaultMapping` command of the Setup Tool user interface (using the `chargedItem` type) to import these parameters in the Core Database
  3. In case you want to use consumption items, it is necessary to load the relevant default mappings related to charged items and consumption items by executing the following operations:
    - In case you want to use consumption items, also copy the `sapci_ci_defaultMapping.xml.sk` file available in the `config/sapci/cit_ci` folder of the Dispatcher instance in a new `sapci_ci_defaultMapping.xml` file
    - Execute the `sapci importDefaultMapping` command of the Setup Tool user interface (using the `chargeableItem` type) to import these parameters in the Core Database
  4. To configure the generation of data files during the execution of the charging and bulkloading processes, execute the following operations:

- Copy the `cif.rater.config.xml.sk` file available in the `config/sapci/<MODE>` folder of the Dispatcher instance in a new `cif.rater.config.xml` file
- In case you need to fit specific needs, modify the newly created `cif.rater.config.xml` file
- Execute the `cif import` command of the Setup Tool user interface (using the `rater` type of targeted instance) to import these parameters in the Core Database
- Copy the `cif.bulkloader.config.xml.sk` file available in the `config/sapci/<MODE>` folder of the Dispatcher instance in a new `cif.bulkloader.config.xml` file
- In case you need to fit specific needs, modify the newly created `cif.bulkloader.config.xml` file
- Execute the `cif import` command of the Setup Tool user interface (using the `bulkLoader` type of targeted instance) to import these parameters in the Core Database

### i Note

For further information about the configuration of the CIF, refer to the [Data Files Generation](#) section of the [SAP CC 5.0 Tuning Guide](#) documentation.

5. To load the configuration parameters related to SAP CI, execute the following operations:
  - Copy the `parameters.xml.sk` file available in the `config/sapci/<MODE>` folder of the Dispatcher instance in a new `parameters.xml` file
  - Execute the `configuration import` command of the Config Tool user interface to load this set of configuration parameters in the Core Database
6. To configure the use of the rerating feature, execute the following operations:
  - Copy the `rif.rater.config.xml.sk` file available in the `config/sapci/<MODE>` folder of the Dispatcher instance in a new `rif.rater.config.xml` file
  - Execute the `rif import` command of the Setup Tool user interface to import these parameters in the Core Database

### 3. Restarting the Updater and Dispatcher instances

Once the Core Database has been updated with the relevant information, it is necessary to restart the Updater and Dispatcher instances to update their cached structures with the imported parameters that are required by the Core Tool in the next step. For further information, refer to the [Starting and stopping the servers \[page 73\]](#) procedure if necessary.

### 4. Configuring required master data

Once the Core Database has been updated with the relevant information, it is necessary to execute the following operations within the Core Tool user interface:

- Creation of the default CMA
  - Synchronization of the currencies defined in SAP CI
1. To work in conjunction with SAP ERP/FI-CA and SAP CRM systems, it is necessary to create a Customer Management Area used for connection purposes. To create this CMA, launch the Core Tool user interface and click the **Home > Tools > Customer Management Areas** menu
  2. As some differences may exist in terms of currencies defined in the 2 systems, it is necessary to synchronize SAP CC and SAP CI. To synchronize the currencies, launch the Core Tool user interface and click the **Home > Tools > Currencies > Synchronize** menu

### i Note

For further information about customer management areas and currencies synchronization, refer to the dedicated sections available in the [SAP Convergent Charging Core Tool online help documentation](#).

## 5. Restarting the Rater instances and starting the Bulkloader instances

Once the Rater and Bulkloader instances have been successfully configured, you need to restart them in order to take this new configuration into account. SAP SE recommends that you first restart the Raters, then start the Bulkloaders. For further information, refer to the [Starting and stopping the servers \[page 73\]](#) procedure if necessary.

Once the instances of your SAP Convergent Charging landscape have been successfully restarted, you can use the Core Tool to set up your master data such as relevant billable item and/or consumption item mappings:

- On Existing Charged/chargeable Item Classes
- On New Charged/chargeable Item Classes

## 5.58 Copying an SAP CC Core Server

### Description

For multiple reasons such as development integration tests, system tuning, performance tests, backup operations, and so on, it might be necessary to copy a Core Server system from one landscape to another, an operation that consists in:

- Preparing the destination system
- Backing-up the tables of the destination Core Database and Session Database, according to the copy scenario
- Backing-up the source Core Database and Session Database
- Transferring the adequate data from the source Core Database and Session Database to the destination ones
- Restoring the adequate data within the destination Core Database and Session Database
- Restarting the destination system

You can use this procedure as **guidelines** for copying a Core Server system (considered as the source system) from:

- A production landscape to another landscape that is used for any purpose
- A non-production landscape to another non-production landscape

#### Caution

This procedure requires to shut down both source and destination Core Server systems. This operation can impact your overall landscape and thus your business in case the source system is part of a production landscape. SAP SE thus recommends you to be very careful when executing this procedure.

## Prerequisites

- A Core Server system must be available within your landscape. This Core Server system will be considered as the source system, whose version must correspond to the destination system
- Both source and destination Core Databases must have the same software version
- If the Session Database is used, both source and destination Session Databases must have the same software version
- Both Core Server systems used as source and destination must be installed on physical hosts:
  - Compatible in terms of hardware sizing to ensure that the instances of the destination Core Server can start after this procedure
  - Running under the same operating system
  - Where concerned third-party systems (such as SAP CI, CA APM, and so on) are already installed and available, running under the same versions

### i Note

If the source Core Server system is integrated with SAP Convergent Invoicing, it is necessary to use a similar configuration for both source and destination systems to ensure that:

- The same currencies are defined in both source and destination SAP CI systems
- The same "SAP Convergent Charging Integration Scenario" is used ("Billing and Invoicing in SAP Convergent Invoicing" or "Billing, Invoicing, and Storage of Consumption Data in SAP Convergent Invoicing")
- The same Consumption Item Classes and Billable Item Classes are defined
- The names of the used JCo destinations are the same
- The targeted SAP systems of the used JCo destinations must be the same if your copy scenario concerns a copy of a Core Server system from a production to another production landscape, or different otherwise

Moreover, when using this procedure to copy a Core Server system from a production to another production landscape, ensure that:

- The same transport destinations are defined in both source and destination systems
- All pending data files containing charged items, chargeable items or notifications are:
  - Processed in the source system
  - Deleted from the destination

## Preparing the destination system

The first step of this procedure consists in preparing the Core Server system that is considered as the destination system, by referring to the [Installing SAP Convergent Charging \[page 12\]](#) section of this documentation and respecting the prerequisites.

Once this destination system has been prepared, SAP SE highly recommends that you back up the configuration of this system, using the Config Tool and Setup Tool user interfaces. This backup will be used at the end of this procedure to ensure that this configuration has been successfully restored on the destination system after the data transfer from the source system. For further information about the Config Tool and Setup Tool user interfaces, refer to the following procedures:

- [Launching Config Tool \[page 136\]](#)
- [Launching Setup Tool \[page 133\]](#)

## Backing-up the destination databases

The second step of this procedure consists in backing-up the tables of the destination Core and Session Databases, which means:

- Shutting down the destination Core Server
  - Exporting all the tables of the Core Database in case of failure during the copy procedure
  - Exporting all the tables of the Session Database in case of failure during the copy procedure
  - Exporting a set of tables of the Core Database that relate to the configuration of the destination Core Server, whose content will be restored later
1. To ensure data consistency and avoid any locking problem during backup operations, it is necessary to shut down all the instances of the destination Core Server. Refer to the [Starting and stopping the servers \[page 73\]](#) procedure if necessary
  2. As data within the destination Core Database will be overwritten in the next steps, it might be necessary to restore the content of the destination Core Database in case of failure during the execution of the copy procedure. Refer to your DBA<sup>63</sup> for further information about backup procedures and associated commands that must be performed to create this safety backup of all the tables of this database
  3. As data within the destination Session Database will be overwritten in the next steps, it might be necessary to restore the content of the destination Session Database in case of failure during the execution of the copy procedure. Refer to your DBA for further information about backup procedures and associated commands that must be performed to create this safety backup of all the tables of this database
  4. In addition to the previously created safety backup, it is necessary to create a dedicated backup containing the following set of tables of the Core Database that relate to the configuration of the destination Core Server. For further information about backup procedures and associated commands, refer to your DBA.
    - **LICENSE** table, that contains information about the SAP Convergent Charging license
    - **VERSION** table, that contains the history of database changes performed on an installed version of SAP CC
    - **CONFIGURATION** table, that contains some specific configuration settings of SAP CC
    - **INSTANCE\_CONFIGURATION** table, that contains all the system parameters set for each type of instance
    - **INSTANCE\_MAP** table, that contains the map of available instances of the Core Server system
    - **KEY\_STORE** table, that contains the private keys and their associated certificates when using SSL/TLS
    - **INSTANCE\_KEY\_STORE** table, that is used to link a service to a key store entry when using SSL/TLS
    - **CERT\_STORE** table, that contains the certificates of allowed clients when using SSL/TLS
    - **INSTANCE\_CERT\_STORE** table, that is used to link a service to a client certificate when using SSL/TLS

And if your copy scenario concerns a copy of a Core Server system from a production to a non-production landscape, also backup the following tables of the Core Database:

- **HCI\_USER** table, that contains information about the authorized users of SAP CC
- **USER\_RIGHT** table, that contains the authorization roles of each SAP CC user

---

<sup>63</sup> DataBase Administrator



- **USER\_PASSWORD** table, that contains the history of passwords of the SAP CC users
- **USER\_FAILED\_AUTHENTICATION** table, that contains the list of failed authentication attempts for the different users since their last successful authentication

## Backing-up the source databases

The third step of this procedure consists in making consistent backups of the tables of the source databases. To ensure data consistency and avoid any locking problem during backup operations, it is necessary to shut down all the instances of the destination Core Server, referring if necessary to the [Starting and stopping the servers \[page 73\]](#) procedure. Then, according if necessary to the recommendations of your DBA, create the consistent backup of:

- The tables of the Core Database
- The tables of the Session Database, in case your copy scenario concerns a copy of a Core Server system between 2 production landscapes

## Transferring adequate data from the source databases

The fourth step of this procedure consists in transferring the content of the consistent backups from the source databases to the destination databases. This operation consists in:

- Emptying the tables of the destination Core Database
- Emptying the tables of the destination Session Database
- Importing the previously created consistent backup related to the Core Database
- Importing the previously created consistent backup related to the Session Database, in case:
  - Your copy scenario concerns a copy of a Core Server system between 2 production landscapes
  - Your Core Server system uses the Session Database

## Restoring the destination Core Database

The fifth step of this procedure consists in managing the content of some tables of the destination Core Database to restore an adequate configuration of the destination Core Server. According to your copy scenario, the following table provides you with the necessary information to decide to:

- **Keep** the content imported from the source database
- **Empty** the content imported from the source database
- **Overwrite** the content imported from the source database with the configuration data backed-up in step 2, after having emptied the concerned table

Table	Action			Notes
	Keep	Empty	Overwrite	
<b>Core Database</b>				
LICENSE	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
VERSION	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
CONFIGURATION	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
INSTANCE_CONFIGURATION	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
INSTANCE_MAP	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
KEY_STORE	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
INSTANCE_KEY_STORE	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
CERT_STORE	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
INSTANCE_CERT_STORE	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
CHARGED_ITEM_FILES	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	This table should be empty due to prerequisites
WS_JOB	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
HCI_USER	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>Overwrite</b> if your copy scenario concerns a copy of a Core Server system from a production to a non-production landscape. <b>Keep</b> otherwise.
USER_RIGHT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
USER_PASSWORD	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
USER_FAILED_AUTHENTICATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
RATING_SESSION_@NUMBER@	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<b>Empty</b> if your copy scenario concerns a copy of a Core Server system from a production to a non-production landscape. <b>Keep</b> otherwise.
RENEW_RESERVATION_NOTIFICATION	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
SPENDING_STATUS_MONITORING	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<b>i Note</b> @NUMBER@ representing the partition number, the RATING_SESSION_@NUMBER@ tables represents a possible set of 480 tables to restore.
SPENDING_STATUS_REPORT	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
CHANGE_LIST	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
CHAN_OBJECT	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
CHAN_OBJECT_SNAPSHOT	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
TRANSPORT_REQUEST	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
TRAN_DESTINATION	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

■: Supported action, □: Unsupported action

### **i Note**

If your RDBMS<sup>64</sup> provides statistics, you can re-compute them on the destination Core Database after the import.

## **Restarting the Core Server systems**

The last step of this procedure consists in:

- Creating a new backup of the configuration of the destination system, used to compare with the configuration backed-up in Step 1 in order to ensure that this configuration has been successfully restored (in Step 4) and avoid situations such as:
  - Bad instance configuration (including database connection parameters)
  - Bad securing information
  - Bad JCo destinations
  - And so on
- Starting the different instances of both source and destination Core Servers. Refer to the [Starting and stopping the servers \[page 73\]](#) procedure if necessary.

### **⚠ Caution**

For security and confidentiality reasons, SAP SE highly recommends that you delete the backed-up content once you ensured that the copy procedure successfully ended.

---



<sup>64</sup> Relational Database Management System

# Important Disclaimers and Legal Information

## Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.

About the icons:

- Links with the icon : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon : You are leaving the documentation for that particular SAP product or service and are entering a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

## Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.

The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

## Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

## Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.



© 2019 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see <https://www.sap.com/about/legal/trademark.html> for additional trademark information and notices.