HITACHI
Inspire the Next

uCosminexus Service Platform

Setup and Operation Guide

3020-3-Y45-40(E)

■ Relevant program products

See the manual *uCosminexus Application Server Overview*.

■ Export restrictions

If you export this product, please check all restrictions (for example, Japan's Foreign Exchange and Foreign Trade Law, and USA export control laws and regulations), and carry out all required procedures.

If you require more information or clarification, please contact your Hitachi sales representative.

■ Trademarks

AIX is a trademark of International Business Machines Corporation in the United States, other countries, or both.

All Borland brand and product names are trademarks or registered trademarks of Borland Software Corporation in the United States and other countries.

HP-UX is a product name of Hewlett-Packard Development Company, L.P. in the U.S. and other countries.

IBM is a trademark of International Business Machines Corporation in the United States, other countries, or both.

IIOP is a trademark of Object Management Group, Inc. in the United States.

Linux(R) is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

Microsoft Office and Excel are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

OMG, CORBA, IIOP, UML, Unified Modeling Language, MDA and Model Driven Architecture are either registered trademarks or trademarks of Object Management Group, Inc. in the United States and/or other countries.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

SOAP is an XML-based protocol for sending messages and making remote procedure calls in a distributed environment.

UNIX is a registered trademark of The Open Group in the United States and other countries.

VisiBroker is a trademark or registered trademark of Micro Focus IP Development Limited or its Subsidiaries or affiliated companies in the United Kingdom, United States and other countries.

Windows, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The other company names and product names are either trademarks or registered trademarks of the respective companies.

Eclipse is an open development platform for tools integration provided by Eclipse Foundation, Inc., an open source community for development tool providers.

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

Other product and company names mentioned in this document may be the trademarks of their respective owners. Throughout this document Hitachi has attempted to distinguish trademarks from descriptive terms by writing the name with the capitalization used by the manufacturer, or by writing the name with initial capital letters. Hitachi cannot attest to the accuracy of this information. Use of a trademark in this document should not be regarded as affecting the validity of the trademark.

■ Microsoft product name abbreviations

This manual uses the following abbreviations for Microsoft product names.

Abbreviation			Full name or meaning
Excel			Microsoft(R) Excel
			Microsoft(R) Office Excel
Windows	Windows Server 2008	Windows Server 2008 x86	Microsoft(R) Windows Server(R) 2008 Standard 32-bit
			Microsoft(R) Windows Server(R) 2008 Enterprise 32-bit
		Windows Server 2008 x64	Microsoft(R) Windows Server(R) 2008 Standard
			Microsoft(R) Windows Server(R) 2008 Enterprise
		Windows Server 2008 R2	Microsoft(R) Windows Server(R) 2008 R2 Standard
			Microsoft(R) Windows Server(R) 2008 R2 Enterprise

Abbreviation			Full name or meaning
Windows	Windows Server 2008	Windows Server 2008 R2	Microsoft(R) Windows Server(R) 2008 R2 Datacenter
	Windows Server 2012	Windows Server 2012 Standard	Microsoft(R) Windows Server(R) 2012 Standard
		Windows Server 2012 Datacenter	Microsoft(R) Windows Server(R) 2012 Datacenter
	Windows XP		Microsoft(R) Windows(R) XP Professional Operating System
	Windows Vista	Windows Vista Business	Microsoft(R) Windows Vista(R) Business (32-bit)
		Windows Vista Enterprise	Microsoft(R) Windows Vista(R) Enterprise (32-bit)
		Windows Vista Ultimate	Microsoft(R) Windows Vista(R) Ultimate (32-bit)
	Windows 7	Windows 7 x86	Microsoft(R) Windows(R) 7 Professional (32-bit)
			Microsoft(R) Windows(R) 7 Enterprise (32-bit)
			Microsoft(R) Windows(R) 7 Ultimate (32-bit)
		Windows 7 x64	Microsoft(R) Windows(R) 7 Professional (64-bit)
			Microsoft(R) Windows(R) 7 Enterprise (64-bit)
			Microsoft(R) Windows(R) 7 Ultimate (64-bit)
	Windows 8	Windows 8 x86	Windows(R) 8 Pro (32-bit)
			Windows(R) 8 Enterprise (32-bit)
		Windows 8 x64	Windows(R) 8 Pro (64-bit)
			Windows(R) 8 Enterprise (64-bit)
Word			Microsoft(R) Office Word

■ Restrictions

Information in this document is subject to change without notice and does not represent a commitment on the part of Hitachi. The software described in this manual is furnished according to a license agreement with Hitachi. The license agreement contains all of the terms and conditions governing your use of the software and documentation, including all warranty rights, limitations of liability, and disclaimers of warranty.

Material contained in this document may describe Hitachi products not available or features not available in your country.

No part of this material may be reproduced in any form or by any means without permission in writing from the publisher.

■ Issued

Jul. 2015: 3020-3-Y45-40(E)

■ Copyright

All Rights Reserved. Copyright (C) 2015, Hitachi, Ltd.

Preface

For details on the prerequisites before reading this manual, see the preface of the manual *uCosminexus Application Server Overview*.

Contents

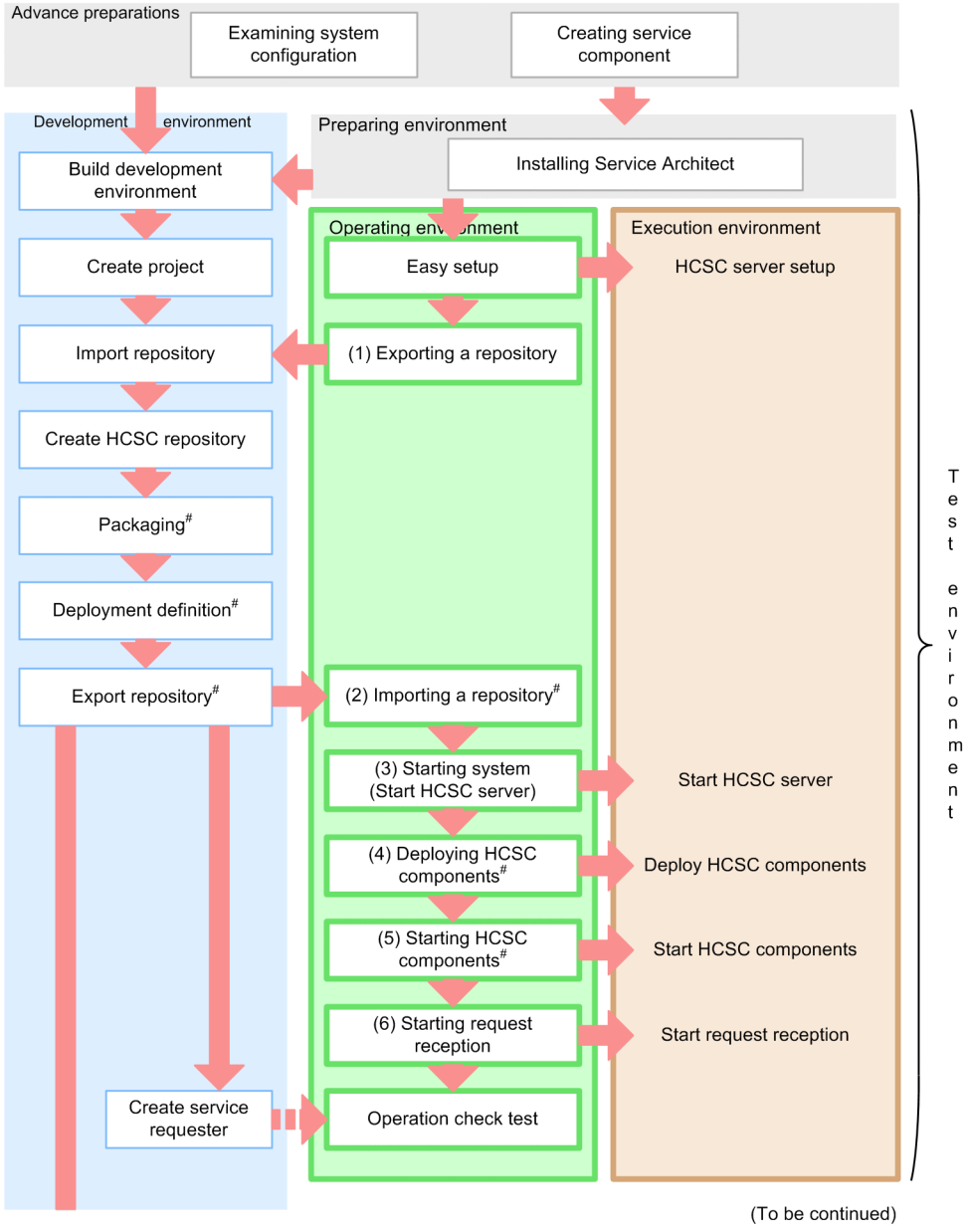
1 Overview of System Operations Based on SOA

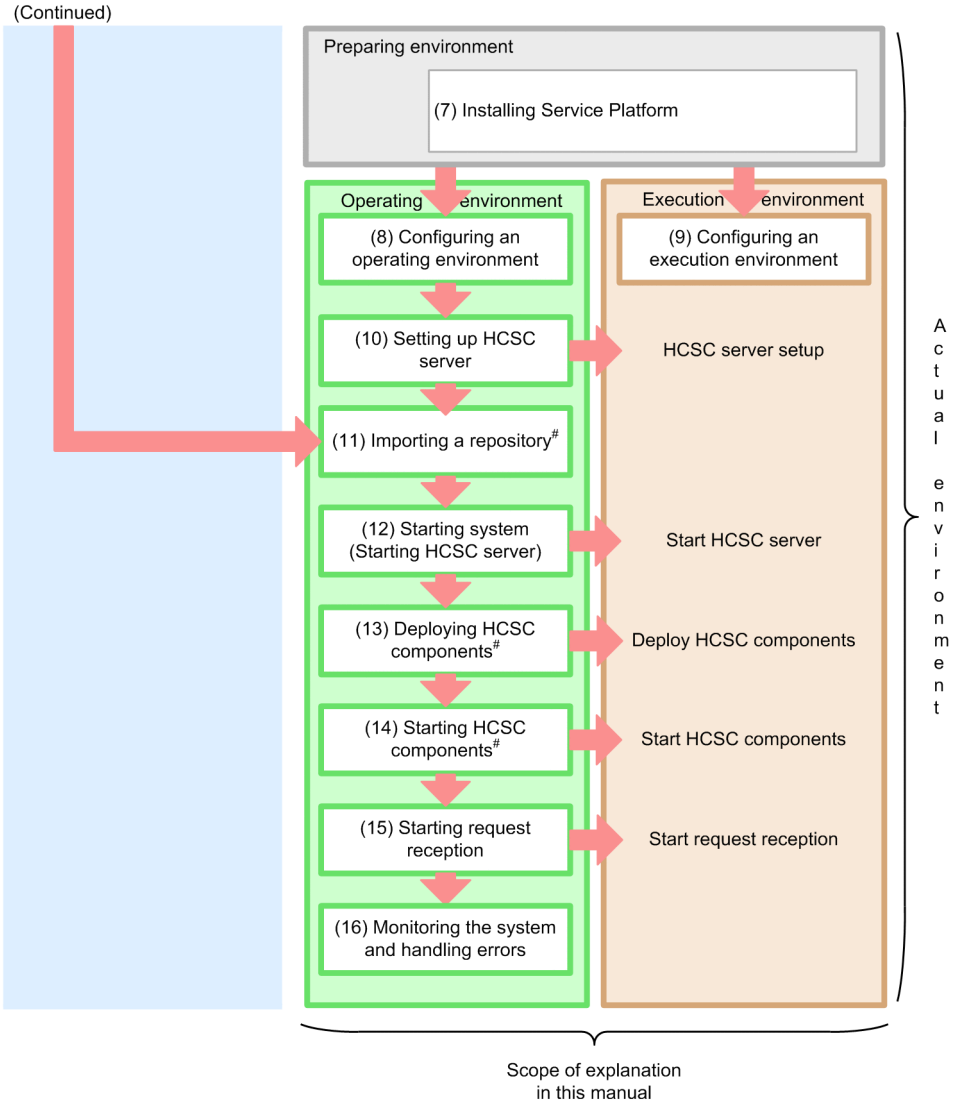
This chapter provides an overview of system operations using a service platform, and describes system configuration and how to set operation guidelines.

1.1 Flow from development to actual operations

The following figure shows the flow from development upto actual operations for a system using Service Platform:

Figure 1–1: FigureFlow from system development to actual operations





#

In a development environment you can also execute these activities in a batch. However, you perform batch execution at the time of system development, or in the duration from unit testing to integration testing. For details, see "7.5 Batch execution of processes starting from deploying HCSC components on the HCSC server" of Service Platform Basic Development Guide.

This manual describes the procedure involved in configuring the operating environment and execution environment, indicated in the figure. For details on activities to be implemented in the development environment and the installation and Easy Setup of the products in the test environment, see "Service Platform Basic Development Guide".

The following is the description of an overview of each activity shown in the figure:

(1) Exporting a repository

After an Easy Setup, you export a repository from the operating environment.

Transfer the HCSC components (service adapters, database adapters, business processes, and user-defined reception) created in the development environment as well as the system configuration definition that defines (deployment definition) how to deploy HCSC components, to a repository exported from operating environment. Additionally, transfer the execution environment setup information (such as the HCSC server configuration and HCSC component deployment information) from the operating environment to the development environment via a repository.

For details on how to export a repository, see "*4.2 Exporting Repository Information*".

(2) Importing a repository

Import the repository in which HCSC components (service adapters, business processes, and user-defined receptions) are created, package and defined in the development environment to the operating environment.

For details on importing a repository, see "*4.3 Importing a repository*".

(3) Starting the system (HCSC server startup)

Start and stop the execution environment from the operating environment.

Use the screen or commands available in operating environment to start and stop HCSC server of the execution environment.

For details on how to start and stop HCSC server, see "*5.3.4 Starting HCSC server*".

Furthermore, start not only HCSC server, but also related systems such as PRF and HTTP Server.

For details on how to start and stop related systems, see, "*5.System Operations*".

For details on screens and commands, see "Service Platform Reference Guide".

(4) Deploying HCSC components

On the HCSC server, deploy HCSC components (service adapters, business processes, and user-defined receptions) imported in the operating environment. Use operating environment commands to deploy HCSC components.

For details on how to deploy HCSC components, see "*3.1.8 Deploying a service adapter*","*3.1.13 Deploying a business process*", and "*3.1.14 Deploying a user-defined reception*".

For details on commands, see " *Service Platform Reference Guide*".

(5) Starting HCSC components

Start the deployed HCSC components (service adapters, business processes, and user-defined receptions).Furthermore, services executed from the service adapter also must be running when you start the service adapter.

Use screens and commands available in the operating environment to start and stop HCSC components.

For details on how to start HCSC components, see "*5.3.6 Starting Service Adapters*","*5.3.7 Starting Business Processes*", and "*5.3.8 Starting user-defined receptions*".

For details on screens and commands, see " Service Platform Reference Guide".

(6) Starting request reception

Start the request reception (standard reception) to receive requests from the service requester.

Use screen and commands available in the operating environment to start and stop standard reception.

For details on how to start a standard reception, see "*5.3.9 Starting standard receptions*".

For details on screens and commands, see "Service Platform Reference Guide".

(7) Installing Service Platform

To configure the execution environment and the operating environment on the same machine, install the Service Platform. To configure the execution environment and the operating environment on separate machines, install the Service Platform on the respective machine on which the execution environment and the operating environment is to be configured.

For details on how to install Service Platform, see "*2.1.2 Installing Service Platform*".

(8) Configuring an operating environment

Configure an operating environment that performs operation management of the HCSC server of the execution environment. Specifically, you make settings for using the Eclipse window to operate the execution environment and each setting required for the operating environment.

For details on settings see "*2.1.5 Embedding HCSC-Manager plug-in in Eclipse*" and "*2.4 Settings Related to the Operating Environment*".

Also, you create definitions required for the setting up the execution environment (HCSC server).

For details on how to create definitions, see "*2.3 Settings related to execution environment*".

(9) Configuring an execution environment

Configure an execution environment to operate HCSC server. However, before setting up the execution environment, you set up the software required for the execution environment.

For details on settings, see "*3.1.2 Setting up the software required for the execution environment*".

(10) Setting up HCSC server

Set up the HCSC server that is the infrastructure for invoking service components in the execution environment (you can unset up this set HCSC server as and when required)

Use commands available in the operating environment to setup the HCSC server.

For details on how to setting up the HCSC server, see "*3.1.3 Setting up an HCSC server*".

Define the runtime information required for the HCSC server to execute as and when required.

For runtime information settings, see "*3.1.4 Setting up the HCSC server definition information*".

For details on commands, see "Service Platform Reference Guide".

(11) Importing repositories

Import repositories used in the test environment to the operating environment. Furthermore, modify the definitions of HCSC components (service adapters, business processes, and user-defined receptions) in repositories, as and when required.

In test and production environments, for some cases in which settings of the usage or non-usage of Reliable Messaging and database are different, you cannot import a repository that was used in the test environment as is to the operating environment. In that case, to incorporate the system configuration definition of the HCSC server set up in the production environment, you must export the repository from the production environment (operating environment) and import the repository to the development environment. For details, see "*1.3 Relationship between Test Environment and Production Environment*".

For details on the method to import repositories, see "*4.3 Importing a repository*".

Furthermore, you change the connection destination, flow-volume control, and communication timeout value for HCSC components created in the development environment at this timing.

For details, see "*5.3.24 Changing the Component Service Connection Point*", "*5.3.25 Changing the Flow Control Value*", and "*5.3.26 Changing the Communication Timeout Value for Invoking Service Modules*".

(12) Starting the system (HCSC server startup)

Start and stop the HCSC server in the operating environment along with the starting and ending of the business in the execution environment.

Use the operating environment screen or commands to start and stop the HCSC server of the execution environment.

For details on the method to start HCSC servers, see "*5.3.4 Starting HCSC server*".

Furthermore, start not only HCSC servers, but also related systems such as PRF and HTTP Server.

For details on the method to start and stop the related systems, see, "*5.System Operations*".

For details on screens and commands, see "Service Platform Reference Guide".

(13) Deploying HCSC components

Deploy HCSC components (service adapters, business processes, and user-defined receptions) imported from the operating environment, to HCSC server.Use commands of the operating environment to deploy HCSC components.

For details on the method to deploy HCSC components, see "*3.1.8 Deploying a service adapter*","*3.1.13 Deploying a business process*", and "*3.1.14 Deploying a user-defined reception*".

For details on commands, see "Service Platform Reference Guide".

(14) Starting HCSC components

Start the deployed HCSC components (service adapters, business processes, and user-defined receptions).Furthermore, the services executed from the service adapter must also be in started status when you start the service adapter. Use the operating environment screen or commands to start and stop HCSC components.

For details on the how to start HCSC components, see "*5.3.6 Starting Service Adapters*","*5.3.7 Starting Business Processes*", and "5.3.8 Starting user-defined receptions".

For details on screens and commands, see "Service Platform Reference Guide".

(15) Starting request reception

Start the request reception (standard reception) that receives requests from the service requestor.

Use the operating environment screen and commands to start and stop standard reception.

For details on starting standard reception, see "*5.3.9 Starting standard receptions*".

For details on screens and commands, see "Service Platform Reference Guide".

(16) Correspondence at the time of monitoring the system and failure occurrence

Monitor the system in the operating environment after starting the business in the execution environment. When a failure occurs, specify the cause of failure, and take countermeasures.

(a) Monitoring the System

After starting business in the execution environment, you can confirm the status of HCSC servers and HCSC components from the operating environment as and when required.

Use the operating environment screen or commands to confirm system status.

For details on the method to confirm system status, see "*5. System Operations*".

Furthermore, in the operating environment, you can confirm its status, delete execution logs, and re-execute process instances, by specifying the target process instance as and when required from the execution logs of process instances of the business processes that are recorded in the database.

Use the command screen or operating environment for confirming process instances, and deleting and re-executing execution logs.

For details on how to manage the execution log of process instances, see "*6.Management of Execution Log*".

For details on screens and commands, see "Service Platform Reference Guide".

(b) Troubleshooting

If a failure occurs during system operations, collect the trace file and the log file from respective environments. Acquire the trace file and the log file, identify the location and cause for the occurrence of the failure, and implement troubleshooting.

Furthermore, if you build a system linking with JP1, the system sends a message to notify the failure as a JP1 event to JP1in service platform. This enables you to collect error messages that are output and monitor those collectively in the integrated console of JP1.

In addition, commands can be automatically executed at the time of responding to the reception of a specific JP1 event (error message) at JP1 side. This allows you to automate (notifying the system administrator when a failure has occurred, executing the command for recovery) system operations.

For acquiring the log file and the trace file at the time of failure occurrence, and confirming detailed information of a JP1 event, see "*7.Troubleshooting*".

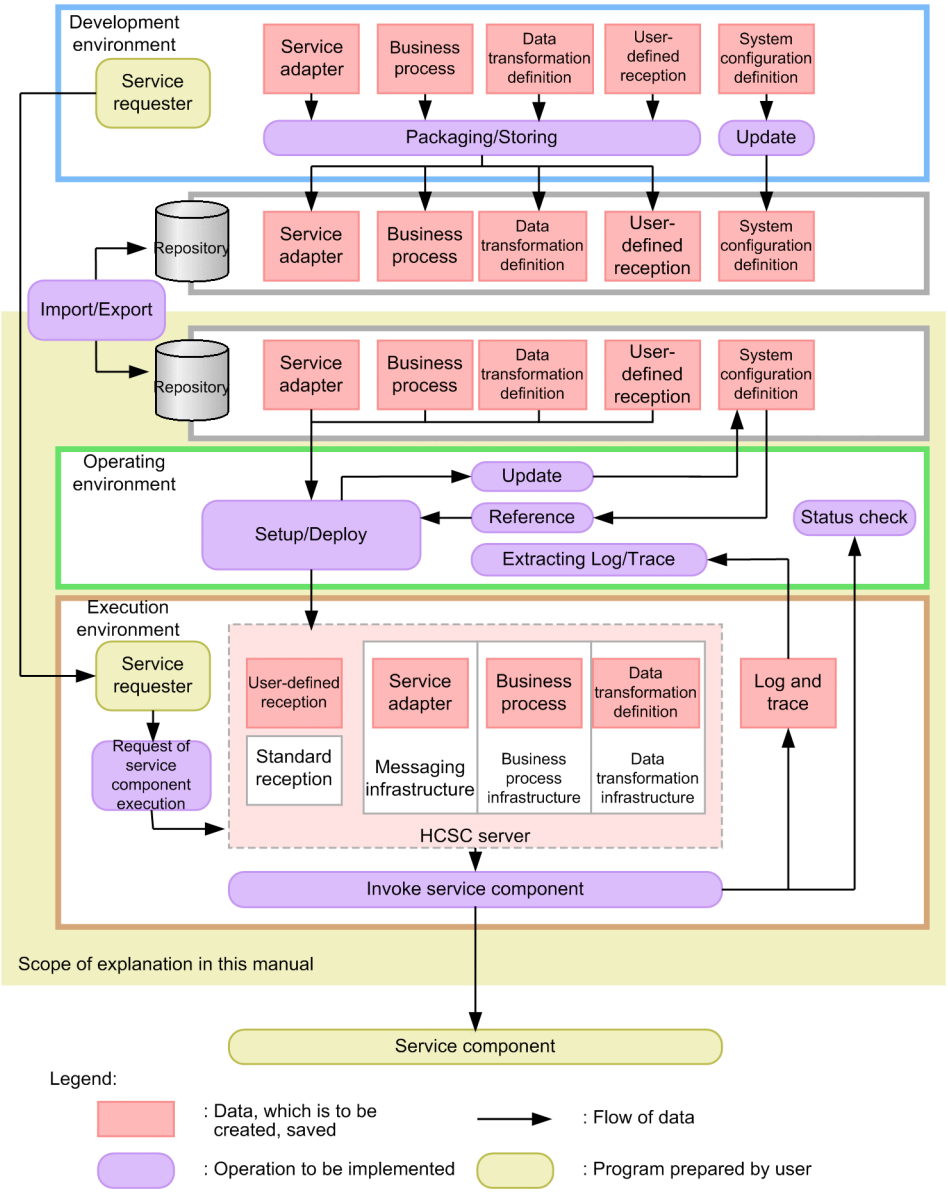
1.2 Relationship of the operating environment and the execution environment with the entire system

In service platform, the development environment, operating environment, and execution environment mutually connect with each other to configure the entire system. This subsection describes the positioning of the execution environment and operating environment.

(1) Positioning in operations

The following figure shows the positioning of the operating environment and the execution environment in the operations of the entire system

Figure 1–2: FigurePositioning in operations



In the operating environment, read the (service adapters, business processes, and user-defined receptions) from HCSC components created in the development environment, and deploy to the execution environment. In addition, you can set up an HCSC server to use in the execution environment.

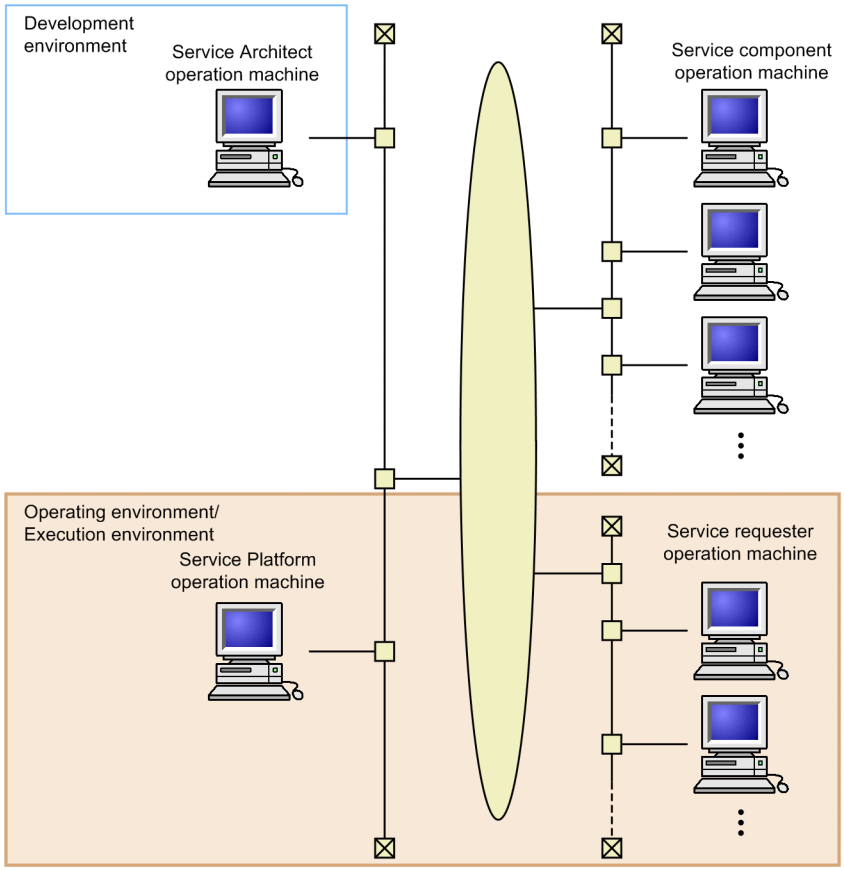
Monitor the starting and stopping status of the system after you start the operation.In the execution environment, invoke service components and business processes through the HCSC server and execute business according to the request message received by the service requester.

(2) Positioning on the network

The development environment, operating environment, and execution environment configure the system by connecting through a network such as the internet or an intranet.

The following figure shows the positioning of the operating environment and the execution environment on the network in the entire system. Furthermore, the configuration of the execution environment differs according to the type of the operation. For the configuration of the execution environment, see "*1.4 Determining the operations policy*".

Figure 1–3: FigurePositioning of the operating environment and the execution environment on the network in the entire system



It is recommended that you set up the operating environment and the execution environment on the same machine.

Furthermore, you can set up the development environment on a different network.

Information such as the execution status of service components in the execution environment is accumulated in the database built on the machine on which Service Platform is operating. In addition, you can also build a database to another machine on which Service Platform is operating, and a machine that can be connected through the network. In this case, you connect the machine on which Service Platform is running and the machine on which you build the database through LAN line.

Furthermore, the database used by the machine on which Service Platform is operating, can take the following configuration.

When you do not set to cluster configuration

Create one database for Service Platform. Also, by dividing the schema of the database for each Service Platform, you can use multiple Service Platforms in a single database.

When you set to cluster configuration

Create one database for the cluster, and share database in multiple Service Platforms.

(3) Configuration of the operating environment and the execution environment

The following table describes the configuration pattern of the operating environment and the execution environment that can be achieved if you set to cluster configuration:

Table 1–1: TableConfiguration of the operating environment and the execution environment at the time of using the cluster

Configuration pattern	Explanation	Database
Operation and execution one-to-one configuration	Deploys the operating environment and the execution environment on a one-to-one basis.	A#
Operation consolidated configuration	Consolidates the operating environment in the server used at the time of execution.	Y

Legend:

Y: Database can be used.

A: Database can be used only in case of new installation.

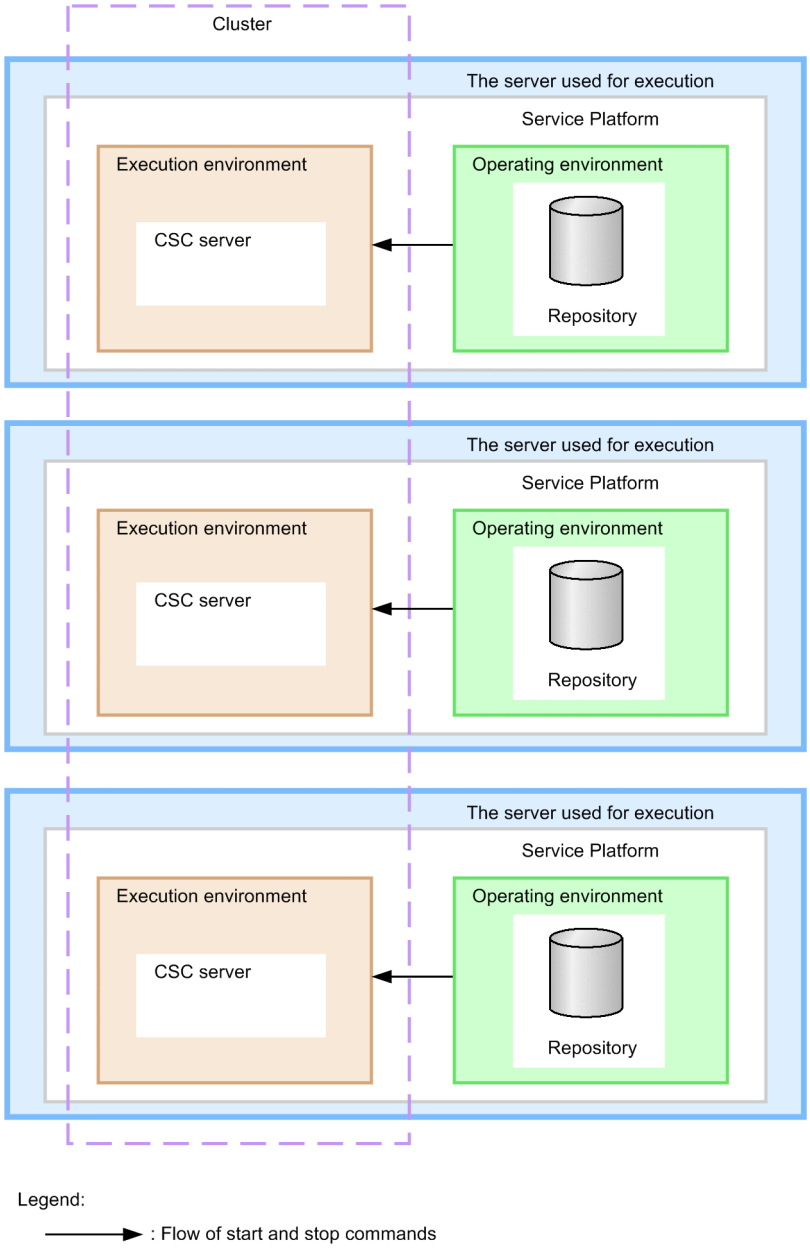
#

You cannot use the database if the version is earlier than 08-70. Also, when you upgrade to version 08-70 and later, you cannot migrate to the operation and execution one-to-one configuration using the database.

To implement the operation and execution one-to-one configuration using the database, you must newly build, and not migrate the operation and execution one-to-one configuration operation rather than the migration to unsetup all HCSC servers in the cluster. At that time, the shared table (information such as shared process instances and execution logs) of the cluster stored in the database is deleted.

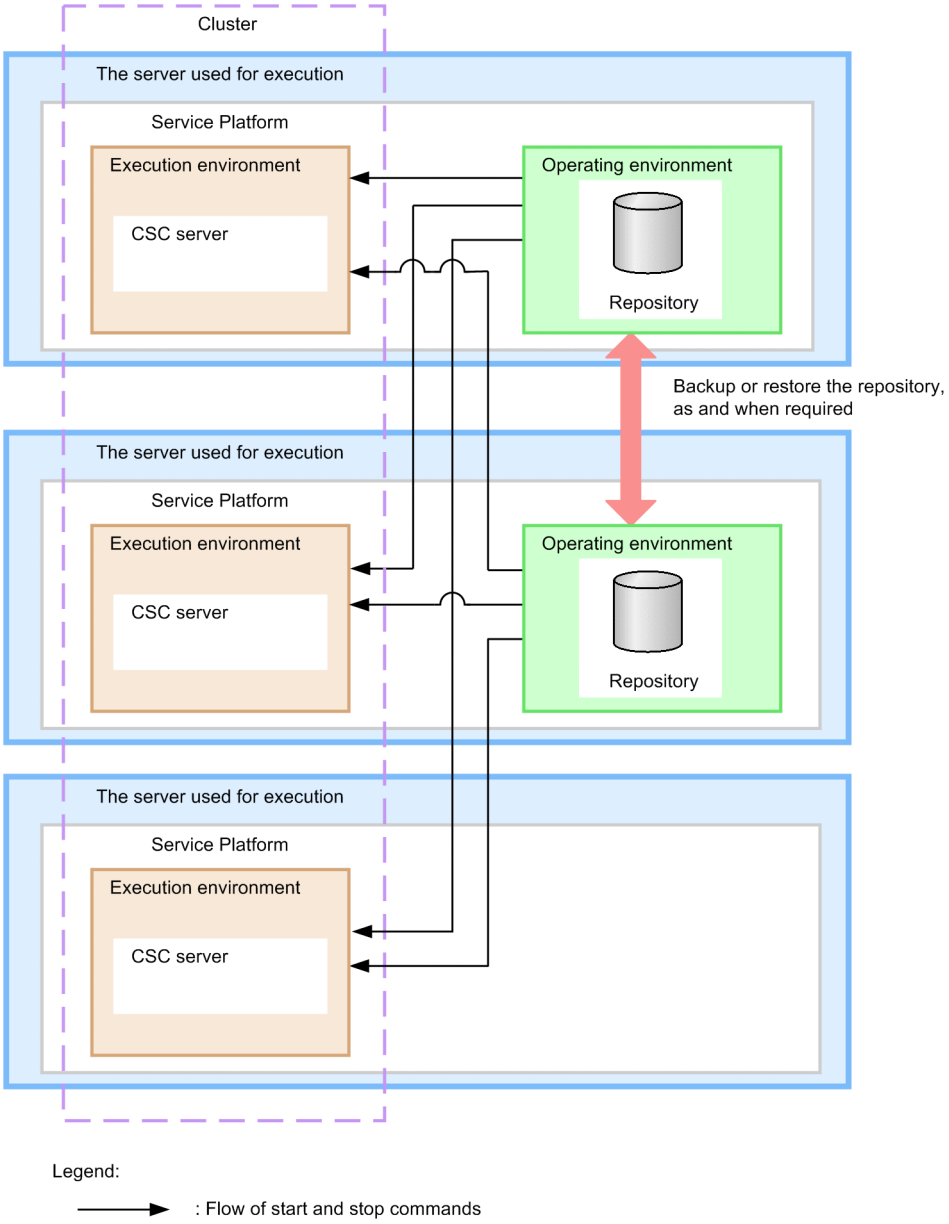
The following figure shows the configuration example of operation and execution one-to-one configuration:

Figure 1–4: FigureConfiguration example of operation and execution one-to-one configuration



The following figure shows the configuration example of the operation consolidated configuration.

Figure 1–5: FigureConfiguration example of the Operation consolidated configuration



1.3 Relationship between Test Environment and Production Environment

On the Service Platform, you first configure a test environment, and then test and debug. You can use the HCSC Easy Setup functionality for configuring the test environment.

When developing a real system, you must configure a production environment other than the test environment. For this reason, you must move the repository used in the test environment to the production environment.

The following are the three cases to move the repository used in the test environment to the production environment:

Case 1

When configuring with the same settings of the database and Reliable Messaging, in the test environment and production environment

Case 2

When configuring with the different settings of the database and Reliable Messaging, in the test environment and in the production environment, the repository used in the test environment can be moved to the production environment as it is#

Case 3

When you re-create a repository of the production environment from the repository used in the test environment because the environments are configured with the different settings of the database and Reliable Messaging in the test environment and production environment#

Note:

For details about whether the repository used in the test environment can be moved to the production environment as it is, see *4.3 Importing a repository*.

The following table describes the settings used for databases and Reliable Messaging corresponding to the above cases. For details about configuration types depending on the usage of databases and Reliable Messaging, see *2.2 Selecting configuration types and SOAP modes*.

Table 1–2: Cases corresponding to the settings used for a database and Reliable Messaging

Test environment settings	Production environment settings		
	Both database and Reliable Messaging are used	Database is used and Reliable Messaging is not used	Both database and Reliable Messaging is not used
Both database and Reliable Messaging are used	Case 1#	Case 3	Case 3
Database is used and Reliable Messaging is not used	Case 2	Case 1#	Case 3
Both database and Reliable Messaging is not used	Case 2	Case 2#	Case 1#

#

Setting to which a user corresponds with the settings of the test environment and the production environment.

An overview of migration in each case is as follows:

(1) Case 1: When configuring with the same settings of the database and Reliable Messaging, in the test environment and the production environment

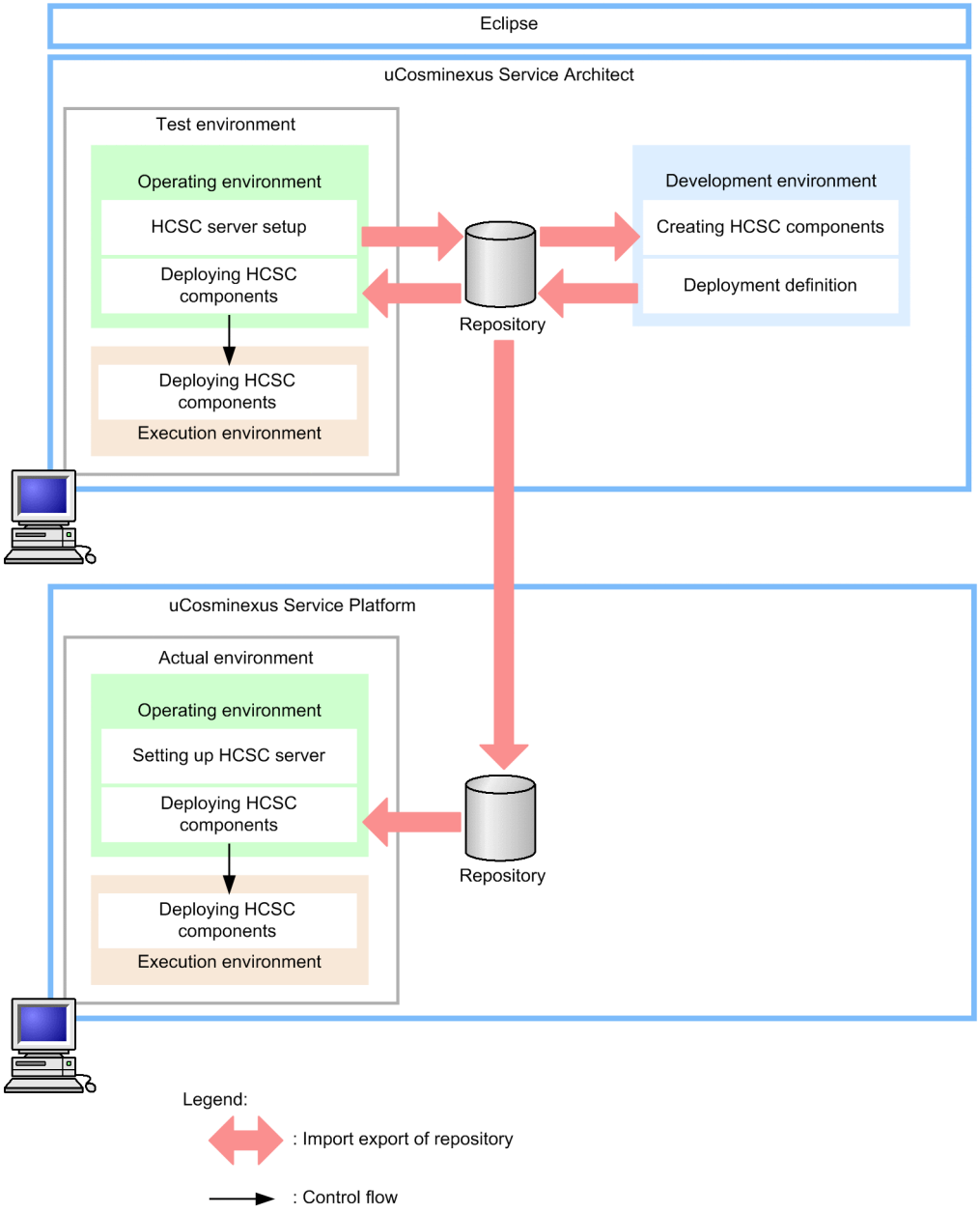
When configuring with the same settings of the database and Reliable Messaging in the following test environment and production environments, the repository used in the test environment can be migrated to the production environment as it is:

- When both database and Reliable Messaging are used in the test environment and in the production environment

- When both database and Reliable Messaging are not used in the test environment and in the production environment
- When database is used and Reliable Messaging is not used in the test environment and in the production environment

The following figure shows the procedure of migration when configuring with same settings of the database and Reliable Messaging, in the test environment and production environments:

Figure 1–6: Procedure of migration when configuring with the same settings of the database and Reliable Messaging



For details about specific procedures for migrating, see "*3.4.1 Procedure of migration when the existence of usage of the database and Reliable Messaging in the test and production environments is the same*".

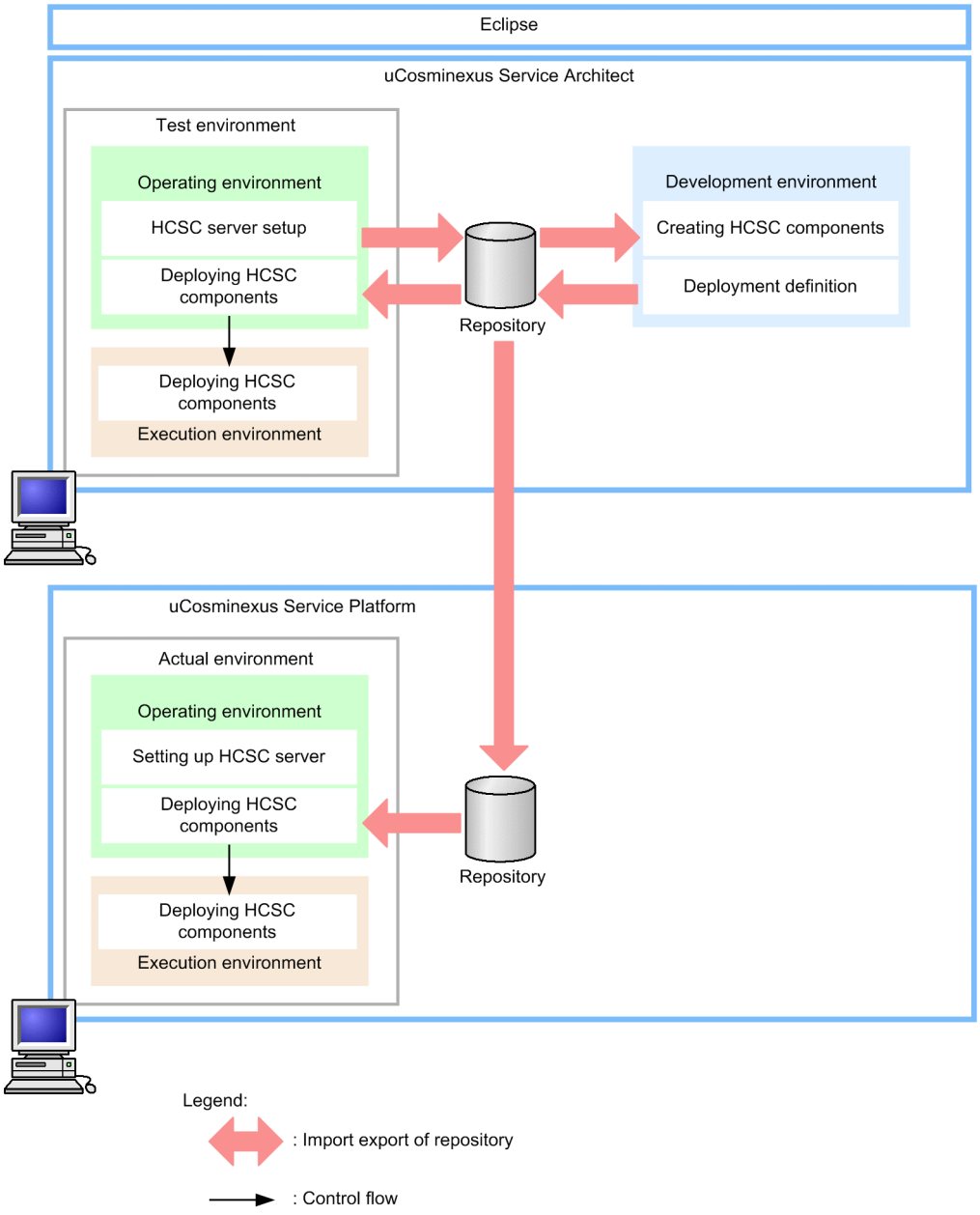
(2) Case 2: When configuring with different settings of the database and Reliable Messaging, in the test environment and the production environment (When repository can be moved as it is)

Even when configuring with the different settings of the database and Reliable Messaging, in the test environment and the production environment, the repository used in the test environment can be moved to the production environment as it is in the following cases:

- When both database and Reliable Messaging are not used in the test environment, but used in the production environment
- When both database and Reliable Messaging are not used in the test environment, and when database is used and Reliable Messaging is not used in the production environment
- When database is used and Reliable Messaging is not used in the test environment, and both database and Reliable Messaging are used in the production environment

The following figure shows the procedure of migration when the repository used in the test environment can be migrated to the production environment as it is when you configure with different settings of the database and Reliable Messaging, in the test environment and in the production environment:

Figure 1–7: Procedure of migration when configuring with the different settings of the database and Reliable Messaging (When repository can be migrated as it is)



For details about specific procedures for moving, see *3.4.3 Procedure of migration from an environment where both database and Reliable Messaging are not used to an environment where both are used* and *3.4.5 Procedure of migration from an environment where both database and Reliable Messaging are not used to an environment where database is used and Reliable Messaging is not used*.

(3) Case 3: When configuring with the different settings of the database and Reliable Messaging, in the test environment and in the production environment (When re-creating a repository)

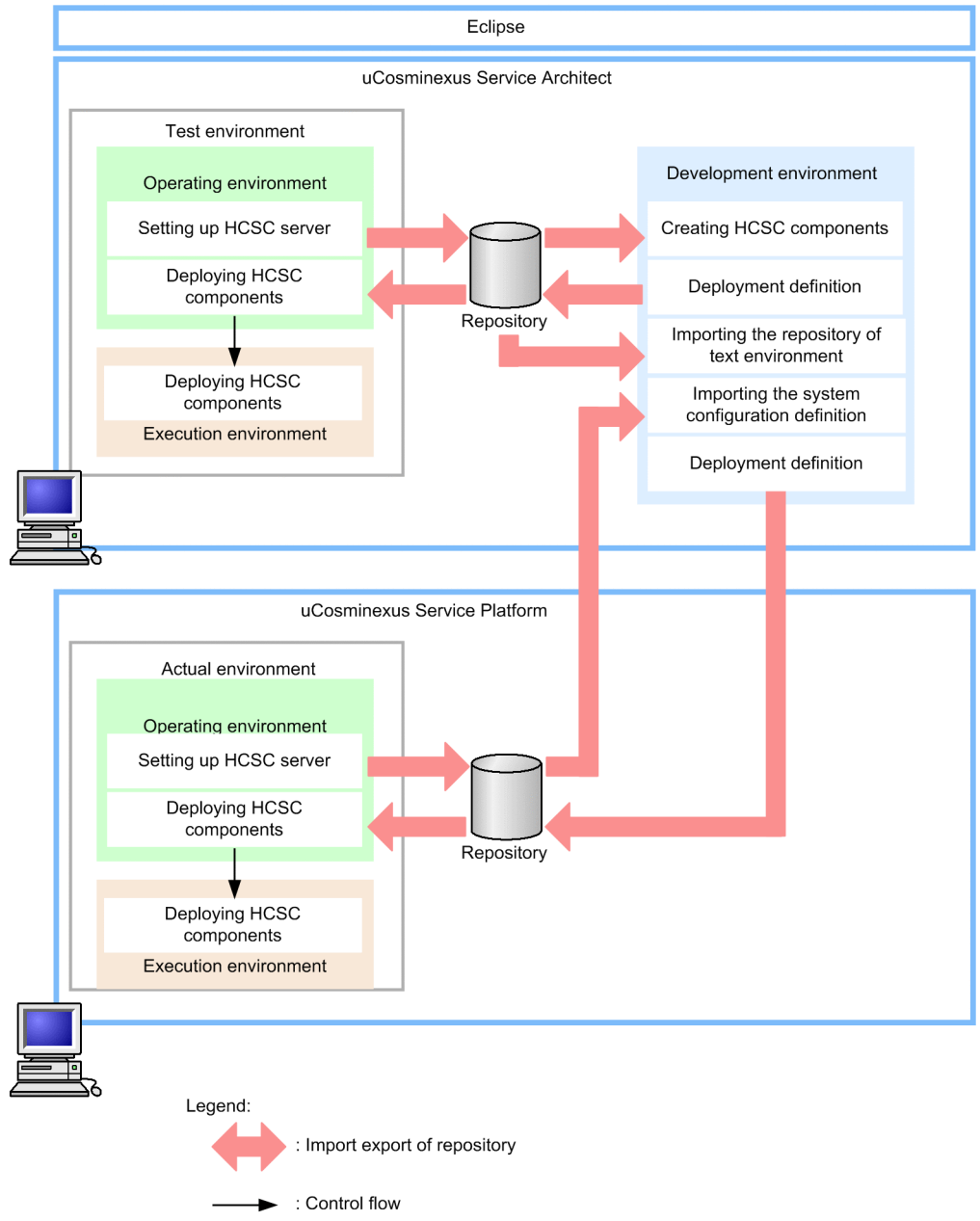
When configuring with the different settings of the database and Reliable Messaging, in the test environment and the production environment, the repository used in the test environment cannot be migrated to the production environment as it is in the following cases:

- When both database and Reliable Messaging are used in the test environment and not in the production environment
- When both database and Reliable Messaging are used in the test environment, and when database is used and Reliable Messaging is not used in the production environment
- When database is used and Reliable Messaging is not used in the test environment, and both database and Reliable Messaging are not used in the production environment

In this case, reset the system configuration definition set in the test environment to the system configuration definition used in the production environment, and then create a repository.

The following figure shows the procedure of migration when re-creating a repository used in the production environment from the repository of the test environment when configuring with different settings of the database and Reliable Messaging, in the test environment and in the production environment:

Figure 1–8: Procedure of migration when configuring with the different settings of the database and Reliable Messaging (When re-creating a repository)



For details about specific procedures for migrating, see "*3.4.2 Procedure of migration from an environment where both database and Reliable Messaging are used to an environment where both are not used*" and "*3.4.4 Procedure of migration from an environment where both database and Reliable Messaging are used to an environment where database is used and Reliable Messaging is not used*".

1.4 Determining the operations policy

Determines to which configuration the execution environment is to be set to and operated at the time of building and setting up an execution environment (HCSC server).

The configuration of the execution environment differs depending on the relationship between the number of HCSC servers on which HCSC components requesting the execution of service components are deployed and multiple HCSC servers. The configuration of the execution environment and operation policy is determined on judging the scale and content of the business, the constraints of hardware that can be prepared, whether or not the migration from existing systems is easy, to what extent can the performance and reliability due to the load balancing be ensured.

In the execution environment of Service Platform, you can perform the following configurations and operations as per the relationship of the number of HCSC servers and multiple HCSC servers.

- Operations through a single HCSC server
- Operations through multiple HCSC servers
- Operations configuring the load-balancing cluster in multiple HCSC servers
- Operations configuring the HA cluster in multiple HCSC servers
- Operations configuring the N-to-1cluster in multiple HCSC servers

In the operations through multiple HCSC servers, and operations that configure the cluster in HCSC multiple servers, you must match the SOAP mode of the HCSC server. For SOAP mode, see " *2.2.3 Used SOAP mode*".

For HCSC server and cluster setup, see "*3. System Setup and Unsetup*".

The configurations (operations) listed above are described in the subsections of this section.

! Important note

If you correct the system time by using NTP software #, note the following points:

- Execute the time correction in slew mode to gradually correct the deviation of the time to avoid time-skip.
- If you need to do significant time correction of several tens of seconds or more at a time, stop the process of the product and then execute the time correction.
- If you advance or return the system time due to time correction, this might cause a timeout of transaction, communication, or system monitoring transactions that becomes faster or slower than assumed. Also, incidents such as collapse of the time-series of logs and history, or duplication of the unique ID serialized in the system might occur. Review these points, and then create a system design and time-out design.

#

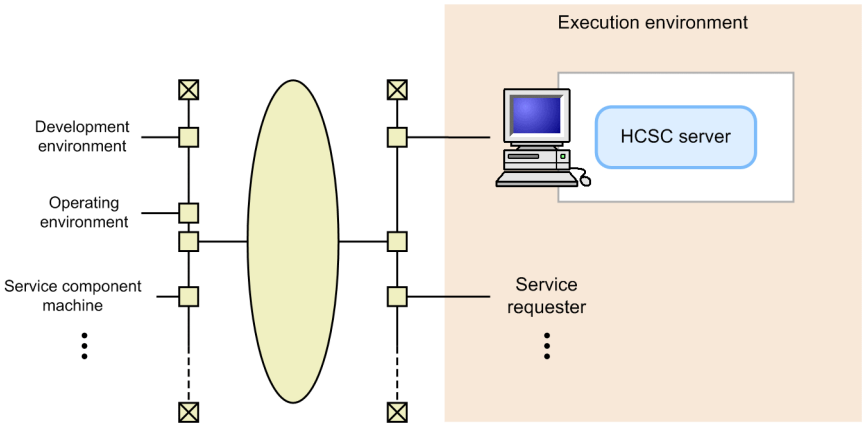
Indicates the ntpd command, ntpdate command of Windows Time service and UNIX-based platforms.

For details on system time correction, see the manual of the OS that you are using.

1.4.1 Operations Using a Single HCSC Server

The following figure shows a configuration consisting of a single HCSC server.

Figure 1–9: Configuration of HCSC server (For a single HCSC server)



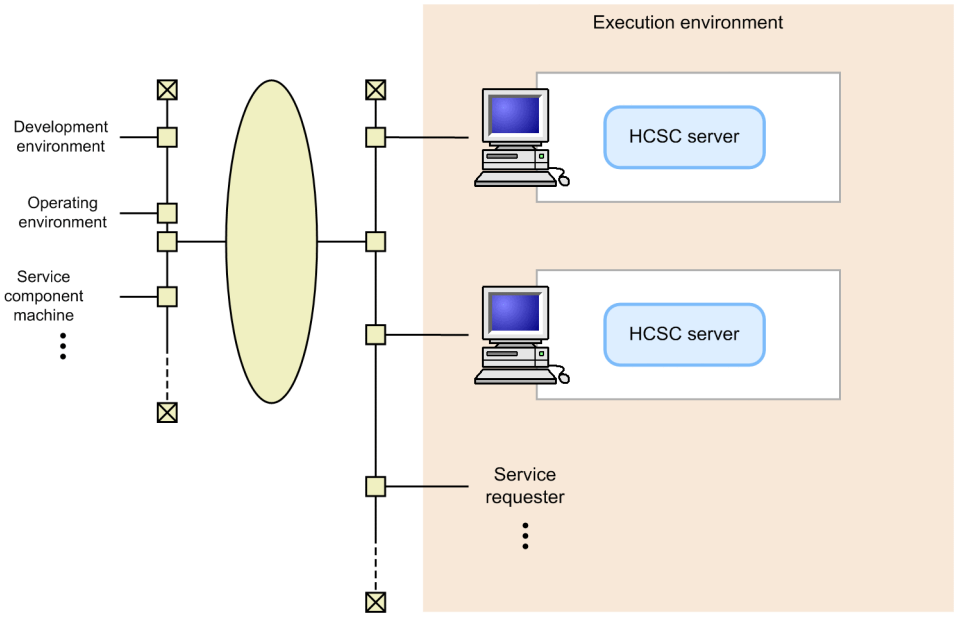
When there is only one HCSC server, all HCSC components are deployed on that HCSC server. In this case, all service modules are called from the same HCSC server.

1.4.2 Operations Using Multiple HCSC Servers

A Service platform enables you to set up multiple HCSC servers in the execution environment.

The following figure shows a configuration consisting of multiple HCSC servers.

Figure 1–10: Configuration of HCSC server (For multiple HCSC servers)



When the execution environment consists of multiple HCSC servers, deploy a different HCSC component on each server. In this case, a different service module is called from each HCSC server. You can use this configuration to manage HCSC servers according to the type of service module that is called by HCSC component.

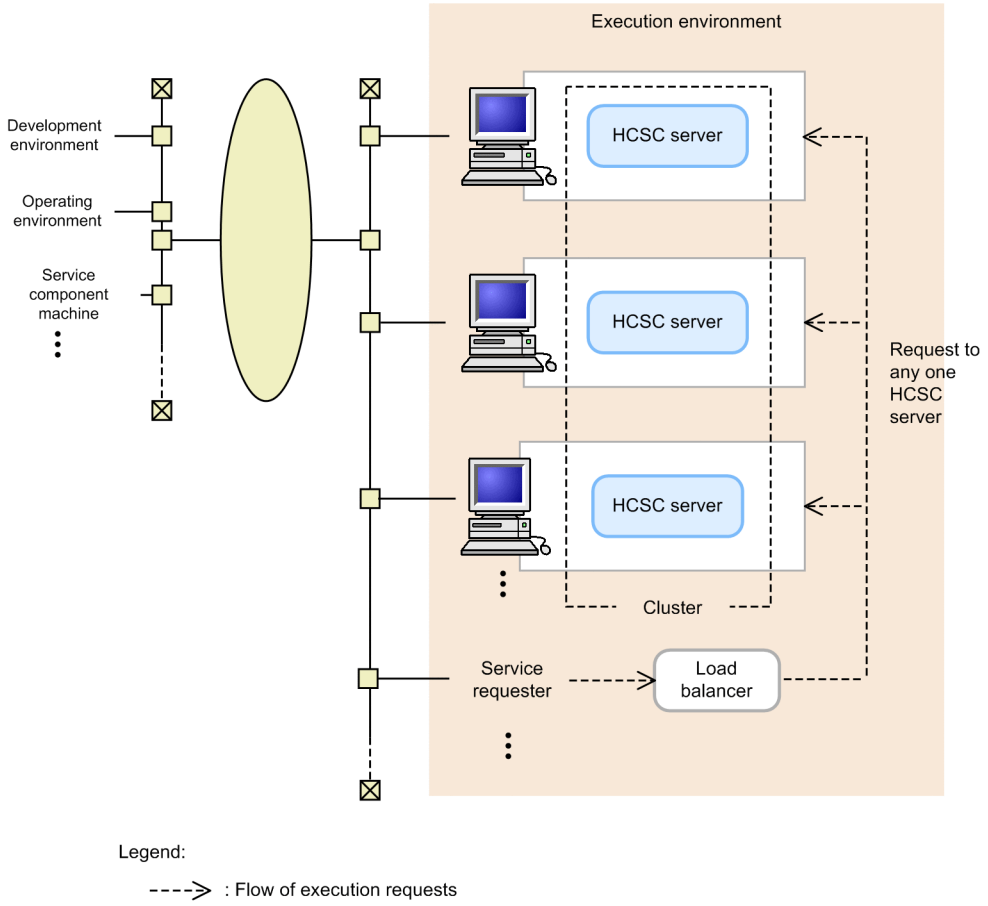
1.4.3 Operations Using a Load-balancing Cluster Consisting of Multiple HCSC Servers

A Service platform enables you to configure a system that can cluster multiple HCSC servers to distribute workload using a load balancer or CTM, so that the execution requests of service modules are not concentrated on one specific

HCSC server. This configuration is called a *load-balancing cluster configuration*. In this manual, both load balancers and CTMs are referred to collectively as load balancers.

The following figure shows a configuration in which HCSC servers are clustered (load-balancing cluster configuration).

Figure 1–11: Configuration of HCSC server (For load-balancing cluster configuration)



The load-balancing cluster configuration enables you to add, change, or remove the HCSC servers that constitute the load-balancing cluster without having to stop operations.

The load balancer used in a load-balancing cluster configuration accepts only service modules execution requests issued to a standard synchronous reception (Web Services or SessionBean). It cannot accept a service module execution request issued to a standard asynchronous reception (MDB (WS-R) or MDB (database queue)). Note that the choice of load balancer used depends on the standard synchronous reception, that is, either Web Services or SessionBean, to which service module execution requests are to be sent. For details about which load balancer should be used, see "*2.5 Environment setup to change HCSC server toload balancing cluster configuration*".

Important note

With a load-balancing cluster configuration, asynchronous execution requests (MDB (WS-R)/MDB (database queue)) issued via a load-balancing cluster cannot be accepted, but direct asynchronous execution requests issued to individual HCSC servers (MDB (WS-R)/MDB (database queue)) can be accepted. Make sure that you set the destination of the service requester in the HCSC server to which the service module execution request is to be sent. If the destination is set for a load-balancing cluster configuration, the service module execution request may not be processed correctly. Therefore, specify settings in such a manner that the load balancer will not accept a service module execution request to a standard asynchronous reception (MDB (WS-R)/MDB (database queue)).

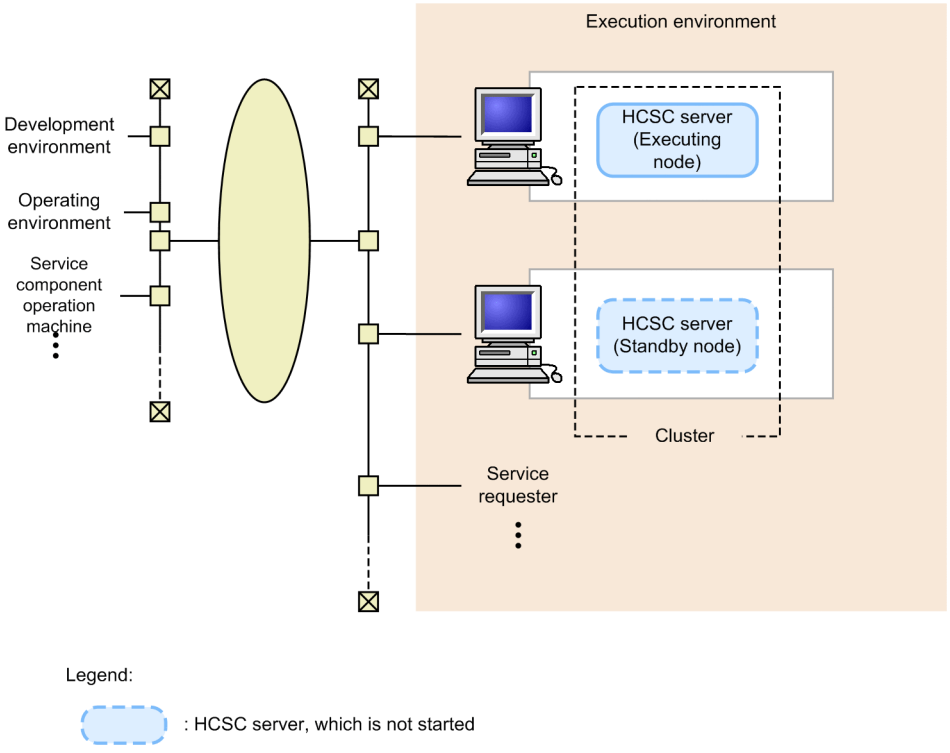
1.4.4 Operations to configure High availability clusterin multiple HCSC servers

In Service Platform, you can build a system (1-to-1 node switching system) that operates the executing node and the standby node on a one-to-one basis by clustering multiple HCSC servers that are set up in the execution environment in a cold standby configuration that combines a set of 2 HCSC servers.

This configuration is called as **Cluster configuration**.

The following figure shows the configuration (High availability cluster configuration) when HCSC servers are clustered:

Figure 1–12: FigureConfiguration of HCSC servers (in case of High availability cluster configuration)



You require cluster software to configure the High availability cluster. Use the following cluster software in Service Platform:

- In Windows: Windows Server Failover Cluster
- In UNIX: HA monitor

In the clustered 1-to-1 node switching system, if any failure occurs in the executing node, the cluster software detects this, and continues the business by automatically switching to a standby node. The configuration of the system becomes more redundant, and you can continue and operate service components even if a failure occurs in one node.

Furthermore, in the cluster software, you perform the following settings so that the standby node HCSC server starts automatically when a failure is detected:

- Starting the standby node HCSC server
- Starting the standard reception of the standby node HCSC server

! Important note

- The same HCSC components must be deployed in the 2 HCSC servers that configure the High availability cluster. You must also set the same OS and user in the executing node and the standby node.

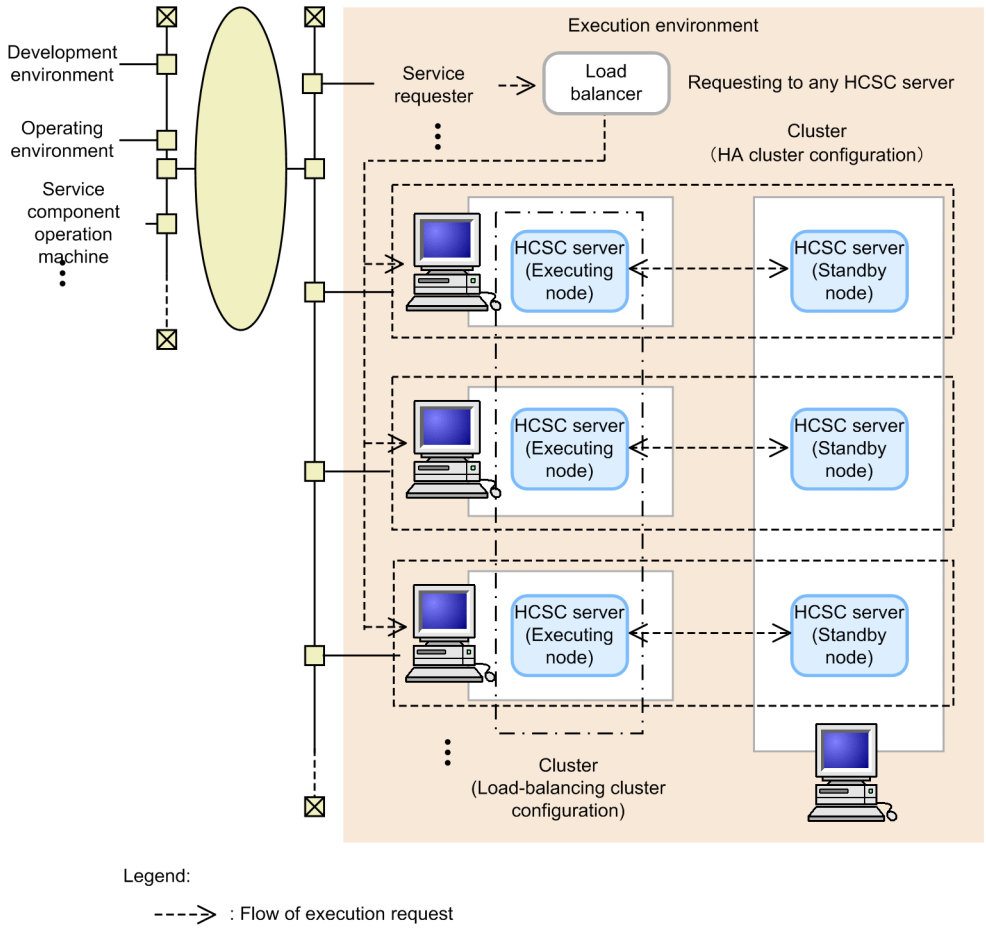
- If a failure occurs at the time of building the High availability cluster, and if the file that inputs and outputs the common folder and the file adapter is stored in the shared disk, you can re-execute the business process. However, because you cannot use the common folder for FTP reception and HTTP reception, you cannot re-execute the business process.

1.4.5 Operations that build N-to-1 clusterin multiple HCSC servers

In Service Platform, you can configure all standby nodes on a single machine by setting the HCSC server configuring the load-balancing cluster to a cold standby configuration equivalent to the High availability cluster.This configuration is called as **N-to-1 cluster configuration**.

The following figure shows the configuration (N-to-1cluster configuration) when HCSC servers are clustered:

Figure 1–13: FigureConfiguration of the HCSC server (in the case of N-to-1cluster configuration)



The follow table describes whether or not the execution requests of service components are received with the load balancer used in the N-to-1 cluster configuration.

Table 1–3: TableReceipt of the execution requests of service components with the load balancer used in the N-to-1 cluster configuration

Standard reception	Received/Not received
Standard synchronous reception (Web services)	Y
Standard synchronous reception (SessionBean)	Y
Standard asynchronous reception (MDB(WS-R))	N
Standard asynchronous reception (MDB (DB queue))	N

Legend:

Y: Receives the execution request.

The used load balancer is the same as the load balancer used when you set the HCSC server to load-balancing cluster configuration. For details, see "*2.5 Environment setup to change HCSC server to load balancing cluster configuration*".

N: Does not receive the execution request.

However, you can receive asynchronous execution requests made directly to individual HCSC servers. In this case, you set the destination of the service requester sending execution requests of service components to the set of HCSC servers equivalent to the HA cluster without fail.

If you set the destination for load-balancing cluster configuration, the execution request of service components might get processed incorrectly. Therefore, set such that the execution request for service components to standard asynchronous reception (MDB (WS-R) / MDB (DB queue)) with the load balancer is not received.

2 System Configuration

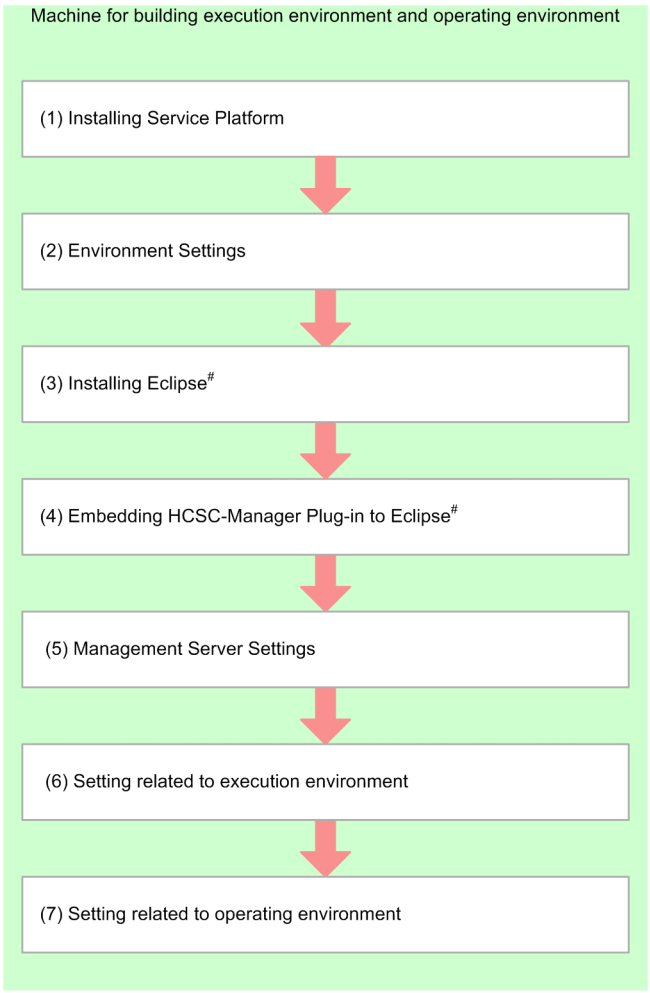
This chapter describes how to install products such as Service Platform, and the setup method to use after installation.

2.1 Installing and Uninstalling

2.1.1 Installation flow

The following figure shows installation flow:

Figure 2–1: FigureInstallation flow



Note #
Implement when using GUI in operating environment.

(1) Installing Service Platform

For installation methods of Service Platform, see "2.1.2 Installing Service Platform".

For uninstallation of an installed Service Platform, see "*2.1.7 Uninstalling*".

(2) Environment settings

Set the repository for environment settings.

For environment settings, see "*2.1.3 Environment settings*".

(3) Installing Eclipse

Install Eclipse to use the screen in the operating environment.

For Eclipse installation procedures, see "*2.1.4 Installing Eclipse*".

(4) Embedding HCSC-Manager Plug-in in Eclipse

Embed HCSC-Manager Plug-in in Eclipse to use the screen in the operating environment.

For embedding HCSC-Manager Plug-in in Eclipse, see "*2.1.5 Embedding HCSC-Manager plug-in in Eclipse*".

(5) Management Server settings

Perform settings of Management Server to use HCSC-Manager in the execution environment that becomes the connection destination of HCSC-Manager.

For Management Server settings, see "*2.1.6 Management Server settings for using HCSC-Manager*".

(6) Settings related to execution environment

Set HCSC server configuration. For details on settings related to the execution environment, see "*2.3 Settings related to execution environment*".

(7) Settings related to operating environment

Set user permission. For details on settings related to the operating environment, see "*2.4 Settings Related to the Operating Environment*".

2.1.2 Installing Service Platform

(1) Installation method

For details on how to install Service Platform, see "2.2 Application server setup" in "Application Server System Setup and Operation Guide". For points to be considered for installation, see "Appendix J Points to be considered when installing and uninstalling" in "Application Server System Setup and Operation Guide". Read the installation procedure product name "Application Server" as "Service Platform".

Configuration software included in Service Platform in UNIX is as follows:

- Component Container
- Component Transaction Monitor
- DABroker Library#
- Developer's Kit for Java
- Performance Tracer
- Reliable Messaging
- Service Coordinator
- TPBroker
- Web Services - Security
- XML Processor
- HTTP Server
- Service Platform- Base

Note #

These are included only in HP-UX (IPF) version Service Platform.

(2) Directory configuration after installation

The following figure shows directory configuration after installation of Service Coordinator from among the software that configures Service Platform. For directory configuration after installation of configuration software other than

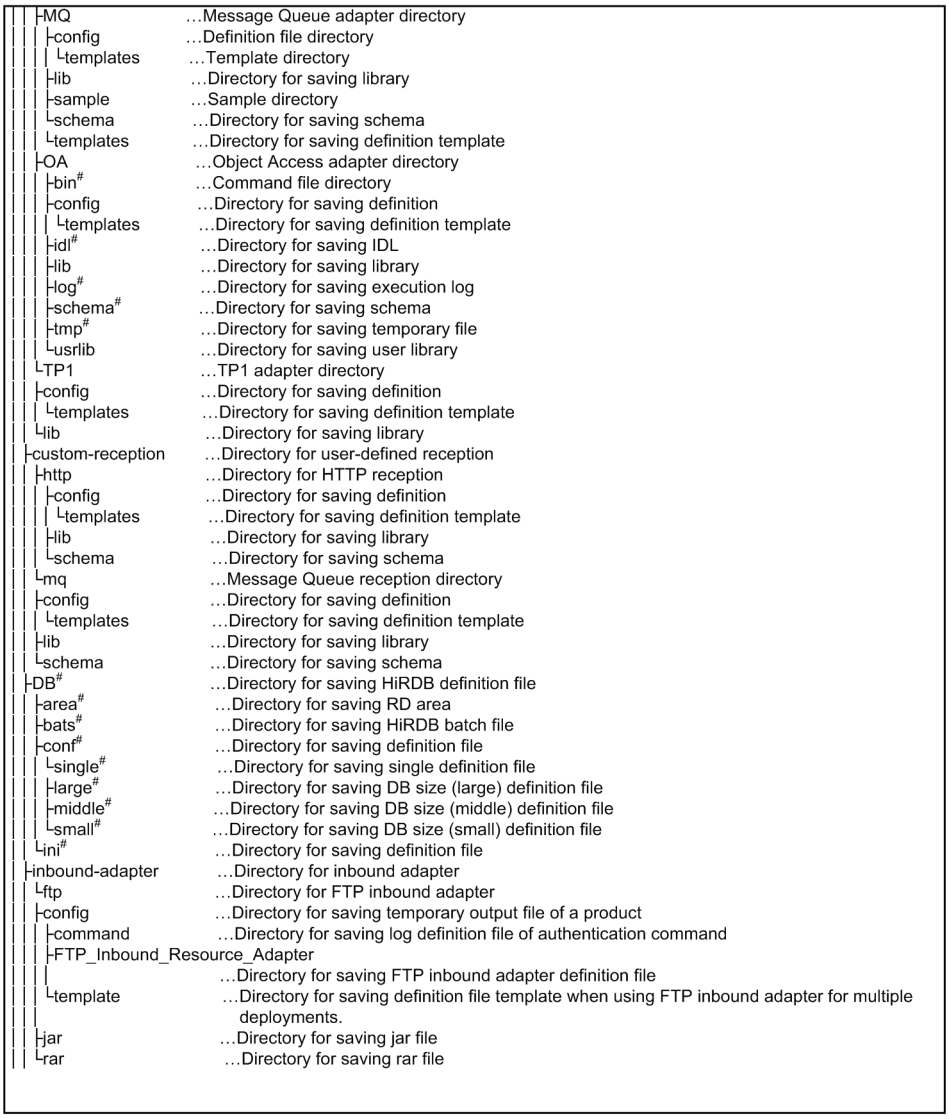
Service Coordinator, see "Appendix B Directory configuration after installation" in "Application Server System Setup and Operation Guide".

Figure 2–2: FigureDirectory configuration after installation

```
<Service Platform Installation Directory>
 ├CSC                        …HCSC installation directory
 │ ├bin                      …Directory for saving a batch file for executing command
 │ ├config                   …Directory for saving definition type
 │ │ ├adpfop                ⋯Directory for saving file operations adapter definition
 │ │ │ └templates            ⋯Directory for saving file operations adapter definition template
 │ │ ├dba                    ⋯Directory for saving HCSC-DB Adapter definition
 │ │ │ └templates            ⋯Directory for saving HCSC-DB Adapter definition template
 │ │ ├definition             ⋯Directory for saving development  environment adapter and reception extension definition
 │ │ ├ftprecp                ⋯Directory for saving FTP reception definition
 │ │ │ └templates            ⋯Directory for saving FTP reception definition template
 │ │ ├mail                   ⋯Directory for saving mail adapter definition
 │ │ │ └templates            ⋯Directory for saving mail adapter definition template
 │ │ ├manager                ⋯Directory for saving HCSC-Manager definition
 │ │ │ └templates            ⋯Directory for saving HCSC-Manager definition template
 │ │ │  └hsetup              ⋯Directory for saving template file for simple building of production environment
 │ │ │   └esb                ⋯Directory for saving template file for ESB module
 │ │ └msg                    ⋯Directory for saving HCSC-Messaging definition at the time of execution.
 │ ├custom-adapter           ⋯Directory for TP1 adapter, file adapter, Object Access adapter, Message queue
 │ │ │                         adapter, FTP adapter,
 │ │ ├File                   ⋯File adapter directory
 │ │ │ ├config               ⋯Definition file directory
 │ │ │ │ └templates          ⋯Template directory
 │ │ │ ├lib                  ⋯Directory for saving library
 │ │ │ ├Sample#              ⋯Sample directory
 │ │ │ │ ├Bin#               ⋯Directory for saving service requestor
 │ │ │ │ ├common#            ⋯Directory for saving sample common file
 │ │ │ │ ├read_csv#          ⋯Directory for saving file for CSV data reading sample
 │ │ │ │ ├read_fix#          ⋯Directory for saving file for fixed length data reading sample
 │ │ │ │ ├read_xm#           ⋯Directory for saving file for XML data reading sample
 │ │ │ │ ├write_csv#         ⋯Directory for saving file for CSV data writing sample
 │ │ │ │ ├write_len#         ⋯Directory for saving file for length tag data writing sample
 │ │ │ │ └write_xml#         ⋯Directory for saving file for XML data writing sample
 │ │ │ └schema               ⋯Schema directory
 │ │ │  └templates           ⋯Schema template directory
 │ │ ├FTP                    ⋯FTP adapter directory
 │ │ │ ├bin                  ⋯Command file directory
 │ │ │ ├config               ⋯Definition file directory
 │ │ │ │ └templates          ⋯Template directory
 │ │ │ ├lib                  ⋯Directory for saving library
 │ │ │ ├log                  ⋯Command message log output directory
 │ │ │ └schema               ⋯Schema directory
 │ │ ├HTTP                   ⋯HTTP adapter directory
 │ │ │ ├config               ⋯Definition file directory
 │ │ │ │ ├common             ⋯Directory for common system definition file
 │ │ │ │ └templates          ⋯Template directory
 │ │ │ ├lib                  ⋯Directory for saving library
 │ │ │ └schema               ⋯Schema directory
```

(To be continued)

(Continued)



To be continued

(continued)

```
│ ├lib                  …Directory for saving ear file or jar file
│ │ ├external           …Directory for saving other product
│ │ │ └table            …Directory for saving code conversion table
│ │ ├ibmB               …Directory for saving code conversion table
│ │ ├ibmE               …Directory for saving code conversion table
│ │ └keisE              …Directory for saving code conversion table
│ ├icons#               …Directory for saving icon file
│ ├interfaces           …Directory for saving stub to be provided to service requester
│ └wsdls                …Directory for saving WSDL to be provided to service requester
├log                    …Directory to output a log at the time of execution or at the time of installation
│ ├adapter              …Directory to output a service adapter log
│ │ └command            …Directory to output a service adapter command log
│ └manager              …Directory to output a HCSC-Manager log
├mbean-plugins          …Directory for saving Mbean definition information and jar file
│ ├config               …Directory for saving MBean definition information
│ └lib                  …Directory for saving MBean jar file
├monitor                …Message monitoring directory
│ ├lib                  …Directory to arrange message monitoring Jar file
│ └spool                …Directory for Message monitoring work
├repository             …Repository directory
├samples                …Directory for saving various types of samples
│ ├customadapter        …Directory for saving custom adapter definition file sample
│ ├routing              …Directory for saving a sample of HCSC-Messaging routing definition file
│ └urecp                …Directory for saving user defined reception sample definition file
├schema                 …Directory for saving schema definition
│ ├adpfop               …Directory for saving message schema definition of file operations adapter
│ ├connection           …Directory for saving destination dynamic change message schema definition
│ ├fault                …Directory for saving fault message schema definition
│ ├ftprecp              …Directory for saving FTP reception message schema definition
│ ├mail                 …Directory for saving mail adapter message schema definition
│ └soap                 …Directory for saving HTTP header message schema template for SOAP adapter
├spool                  …Directory to output temporary file at the time of execution
│ ├ftp                  …Directory to output temporary file of FTP integrated function
│ │ ├com                …Common folder default directory
│ │ └work               …Work folder default directory
│ ├manager              …Directory for saving HCSC-Manager internal information
│ ├migration            …Directory to output temporary file for version migration
│ └msg                  …Directory to output temporary file at the time of HCSC-Messaging execution
├sql                    …Directory for saving sample of table generation and SQL deletion
├system                 …Directory for saving various files used by HCSC
│ ├manager              …Directory for saving various files used by HCSC-Manager
│ │ ├hsetup             …Directory for saving definition file for simple  building of production environment
│ │ └Setup#             …Directory for saving simple build definition file
│ ├migration            …Directory for saving various files for version migration
│ ├msg                  …Directory for saving various files used by HCSC-Messaging
│ └wsdls                …Directory for saving WSDL to be provided to development environment
├userlib                …Directory for saving library created by the user
└customfunc             …Directory for saving jar file to be used in custom function
plugins#                 …Plug-in directory common to service platforms
└eclipse#                …Directory to be specified at the time of embedding to Eclipse
  ├features#             …Directory for saving feature
  └plugins#              …Directory for saving plug-ins to be embedded in Eclipse
```

#
Directories existing only in Windows.

2.1.3 Environment settings

Perform the following settings in machines in which Service Platform is installed:

Repository settings

For repository settings, see "*4.1 Overview of a repository*".

2.1.4 Installing Eclipse

You must install Eclipse to use the screen in the operating environment.

If Service Platform is used, install Eclipse by the following procedures. If Service Architect is used, use Eclipse setup functionality and install Eclipse. For details on Eclipse setup functionality, see "3.3 Setup that uses Eclipse setup functionality" in "Service Platform First Step Guide".

Important note

There is no support for Eclipse other than Eclipse plug-in functionality provided by the application server and Service Platform. User investigates Eclipse usage methods and action methods for errors displayed by Eclipse and takes action.

(1) Preparation before installation

The following preparation is required before installing Eclipse:

- Complete installation of Service Platform.
- Prepare the following 2 directories:
  - Eclipse installation directory
  - Directory for operation (directory used while downloading Eclipse)

(2) Installation procedure

The following points show installation procedures. Installation directory in these procedures are represented as "C:\Eclipse" and directory for operation is represented as "C:\Work".

1. Acquire Eclipse 4.2.1 zip file by one of the following methods and store it in the directory for operation:
   - Attached product CD of Service Architect
   - Eclipse download site
     Select "Eclipse IDE for Java EE Developers" from the download site shown in the following URL:
     http://www.eclipse.org/downloads/

   Select one of the following items for zip file according to the environment:
   - Windows x86 (32 bit version): eclipse-jee-juno-SR1-win32.zip
   - Windows x64 (64 bit version): eclipse-jee-juno-SR1-win32-x86_64.zip
2. Start command prompt and move the current directory to the directory for operation.

   Execution example of command prompt
   cd C:\Work

   Also execute the following command and extract zip file:
   "<Service Platform installation directory>\jdk\bin\jar.exe" xvf <Eclipse zip file name>
3. Copy the extracted file in the Eclipse installation directory.
   Use explorer and copy all files and directories under C:\Work\eclipse in C:\Eclipse.
4. Use explorer and delete the directory for operation.
   Note: Since the downloaded file is also deleted, take back up in advance if required.
5. From the file copied by procedure 3, open eclipse.ini file by editor and add the following 2 options:
   - -vm option
     <Service Platform installation directory>\jdk\bin\javaw.exe
   - -vmargs option
     -Djava.endorsed.dirs=<Service Platform installation directory>\jaxp\lib

   An example of eclipse.ini file contents after the option is added is described here:
   - In Windows 32 bit version

```
-vm
C:\Program Files\Hitachi\Cosminexus\jdk\bin\javaw.exe
-startup
plugins/org.eclipse.equinox.launcher_1.3.0.v20120522-1813.jar
--launcher.library
plugins/org.eclipse.equinox.launcher.win32.win32.x86_1.1.200.v20120522-1813
-product
org.eclipse.epp.package.jee.product
--launcher.defaultAction
openFile
--launcher.XXMaxPermSize
```

```
256M
-showsplash
org.eclipse.platform
--launcher.XXMaxPermSize
256m
--launcher.defaultAction
openFile
-vmargs
-Dosgi.requiredJavaVersion=1.5
-Dhelp.lucene.tokenizer=standard
-Xms40m
-Xmx512m
-Djava.endorsed.dirs=C:\Program Files\Hitachi\Cosminexus\jaxp\lib
```

- In Windows 64 bit version

```
-vm
C:\Program Files\Hitachi\Cosminexus\jdk\bin\javaw.exe
-startup
plugins/org.eclipse.equinox.launcher_1.3.0.v20120522-1813.jar
--launcher.library
plugins/org.eclipse.equinox.launcher.win32.win32.x86_64_1.1.200.v20120522-1813
-product
org.eclipse.epp.package.jee.product
--launcher.defaultAction
openFile
--launcher.XXMaxPermSize
256M
-showsplash
org.eclipse.platform
--launcher.XXMaxPermSize
256m
--launcher.defaultAction
openFile
-vmargs
-Dosgi.requiredJavaVersion=1.5
-Dhelp.lucene.tokenizer=standard
-Xms40m
-Xmx512m
-Djava.endorsed.dirs=C:\Program Files\Hitachi\Cosminexus\jaxp\lib
```

6. Execute the following command and start Eclipse:

   ```
   C:\Eclipse\eclipse.exe
   ```

   Check that Eclipse is started.

With this, installation of Eclipse is complete.

2.1.5 Embedding HCSC-Manager plug-in in Eclipse

Embed HCSC-Manager Plug-in in Eclipse.

The following points show the procedures to embed HCSC-Manager Plug-in:

1. Copy the following link file:

   Copy source file

   <Service Platform installation directory>\common\dropins\com.cosminexus.common.plugin.link

   <Service Platform installation directory>\plugins\dropins\com.cosminexus.plugin.link

   Copy destination directory

   <Eclipse installation directory>\dropins

2. Restart Eclipse.

   When Eclipse restarts, embedding is completed.

   To check whether HCSC-Manager Plug-in is embedded correctly, select [Help]-[Eclipse Platform]-[Installation Details] from the menu and check [Installed Software] tab of the displayed [Eclipse Platform Installation Details] dialog.

Points to be considered when Service Platform is re-installed

When Service Platform is re-installed by version-up, you must re-embed HCSC-Manager Plug-in after embedding of HCSC-Manager Plug-in is cancelled.

The following points show the procedures to cancel embedding of HCSC-Manager Plug-in:

1. Delete the following link file:
   <Eclipse installation directory>\dropins\com.cosminexus.common.plugin.link
   <Eclipse installation directory>\dropins\com.cosminexus.plugin.link
2. Restart Eclipse.

2.1.6 Management Server settings for using HCSC-Manager

Perform the settings for using HCSC-Manager in a machine that has the execution environment of HCSC-Manager connection destination. The following points show setting procedures:

(1) Setting mserver.properties (Management Server environment settings file)

Add properties in mserver.properties (Management Server environment settings file) of the execution environment. Properties added in mserver.properties storage location and mserver.properties is described here:

(a) Storage location of mserver.properties

```
<Service Platform installation directory>\manager\config\mserver.properties
```

(b) Added properties

```
com.cosminexus.mngsvr.management.enabled=true
com.cosminexus.mngsvr.management.connector.enabled=true
com.cosminexus.mngsvr.management.port=28099#1
ejbserver.naming.port=28900#2
ejbserver.server.edition.settingforce=
mngsvr.myhost.name=localhost
```

Note #1

Specify the connection port number from HCSC-Manager. If specification is omitted, 28099 set by default.

Note #2

Specify the connection port number from HCSC-Manager. If specification is omitted, 28900 set by default.

Note

Always specify before starting Management Server. If you start Management Server before specifying, commands beginning with csc may throw errors.

(2) Setting mserver.cfg (option definition file for Management Server)

Add properties in mserver.cfg (option definition file for Management Server) of the execution environment.

Properties added in mserver.cfg storage location and mserver.cfg is described here.

(a) Storage location of mserver.cfg

```
<Service Platform installation directory>\manager\config\mserver.cfg
```

(b) Adding properties

When Oracle is used in the database

```
web.add.class.path=< JAR file name of Oracle JDBC Thin Driver (full path)>#
```

Note #

Applicable JAR file is described here:

Oracle version	Applicable JAR file
Oracle 11g (JDK6)	<Oracle Client installation directory>/jdbc/lib/ojdbc6.jar

When HiRDB is used in the database

When HiRDB/Single Server, HiRDB/Parallel Server or HiRDB Server is installed

- **In Windows**

```
add.library.path=<HiRDB installation directory>\CLIENT\UTL
```

- **In UNIX**

```
add.library.path=<Operation directory of HiRDB>/client/lib
```

When HiRDB/Run Time or HiRDB/Developer's Kit is installed

- **In Windows**

```
add.library.path=<HiRDB installation directory>\utl
```

- **In UNIX**

```
add.library.path=<HiRDB installation directory>/client/lib
```

When HiRDB Type4 JDBC Driver is used in JDBC driver

```
web.add.class.path=<JAR file name of HiRDB Type4 JDBC Driver (full path)>#
```

Note #

The applicable JAR file is "pdjdbc2.jar" under the HiRDB installation directory.

(3) Checking adminagent.properties (Administration Agent properties file)

(a) Storage location of adminagent.properties

```
<Service Platform installation directory>\manager\config\adminagent.properties
```

(b) Property to be checked

Check whether "2" is set in the following property or whether the property is omitted:

```
adminagent.j2ee.watch.level=2
```

(4) Starting Administration Agent (restarting if started)

You must start Administration Agent after Management Server environment settings file and option definition file for Management Server are set. Restart Administration Agent if it is already started.

For details on how to start Administration Agent, see "4.1.17 Starting Administration Agent" in "Application Server System Setup and Operation Guide".

(5) Starting Management Server (restarting if started)

You must start Management Server after Management Server environment settings file and option definition file for Management Server are set. Restart Management Server if it is already started.

For details on how to start Management Server, see "4.1.18 Start Management Server" in "Application Server System Setup and Operation Guide".

(6) Checking MBean start

Check whether 22 items are output by KEOS27010-I message in the latest mngmessage[n].log file under <Service Platform installation directory>\manager\log\message\.

One of the following items is output in the variable value file name of KEOS27010-I message:

- 50cscbp.xml
- 50cscmsg.xml

- 50cscmt.xml

Important note

In 07-50 or higher version, the operation to copy the file under "<Service Platform installation directory>\CSC\mbean-plugins" in "<Service Platform installation directory>\manager\mbean-plugins" is not required.

If the following files exist, delete the files and then perform procedures (3) to (5):

- <Service Platform installation directory>\manager\mbean-plugins\config\50cscbp.xml
- <Service Platform installation directory>\manager\mbean-plugins\config\50cscmsg.xml
- <Service Platform installation directory>\manager\mbean-plugins\lib\cscbp_mbean.jar
- <Service Platform installation directory>\manager\mbean-plugins\lib\cscmsg_mbean.jar

2.1.7 Uninstalling

This section describes Service Platform and configuration software to be uninstalled and the method for uninstallation.

(1) Before uninstalling

This section describes Service Platform and contents that must be known before uninstalling Service Coordinator that is the configuration software of Service Platform as well as the operations to be performed before uninstalling.

(a) Target files and directories

Only files and directories created by normal installer are deleted. Please note that files created under directories to be deleted are deleted while uninstalling.

However, if files exist under the following directories of <Service Platform installation directory>\CSC, the directories are not deleted.

Table 2–1: TableFiles under <Service Platform installation directory>\CSC that are not deleted by uninstalling

Directory		Files that are not deleted from the directory on the left
config	adpfop	Those under the templates of the directory on the left are deleted.
	ftprecp	
	mail	
	manager	
	msg	cmdconf.bat might not be deleted in Windows version. #
custom-adapter	File\config	Those under the templates of the directory on the left are deleted.
	FTP\config	
	FTP\log	-
	HTTP\config	Those under the templates of the directory on the left are deleted.
	HTTP\config\common	-
	MQ\config	Those under the templates of the directory on the left are deleted.
	OA	The following files under config of the directory on the left are deleted: • Under templates • adpoacmd.properties • wrappercode.properties • wrappertype.properties

Directory		Files that are not deleted from the directory on the left
custom-adapter	OA	Files under the log of the directory on the left are not deleted.
	TP1\config	Those under the templates of the directory on the left are deleted.
inbound-adapter	ftp\config	The following files are deleted: • Under inbound-adapter\ftp\config\command • Under inbound-adapter\ftp\config\template • FTP_Inbound_Resource_Adapter\log4j.xml • FTP_Inbound_Resource_Adapter\serverstatus.properties
	ftp\logs	-
log		-
repository		-
spool	ftp	-
userlib	customfunc	-

(Legend)

-: Not applicable (all are deleted)

Note #

In Windows version, if Service Coordinator 01-50 or lower version is upgraded by updated installation to Service Coordinator 01-60 or higher version and then uninstalled, <Service Platform installation directory>\CSC\config\msg\cmdconf.bat is deleted. Due to this, when you configure system and re-install after uninstallation, you must reset the contents in cmdconf.bat.

If Service Coordinator 01-60 or higher version is newly installed and then uninstalled, <Service Platform installation directory>\CSC\config\msg\cmdconf.bat is not deleted.

Files under the following directories are created according to the product after installation but are deleted while uninstalling.

- <Service Platform installation directory>\CSC\custom-adapter\OA\tmp
- <Service Platform installation directory>\CSC\DB\area
- <Service Platform installation directory>\CSC\DB\bats
- <Service Platform installation directory>\CSC\monitor\spool
- <Service Platform installation directory>\CSC\spool\manager
- <Service Platform installation directory>\CSC\spool\migration
- <Service Platform installation directory >\CSC\spool\msg
- <Service Platform installation directory>\CSC\system\msg

(b) Operations before uninstalling

You must perform following operations before uninstalling Service Coordinator:

System unsetup

Perform unsetup of the system. If you uninstall without system unsetup, database tables, J2EE applications of J2EE server and Reliable Messaging queues are not deleted.

For details on how to unset up the system, see "*3.3 Cancelling System Setup*".

Stopping J2EE server and Management Server

Stop J2EE server and Management Server.

For details on how to stop the J2EE server, see "11.11.7 Stopping J2EE server" in "Application Server Management Portal Operation Guide". For details on how to stop Management Server, see "3.1.3 Stopping the system (while using GUI)" in "Application Server System Setup and Operation Guide".

(2) Uninstalling Service Platform

For details on how to uninstall Service Platform, see "3.3 System environment unsetup and Application Server uninstallation" in "Application Server System Setup and Operation Guide". For points to be considered when uninstallation, see "Appendix J Points to be considered when installing and uninstalling" in "Application Server System Setup and Operation Guide". Read the uninstallation procedure product name "Application Server" as "Service Platform".

2.2 Selecting configuration types and SOAP modes

Before developing a system on the Service platform, you must define the functionality to be used in the system and SOAP modes.

This section describes the functionality to be used in the system and the usage of a database or Reliable Messaging. This section also describes the standard specifications for Web Services corresponding to the used SOAP modes.

2.2.1 Existence of usage of database and Reliable Messaging

Existence of usage of the database and Reliable Messaging differs according to the functionality of Service Platform to be used and the kind of operation required. The following table describes the existence of usage of Reliable Messaging and database as per each functionality:

Table 2–2: TableDatabase of each functionality to be used and existence of usage of Reliable Messaging

Functionality to be used		Database	Reliable Messaging
Synchronous reception is to be used		N	N
Asynchronous reception (standard reception (MDB(WS-R)), standard reception (MDB(DB queue))) are to be used		N	N
Synchronous service adapter is to be used		N	N
Asynchronous service adapter (MDB(WS-R) adapter, MDB(DB queue) adapter) are to be used		Y	Y
Business process is to be used	Persistent business process is to be used	Y	N
	Non-persistent business process is to be used#1	N	N
Process instance execution history is to be managed		Y	N
DB adapter is to be used		N#2	N

(Legend)

Y: Mandatory.

N: Not mandatory.

Note #1

Please note that when a non-persistent business process is used, there are restrictions in the processes that can be defined in the start environment. For details, see "3.3 Business processes that are to be made persistent and that are not to be made persistent" in "Service Platform Overview".

Note #2

When you use DB adapter, a database is not required in a machine on which HCSC server is running. However, database is required on a service running machine connected from DB adapter.

From the above table it is understood that the configuration format according to existence of usage of the database and Reliable Messaging contains the following 3 patterns:

- Both database and Reliable Messaging are used
- Both database and Reliable Messaging are not used
- Database is used and Reliable Messaging is not used

Contents of settings related to the execution environment are different during system setup according to each pattern. For details on execution environment setting contents in each pattern, see "*2.3 Settings related to execution environment*".

Setting of existence of usage of the database and Reliable Messaging is defined in HCSC server setup definition file. Database settings are not required if the database is not used and Reliable Messaging setting is not required if Reliable Messaging is not used.

Important note

Provide appropriate access permission to the following directories and files to be accessed in the execution environment or operating environment:

- Service Platform installation directory
- Directories and files specified by the command argument
- Directories and files specified in all types of definition files used in HCSC

2.2.2 Existence of usage of table partition functionality

While managing process instance execution history, existence of usage and partition configuration of the table partition functionality must be clarified and you must check used database before setting up a system in Service Platform. For details on table partition functionality, see "7.3Managing execution logs linked with HiRDB" in "Service Platform Overview".

(1) Examining usage method of table partition functionality

The following table describes the relation of table partition functionality and the database to be used:

Table 2–3: TableRelation of table partition functionality and the database to be used

Usage method of table partition functionality	HiRDB Server Version 9		Other DBMS
	HiRDB/Single Server	HiRDB/Parallel Server	
Partition by date data (month)	Y	Y	N
Partition by date data (month) and also to manage by distributing in multiple servers	N	Y#	N
When table partition functionality is not used	Y	Y	Y

(Legend)

Y: Can be executed.

N: Cannot be executed.

Note #

HiRDB Advanced High Availability Version 9 is required for use.

(2) Examining table partition configuration

While using table partition functionality, examine data volume of 1 month (potential value) on the basis of the following points and decide the partition configuration:

- How many back-end servers are to be used?
- Data of which month is to be compiled and handled?
- How many months are to be used as units for circulation? (Data of how many months is to remain in the database?)

(3) HCSC server setup

When table partition functionality is used, definition as follows is required in HCSC server setup definition file:

```
db-tbl-split-key=MONTH
db-tbl-split-corcheck-use=ON
sql-scriptfilename=Path of SQL script file defining table partition#
```

Note #

This definition is required when the 1st HCSC server in a cluster is setup.

Since creation of the table, index and view table that are the targets of table partition functionality is complete during the 1st HCSC server setup, SQL script file need not be created for HCSC server setup from the 2nd server onwards.
For details on SQL script file, see "*Appendix D.2(2) Renaming RD Areas or table areas*".

For details on HCSC server setup definition file, see "HCSC server setup definition file" in "Service Platform Reference Guide".

2.2.3 Used SOAP mode

Select SOAP mode to be used before starting the system in Service Platform.

This section describes SOAP mode type and the support range of each mode.

(1) SOAP mode type

The following items show SOAP mode type, corresponding Web service standard specifications and the execution environment.

- **SOAP1.1 mode**
  Select the system corresponding to SOAP1.1 when you start development. SOAP1.1 mode corresponds to WS-I Basic Profile1.0a.
  Use SOAP communication infrastructure for SOAP message sending and receiving in SOAP1.1 mode.
- **SOAP1.1/1.2 combined mode**
  Select the system corresponding to SOAP1.1 or SOAP1.2 when you start development. SOAP1.1/1.2 combined mode corresponds to WS-I Basic Profile1.1.
  Use JAX-WS engine for SOAP message sending and receiving in SOAP1.1/1.2 combined mode.

(2) SOAP mode support range

The following table describes correspondence of reception and service adapter functionalities and SOAP mode:

Table 2–4: TableSOAP mode support range (reception and service adapter functionalities)

Classification	Functionality name	SOAP mode	
		1.1	1.1/1.2 combined
Reception	Standard reception (Web service (SOAP1.1))	Y	Y
	Standard reception (Web service (SOAP1.2))	N	Y
	Standard reception (SessionBean)	Y	Y
	Standard reception (MDB(WS-R))	Y	N
	Standard reception (MDB(DB queue))	Y	Y
	User-defined reception	Y	Y
Service adapter	SOAP adapter	Y	Y
	SessionBean adapter	Y	N
	MDB(WS-R) adapter	Y	N
	MDB(DB queue) adapter	Y	Y
	DB adapter	Y	Y
	TP1 adapter	Y	Y
	File adapter	Y	Y
	Object Access adapter	Y	Y

Classification	Functionality name	SOAP mode	
		1.1	1.1/1.2 combined
Service adapter	Message Queue adapter	Y	Y
	FTP adapter	Y	Y
	File operation adapter	Y	Y
	Mail adapter	Y	Y
	HTTP adapter	Y	Y
	Universal custom adapter	Y	Y
Business process		Y	Y

(Legend)
Y: Supported.
N: Not supported.

The following table describes WSDL definition style and SOAP mode support:

Table 2–5: TableSOAP mode support range (WSDL definition style)

SOAP version	WSDL definition style	SOAP mode	
		1.1	1.1/1.2 combined
SOAP1.1	rpc/literal	Y	N
	document/literal	Y	Y
SOAP1.2	rpc/literal	N	N
	document/literal	N	Y

(Legend)
Y: Supported.
N: Not supported.

(3) Setting SOAP mode in the execution environment

Container extension library of J2EE server must be set up during system setup according to the selected SOAP mode. For details on how to set the container extension library of J2EE server, see "*3.1.2(4)(e) Setting up the container extension library*".

2.3 Settings related to execution environment

The following types of settings are related to the execution environment. Setting contents differ according to existence of usage of the database and Reliable Messaging.

- Settings of HCSC server configuration definition file
- Settings of HCSC server setup definition file
- Settings of HCSC server runtime definition file
- Definition file settings for user-defined reception runtime
- Database settings
- Registration of conversion table used in change value functionality
- Storage of jar file used in custom functionality
- Settings of XML parser pool functionality option

2.3.1 Setting HCSC server configuration definition file

Information required while defining HCSC server configuration is defined in HCSC server configuration definition file.

(1) Creating HCSC server configuration definition file

Create definition information settings of HCSC server configuration by using the sample file stored in the following directory as HCSC server configuration definition file in XML format:

```
<Service Platform installation directory>\CSC\config\manager\templates\cscsvsetup.xml
```

Use the defined file during HCSC server setup. For HCSC server setup, see "*3.1.3 Setting up an HCSC server*".

Since this file contains information such as user ID and passwords, access permission must be set and managed.

(2) Elements that can be set

The following table describes the elements you can set in HCSC server configuration definition file:

Table 2–6: TableElements that can be set in HCSC server configuration definition file

Classification	Used tag name	Element	Possibility of specification		
			When database is used and Reliable Messaging is not used	When both database and Reliable Messaging are used	When both database and Reliable Messaging are not used
Cluster definition[#1]	name	Cluster name	Y	Y	Y
	type[#1]	Cluster type (LB or HA)	Y	Y	Y
manager definition	name	Manager name	Y	Y	Y
	ip-address[#2]	Manager IP address	Y	Y	Y
	port[#2]	External connection port number to Manager remote management functionality	Y	Y	Y
	id	Management user ID of Management Server	Y	Y	Y

Classification	Used tag name	Element	Possibility of specification		
			When database is used and Reliable Messaging is not used	When both database and Reliable Messaging are used	When both database and Reliable Messaging are not used
manager definition	password[#1]	Management user password of Management Server	Y	Y	Y
csc-server definition	name	HCSC server name	Y	Y	Y
	id	User ID of the database used by HCSC server	Y	Y	N
	password	Password of the database used by HCSC server	Y	Y	N
	j2ee-server-name	J2EE server name used by HCSC server	Y	Y	Y
	setup-properties	HCSC server setup definition file name	Y	Y	Y
soap-reception definition[#1]	ip-address[#1#2]	Web server IP address	Y	Y	Y
	port[#2]	Web server port number	Y	Y	Y
	protocol[#2]	Protocol type (http or https)	Y	Y	Y
jms-reception definition[#1#3]	ip-address[#1#2]	Web server IP address	N	Y	N
	port[#2]	Web server port number	N	Y	N
	protocol[#2]	Protocol type (http or https)	N	Y	N
	rm-service-context-root[#2]	Reliable Messaging service context root	N	Y	N
jms-physical-reception definition[#1#4]	ip-address[#1#2]	Web server IP address	N	Y	N
	port[#2]	Web server port number	N	Y	N
	protocol[#2]	Protocol type (http or https)	N	Y	N
	rm-service-context-root[#2]	Reliable Messaging service context root	N	Y	N
ejb-reception definition[#1]	ip-address[#1#2]	NameServer IP address	Y	Y	Y
	port[#2]	NameServer port number	Y	Y	Y

(Legend)

Y: Can be specified.

N: Cannot be specified.

Note #1

Can be omitted.

Note #2

From the 2nd time onwards, if the setting is changed and reset up is performed, the value is overwritten.

Note #3

Set if the cluster type is "HA". If the cluster type is "LB", it is ignored even if set.

Note #4

Set if the cluster type is "LB". If the cluster type is "HA", it is ignored even if set.

For details on HCSC server configuration definition file, see "HCSC server configuration definition file" in "Service Platform Reference Guide".

2.3.2 Setting HCSC server setup definition file

Define information required for each HCSC server setup in HCSC server setup definition file.

(1) Creating HCSC server setup definition file

Create HCSC server setup information settings by using the sample file stored in the following directory as HCSC server setup definition file in J2SE property format.

```
<Service Platform installation directory>\CSC\config\manager\templates\cscsvsetup.properties
```

(2) Properties that can be set

The following table describes the properties defined in HCSC server setup definition file:

Table 2–7: TableProperties defined in HCSC server setup definition file

Classification	Property name	Contents	Possibility of specification		
			When database is used and Reliable Messaging is not used	When both database and Reliable Messaging are used	When both database and Reliable Messaging are not used
Setup configuration relation	db-use	Existence of database usage	Set ON or omit property	Set ON or omit property	Set OFF
	rm-use	Existence of usage of Reliable Messaging	Set OFF	Set ON or omit property	Set OFF
	hcscserver-data-filepath	Output destination of system management information of HCSC server	Y	Y	Y
Standard reception relation	request-ejb	Existence of usage of standard synchronous reception (SessionBean)	Y	Y	Y
	request-soap	Existence of usage of standard synchronous reception (Web service)	Y	Y	Y
	request-jms	Existence of usage of standard asynchronous reception (MDB(WS-R))	Set OFF	Y	Set OFF
	request-jms.maxmessage	Maximum number of messages in standard asynchronous reception (MDB(WS-R)) queue	N	Y	N
	request-dbq	Existence of usage of standard asynchronous reception (MDB(DB queue))	Set OFF	Y	Set OFF
	request-dbq.maxmessage	Maximum number of messages in standard asynchronous reception (MDB(DB queue)) queue	N	Y	N

Classification	Property name	Contents	Possibility of specification		
			When database is used and Reliable Messaging is not used	When both database and Reliable Messaging are used	When both database and Reliable Messaging are not used
Standard reception relation	request-jms-rdarea	RD area name in standard asynchronous reception (MDB(WS-R))	N	Y	N
	request-dbq-rdarea	RD area name in standard asynchronous reception (MDB(DB queue))	N	Y	N
	request-dbq-maxlen	Maximum message length in standard asynchronous reception (MDB(DB queue))	N	Y	N
User-defined reception relation	request-userdef-soap	Existence of usage of user-defined reception	Y	Y	Y
J2EE relation	naming-service-hostname	Naming service host name	Y	Y	Y
	naming-service-port	Naming service port number	Y	Y	Y
Reliable Messaging relation	rm-systemname	Reliable Messaging system name	N	Y	N
	rm-displayname	Reliable Messaging display name	N	Y	N
DB connector relation	dbcon-xadisplayname	DB Connector display name for XATransaction or for LocalTransaction	Y	Y	N
	dbcon-nodisplayname	DB Connector display name for NoTransaction	Y	Y	N
Database relation	dbtype	Used database type	Y	Y	N
	jdbc-type	JDBC driver type	Y	Y	N
	jdbc-url	Database URL for JDBC	Y	Y	N
	jdbc-dbhostname	Database host name	Y	Y	N
	jdbc-dbconnectinfo	Database connection information	Y	Y	N
	db-character-sets	Database character code type	Y	Y	N
	db-tbl-split-key	Existence of usage of table range partition functionality by date data	Y	Y	N
	db-tbl-split-corcheck-use	Existence of enhancement of correlation set duplication check	Y	Y	N
Business process status compatibility	bp-status-compatible	Existence of usage of business process status compatibility	Y	Y	Y
Compatibility of invoke service activity status	bp-invoke-status-compatible	Existence of compatibility of invoke service activity status	Y	Y	Y
Information of RD area of	cscserverinfo-tbl-area	Table area for basic HCSC information	Y	Y	N

Classification	Property name	Contents	Possibility of specification		
			When database is used and Reliable Messaging is not used	When both database and Reliable Messaging are used	When both database and Reliable Messaging are not used
the database (table area)	server-trans-tbl-area	Table area for linked HCSC	Y	Y	N
	location-tbl-area	Table area for location	Y	Y	N
	routing-tbl-area	Table area for routing	Y	Y	N
	cv-tbl-area	Table area for data transformation	Y	Y	N
	exehistory-tbl-area	Table area for execution history information	Y	Y	N
	exehistory-idx-area	Area to store index of execution history information table	Y	Y	N
	process-tbl-area	Area to store PROCESS table for business process infrastructure	Y	Y	N
	process-idx-area	Area to store PROCESS table index for business process infrastructure	Y	Y	N
	activity-tbl-area	Area to store ACTIVITY table for business process infrastructure	Y	Y	N
	activity-idx-area	Area to store ACTIVITY table index for business process infrastructure	Y	Y	N
	link-tbl-area	Area to store LINK table for business process infrastructure	Y	Y	N
	link-idx-area	Area to store LINK table index for business process infrastructure	Y	Y	N
	correlationset-tbl-area	Area to store CORRELATIONSET table for business process infrastructure	Y	Y	N
	correlationset-idx-area	Area to store CORRELATIONSET table index for business process infrastructure	Y	Y	N
	string-variable-tbl-area	Area to store STRING-VARIABLE table for business process infrastructure	Y	Y	N
	string-variable-idx-area	Area to store STRING-VARIABLE table index for business process infrastructure	Y	Y	N
	numeric-variable-tbl-area	Area to store NUMERIC-VARIABLE table for business process infrastructure	Y	Y	N
	numeric-variable-idx-area	Area to store NUMERIC-VARIABLE table index for business process infrastructure	Y	Y	N
	boolean-variable-tbl-area	Area to store BOOLEAN-VARIABLE table for business process infrastructure	Y	Y	N

Classification	Property name	Contents	Possibility of specification		
			When database is used and Reliable Messaging is not used	When both database and Reliable Messaging are used	When both database and Reliable Messaging are not used
	boolean-variable-idx-area	Area to store BOOLEAN-VARIABLE table index for business process infrastructure	Y	Y	N
	message-variable-tbl-area	Area to store MESSAGE-VARIABLE table for business process infrastructure	Y	Y	N
	message-variable-idx-area	Area to store MESSAGE-VARIABLE table index for business process infrastructure	Y	Y	N
	message-variable-val-area	Area to store VariableValue column of MESSAGE-VARIABLE table for business process infrastructure	Y	Y	N
	message-relation-tbl-area	Area to store MESSAGE-RELATION table for business process infrastructure	Y	Y	N
	message-relation-idx-area	Area to store MESSAGE-RELATION table index for business process infrastructure	Y	Y	N
	clusterinfo-tbl-area	Area to store cluster information	Y	Y	N
	haasyncadp-tbl-area	Area to store asynchronous adapter service ID deployed in the cluster	Y	Y	N
	sql-scriptfilename	SQL script file path	Y	Y	N
Compatibility of maximum number of activity instances	activitynumber-maximum-compatible	Existence of usage of compatibility of the maximum number of activity instances that can be created in 1 process instance	Y	Y	Y
XML analysis	xmlanalyze-mode	XML analysis mode	Y	Y	Y

(Legend)

Y: Can be specified.

N: Cannot be specified.

For details on HCSC server setup definition file, see "HCSC server setup definition file" in "Service Platform Reference Guide".

2.3.3 Setting HCSC server runtime definition file

HCSC server runtime definition file defines the runtime information required to run HCSC server.

(1) Creating HCSC server runtime definition file

Create HCSC server runtime definition by using the sample file stored in the following directory as HCSC server runtime definition file. Create this file in J2SE property file format.

```
<Service Platform installation directory>\CSC\config\manager\templates
\cscsvconfig.properties
```

Use this file while setting HCSC server definition information. For details on HCSC server definition, see "*3.1.4 Setting up the HCSC server definition information*".

(2) Properties that can be set

The following table describes the properties defined in HCSC server runtime definition file:

Table 2–8: TableProperties defined in HCSC server runtime definition file

Classification	Property name	Contents	Possibility of specification		
			When database is used and Reliable Messaging is not used	When both database and Reliable Messaging are used	When both database and Reliable Messaging are not used
Log trace	methodtrace-filepath	Method trace/exception log output destination path	Y	Y	Y
	requesttrace-filepath	Request trace output destination path	Y	Y	Y
	telegramtrace-filepath	User message trace output destination path	Y	Y	Y
	methodtrace-filenum	Maximum number of method trace files	Y	Y	Y
	requesttrace-filenum	Maximum number of request trace files	Y	Y	Y
	telegramtrace-filenum	Maximum number of user message trace files	Y	Y	Y
	methodtrace-filesize	Maximum size of 1 method trace file	Y	Y	Y
	requesttrace-filesize	Maximum size of 1 request trace file	Y	Y	Y
	telegramtrace-filesize	Maximum size of 1 user message trace file	Y	Y	Y
	telegramtrace-trigger	Trigger for output of user message trace	Y	Y	Y
	methodtrace-level	Method trace output level	Y	Y	Y
	requesttrace	Existence of request trace extraction	Y	Y	Y
	telegramtrace	Existence of user message trace extraction	Y	Y	Y
	bptrace-level	Output level of method trace of business process infrastructure	Y	Y	Y
	bptrace-filenum	Number of method trace files of business process infrastructure	Y	Y	Y
	bptrace-filesize	Size of method trace of business process infrastructure	Y	Y	Y
	bpexptrace-filenum	Number of exception log files of business process infrastructure	Y	Y	Y
	bpexptrace-filesize	Size of exception log files of business process infrastructure	Y	Y	Y

Classification	Property name	Contents	Possibility of specification		
			When database is used and Reliable Messaging is not used	When both database and Reliable Messaging are used	When both database and Reliable Messaging are not used
Log trace	cscexptrace-filenum	Number of exception log files of messaging infrastructure	Y	Y	Y
	cscexptrace-filesize	Size of exception log files of messaging infrastructure	Y	Y	Y
Standard reception relation	request-ejb.instance.minimum	Minimum number of instances of standard synchronous reception (SessionBean)	Y	Y	Y
	request-ejb.instance.maximum	Maximum number of instances of standard synchronous reception (SessionBean)	Y	Y	Y
	request-ejb.ctm	Existence of use of CTM integration	Y	Y	Y
	request-ejb.parallel.count	Number of threads prepared for invocation of application by CTM	Y	Y	Y
	request-ejb.optional.name	Optional name of standard synchronous reception (SessionBean)	Y	Y	Y
	request-soap.instance.minimum	Minimum number of simultaneous executions of standard synchronous reception (Web service or SOAP1.1)	Y	Y	Y
	request-soap.instance.maximum	Maximum number of simultaneous executions of standard synchronous reception (Web service or SOAP1.1)	Y	Y	Y
	request-soap.exclusive.threads	Number of dedicated threads of standard synchronous reception (Web service or SOAP1.1)	Y	Y	Y
	request-soap.queue-size	Size of pending queue of standard synchronous reception (Web service or SOAP1.1)	Y	Y	Y
	request-soap1_2.instance.minimum	Minimum number of simultaneous executions of standard synchronous reception (Web service or SOAP1.2)	Y	Y	Y
	request-soap1_2.instance.maximum	Maximum number of simultaneous executions of standard synchronous reception (Web service or SOAP1.2)	Y	Y	Y
	request-soap1_2.exclusive.threads	Number of dedicated threads of standard synchronous reception (Web service or SOAP1.2)	Y	Y	Y
	request-soap1_2.queue-size	Size of pending queue of standard synchronous reception (Web service or SOAP1.2)	Y	Y	Y
	request-jms.instance.maximum	Maximum number of instances of standard asynchronous reception (MDB(WS-R))	N	Y	N
	request-jms.rollback-count	Number of times that rollback warning message of standard asynchronous reception (MDB(WS-R)) is output	N	Y	N

Classification	Property name	Contents	Possibility of specification		
			When database is used and Reliable Messaging is not used	When both database and Reliable Messaging are used	When both database and Reliable Messaging are not used
Standard reception relation	receptionstop-monitor-timer	Timeout time of reception queue monitoring	N	Y	N
	csc-receptionstop-timeout	Communication timeout time of reception end standby	Y	Y	Y
Service adapter relation	soapfault-targetnamespace-filepath	Whether to handle SOAP Fault as a user-defined exception	Y	Y	Y
Data transformation relation	formatdef-maxcache-num	Number of format definitions that can be cached	Y	Y	Y
	transformdef-maxcache-num	Number of data transformation definitions that can be cached	Y	Y	Y
	xmltelegram-maxcache-num	Number of XML messages that can be cached	Y	Y	Y
	telegram-validation	Whether or not to validate whether sending and receiving messages is suitable for the message format	Y#	Y#	Y
	xmltelegram-namespace-complement	Whether to supplement the name space declaration corresponding to the name space prefix specified in the attribute value in XML message	Y	Y	Y
	telegram-undefined-character-code	Whether to continue the process if an undefined character code is detected in the character code conversion process of binary data	Y	Y	Y
	telegram-notfound-soapheader	Whether to continue the process if the header specified in sent and received messages does not exist for the reception definition file, service adapter definition file or business process definition file	Y	Y	Y
	validation-activity	Whether to validate the message type variable (XML) by validation activity	Y	Y	Y
	transform-binary-error-check	Whether to check errors during binary data transformation	Y	Y	Y
Business process relation	syserr-to-fault-convert	Whether to cause universal fault if a system exception occurs in data transformation activity, assign activity or switch activity	Y	Y	Y
	validate-fault-compatible	Whether the fault message format sent by validation fault is to be in the format used in 09-00 or lower	Y	Y	Y
	bp-reply-after-min-thread-pool-size	Minimum number of threads used to perform activities after response activity	Y	Y	Y

Classification	Property name	Contents	Possibility of specification		
			When database is used and Reliable Messaging is not used	When both database and Reliable Messaging are used	When both database and Reliable Messaging are not used
Business process relation	bp-reply-after-max-thread-pool-size	Maximum number of threads used to perform activities after response activity	Y	Y	Y
	bp-reply-after-thread-pool-keep-alive	Maintenance time of threads used to perform activities after response activity	Y	Y	Y
J2EE relation	j2ee-stopapp-timeout	Monitoring time when J2EE application stops	Y	Y	Y
	startcsc-timeout	Monitoring time when J2EE server starts	Y	Y	Y
	stopcsc-timeout	Monitoring time when J2EE server stops	Y	Y	Y
Monitoring command communication timeout time	csc-command-timeout	Command communication timeout time	Y	Y	Y
	csc-precache-timeout	EJB communication timeout in the business process for advance cache process	Y	Y	Y
Cookie information inheritance	cookie-parsing	Whether to inherit Cookie	Y	Y	Y
Folder relation	work-folder	Absolute path of operation folder route	Y	Y	Y
	common-folder-<Common folder definition name>	Absolute path of common folders	Y	Y	Y
DB adapter relation	dba-separate-transaction	Whether to start DB adapter transaction separately from the business process	Y	Y	Y
Component common UOC relation	common-uoc-prop-path	Property file storage folder for component common UOC	Y	Y	Y
HCSC server relation	short-processid-servername	HCSC server name identifier used by process instance identifier	Y	Y	Y
	short-processid	Whether to reduce process instance identifier	Y	Y	Y
Instance pool	xml-pooled-instance-minimum	Minimum number of instance pools of the class used in XML process	Y	Y	Y
	xml-pooled-instance-maximum	Maximum number of instance pools of the class used in XML process	Y	Y	Y

(Legend)

Y: Can be specified.

N: Cannot be specified.

Note #

Validate whether the messages sent and received in the message format are suitable if telegram-validation property is turned "ON" in 07-60 or higher version. Please note that in the following cases error has always occurred in the service adapter if the message succeeded in service invocation.

- If telegram-validation property was set "ON" after version-up from 07-50 or lower version to 07-60 or higher version
- If telegram-validation property in 07-60 or higher version was reset from "OFF" to "ON"

If telegram-validation property is set "OFF" in 07-50 or lower version or 07-60 or higher version, do not validate whether the messages sent and received in the message format is suitable or not.

For details on HCSC server runtime definition file, see "HCSC server runtime definition fil" in "Service Platform Reference Guide".

2.3.4 Setting the definition file for user-defined reception runtime

Set SOAP reception information in the definition file for user-defined reception runtime.

(1) Creating the definition file for user-defined reception runtime

Create SOAP reception runtime definition by using the sample file stored in the following directory as the definition file for user-defined reception runtime. Create this file in J2SE property file format.

```
<Service Platform installation directory>\CSC\config\manager\templates
\cscurcptnconfig.properties
```

After creating the definition file for user-defined reception runtime, set definition information by csccompoconfig command. For details on how to set the SOAP reception definition information, see "*3.1.15 Setting the definition information for user-defined receptions*".

Use this file while deploying SOAP reception. For details on how to deploy the user-defined reception included in SOAP reception, see "*3.1.14 Deploying a user-defined reception*".

(2) Properties that can be set

The following table describes the properties defined in the definition file for user-defined reception runtime:

Table 2–9: TableProperties defined in definition file for user-defined reception runtime

Property name	Contents	Possibility of specification		
		When database is used and Reliable Messaging is not used	When both database and Reliable Messaging are used	When both database and Reliable Messaging are not used
user-defined-reception-soap.threads.maximum	Maximum number of simultaneous executions of SOAP reception	Y	Y	Y
user-defined-reception-soap.exclusive.threads	Number of dedicated threads of SOAP reception	Y	Y	Y
user-defined-reception-soap.queue-size	Size of pending queue in SOAP reception	Y	Y	Y

(Legend)

Y: Can be specified.

For details on the definition file for user-defined reception runtime, see "Definition file for user-defined reception runtime" in "Service Platform Reference Guide".

2.3.5 Estimating database table capacity

You must estimate database table capacity in advance in order to manage execution history and to set the execution environment. Setting is not necessary if the database is not used.

(1) Estimating table capacity related to execution history management of process instances

The following table describes the list of database tables related to execution history management of process instances:

Table 2–10: TableList of database tables related to execution history management of process instances

Classification	Table name	Description
Basic information table	CSCBP_<Cluster name>_PROCESS	Store process instance status.
	CSCBP_<Cluster name>_ACTIVITY	Store activity instance status.
	CSCBP_<Cluster name>_LINK	Store link status.
	CSCBP_<Cluster name>_CORRELATIONSET	Store correlation set value.
Variable information table	CSCBP_<Cluster name>_STR_VARIABLE	Store string type variable value.
	CSCBP_<Cluster name>_NUM_VARIABLE	Store numeric type variable value.
	CSCBP_<Cluster name>_BOOL_VARIABLE	Store boolean type variable value.
	CSCBP_<Cluster name>_MSG_VARIABLE	Store message type variable value (XML, non-XML, any).
Message history correlated information table	CSCBP_<Cluster name>_MSG_RELATION	Store correlated information of message ID and process instance identifier or activity instance identification number.

While designing a database, see all types of database manuals and estimate contents on the basis of the following information:

(a) Table and index definitions

For details on table and index definitions, see "*Appendix C.1 Table information about process instance execution log management*".

(b) Estimation methods of number of records

Calculate estimation of the number of records for each table as follows:

- **CSCBP_<Cluster name>_PROCESS table**

$$\text{Number of records} = \sum_{\text{Entire business process}} \text{Number of processes}$$

- **CSCBP_<Cluster name>_ACTIVITY table**

$$\text{Number of records} = \sum_{\text{Entire business process}} \text{Number of activities}$$

Number of activities={Number of activity definitions in business process definition
+Number of activity definitions in repeat activities
x (Repeat activity loop frequency-1)}
x Number of processes

- **CSCBP_<Cluster name>_LINK table**

  Number of records = Number of service adapters [#1]
  + Number of business processes[#2]
  + Number of user-defined receptions[#3]

  Note#1 It is the number of service adapters deployed using the csccompodeploy (deploying HCSC components) command.
  Note#2 It is the number of business processes deployed using the csccompodeploy (deploying HCSC components) command.
  Note#3 It is the number of user-defined receptions deployed using the csccompodeploy (deploying HCSC components) command.

  Number of links={Number of link definitions in business process definition
  +Number of link definitions in repeat activities
  x (Repeat activity loop frequency-1)}
  x Number of processes

- **CSCBP_<Cluster name>_CORRELATION-SET table**

  Number of records = Σ (Number of correlation set definition ×Number of process)
  Entire business process

- **CSCBP_<Cluster name>_STR_VARIABLE table**

  Number of records = Σ (Number of string type variable definition count × Number of processes)
  Entire business process

- **CSCBP_<Cluster name>_NUM_VARIABLE table**

  Number of records = Σ (Number of numeric values variable type definition × Number of processes)
  Entire business process

- **CSCBP_<Cluster name>_BOOL_VARIABLE table**

  Number of records = Σ (Number of Boolean type variable definitions x Number of processes)
  Entire business process

- **CSCBP_<Cluster name>_MSG_VARIABLE table**

  Number of records = Σ (Message type variable definition x Number of processes)
  Entire business process

- **CSCBP_<Cluster name>_MSG_RELATION table**

  Number of records = Σ (Number of received messages x Number of processes)
  Entire business process

  Number of messages sent and received=Number of reception activity definitions
  + Number of invoke service activity definitions

(c) All types of index estimation methods

All types of index estimation methods are derived from index definitions and the number of records. For estimation methods, see the used database manual.

(2) Estimating table capacity related to execution environment settings

The following table describes the list of database tables related to execution environment settings:

Table 2–11: TableList of database tables related to execution environment settings

Classification	Table name	Description
Basic HCSC information table	CSCMSG_S<HCSC server name>_CSC_PERSIST	HCSC server status persists.

Classification	Table name	Description
HCSC linkage directory information table	CSCMSG_C<Cluster name>_CSC_CONNECT	This table is not used.
Location directory information table	CSCMSG_S<HCSC server name>_LC_DIRECTORY	Store location information of service adapter, business process and service group.
	CSCMSG_S<HCSC server name>_LC_BPFORMAT	Store business process format information.
Routing rules directory information table	CSCMSG_S<HCSC server name>_RT_RULE	Store rule information for service routing.
Directory information table for data transformation definition	CSCMSG_S<HCSC server name>_CV_MAPPING	Store data transformation definition information.
	CSCMSG_S<HCSC server name>_CV_FORMAT	Store message format definition information for data transformation.
Basic cluster information table	CSCMSG_C<Cluster name>_CLUSTER	Store set up HCSC server name.
Management table of asynchronous adapter service ID	CSCMSG_C<Cluster name>_HA_ASYNC_ADP	Store deployed asynchronous adapter service ID.

While designing a database, see all types of database manuals and estimate contents on the basis of the following information:

- Table and index definitions
- Estimation methods of number of records
- All types of index estimation methods

(a) Table and index definitions

For details on table and index definitions, see "*Appendix C.3 Table information about execution environment setup*".

(b) Estimation methods of number of records

Calculation of the number of records for each table as follows:

- **CSCMSG_S<HCSC server name>_CSC_PERSIST table**

  Number-of-records = 1

- **CSCMSG_C<Cluster name>_CSC_CONNECT table**

  Number-of-records = 0

- **CSCMSG_S<HCSC server name>_LC_DIRECTORY table**

  Number of records = Number of service adapters #1

  + Number of business processes#2

  + Number of user-defined receptions#3

  Note#1 It is the number of service adapters deployed using the csccompodeploy (deploying HCSC components) command.
  Note#2 It is the number of business processes deployed using the csccompodeploy (deploying HCSC components) command.
  Note#3 It is the number of user-defined receptions deployed using the csccompodeploy (deploying HCSC components) command.

- **CSCMSG_S<HCSC server name >_LC_BPFORMAT table**

Number of records = Number of business processes#1
× Number of receive activities defined in the deployed business processes#2

#1 This is the number of business processes deployed using csccompodeploy (deploying HCSC component) command.
#2 this is the number of reception activity (operation name of the receipt) defined by business process definition of development environment. Business process deployment uses csccompodeploy (deploying HCSC component) command.

- **CSCMSG_S<HCSC server name>_RT_RULE table**

  Number-of-records = 0

- **CSCMSG_S<HCSC server name>_CV_MAPPING table**

  Number-of-records = 0

- **CSCMSG_S<HCSC server name>_CV_FORMAT table**

  Number-of-records = Number of receive-activities-defined-in-deployed-business-process#

  # Number of receive activities (reception operation name) defined in business process definition of the development environment. Use the csccompodeploy (deploying HCSC components) command for deploying business process.

- **CSCMSG_C<Cluster name>_CLUSTER table**

  Number of records＝Number of HCSC servers set in the cluster

- **CSCMSG_C<Cluster name>_HA_ASYNC_ADP table**

  Number of records＝ Number of asynchronous adapters deployed in the cluster#

  # Number of records when cluster type is "LB" : 0
  Number of records when cluster type is "HA": Number of asynchronous adapters deployed in the cluster

(c) All types of index estimation methods

All types of index estimation methods are derived from index definitions and the number of records. For estimation methods, see the used database manual.

2.3.6 Estimating the number of exclusive requests of the database (HiRDB)

The number of exclusive requests must be estimated while deleting execution history if the database used by HCSC server is HiRDB. Setting is not necessary if the database is not used.

This section describes the estimation method of the number of exclusive requests when execution history is deleted. The number of estimated exclusive requests must be defined in HiRDB definition file. For details on HiRDB definition file and the operands defined in the definition file, see the contents related to estimation of the number of exclusive resources in "HiRDB Version 9 System Definition".

(1) Estimating the number of exclusive requests while deleting process instance execution history (cscpidelete command)

This section describes estimation of the number of exclusive requests while deleting process instance execution history (cscpidelete command). For details on the how to delete process instance execution history by cscpidelete command, see "*6.1.4(2) Using commands to delete execution logs*".

Estimation target

Estimation target SQL is "DELETE (if there is no LOCK TABLE and for index key value non-exclusive method)" of operation system SQL.

For details on "DELETE (if there is no LOCK TABLE and for index key value non-exclusive method)", see the contents related to estimation of the number of exclusive resources in "HiRDB system definition".

Estimation method

Calculate the number of exclusive resources in all tables in estimation of the number of exclusive requests. For the number of exclusive resources, use the values shown in "*Table2-12 TableValues used in estimating the number of exclusive resources (deleting process instance execution history by cscpidelete command)*" and calculate.

After calculation, add the surplus value in the largest number of exclusive resources in the number of exclusive resources and then estimate the number of exclusive requests.

Define the number of estimated exclusive requests in HiRDB definition file.

For details on how to estimate the number of exclusive resources and how to set the number of estimated exclusive requests, see the contents related to estimation of the number of exclusive resources in "HiRDB system definition" and the contents related to "pd_lck_pool_size" of the operand related to exclusive control.

The following table describes the values used in estimating the number of exclusive resources when process instance execution history is to be deleted (cscpidelete command):

Table 2–12: TableValues used in estimating the number of exclusive resources (deleting process instance execution history by cscpidelete command)

Item number	Item	Specified value								
		A	B	C	D	E	F	G	H	I
1	Number of RD areas to be deleted	2	2	3	2	2	2	2	4	2
2	Number of deleted rows	1	Maximum value of the number of activities defined in 1 business process	Maximum value of the number of links defined in 1 business process	Maximum value of the number of correlation sets defined in 1 business process	Maximum value of the number of string type variables of global variables defined in 1 business process	Maximum value of the number of numeric type variables of global variables defined in 1 business process	Maximum value of the number of boolean type variables of global variables defined in 1 business process	Maximum value of the number of message type variables of global variables defined in 1 business process	Maximum value of the number of activities defined in 1 business process
3	Number of switches	1	1	1	1	1	1	1	1	1
4	Number of columns over 256 bytes in VARCHAR, NVARCHAR, MVARCHAR	0	0	0	0	0	0	0	0	0
5	Number of BINARY types that cannot be stored in 1 page	0	0	0	0	0	0	1	0	0
6	Number of deleted LOB data items	-	-	-	-	-	-	-	-	-
7	Number of deleted LOB data storage segments	-	-	-	-	-	-	-	-	-

Item number	Item	Specified value								
		A	B	C	D	E	F	G	H	I
8	Data type plug-in or index type plug-in	-	-	-	-	-	-	-	-	-
9	pd_inner_replica_control operand (in UNIX version HiRDB)	-	-	-	-	-	-	-	-	-
10	Routine	-	-	-	-	-	-	-	-	-
11	Preprocessing	See "*Table2-13 TableValues used in estimating the number of exclusive requests for preprocessing (while deleting process instance execution history)*".								

(Legend)

A:CSCBP_<Cluster name>_PROCESS table
B:CSCBP_<Cluster name>_ACTIVITY table
C:CSCBP_<Cluster name>_LINK table
D:CSCBP_<Cluster name>_CORRELATIONSET table
E:CSCBP_<Cluster name>_STR_VARIABLE table
F:CSCBP_<Cluster name>_NUM_VARIABLE table
G:CSCBP_<Cluster name>_BOOL_VARIABLE table
H:CSCBP_<Cluster name>_MSG_VARIABLE table
I:CSCBP_<Cluster name>_MSG_RELATION table
-: Undefined or unused item.

The following table describes the values used in estimating the number of exclusive requests for preprocessing. For the number of exclusive requests for preprocessing, see "HiRDB Version 9 System Definition".

Table 2–13: TableValues used in estimating the number of exclusive requests for preprocessing (while deleting process instance execution history)

Item number	Item	Specified value								
		A	B	C	D	E	F	G	H	I
1	Number of tables used	1	1	1	1	1	1	1	1	1
2	Number of view tables used	0	1	1	0	1	1	1	1	1
3	Number of columns	8	13	4	8	4	4	4	4	5
4	Number of indices	4	1	1	2	1	1	1	1	3
5	Number of table partitions	-	-	-	-	-	-	-	-	-
6	Number of index partitions	-	-	-	-	-	-	-	-	-
7	User definition type or functionality use	-	-	-	-	-	-	-	-	-
8	Optimization information	-	-	-	-	-	-	-	-	-
9	View table use	0	1	1	0	1	1	1	1	0
10	Number of columns configuring view tables	0	14	6	0	7	7	7	7	0
11	LOB column definition	-	-	-	-	-	-	-	-	-
12	Definition of user definition type column	-	-	-	-	-	-	-	-	-
13	LOB attribute	-	-	-	-	-	-	-	-	-

Item number	Item	Specified value								
		A	B	C	D	E	F	G	H	I
14	Parent type	-	-	-	-	-	-	-	-	-
15	Functionality use	-	-	-	-	-	-	-	-	-
16	Plug-in use	-	-	-	-	-	-	-	-	-
17	Routine use	-	-	-	-	-	-	-	-	-

(Legend)

A:CSCBP_<Cluster name>_PROCESS table
B:CSCBP_<Cluster name>_ACTIVITY table
C:CSCBP_<Cluster name>_LINK table
D:CSCBP_<Cluster name>_CORRELATIONSET table
E:CSCBP_<Cluster name>_STR_VARIABLE table
F:CSCBP_<Cluster name>_NUM_VARIABLE table
G:CSCBP_<Cluster name>_BOOL_VARIABLE table
H:CSCBP_<Cluster name>_MSG_VARIABLE table
I:CSCBP_<Cluster name>_MSG_RELATION table
-: Undefined or unused item.

(2) Estimating the number of exclusive requests while deleting process instance execution history (RD area unit)

This section describes estimation of the number of exclusive requests while deleting process instance execution history (RD area unit). For details on how to delete process instance execution history in RD area unit, see "*6.1.4(3) Using database creation utility (pdload) to delete execution logs*".

Estimation target

The estimation target is the database creation utility (pdload) and the database reorganization utility (pdrorg).

For details on the database creation utility (pdload) and the database reorganization utility (pdrorg), see the description related to exclusive resource estimation in "HiRDB Version 9 System Definition".

Estimation method

Calculate the number of exclusive resources by using the values shown in "*Table2-14 TableValues used in estimating the number of exclusive resources (while deleting process instance execution history in RD area units)*".

After calculation, add the surplus value in the largest number of exclusive resources in the number of exclusive resources and then estimate the number of exclusive requests.

Define the number of estimated exclusive requests in HiRDB definition file.

The following table describes the values used in estimating the number of exclusive resources while deleting process instance execution history (RD area unit).

Table 2–14: TableValues used in estimating the number of exclusive resources (while deleting process instance execution history in RD area units)

Item number	Item	Specified value								
		A	B	C	D	E	F	G	H	I
1	Number of table columns	9	14	5	9	5	5	5	5	6
2	Number of table indices	4	1	1	2	1	1	1	1	3
3	Number of storage RD areas in table	This depends on the contents of the SQL script file when HCSC server is set up.								

Item number	Item	Specified value								
		A	B	C	D	E	F	G	H	I
4	Number of RD area segments being used for storage in table storage	You can confirm this by specifying -r option in pddbst command and executing. For details on pddbst command, see the description of database status analysis utility (pddbst) in "HiRDB command reference".								
5	Number of RD area segments used for index storage									
6	Number of RD area segments used for LOB	-	-	-	-	-	-	-	-	-
7	Number of items generated in used ordinal number	-	-	-	-	-	-	-	-	-
8	Number of RD areas for storage of items generated in used ordinal number	-	-	-	-	-	-	-	-	-

(Legend)

A:CSCBP_<Cluster name>_PROCESS table
B:CSCBP_<Cluster name>_ACTIVITY table
C:CSCBP_<Cluster name>_LINK table
D:CSCBP_<Cluster name>_CORRELATIONSET table
E:CSCBP_<Cluster name>_STR_VARIABLE table
F:CSCBP_<Cluster name>_NUM_VARIABLE table
G:CSCBP_<Cluster name>_BOOL_VARIABLE table
H:CSCBP_<Cluster name>_MSG_VARIABLE table
I:CSCBP_<Cluster name>_MSG_RELATION table
-: Undefined or unused item.

2.3.7 Designing mapping in database areas

After estimating database table capacity, the method to map each table and index in the database area (RD area in HiRDB and table area in Oracle (table space)) must be designed. Setting is not necessary if the database is not used.

Set mapping for the database area in the properties of HCSC server setup definition file. For details, see the line "Information of RD area of the database (table area)" of "*Table2-7 TableProperties defined in HCSC server setup definition file*" in "*2.3.2(2) Properties that can be set*".

! Important note

Consider the following points and then design the table and index database area:

- Data volume based on setup operations
- Balance with business system

2.3.8 Registering the conversion table used in change value functionality

If the data transformation definition created in the development environment contains the change value functionality, register the conversion table used in the change value functionality in the system properties file, (usrconf.properties).

Storage location of usrconf.properties

```
<Service Platform installation directory>\CC\server\usrconf\ejb\<server
name>\usrconf.properties
```

Registration method in usrconf.properties

usrconf.properties describes conversion table ID, conversion table file path, total file size of conversion table and used character code. Storage location and character code information are described as sets. Multiple conversion tables can be described.

Contents and formats described in usrconf.properties are as follows:

```
   :
csc.dt.valueTable.<Conversion table ID>=<Conversion table file path>
csc.dt.valueTableSize=<Total file size of conversion table>
csc.dt.encodeType.<Conversion table ID>=[MS932|UTF8|UTF16_BIG|UTF16_LITTLE]
   :
```

<Conversion table ID>

Specify any name as conversion table ID. Conversion table ID is used to specify the conversion table used while defining the change value functionality in the change value dialog of the development environment.

<Conversion table file path>

Specify the conversion table file path by the absolute path.

<Total file size of conversion table><<10>>

Specify the total file size of the conversion table (unit: kilobyte).

Specify a positive integer in the total file size. Specification range is 1 - 2097151. If you omit specification, 10 is reflected.

If a conversion table the size of which exceeds the maximum value is read, KDEC40730-E is output in J2EE server log file and HCSC server start is interrupted.

[MS932 | UTF8 | UTF16_BIG | UTF16_LITTLE]

Specify the character code used in the conversion table.

2.3.9 Storing jar file used in custom functionality

If the data transformation definition created in the development environment contains the custom functionality, store the jar file used in the custom functionality in the execution environment.

Storage location of jar file

```
<Service Platform installation directory>\CSC\userlib\customfunc
```

Restart J2EE server after storing the jar file in the execution environment.

Changing the storage location of the jar file used in custom functionality

Set the file path in the system properties file, (usrconf.properties).

Storage location of usrconf.properties

```
<Service Platform installation directory>\CC\server\usrconf\ejb\< server
name>\usrconf.properties
```

Description format in usrconf.properties

```
csc.dt.customFuncDir=<Change destination directory path>
```

Example of description in usrconf.properties

An example of description when the storage location of jar file used in the custom functionality is changed to "C:\\USER\\FUNC" is described here.

```
csc.dt.customFuncDir=C:\\USER\\FUNC
```

Points to be considered when setting file path in usrconf.properties

If you specify under the Service Platform installation directory in the storage location of jar file used in the custom functionality, specification might be deleted while uninstalling. To avoid this, set a location other than under the Service Platform installation directory while changing the storage location of jar file used in the custom functionality.

2.3.10 Using XML parser pool functionality option

XML is analyzed in HCSC server by the following Java XML parser:

- DOM parser (javax.xml.DocumentBuilder class)
- SAX parser (org.xml.sax.XMLReader class)

Since multiple threads cannot share these XML parser instances, XML parser is created for each thread for simultaneous use by multiple threads. Since XML parser creation process requires time and performance deteriorates if the parser is created for each analysis.

You can use XML parser pool functionality to save in advance XML parser generated in XML parser pool created in the memory. The entire system shares XML parser saved in XML parser pool and process efficiency is expected to improve because the parser can be reused.

Specify XML parser pool functionality option in usrconf.properties (user properties file for J2EE server). These options are exclusive to Service Platform. The following points describe each option of XML parser pool functionality:

(1) DOM parser pool functionality option

Specify DOM parser pool option used to analyze XML in HCSC server as follows:

Table 2–15: TableList of DOM parser pool functionality options

Item number	Key name	Contents	Default value
1	csc.dt.pool.DocumentBuilder.initialSize	Specify the number of default allocations when DOM parser pool is created by integers between 0 - 2,147,483,647. When you first create DOM parser, compile the number of default allocations and store in the pool. This enables you to reduce further creation time. If you specify a value larger than the maximum number of pools (specified by csc.dt.pool.DocumentBuilder.maxSize), initialization is by maximum number of pools. Operation is by default value if you specify a negative integer or a character string other than an integer.	0
2	csc.dt.pool.DocumentBuilder.maxSize	Specify the maximum number of pools of DOM parser by integers between 0 - 2,147,483,647. If DOM parser used exceeds the maximum number of pools specified here, standby status occurs till use by another thread ends. If you specify integers under 0, pool functionality is disabled. Operation is by default value if you specify character string other than integers.	64

Set the number of default allocations (specified by csc.dt.pool.DocumentBuilder.initialSize) and the maximum number of pools (specified by csc.dt.pool.DocumentBuilder.maxSize) to fulfill the following relation:

```
Number of default allocations ? Maximum number of pools ? Number of maximum simultaneous
request executions
```

(2) SAX parser pool functionality option

Specify SAX parser pool option used to analyze XML in the following process:

- Validation activity process of business process
- Data validation functionality (specify ON in telegram-validation property in HCSC server runtime definition file)

The following table describes SAX parser pool options:

Table 2–16: TableList of SAX parser pool functionality options

Item number	Key name	Contents	Default value
1	csc.dt.pool.XMLReader.initialSize	Specify the number of default locations while creating SAX parser pool by integers between 0 - 2,147,483,647. When you first create SAX parser, compile the number of default allocations and store in the pool. This enables you to reduce further creation time. If you specify a value larger than the maximum number of pools (specified by csc.dt.pool.XMLReader.maxSize), initialization is by maximum number of pools. Operation is by default value if you specify a negative integer or a character string other than an integer.	0
2	csc.dt.pool.XMLReader.maxSize	Specify the maximum number of pools of SAX parser by integers between 0 - 2,147,483,647. If SAX parser used exceeds the maximum number of pools specified here, standby status occurs till use by another thread ends. If you specify integers under 0, pool functionality is disabled. Operation is by default value if you specify character string other than integers.	64

Set the number of default allocations (specified by csc.dt.pool.XMLReader.initialSize) and the maximum number of pools (specified by csc.dt.pool.XMLReader.maxSize) to fulfill the following relation:

```
Number of default allocations  ? Maximum number of pools

<If data validation functionality is used>
Maximum number of pools  ? Maximum number of simultaneous executions of each business
process/service adapter (multiplicity)

<If data validation functionality is not used>
Maximum number of pools  ? Total of maximum number of simultaneous executions of validation
activities of each business process
```

2.4 Settings Related to the Operating Environment

Settings related to the operating environment include the following:

- Various customization settings
- User information settings
- Settings common to all HCSC-Manager commands

Important note

When multiple operating environments are configured on one machine, you must set up the CSCMNG_HOME environmental variable before you specify the settings related to the operating environment. For details about the CSCMNG_HOME environment variable, see *2.9.2(1) Setting the CSCMNG_HOME environment variables*.

2.4.1 Customizing operating environment

You can customize the following contents in the operating environment:

- Directory that is the import destination repository
- Output destination directory of HCSC-Manager log file
- Log file size
- Number of log files
- Read timeout value during connection between HCSC-Manager and Manager
- If a response message is received by process instance re-execution, directory to store the response message
- If a response message is received by process instance re-execution, output character code when the response message is stored

Information required for customization is defined in HCSC-Manager definition file.

(1) Storage directory of HCSC-Manager definition file

HCSC-Manager definitions are stored in the following directory as HCSC-Manager definition file in the property format of J2SE format:

```
<Service Platform installation directory>\CSC\config\manager\cscmng.properties
```

(2) Properties defined in HCSC-Manager definition file

The following table describes the properties defined in HCSC-Manager definition file:

Table 2–17: TableProperties defined in HCSC-Manager definition file

Item number	Classification	Key name	Contents
1	Repository settings	cscmng.repository.root	Root directory path of repository
2	Log file settings	cscmng.log.dir	Directory path of log output destination
3		cscmng.log.<Channel name>.filesize	Log file size
4		cscmng.log.<Channel name>.filenum	Number of log files
5	Manager settings	cscmng.manager.<Manager identifier>.timeout	Timeout value
6	Process instance re-execution settings	cscmng.pireexec.response.dir	Response message storage directory path

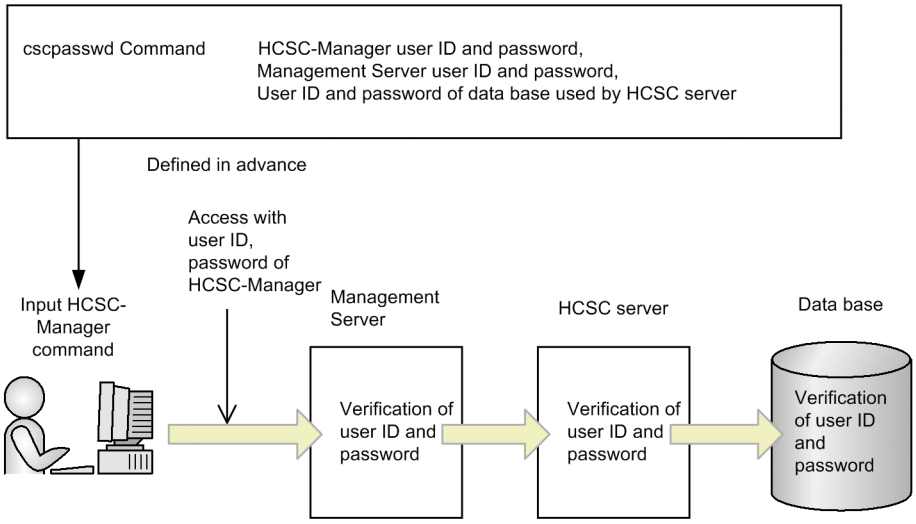
Item number	Classification	Key name	Contents
7	Process instance re-execution settings	cscmng.pireexec.response.encoding	Response message storage character code
8	HCSC server operation settings	cscmng.server.<HCSC server name>.system	Logical server under HCSC system management
9	Repository export	cscmng.repctl.export.dir	Output destination directory path of export file
10	Environment backup	cscmng.envbackup.dir	Output destination directory path of environment backup
11		cscmng.envbackup.dir.envrestore	Output destination directory path of environment backup before restoration
12		cscmng.envbackup.dir.import	Output destination directory path of environment backup before import
13		cscmng.envbackup.autoget	Existence of auto-backup specifications
14		cscmng.envbackup.autoget.off	Prevention of environment backup while restoring an environment or while importing a repository
15	Thread setting for commands	cscmng.precache.thread.maximum	Maximum number of threads for parallel processing by cscprecache command
16	HTTP Server operation settings	cscmng.server.<HCSC server name>.hws.svstop	Operation when HTTP Server is stopped
17		cscmng.server.<HCSC server name>.hws.svstop.timeout	Timeout time during planned stop of HTTP Server

For details on HCSC-Manager definition file, see "HCSC-Manager definition file" in "Service Platform Reference Guide".

2.4.2 Setting user information

Set user information by cscpasswd command. Each command of HCSC-Manager accesses HCSC server through Management Server. It also accesses exclusive databases in HCSC server.

Figure 2–3: FigureSetting user information



If user information is changed, the changed user information is reflected at the following timings:

- Reflected in the screen at the next login.
- Reflected in the command from the time the executed command starts after the user management command ends normally.

(1) Changing the user accessing HCSC-Manager

You can change user ID of the Management user and password for access to HCSC-Manager. This is reflected as follows immediately after HCSC-Manager is installed:

- User ID: admin
- Password: admin

Always change the user ID and password for access to HCSC-Manager by cscpasswd command.

! Important note

The Management user accessing HCSC-Manager can access all resources managed by HCSC-Manager. For this, suitably manage the user ID and password for accessing to HCSC-Manager.

In such cases, enter the command as follows:

```
cscpasswd [-user <Login user ID>]
          [-pass <Login password>]
           -cscmnguser <Changed user ID>
           -cscmngpass <Changed password>
```

If user ID (-user option) and password (-pass option) required in each command is set in HCSC-Manager command common definition files, you can omit option input.

For details on cscpasswd command, see "cscpasswd (user-managed) " in "Service Platform Reference Guide".

(2) User settings to access Manager

HCSC-Manager can change the Management user ID and Management user password for access to Management Server. Change occurs after HCSC server setup. Management user ID and Management user password managed by Management Server itself cannot be changed.

In such cases, enter the command as follows:

```
cscpasswd [-user <Login user ID>]
          [-pass <Login password>]
           -mng <Manager name>
           -mnguser <Changed user ID>
           -mngpass <Changed password>
```

If user ID (-user option) and password (-pass option) required in each command is set in HCSC-Manager command common definition files, you can omit option input.

For details on cscpasswd command, see "cscpasswd (user-managed)" in "Service Platform Reference Guide".

(3) User settings to access HCSC server

HCSC-Manager can change the user ID and password of the database maintained by HCSC server for access to HCSC server. Change occurs after HCSC server setup. User ID and password managed by the database itself cannot be changed.

In such cases, enter the command as follows:

```
cscpasswd [-user <Login user ID>]
          [-pass <Login password>]
           -csc <HCSC server name>
           -cscuser <Changed user ID>
           -cscpass <Changed password>
```

If user ID (-user option) and password (-pass option) required in each command is set in HCSC-Manager command common definition files, you can omit option input.

If the user ID and password of the database to be accessed contain double quotation marks ("), escape by using the escape sign. An example of HCSC server name changing the user ID of the database for accessing HCSC to "user1" and the password to "pass" is described here.

```
cscpasswd -user <Login user ID> -pass <Login password> -csc HCSC -cscuser \"user1\" -
cscpass \"pass\"
```

For details on cscpasswd command, see "cscpasswd (user-managed)" in "Service Platform Reference Guide".

2.4.3 Setting common items of HCSC-Manager command

If you define in advance the omitted value of mandatory items of each command used in the operating environment in the common definitions of HCSC-Manager command, you can omit the option input while entering the command.

Define information required as common omitted values in HCSC-Manager commands in the common definition files of HCSC-Manager command.

(1) Creating common definition files of HCSC-Manager command

HCSC-Manager command common definitions are stored in the following directory as common definition files of HCSC-Manager command in J2SE properties file format:

```
<Service Platform installation directory>\CSC\config\manager\csccmd.properties
```

After an omitted value is set or changed in the common definition files of HCSC-Manager command, the set omitted value is reflected from the entered command. If the definition exists in both common definition files of HCSC-Manager command as well as command options, the command option is valid.

Since this file contains information such as user ID and passwords, access permission must be set and managed.

(2) Contents that can be set

The following items show the values that can be set in common items of HCSC-Manager command:

- Default value of arguments common to all commands
  Parameter: csc.all.<Command argument name>=Value

- Default argument of command corresponding to command identifier
  Parameter: csc.<Command identifier>.<Command argument name>=Value

For details on common definition files of HCSC-Manager command, see "Common definition files of HCSC-Manager command" in "Service Platform Reference Guide".

2.5 Environment setup to change HCSC server to load balancing cluster configuration

You can arrange multiple parallel HCSC servers and reduce the load of J2EE server by narrowing the focus of service component execution requests from the service requester. This is referred to as **Load balance cluster functionality**.

To distribute the load by using the load balance cluster functionality, use the load balancer or CTM. The load balancer and CTM are combined here and represented as load balancer.

You can distribute loads by the load balancer only for service component execution requests to standard synchronous reception (Web service /SessionBean). The load balancer to be used differs depending on whether a service component execution request is to be sent to standard synchronous reception (Web service) or standard synchronous reception (SessionBean). The following table describes standard reception to send the service component execution request and the used load balancer:

Table 2–18: TableStandard reception to send service component execution request and used load balancer

Standard reception	Load balancer
Standard synchronous reception (Web service)	Load balancer (load distribution functionality that can distribute HTTP load)
Standard synchronous reception (SessionBean)	CTM#

Note #

The optional name shared in the cluster must be set in each HCSC server.

The following section describes environment setup and setup methods for load balance cluster configuration of HCSC server.

2.5.1 Environment setup during load balancing cluster configuration

Figure2-4 shows system setup using load balancer and Figure2-5 shows system setup using CTM.

Figure 2–4: FigureSystem setup using load balancer

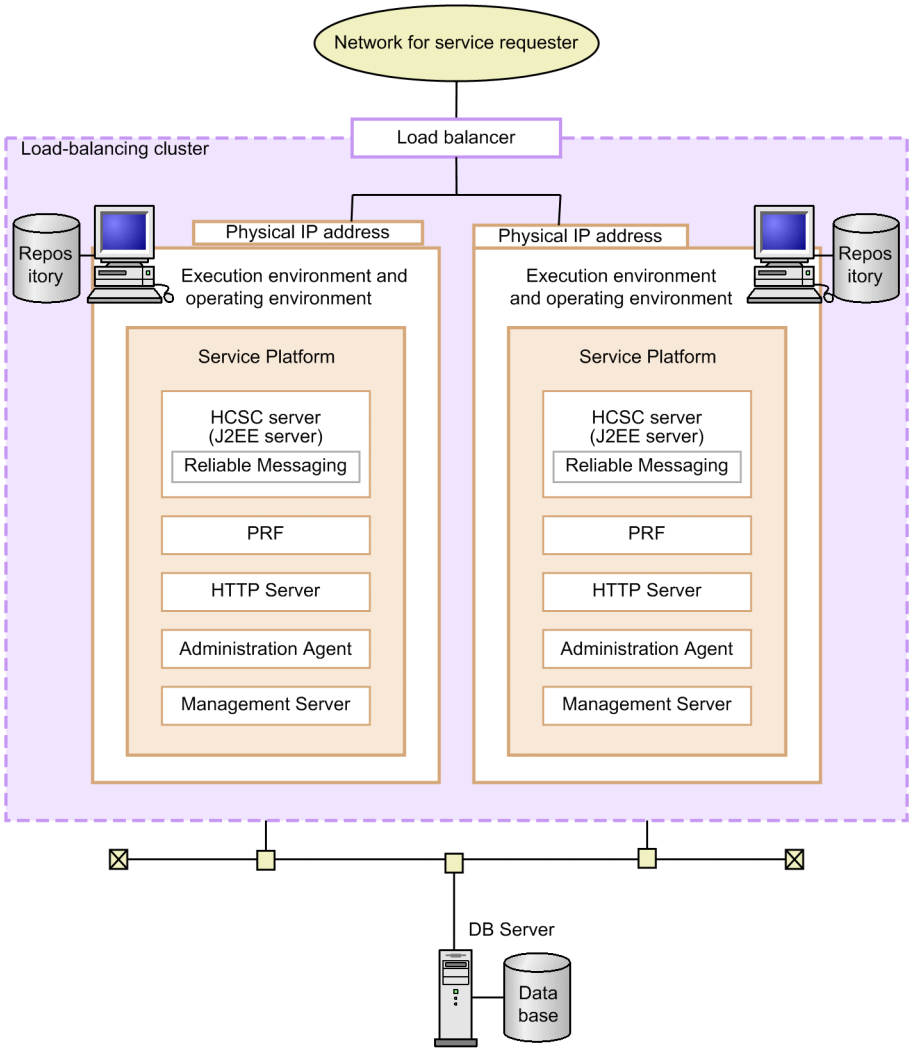
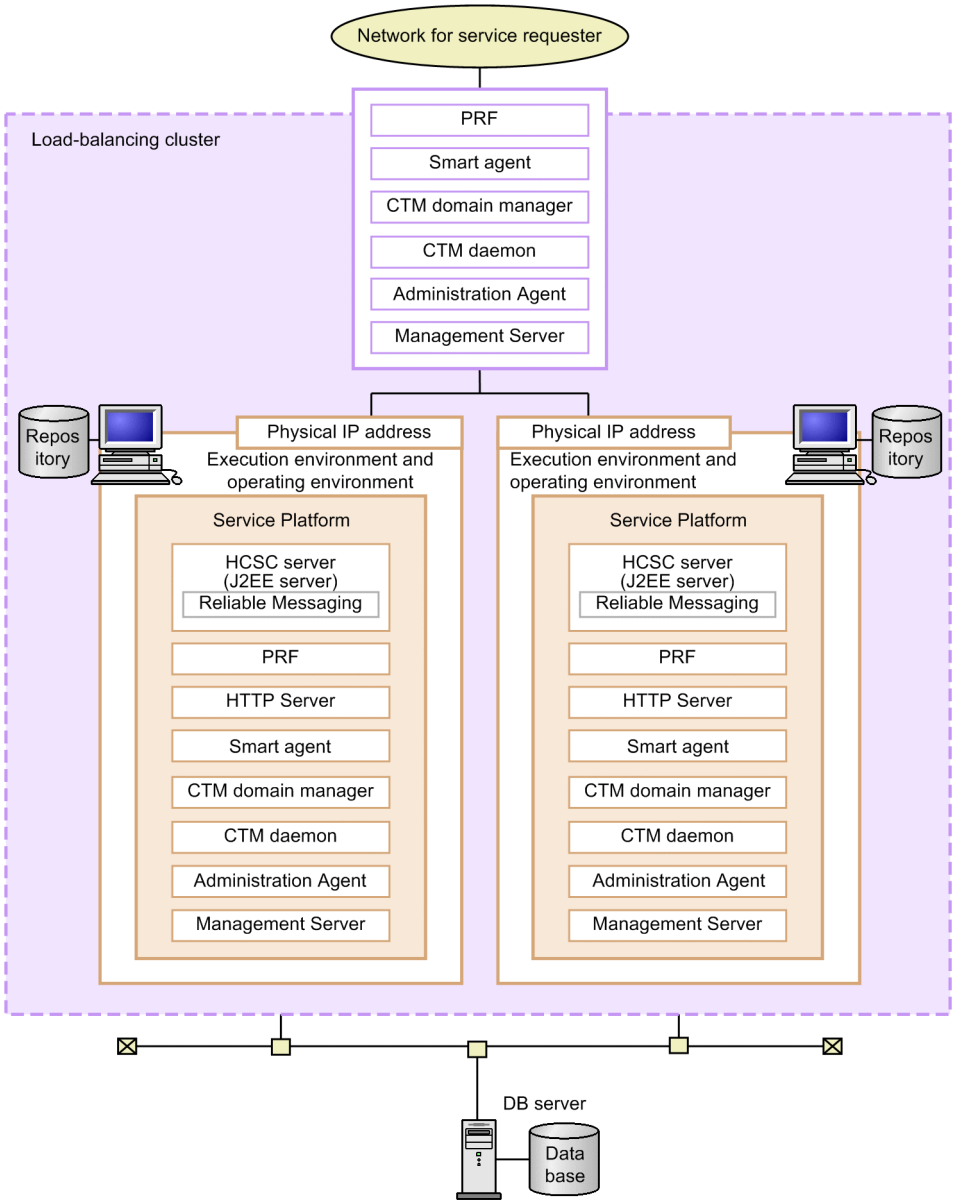


Figure 2–5: FigureSystem setup using CTM



In case of new setup in version 08-70 or higher version, you can store HCSC-Manager environment in each execution environment. This enables you to omit the number of operating environment servers.

Important note

Create a unique GUI display name of HCSC cluster in the system.

Re-executing a business process from another HCSC server in case of server fault

The following information must be stored in the common disk device in order to re-execute a business process from another HCSC server:

- Operation folder
- Common folder
- I/O enabled file used in the file adapter

Store the following information in the local disk device. However, the same value must be set in each HCSC server.

- Text file of main text in mail used in the mail adapter, and the attached file

- Definition file used in HCSC server operations
- Definition file used in HCSC component

Re-executing a business process using the operation folder

You cannot re-execute a business process from another HCSC server if the business process uses the operation folder and if the business process is executed in a version lower than 09-51.

You can re-execute a business process if the common folder is used instead of the operation folder or if the business process has been executed in 09-51 or higher version. However, you cannot re-execute a business process executed in a version lower than 09-51 because the common folder cannot be used for business processes using the following components:

- FTP reception
- HTTP reception

The following points show the execution environment, operating environment and DB server setup methods.

(1) Setting up an execution environment

Implement the following operations to set up the execution environment.

(a) Installing Service Platform

For details on installation methods of Service Platform, see "*2.1.2 Installing Service Platform*".

(b) Management Server settings

Implement Management Server settings to use HCSC-Manager in the operating environment by the execution environment of HCSC-Manager connection destination.

For details on Management Server settings, see "*2.1.6 Management Server settings for using HCSC-Manager*".

(c) SOAP mode settings

SOAP modes used in the configured execution environment and operating environment must match for load balance cluster configuration of HCSC server. Different SOAP mode environments cannot co-exist.

The container extension library of J2EE server must be set in order to set SOAP mode. For details on container extension library settings of J2EE server, see "*3.1.2(4)(e) Setting up the container extension library*".

(d) HCSC server configuration settings

Perform settings related to the execution environment of HCSC server configuration. For details on setting contents and how to execute setting, see "*2.3 Settings related to execution environment*".

To set HCSC server configuration definition file, HCSC server setup definition file and HCSC server runtime definition file by the settings related to the execution environment, consider the following contents:

Points to be considered when setting HCSC server configuration definition file

To set HCSC server configuration definition file, consider the following contents. For details on how to set the HCSC server configuration definition file, see "*2.3.1 Setting HCSC server configuration definition file*". For details on contents to be set in HCSC server configuration definition file, see "HCSC server configuration definition file" in "Service Platform Reference Guide".

- Cluster display name
  Set the same value in all HCSC servers in the load balance cluster.
- Cluster type
  Set "LB".
- Manager name
  Set a unique identifier in Manager unit in HCSC-Manager.
- Manager IP address
  Set the physical IP address.
- Web server IP address (to invoke synchronous service (Web service))
  Set IP address value of the load balancer in all HCSC servers in the load balance cluster.

- Web server IP address (to invoke asynchronous service (MDB(WS-R))
  Set each HCSC server IP address. Set in jms-physical-reception in load balance cluster configuration.
- NameServer IP address
  Set IP address of global CORBA naming service in all HCSC servers in the load balance cluster. However, Specify localhost if CTM is not used.
- HCSC server name
  Set a unique identifier in the load balance cluster to set up an environment using the database.
  Set a unique identifier in HCSC-Manager to set up an environment that does not use either the database or Reliable Messaging.

Points to be considered when setting HCSC server setup definition file

To set HCSC server setup definition file, consider the following contents. For details on how to set the HCSC server setup definition file, see "*2.3.2 Setting HCSC server setup definition file*". For details on contents to be set in HCSC server setup definition file, see "HCSC server setup definition file" in "Service Platform Reference Guide".

Properties in which to set the same value in all HCSC servers

The same value must be set in all HCSC servers in the load balance cluster for properties shown in the following table from among the properties set in HCSC server setup definition file.

Table 2–19: TableProperties in which to set the same value in HCSC servers in load balance cluster

Property in which same value is set	Value set in property
db-use	Existence of database use
rm-use	Existence of use of Reliable Messaging
request-ejb	Existence of use of standard synchronous reception (SessionBean)
request-soap	Existence of use of standard synchronous reception (Web service)
request-jms	Existence of use of standard asynchronous reception (MDB(WS-R))
request-jms.maxmessage	Maximum number of messages in standard asynchronous reception (MDB(WS-R)) queue
request-dbq	Existence of use of standard asynchronous reception (MDB(DB queue))
request-dbq.maxmessage	Maximum number of messages in standard asynchronous reception (MDB(DB queue)) queue
request-jms-rdarea	RD area name in standard asynchronous reception (MDB(WS-R))
request-dbq-rdarea	RD area name in standard asynchronous reception (MDB(DB queue))
request-dbq-maxlen	Maximum message length in standard asynchronous reception (MDB(DB queue))
request-userdef-soap	Existence of use of SOAP reception
rm-displayname	Reliable Messaging display name
dbcon-xadisplayname[#1]	DB Connector display name for XATransaction or LocalTransaction
dbcon-nodisplayname[#1]	DB Connector display name for NoTransaction
dbtype	Used database type
jdbc-type	JDBC driver type
jdbc-url[#2]	Database URL for JDBC
jdbc-dbhostname	Database host name
jdbc-dbconnectinfo	Database connection information
db-character-sets	Database character code type

Property in which same value is set	Value set in property
db-tbl-split-key	Existence of use of table range partition functionality by date data
db-tbl-split-corcheck-use	Existence of enhancement of correlation set duplication check

Note #1

DB Connector settings are the same in all HCSC servers in the load balance cluster.

Note #2

In the host name to be specified, specify the machine in which the database is stored.

Points to be considered when setting HCSC server runtime definition file

To set HCSC server runtime definition file, the same value must be set in all HCSC servers in the load balance cluster.

Add the following property if CTM is used:

- request-ejb.ctm=true

Add the following property if J2EE server name is different in HCSC server configuring the cluster:

- request-ejb.optional.name=<Optional name of synchronous requester service (SessionBean) shared in the cluster>

For details on how to set the HCSC server runtime definition file, see "*2.3.3 Setting HCSC server runtime definition file*".

For details on contents to be set in HCSC server runtime definition file, see "HCSC server runtime definition file" in "Service Platform Reference Guide".

(2) Setting up an operating environment

Set up the operating environment in HCSC server machine configuring the cluster. 1 to 1 mapping of the operating environment and execution environment is recommended. For configuration of operating environment and execution environment, see "*1.2(3) Configuration of the operating environment and the execution environment*".

Implement the following operations to set up the operating environment:

Environment settings

Implement repository settings and environment variable settings as the environment settings of the operating environment.

For details on environment settings, see "*2.1.3 Environment settings*".

Embedding HCSC-Manager Plug-in in Eclipse

Embed HCSC-Manager Plug-in in Eclipse.

For embedding HCSC-Manager Plug-in in Eclipse, see "*2.1.5 Embedding HCSC-Manager plug-in in Eclipse*".

Setting user permission

Set user permission related to the operating environment. For details on setting contents and how to set methods, see "*2.4 Settings Related to the Operating Environment*".

(3) Setting up DB server

Set up DB server isolated from HCSC server configuring the load balance cluster and share it with HCSC server in the load balance cluster.

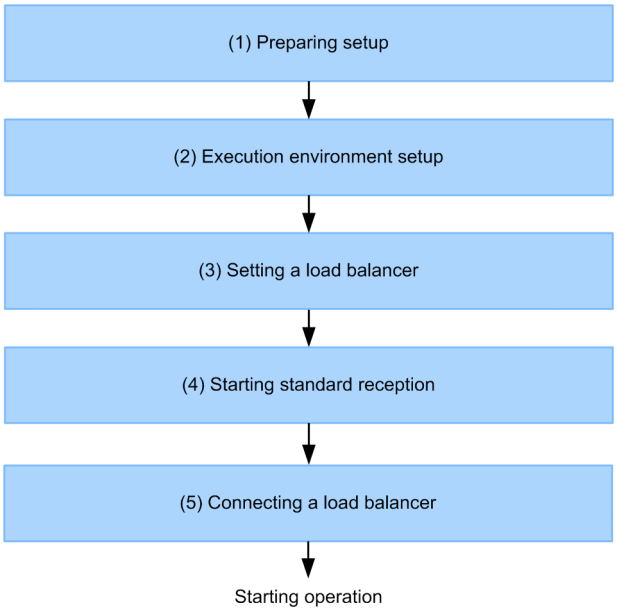
Install the database to be used in the machine used as DB server. For details on how to install, see documents of the used database.

2.5.2 Setup of execution environment in load balance cluster configuration

After setting up the environment, set up the execution environment configuring the load balance cluster.

The following figure shows the flow of execution environment setup in load balance cluster configuration:

Figure 2–6: FigureFlow of setup in load balance cluster configuration



Steps 1 to 5 given in the figure are described here:

For details on operations in load balance cluster configuration, see "*5.6.1 Operations in the load-balancing cluster configuration*".

(1) Preparing setup

Perform the following operations before setup. Perform the following operations in all HCSC servers configuring the load balance cluster:

Setting software required in the execution environment

Perform J2EE server setup. For details on setting contents and how to set, see "*3.1.2 Setting up the software required for the execution environment*".

A unique name must be set in each HCSC server in the load balance cluster for Reliable Messaging system name.

Settings when using CTM

Set true in request-ejb.ctm in HCSC server runtime definition file while using CTM.

For details on HCSC server runtime definition file, see "HCSC server runtime definition file" in "Service Platform Reference Guide".

Sending control in the service requester

Disconnect the network for the service requester and change to the status in which HCSC server does not receive the service component execution request.

(2) Execution environment setup

The following table describes execution environment setup procedure:

1. Start the process in the following order:

Start order	Process to be started	Start method
1	Administration Agent	See "Application Server System Setup and Operation Guide".
2	Management Server	
3	PRF	
4	Smart Agent	

Start order	Process to be started	Start method
5	CTM domain manager (if CTM is used)	See "Application Server System Setup and Operation Guide".
6	CORBA naming service (if CORBA naming service is used)	
7	CTM daemon (if CTM is used)	
8	J2EE server	
9	HTTP Server (if HTTP Server is used)	See"*5.3.5 Starting HTTP Server*".

2. Set up HCSC server.
   For details on how to set up HCSC server, see "*3.1.3 Setting up an HCSC server*".
3. Start HCSC server.
   For details on how to start HCSC server, see "*5.3.4 Starting HCSC server*".
4. Deploy service adapter and business process.
   For details on how to deploy the service adapter and business process, see "*3.1.8 Deploying a service adapter*" and "*3.1.13 Deploying a business process*".
5. Start service adapter and business process.
   For details on how to start the service adapter and business process, see "*5.3.6 Starting Service Adapters*" and "*5.3.7 Starting Business Processes*".

(3) Setting a load balancer

Set to send the service product execution request to all HCSC servers configuring the load balance cluster.

The same value must be set in CTM domain manager name and smart agent port number in all HCSC servers while using CTM.

For details on how to set up the load balancer, see the used load balancer document.

(4) Starting standard reception

Start standard reception of all HCSC servers. For details on how to start the standard reception, see "*5.3.9 Starting standard receptions*".

(5) Connecting a load balancer

Connect the load balancer and change it to usable status.

These procedures are unnecessary while using CTM.

For details on how to start connection of the load balancer, see the used load balancer document.

2.6 Environment setup to change HCSC Server to HA class configuration

In HA cluster configuration, you can cluster 2 HCSC servers by combined cold standby configuration and configure a system operated by 1 executing node to 1 standby node (1:1node switching system). Use cluster software to configure HA cluster. You can use the following cluster software in Service Platform:

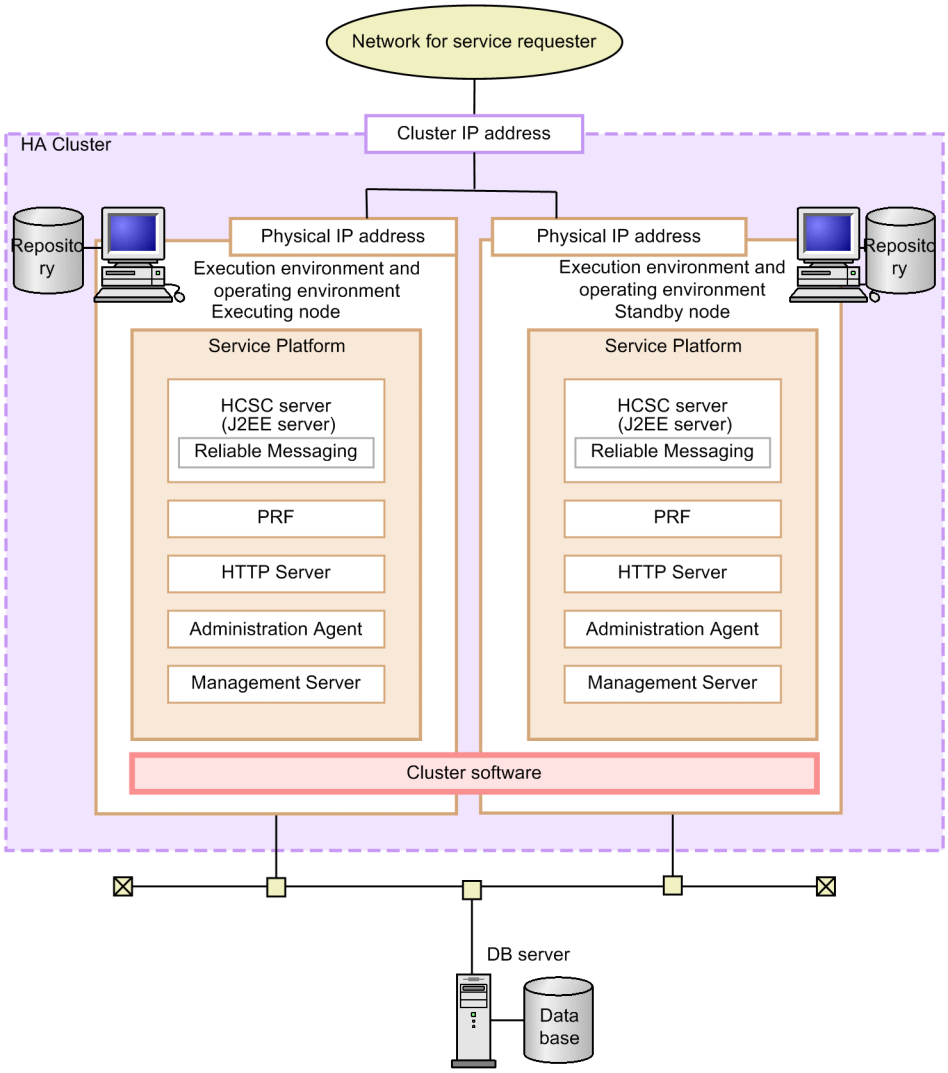
- In Windows
  Windows Server Failover Cluster
- In UNIX
  HA monitor

The following section describes environment setup and setup methods to configure HCSC server in HA cluster:

2.6.1 Environment setup in HA class configuration

The following figure shows the system configuration when HCSC server is configured in HA cluster:

Figure 2–7: FigureSystem configuration when HCSC server is configured in HA cluster



Note Cluster IP address is the IP address that is set in cluster unit.
Set any address to cluster software.
Execution request sent from service requester for cluster IP address is converted to physical IP address in HA cluster.

Setting methods of cluster IP address differ according to the used cluster software. See the cluster software manual.

In case of new setup in version 08-70 or higher version, you can store HCSC-Manager environment in each execution environment. This enables you to omit the number of operating environment servers.

Important note

Create a unique GUI display name of HCSC cluster in the system.

Using common disk devices

While changing HCSC server to HA cluster configuration, common disk device usage is different for local transactions and for global transactions.

- In local transactions

  Common disk device is not required. Since HCSC server manages inherited information in the database, common disk device is not used in local transactions.

- In global transactions

Common disk device is required. Common disk device is used to inherit transaction information such as OTS status during node switching.

Re-executing a business process after node switching process during server fault

When a business process is re-executed after node switching process to standby node, the following information must be stored in the common disk device:

- Operation folder
- Common folder
- Files in which I/O of file adapter is performed

Store the following information in the local disk device. However, the same value must be set in executing node and standby node.

- Text file of main text in mail used in the mail adapter, and the attached file
- Definition file used in HCSC server operations
- Definition file used in HCSC component

Re-executing a business process using the operation folder

You cannot re-execute a business process after the node switching process to standby node if the business process uses the operation folder and if the business process is executed in a version lower than 09-51.

You can re-execute a business process if the common folder is used instead of the operation folder or if the business process has been executed in 09-51 or higher version. However, you cannot re-execute a business process executed in a version lower than 09-51 because the common folder cannot be used for business processes using the following components:

- FTP reception
- HTTP reception

The following points show the execution environment (executing node/standby node), operating environment and DB server configuration methods.

(1) Setting up an execution environment (executing node and standby node)

To set up the execution environment, implement the following operations by executing node and standby node:

(a) Installing Service Platform

For details on how to install Service Platform, see "*2.1.2 Installing Service Platform*".

(b) Management Server settings

Implement Management Server settings to use HCSC-Manager in the operating environment by the execution environment of HCSC-Manager connection destination.

For details on how to perform Management Server settings, see "*2.1.6 Management Server settings for using HCSC-Manager*".

(c) SOAP mode settings

While changing HCSC server to HA cluster configuration, SOAP modes used in the configured execution environment and operating environment must match. Different SOAP mode environments cannot co-exist.

The container extension library of J2EE server must be set in order to set SOAP mode. For details on how to set up container extension library of J2EE server, see "*3.1.2(4)(e) Setting up the container extension library*".

(d) HCSC server configuration settings

Perform settings related to the execution environment of HCSC server configuration. For details on setting contents and how to set, see "*2.3 Settings related to execution environment*".

To set HCSC server configuration definition file, HCSC server setup definition file and HCSC server runtime definition file in settings related to the execution environment, note the following contents. In all other functionalities, set the same value in the executing node and standby node.

Points to be considered when setting HCSC server configuration definition file

Set "HA" in the cluster type set in HCSC server configuration definition file.

While using the database, set a unique name in HCSC server name.

To invoke Web server IP address of asynchronous service (MDB(WS-R), set in jms-reception.

Different values must be set in executing node and standby node for the following values from among the values set in HCSC server configuration definition file:

- Manager name
- Manager IP address

  Specify the physical IP address for each executing node/standby node in Manager IP address.

Set the same value in the executing node and standby node in elements other than the above.

Set the logical IP address in the following definitions:

- ip-address of soap-reception definition
- ip-address of jms-reception definition
- ip-address of ejb-reception definition

For details on how to set the HCSC server configuration definition file, see "*2.3.1 Setting HCSC server configuration definition file*".

For details on contents to be set in HCSC server configuration definition file, see "HCSC server configuration definition file" in "Service Platform Reference Guide".

Points to be considered when setting HCSC server setup definition file

To set HCSC server setup definition file, consider the following contents.

For details on how to set HCSC server setup definition file, see "*2.3.2 Setting HCSC server setup definition file*".

For details on contents to be set in HCSC server setup definition file, see "HCSC server setup definition file" in "Service Platform Reference Guide".

Properties in which to set the same values in executing node and standby node

For properties shown in the following table from among the properties set in HCSC server setup definition file, the same value must be set in executing node and standby node. It is not necessary to set naming-service-hostname. Set localhost or physical IP address in IP addresses that are not described in the following table:

Table 2–20: TableProperties in which to set the same values in executing node and standby node

Property in which same value is set	Value set in property
db-use	Existence of database use
rm-use	Existence of use of Reliable Messaging
request-ejb	Existence of use of standard synchronous reception (SessionBean)
request-soap	Existence of use of standard synchronous reception (Web service)
request-jms	Existence of use of standard asynchronous reception (MDB(WS-R))
request-jms.maxmessage	Maximum number of messages in standard asynchronous reception (MDB(WS-R)) queue
request-dbq	Existence of use of standard asynchronous reception (MDB(DB queue))
request-dbq.maxmessage	Maximum number of messages in standard asynchronous reception (MDB(DB queue)) queue
request-jms-rdarea	RD area name in standard asynchronous reception (MDB(WS-R))
request-dbq-rdarea	RD area name in standard asynchronous reception (MDB(DB queue))
request-dbq-maxlen	Maximum message length in standard asynchronous reception (MDB(DB queue))
request-userdef-soap	Existence of use of SOAP reception
rm-systemname	Reliable Messaging system name
rm-displayname	Reliable Messaging display name

Property in which same value is set	Value set in property
dbcon-xadisplayname[#1]	DB Connector display name for XATransaction or LocalTransaction
dbcon-nodisplayname[#1]	DB Connector display name for NoTransaction
dbtype	Used database type
jdbc-type	JDBC driver type
jdbc-url[#2]	Database URL for JDBC
jdbc-dbhostname	Database host name
jdbc-dbconnectinfo	Database connection information
db-character-sets	Database character code type
db-tbl-split-key	Existence of use of table range partition functionality by date data
db-tbl-split-corcheck-use	Existence of enhancement of correlation set duplication check

Note #1

DB connector setting is also the same in executing node and standby node.

Note #2

In the host name to be specified, specify the machine in which the database is stored.

Points to be considered when setting HCSC server runtime definition file

To set HCSC server runtime definition file, the same value must be set in executing node and standby node in all properties.

For details on how to set HCSC server runtime definition file, see "*2.3.3 Setting HCSC server runtime definition file*".

For details on contents to be set in HCSC server runtime definition file, see "HCSC server runtime definition file" in "Service Platform Reference Guide".

Add the following property if J2EE server name is different in HCSC server configuring the cluster:

- request-ejb.optional.name=<Optional name of synchronous requester service (SessionBean) shared in the cluster>

(e) Installing cluster software

Install cluster software. For details on how to install, see the used cluster software document.

(2) Setting up an operating environment

Set up the operating environment in HCSC server machine configuring the cluster. 1 to 1 mapping of the operating environment and execution environment is recommended. For details on how to configure the operating environment and execution environment, see "*1.2(3) Configuration of the operating environment and the execution environment*".

Implement the following operations to set up the operating environment:

Environment settings

Implement repository settings and environment variable settings as the environment settings of the operating environment.

For details on how to perform environment settings, see "*2.1.3 Environment settings*".

Embedding HCSC-Manager Plug-in in Eclipse

Embed HCSC-Manager Plug-in in Eclipse.

For details on embedding HCSC-Manager Plug-in in Eclipse, see "*2.1.5 Embedding HCSC-Manager plug-in in Eclipse*".

Setting user permission

Set user permission related to the operating environment. For details on setting contents and how to set, see "*2.4 Settings Related to the Operating Environment*".

(3) Setting up DB server

Set up DB server isolated from HCSC server configuring HA cluster and share it with HCSC server in executing node and standby node.

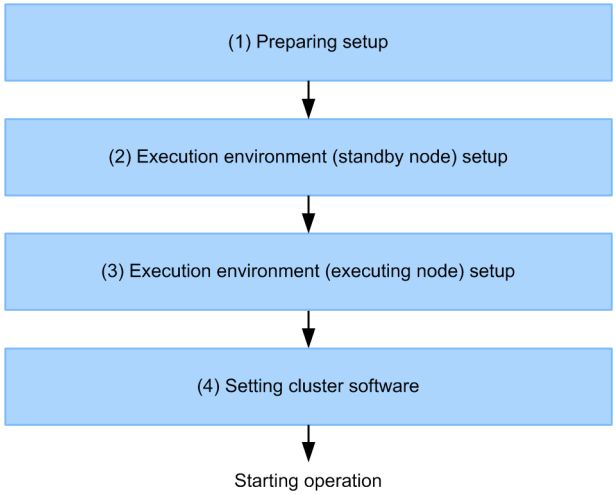
Install the database to be used in the machine used as DB server. For details on how to install, see documents of the used database.

2.6.2 Execution environment setup in HA cluster configuration

After environment setup, set up the execution environment configuring HA cluster.

The following figure shows the flow of execution environment setup in HA cluster configuration:

Figure 2–8: FigureFlow of execution environment setup in HA cluster configuration



Steps 1 to 4 given in the figure are described here:

For details on operations in HA cluster configuration, see "*5.6.2 Operations Using a High Availability Cluster Configuration*".

(1) Preparing setup

Perform the following operations before setup. Perform the following operations in executing node and standby node respectively.

Setting software required in the execution environment

Perform J2EE server setup. For details on setting contents and how to set, see "*3.1.2 Setting up the software required for the execution environment*".

During setup, Reliable Messaging system name must be the same as the name set in executing node and standby node.

To use a global transaction, the host must be fixed in the cluster IP address of J2EE server. For the method to fix the host, see the following location:

Setting 1:1 node switching system for the application server

- In Windows

  "17.4.2 Cluster server environment settings" in "Application Server Operation, Monitoring, and Linkage Guide"

- In UNIX

  "17.6.2 Cluster server environment settings" in "Application Server Operation, Monitoring, and Linkage Guide"

To use a local transaction, the host need not be fixed. Set the local host or physical IP address.

Sending control in the service requester

Disconnect the network for the service requester and change to the status in which service product execution request is not received in executing node and standby node.

(2) Execution environment (standby node) setup

The following table describes the procedures of execution environment (standby node) setup:

1. Start the process in the following order:

Start order	Process to be started	Start method
1	Administration Agent	See "Application Server System Setup and Operation Guide".
2	Management Server	
3	PRF	
4	J2EE server	
5	HTTP Server	See "*5.3.5 Starting HTTP Server*".

2. Set up HCSC server.
   For details on how to set up HCSC server, see "*3.1.3 Setting up an HCSC server*".
3. Start HCSC server.
   For details on how to start the HCSC server, see "*5.3.4 Starting HCSC server*".
4. Deploy service adapter and business process.
   For details on how to deploy the service adapter and business process, see "*3.1.8 Deploying a service adapter*" and "*3.1.13 Deploying a business process*".
5. Start service adapter and business process.
   For details on how to start the service adapter and business process, see "*5.3.6 Starting Service Adapters*" and "*5.3.7 Starting Business Processes*".
6. Stop HCSC server.
   Stop HCSC server while the service adapter and business process are running.
   For details on how to stop the HCSC server, see "*5.3.33 Terminating the HCSC Server*".
7. Stop Management Server and Administration Agent.
   For details on how to stop Management Server and Administration Agent (operation management functionality), see "3.1.3 Stopping the system (while using GUI) " in "Application Server System Setup and Operation Guide".

(3) Execution environment (executing node) setup

The following table describes procedures for execution environment (executing node) setup:

1. Start the process in the following order:

Start order	Process to be started	Start method
1	Administration Agent	See "Application Server System Setup and Operation Guide".
2	Management Server	
3	PRF	
4	J2EE server	
5	HTTP Server	See "*5.3.5 Starting HTTP Server*".

2. Set up HCSC server.
   For details on how to set up HCSC server, see "*3.1.3 Setting up an HCSC server*".
   While setting up HCSC server in executing node, the file name specified in -cluster option of cscsvsetup command must contain the same value as in standby node.

For details on cscsvsetup command, see "cscsvsetup(HCSC server setup) " in "Service Platform Reference Guide".

3. Start HCSC server.

   For details on how to start the HCSC server, see "*5.3.4 Starting HCSC server*".

4. Deploy service adapter and business process.

   Deploy the same service adapter and business process as the ones deployed in standby node. Ensure that sufficient service adapters and business processes are deployed between executing node and standby node.

   For details on how to deploy the service adapter and business process, see "*3.1.8 Deploying a service adapter*" and "*3.1.13 Deploying a business process*".

5. Start service adapter and business process.

   Start the same service adapter and business process as those started in standby node. Ensure that there is no difference in service adapter and business process status between executing node and standby node.

   For details on how to start the service adapter and business process, see "*5.3.6 Starting Service Adapters*" and "*5.3.7 Starting Business Processes*".

6. Start standard reception.

   For details on how to start the standard reception, see "*5.3.9 Starting standard receptions*".

(4) Setting cluster software

Set to switch to standby node if executing node fails in cluster software.

Set to execute the script for the following operations while switching to standby node. Set to execute in the following order.

OS and HCSC-Manager user must match with the executing node.

1. Start standby node process

   Set to start the process in the following order:

   - Administration Agent
   - Management Server
   - PRF
   - HTTP Server

2. Start HCSC server in standby node#

3. Start standard reception of HCSC server in standby node

Note #

If you start HCSC server in standby node in the cluster software by cscutil command, set the following options:

-host option

Combine the host name (or IP address) starting Management Server with the port number by a colon (:) and specify. Specify "localhost" in host name. An example of specification if the port number is "28099" is described here.

```
-host localhost:28099
```

-mnguser option

Specify user ID of the Management user of Management Server.

-mngpass option

Specify password of the Management user of Management Server.

2.7 Environment setup when executing node machine and standby node machine are in 1 to N configuration because load balancing cluster configuration and HA cluster configuration are combined

You can set up all standby nodes in 1 machine for N executing node machine by configuring cold standby suitable for HA cluster of HCSC server configuring the load balance cluster. This configuration is referred to as **1 to N cluster configuration**.

Use cluster software to configure HA cluster. You can use the following cluster software in Service Platform:

- In Windows
  Windows Server Failover Cluster
- In UNIX
  HA monitor

The following section describes environment setup and setup methods to configure HCSC server in N to 1 cluster configuration.

2.7.1 Environment setup in 1 to N cluster configuration

Set "HA" as the cluster to be set in HCSC server configuration definition file for all HCSC servers configuring clusters in 1 to N cluster configuration. You cannot set up 1 to N cluster configuration if cluster type is "LB".

While using standard asynchronous reception (MDB (WS-R)/MDB (DB queue)), the requester must be set to send a request to HCSC server group suitable for HA cluster.

! Important note

Create a unique GUI display name of HCSC cluster in the system.

Re-executing a business process from another HCSC server in case of server fault

The following information must be stored in the common disk device in order to re-execute a business process from another HCSC server:

- Operation folder
- Common folder
- I/O enabled file used in the file adapter

Store the following information in the local disk device. However, the same value must be set in each HCSC server.

- Text file of main text in mail used in the mail adapter, and the attached file
- Definition file used in HCSC server operations
- Definition file used in HCSC component

Re-executing a business process using the operation folder

You cannot re-execute a business process from another HCSC server if the business process uses the operation folder and if the business process is executed in a version lower than 09-51.

You can re-execute a business process if the common folder is used instead of the operation folder or if the business process has been executed in 09-51 or higher version. However, you cannot re-execute a business process executed in a version lower than 09-51 because the common folder cannot be used for business processes using the following components:

- FTP reception
- HTTP reception

The following points show the environment setup procedures to operate HCSC server in 1 to N cluster configuration.

(1) Setting up an execution environment (executing node and standby node)

To set up the execution environment, implement the following operations by executing node and standby node:

(a) Installing Service Platform

Install Service Platform in each machine.

For details on how to install Service Platform, see "*2.1.2 Installing Service Platform*".

(b) Management Server settings

Implement Management Server settings to use HCSC-Manager in the operating environment by the execution environment of HCSC-Manager connection destination.

For details on how to perform settings of Management Server, see "*2.1.6 Management Server settings for using HCSC-Manager*".

(c) SOAP mode settings

To change HCSC server to 1 to N cluster configuration, SOAP modes used in the configured execution environment and operating environment must match. Different SOAP mode environments cannot co-exist.

The container extension library of J2EE server must be set in order to set SOAP mode. For details on how to set up container extension library of J2EE server, see "*3.1.2(4)(e) Setting up the container extension library*".

(d) HCSC server configuration settings

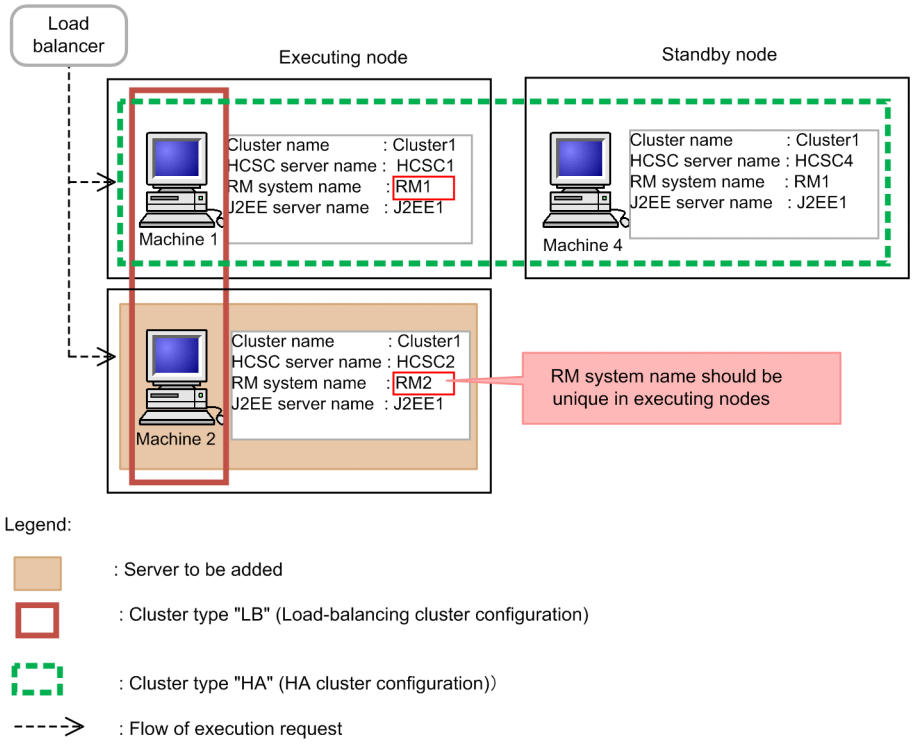
Implement in each machine the settings related to the execution environment such as HCSC server configuration according to the configured HCSC server type (executing node/standby node). Setting contents and setting methods are the same as in the load balance cluster configuration and HA cluster configuration. For details on setting contents and how to set up, see "*2.3 Settings related to execution environment*".

The following items show configuration examples when HCSC server is configured in executing node or standby node as well as HCSC server configuration setting procedures.

●Setting up an executing node HCSC server

The following figure shows an example of setup when HCSC server (HCSC server2) suitable for the load balance cluster is added in HA cluster configuration (HCSC server1/HCSC server4).

Figure 2–9: FigureSetup example of HCSC server in executing node (example when HCSC server2 is added)



While setting procedures for setting up HCSC server in executing node are basically the same as setting procedures of the load balance cluster configuration, please note the following points:

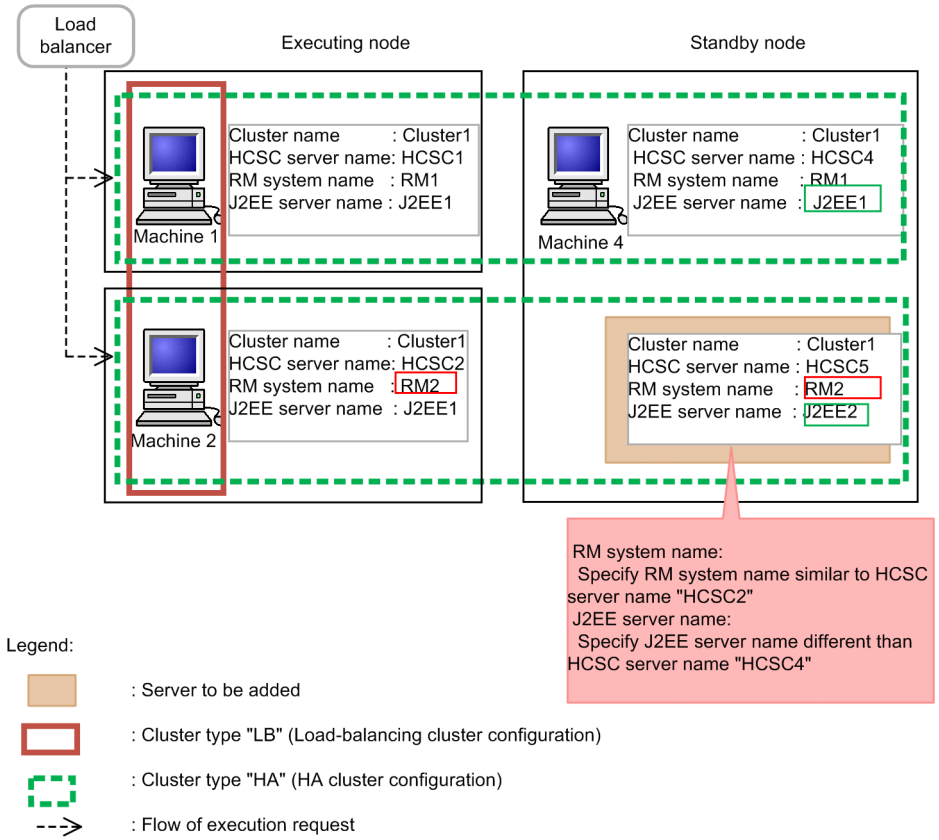
- Specify "HA" for the cluster type set in HCSC server configuration definition file.
- Specify a unique name for RM system name set in HCSC server setup definition file between HCSC servers in executing node in the cluster. Error does not occur in setup if a duplicate RM system name is set but dead lock occurs when Reliable Messaging starts.

For details on how to set the load balance cluster configuration, see HCSC server configuration settings in "*2.5.1 Environment setup during load balancing cluster configuration*".

●Setting up HCSC server in standby node

The following figure shows an example of setting up HCSC server 5 in standby node of HCSC server 2 in machine 4 in the configuration shown in the figure in "*Setting up an executing node HCSC server*":

Figure 2–10: FigureExample of setting up HCSC server in executing node (example when HCSC server is set up in machine 4)



While setting procedures for setting up HCSC server in standby node are basically the same as the setting procedures of HA cluster configuration, please note the following points:

- Specify a unique name for J2EE server name set in HCSC server configuration definition file to set up HCSC server in standby node in 1 machine.
- Specify the same name for RM system name in HCSC server setup definition file as in HCSC server in executing node in the load balance cluster configuration. Error does not occur in setup if you set RM system name different from executing node but the process using Reliable Messaging is not inherited.

For details on how to perform of HA cluster configuration, see HCSC server configuration settings in "2.6.1 Environment setup in HA class configuration".

To set HCSC server configuration definition file, HCSC server setup definition file and HCSC server runtime definition file in the settings related to the execution environment, note the following contents:

Points to be considered when setting HCSC server configuration definition file

Set the following values for HCSC server configuration definition file during setup.

For details on how to set the HCSC server configuration definition file, see "*2.3.1 Setting HCSC server configuration definition file*".

For details on contents to be set in HCSC server configuration definition file, see "HCSC server configuration definition file" in "Service Platform Reference Guide".

Setting items	Setting values
Cluster display name	Same value as in cluster
Cluster type	Same value as in cluster
manager name	Unique value in system
manager IP address	Physical IP address for management

Setting items	Setting values
Web server IP address (to invoke synchronous service (Web service))	Same value as in cluster
Web server IP address (to invoke asynchronous service (MDB(WS-R))	IP address of each HCSC server reception (specify identical IP address as in executing node and standby node (virtual IP address))
NameServer IP address	Same value as in cluster

Points to be considered when setting HCSC server setup definition file

To set HCSC server setup definition file, note the following contents. For details on how to set the HCSC server setup definition file, see "*2.3.2 Setting HCSC server setup definition file*". For details on contents to be set in HCSC server setup definition file, see "HCSC server setup definition file" in "Service Platform Reference Guide".

Properties in which to set the same value in all HCSC servers

For properties shown in the following table from among the properties set in HCSC server setup definition file, the same value must be set in all HCSC servers in N to 1 cluster.

Table 2–21: TableProperties in which to set same value in HCSC server in N to 1 cluster

Property in which same value is set	Value set in property
request-ejb	Existence of use of standard synchronous reception (SessionBean)
request-soap	Existence of use of standard synchronous reception (Web service)
request-jms	Existence of use of standard asynchronous reception (MDB(WS-R))
request-jms.maxmessage	Maximum number of messages in standard asynchronous reception (MDB(WS-R)) queue
request-dbq	Existence of use of standard asynchronous reception (MDB(DB queue))
request-dbq.maxmessage	Maximum number of messages in standard asynchronous reception (MDB(DB queue)) queue
request-jms-rdarea	RD area name in standard asynchronous reception (MDB(WS-R))
request-dbq-rdarea	RD area name in standard asynchronous reception (MDB(DB queue))
request-dbq-maxlen	Maximum message length in standard asynchronous reception (MDB(DB queue))
rm-displayname	Reliable Messaging display name
dbcon-xadisplayname[#1]	DB Connector display name for XATransaction or LocalTransaction
dbcon-nodisplayname[#1]	DB Connector display name for NoTransaction
dbtype	Used database type
jdbc-type	JDBC driver type
jdbc-url[#2]	Database URL for JDBC
jdbc-dbhostname	Database host name
jdbc-dbconnectinfo	Database connection information
db-character-sets	Database character code type
db-tbl-split-key	Existence of use of table range partition functionality by date data
db-tbl-split-corcheck-use	Existence of enhancement of correlation set duplication check

Note #1

DB Connector settings are the same in all HCSC servers in the load balance cluster.

Note #2

In the host name to be specified, specify the machine in which the database is stored.

Points to be considered when setting HCSC server runtime definition file

To set HCSC server runtime definition file, the same value must be set in all HCSC servers in the load balance cluster.

Add the following property if CTM is used:

- request-ejb.ctm=true

Add the following property if J2EE server name is different in HCSC server configuring the cluster:

- request-ejb.optional.name=<Optional name of synchronous requester service (SessionBean) shared in the cluster>

For details on how to set the HCSC server runtime definition file, see "*2.3.3 Setting HCSC server runtime definition file*".

For details on contents to be set in HCSC server runtime definition file, see "HCSC server runtime definition file" in "Service Platform Reference Guide".

(e) Installing cluster software

Install cluster software. For details on how to install, see the used cluster software document.

(2) Setting up an operating environment

Set up the operating environment in HCSC server machine configuring the cluster.

For details on how to configure the operating environment and execution environment, see "1.5 Configuration pattern of an operating environment in the cluster configuration " in "Service Platform Overview".

Implement the following operations to set up the operating environment:

Environment settings

Implement repository settings and environment variable settings as the environment settings of the operating environment.

For details on how to perform environment settings, see "*2.1.3 Environment settings*".

Embedding HCSC-Manager Plug-in in Eclipse

Embed HCSC-Manager Plug-in in Eclipse.

For details on how to embed the HCSC-Manager Plug-in in Eclipse, see "*2.1.5 Embedding HCSC-Manager plug-in in Eclipse*".

Setting user permission

Set user permission related to the operating environment. For details on setting contents and how to set, see "*2.4 Settings Related to the Operating Environment*".

(3) Setting up DB server

Set up DB server isolated from HCSC server configuring the cluster and share it with HCSC server in the cluster.

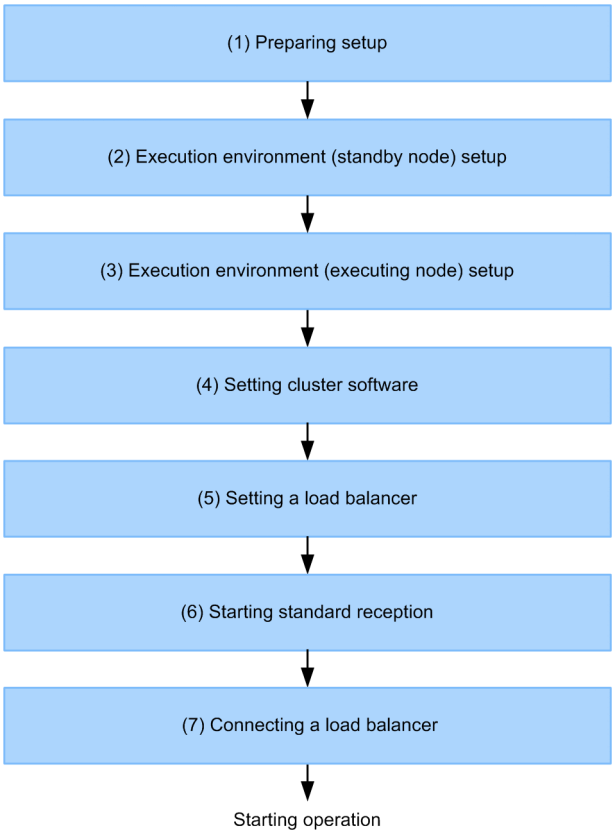
Install the database to be used in the machine used as DB server. For details on how to install, see documents of the used database.

2.7.2 Execution environment setup in 1 to N cluster configuration

After setting up the environment, set up the execution environment configuring N to 1 cluster.

The following figure shows the flow in execution environment setup in 1 to N cluster configuration.

Figure 2–11: FigureFlow of setup in 1 to N cluster configuration



Steps 1 to 5 given in the figure are described here. For details on operations in 1 to N cluster configuration, see "*5.6.2 Operations Using a High Availability Cluster Configuration*".

(1) Preparing setup

Perform the following operations before setup. Perform the following operations in executing node and standby node respectively.

Setting software required in the execution environment

Perform J2EE server setup. For details on setting contents and how to set up, see "*3.1.2 Setting up the software required for the execution environment*".

During setup, set Reliable Messaging system name# according to the cluster type as follows:

- In HA cluster

  Set in the same name as executing node and standby node.

- In load balance cluster

  Set in unique name in each HCSC server.

Note #

The queue name created for each RM system is described here.

- Queue.1.DisplayName= HCSC<Cluster name>ACPT_RCVQ
- Queue.1.QueueName= HCSC<Cluster name>ACPT_RCVQ
- Queue.2.DisplayName= HCSC<Cluster name>ACPT_DBQ
- Queue.2.QueueName= HCSC<Cluster name>ACPT_DBQ
- Queue.3.DisplayName= HCSC<Cluster name>TRNS_RCVQ
- Queue.3.QueueName= HCSC<Cluster name>TRNS_RCVQ

Sending control in the service requester

Disconnect the network for the service requester and change to the status in which service product execution request is not received in executing node and standby node.

Settings while using CTM

Set true in request-ejb.ctm in HCSC server runtime definition file while using CTM.

For details on HCSC server runtime definition file, see "HCSC server runtime definition file" in "Service Platform Reference Guide".

(2) Execution environment (standby node) setup

For details on how set up the execution environment (standby node), see "*2.6.2(2) Execution environment (standby node) setup*".

(3) Execution environment (executing node) setup

For details on how to set up the execution environment (executing node), see "*2.6.2(3) Execution environment (executing node) setup*".

(4) Setting cluster software

Set the cluster software in HA cluster configuration.

For details on how to set up cluster software, see "*2.6.2(4) Setting cluster software*".

(5) Setting a load balancer

Set to send the service product execution request to all HCSC servers configuring the load balance cluster.

While using CTM, the same value must be set in CTM domain manager name in all HCSC servers and the smart agent port number.

For details on how to set up the load balancer, see the used load balancer document.

(6) Starting standard reception

Start standard reception of all HCSC servers. For details on how to start the standard reception, see "*5.3.9 Starting standard receptions*".

(7) Connecting a load balancer

Connect the load balancer and change it to usable status. These procedures are unnecessary while using CTM.

For details on how to start the connection of the load balancer, see the used load balancer document.

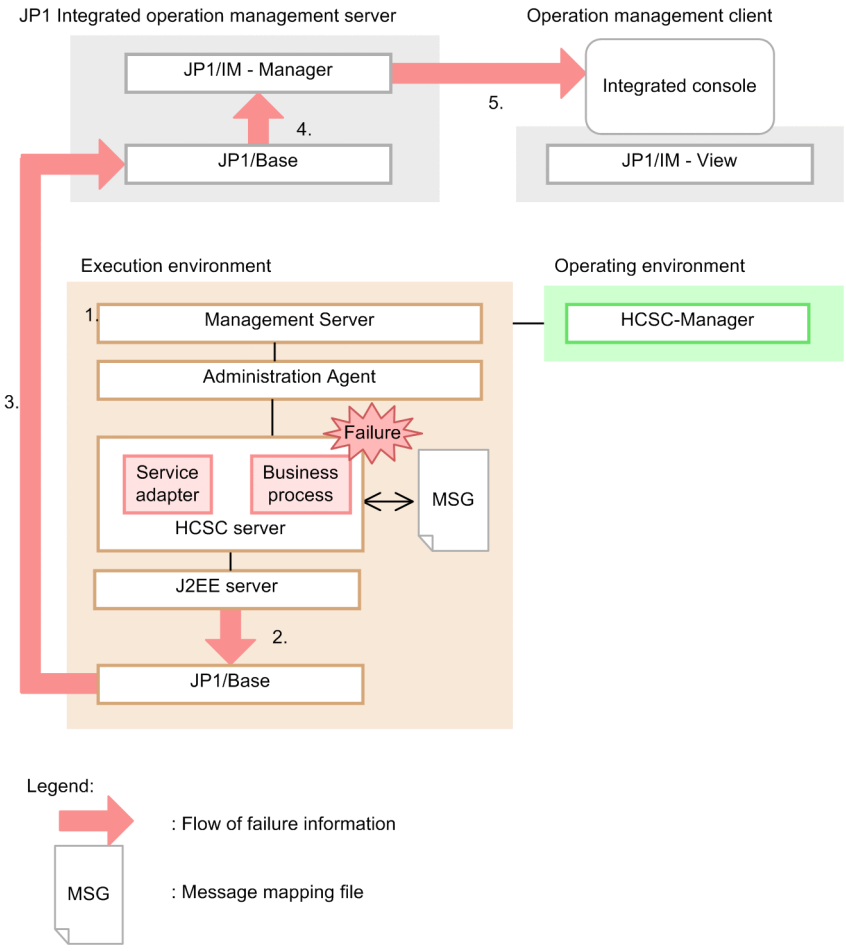
2.8 Environment setup while using JP1 integrated functionality

You can monitor faults occurring in Service Platform by integrating with **JP1**. You can detect problem occurrence, ascertain the cause and take action by monitoring a fault.

In Service Platform, JP1 is notified about occurring fault messages as JP1 events. You can confirm detailed information of JP1 events from JP1 integrated console. For details on how to confirm, see "*7.8.1 Monitoring errors using the JP1 linkage functionality*".

The following figure shows the flow of fault monitoring integrated with JP1:

Figure 2–12: FigureFlow of fault monitoring integrated with JP1



1. Set JP1 event issue.
   Set the kind of error and fault information to be issued as JP1event in Smart Composer. For details on how to set up, see "*2.8.2 Setting JP1 event execution for Service Platform*".
2. If a fault occurs in Service Platform, a message related to the fault is issued to JP1/Base as a JP1 event.
3. JP1 event is notified to JP1 integrated operation management server.
4. JP1/IM - Manager collects JP1 event notified to JP1 integrated operation management server.
   If the setting is to notify the operation manager by using the auto-action functionality of JP1/IM, the operation manager is notified that a fault has occurred.
5. Check detailed information of JP1 event from the integrated console.
   For details on how to confirm, see "*7.8.1 Monitoring errors using the JP1 linkage functionality*".

Important note

If 1 or multiple HCSC servers are deployed in the execution environment, you can set up the following environments in 1 host:

- Execution environment
- Operating environment
- JP1 integrated operation management server
- Operation management client

However, if multiple HCSC servers are deployed in different hosts, set up in separate hosts as in *Figure2-12*.

2.8.1 Flow of JP1 integrated settings

The following JP1 products must be installed and set up in order to use JP1 integrated functionality.

Table 2–22: TableJP1 products required to use JP1 integrated functionality

Installation destination	JP1 product
Execution environment	JP1/Base
JP1 integrated operation management server	• JP1/Base • JP1/IM - Manager
Operation management client	JP1/IM - View#

Note #
You can only install in Windows. You can display the integrated console only in Windows.

For installation and setup of JP1 products, see the following manuals:

- If JP1/Integrated Management - Manager Version 10 or Version 9 is used,
  Manual "JP1/Integrated Management - Manager Users Guide" or manual "JP1/Integrated Management - Manager Operation Guide"

The following points show the flow of settings for integration with JP1:

1. Set the following items in the execution environment:
   - Setting JP1 event execution of Service Platform (see *2.8.2*)
     Set to issue the message of fault occurring in Service Platform as a JP1 event.
   - Setting JP1/Base event server name (see *2.8.3*)
     In HA cluster configuration, set only while issuing a JP1 event by using the logical host JP1/Base event server.
2. Perform the following operations in JP1 integrated operation management server.
   - Creating JP1/Base configuration definitions (see *2.8.4*)
     Define the hierarchical relation of systems managed by JP1 integrated operation management server.
     If this definition is deployed in each host, it is identified as transfer destination information.

2.8.2 Setting JP1 event execution for Service Platform

Set the following 2 items to issue messages of faults occurring in Service Platform as JP1 events:

- JP1 event settings for Management Server
- JP1 event settings for J2EE server

The following points describe each setting method.

(1) JP1 event settings for Management Server

Set as follows in Management Server environment settings file (mserver.properties). If you set this, messages related to faults are issued from Management Server to JP1/Base as a JP1 event.

For details on Management Server environment settings file, see "10.7 mserver.properties (Management Server environment settings file) " in "Application Server Definition Reference Guide".

```
com.cosminexus.mngsvr.jp1event.enabled=true
com.cosminexus.mngsvr.jp1event.warning=true
com.cosminexus.mngsvr.jp1event.emergency=true
com.cosminexus.mngsvr.jp1event.alert=true
com.cosminexus.mngsvr.jp1event.notice=true
com.cosminexus.mngsvr.jp1event.information=true
com.cosminexus.mngsvr.jp1event.error=true
com.cosminexus.mngsvr.jp1event.critical=true
```

Restart Management Server to enable the set information.

(2) JP1 event settings for J2EE server

Specify parameters as follows in J2EE server configuration of Easy Setup definition file. If you specify this, messages related to faults are issued from J2EE server to JP1/Base as JP1 events.

For details on Easy Setup definition file, see "4.6 Easy Setup definition file" in "Application Server Definition Reference Guide".

```
<configuration>
  <logical-server-type>j2ee-server</logical-server-type>
  <param>
    <param-name>ejbserver.manager.jp1event.enabled</param-name>
    <param-value>true</param-value>
  </param>
  <param>
    <param-name>manager.jp1event.system.filtering.severity.emergency</param-name>
    <param-value>true</param-value>
  </param>
  <param>
    <param-name>manager.jp1event.system.filtering.severity.alert</param-name>
    <param-value>true</param-value>
  </param>
  <param>
    <param-name>manager.jp1event.system.filtering.severity.critical</param-name>
    <param-value>true</param-value>
  </param>
  <param>
    <param-name>manager.jp1event.system.filtering.severity.error</param-name>
    <param-value>true</param-value>
  </param>
  <param>
    <param-name>manager.jp1event.system.filtering.severity.warning</param-name>
    <param-value>true</param-value>
  </param>
  <param>
    <param-name>manager.jp1event.system.filtering.severity.notice</param-name>
    <param-value>true</param-value>
  </param>
  <param>
    <param-name>manager.jp1event.system.filtering.severity.information</param-name>
    <param-value>true</param-value>
  </param>
</configuration>
```

2.8.3 Setting JP1/Base event server name

Set the following 2 items in HA cluster configuration while issuing JP1 event by using the logical host JP1/Base event server:

- Event server name settings for the execution environment
- Event server name settings for J2EE server

The following points describe each setting method:

(1) Event server name settings for Management Server

Set the logical host name or logical IP address of JP1 integrated operation management server in Management Server environment settings file (mserver.properties).

For details on Management Server environment settings file, see "10.7 mserver.properties (Management Server environment settings file)" in "Application Server Definition Reference Guide".

```
mngsvr.jp1event.event_server_name=<Logical host name or logical IP address>
```

Restart Management Server to enable the set information.

(2) Event server name settings for J2EE server

Specify the logical host name or logical IP address of JP1 integrated operation management server in J2EE server configuration of Easy Setup definition file.

For details on Easy Setup definition file, see "4.6 Easy Setup definition file" in "Application Server Definition Reference Guide".

```
<configuration>
  <logical-server-type>j2ee-server</logical-server-type>
  <param>
    <param-name>ex.properties.m</param-name>
    <param-value>.ejbserver.manager.jp1event.event_server_name=<Logical host name or
logical IP address></param-value>
  </param>
</configuration>
```

2.8.4 Creating JP1/Base configuration definitions

Define the system configuration managed by JP1/IM in JP1/Base configuration definition file.

You can collectively manage definition information by using JP1/Base deployment functionality and deploying the created definition in JP1/Base of each host.

If the execution environment, operating environment, JP1 integrated operation management server and operation management client are configured in 1 host, JP1/Base configuration definitions need not be created.

The following points show the procedures for creating JP1/Base configuration definitions. For details on how to use JP1/Integrated Management - Manager Version 10 or Version 9, see the descriptions related to setting system configuration definition information in "JP1/Integrated Management - Manager Users Guide" or the manual "JP1/Integrated Management - Manager Operation Guide".

1. Create JP1/Base configuration definition file and define system configuration.
   Configuration definition file (jbs_route.conf) is installed in the following location:
   In Windows
   - While operating in HA cluster configuration
     <Common folder>\jp1base\conf\route\jbs_route.conf
   - While not operating in HA cluster configuration
     <JP1/Base installation destination folder>\conf\route\jbs_route.conf

   In UNIX
   - While operating in HA cluster configuration
     <Common directory>/jp1base/conf/route/jbs_route.conf
   - While not operating in HA cluster configuration
     /etc/opt/jp1base/conf/route/jbs_route.conf

   Contents of configuration definition file
   [Host name of JP1 integrated operation management server]
   Host name of J2EE server machine
2. Execute jbsrt_distrib command and deploy configuration definition information.

jbsrt_distrib command is stored in the following location:

In Windows

- While operating in HA cluster configuration
  <Common folder>\jp1base\bin\jbsrt_distrib.exe
- While not operating in HA cluster configuration
  <JP1/Base installation destination folder>\bin\jbsrt_distrib.exe

In UNIX

- While operating in HA cluster configuration
  <Common directory>/jp1base/bin/jbsrt_distrib
- While not operating in HA cluster configuration
  /etc/opt/jp1base/bin/jbsrt_distrib

Note

To use in HA cluster configuration, the logical server name must be defined in -h option.

2.8.5 Editing message mapping files

The message mapping file (system log message mapping file for JP1/IM integration) defines the severity of faults and notices detected by J2EE server and JP1 event to which it is to be converted. You can edit the message mapping file, control messages issued as JP1 events and customize JP1 events. If there is no mapping definition and if severity is not allocated to a JP1 event, JP1 event is not issued.

The file name of the message mapping file is "manager.jp1event.system.mapping.properties". Since a standard message mapping file is provided to set mapping relations, edit by text editor as required. The storage location of the message mapping file is described here.

In Windows

<Service Platform installation directory>\manager\config

In UNIX

/opt/Cosminexus/manager/config

For details on system log message mapping file for JP1/IM integration, see "10.19 System log message mapping file for JP1/IM integration" in "Application Server Definition Reference Guide".

2.9 Environment configuration for multiple operating environments and execution environments on one machine

Basically, only one HCSC-Manager environment is configured on one machine. However, you can configure more than two environments on one machine by setting up the CSCMNG_HOME environment variable.

The following subsections describe examples of system configuration and the procedure of configuration when multiple environments are configured on one machine:

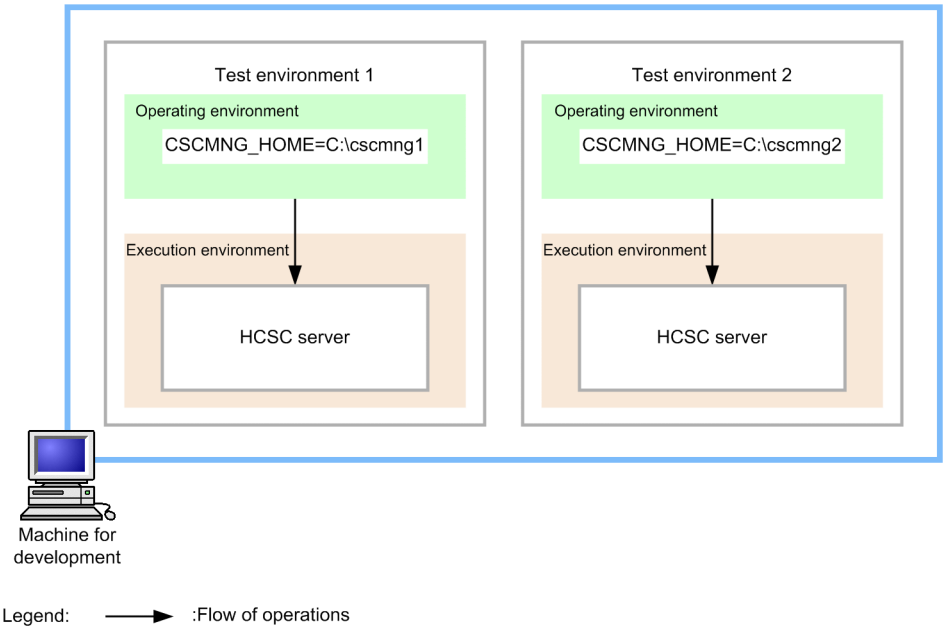
2.9.1 Example of system configuration when multiple environments are configured on one machine

This subsection describes an example of classifying the development environment in multiple environments and the HCSC-Manager environment in each cluster.

(1) Classifying development environment into multiple environments

By assigning the CSCMNG_HOME environment variable to each test environment to be used, you can configure multiple test environments on one machine. The following figure shows an example of configuring multiple operating and execution environments on the machine for development:

Figure 2–13: Example of configuring multiple operating and execution environments on the machine for development



However, since you cannot use the HCSC Easy Setup functionality when you assign CSCMNG_HOME environment variable to each environment, you must build the environment one by one from the HCSC server setup.

Also, if you assign the CSCMNG_HOME environment variable, you cannot use even the HCSC production environment Easy Setup functionality (cscsetup command). Note that when setting up an environment using the HCSC production environment Easy Setup functionality, assign the CSCMNG_HOME environment variable after unsetting up, and then again set up an environment without using the production environment setup functionality.

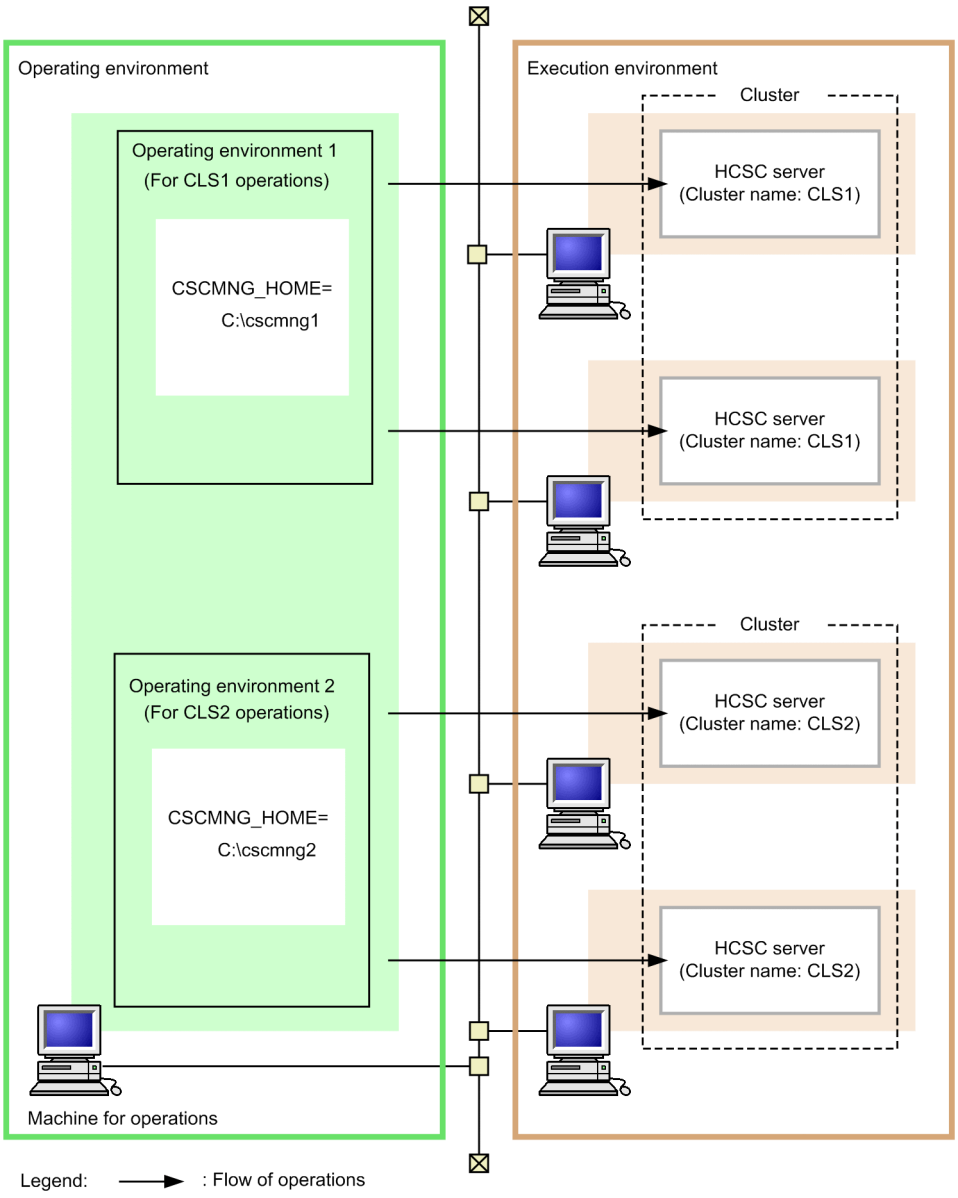
(2) Classifying the HCSC-Manager environment in each cluster

While handling multiple clusters in a large-scale configuration, you can perform localization when error occurs such as though the repository is destroyed due to classification of the repository; the operations are executed without being affecting other clusters.

Hitachi recommends you to execute operations in multiple clusters and to classify operating environment in each cluster when configuring execution and operating environments on different machines.

The following figure shows an example of classifying the operating environment in each cluster:

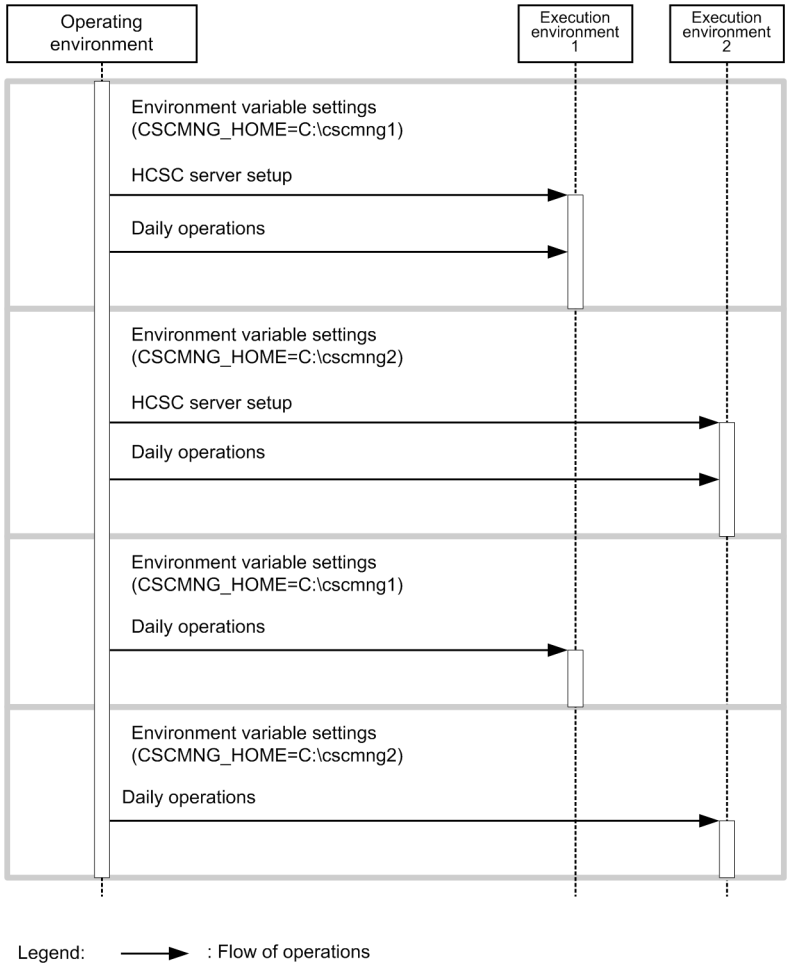
Figure 2–14: Example of classifying the operating environment in each cluster



2.9.2 Procedure for configuring multiple environments on one machine

The following figure shows the procedure for configuring multiple HCSC-Manager environments on one machine:

Figure 2–15: Procedure for configuring multiple HCSC-Manager environments on one machine



(1) Setting the CSCMNG_HOME environment variables

When configuring multiple HCSC-Manager environment on one machine, you must set the `CSCMNG_HOME` environment variable only for the number of configured environments.

Set an absolute path of an optional folder in the `CSCMNG_HOME` environment variables. By setting up this path, the HCSC-Manager references the definition file under the `CSCMNG_HOME` environment variable.

The following table describes the definition file under the `CSCMNG_HOME` environment variable referenced by the HCSC-Manager:

Table 2–23: Definition file under the CSCMNG_HOME environment variables referenced by HCSC-Manager

Directory name	Description
`%CSCMNG_HOME%\config`	Configuration file storage directory used in operating environment
`%CSCMNG_HOME%\log`	Default log directory used in operating environment
`%CSCMNG_HOME%\repository`	Default repository directory used in operating environment
`%CSCMNG_HOME%\spool`	Temporary directory used in operating environment

Tip

Hitachi recommends the setup the absolute path of the optional folder such as `c:\cscmng` which is easy to understand.

Important note

When configuring multiple HCSC-Manager environments with the same CSCMNG_HOME environment variables, execute with the CSCMNG_HOME environment variables that is set to the same value by the CSCMNG commands after setting up the CSCMNG_HOME environment variables.

Hitachi recommends creating user environment variables, command prompt short cuts, shelling script for resource setup to avoid any miss outs in the set up

The following are the examples for settings of CSCMNG_HOME environment variables:

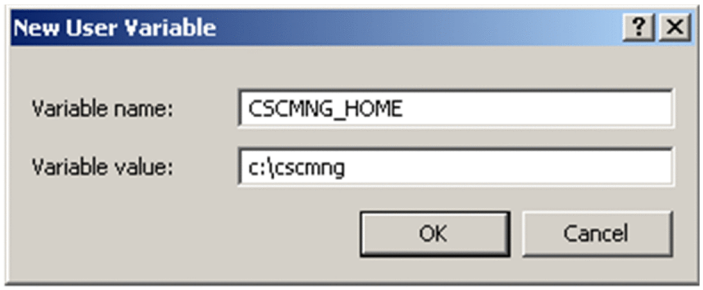
(a) Examples for settings of CSCMNG_HOME environment variables (In Windows)

The following is the example for setting c:\cscmng:

- **Examples for settings of user environment variables**

  The following table shows the example for setting c:\cscmng:

  1. Input the environment variable to be set as shown in the following dialog box:



  2. Click the **OK** button.

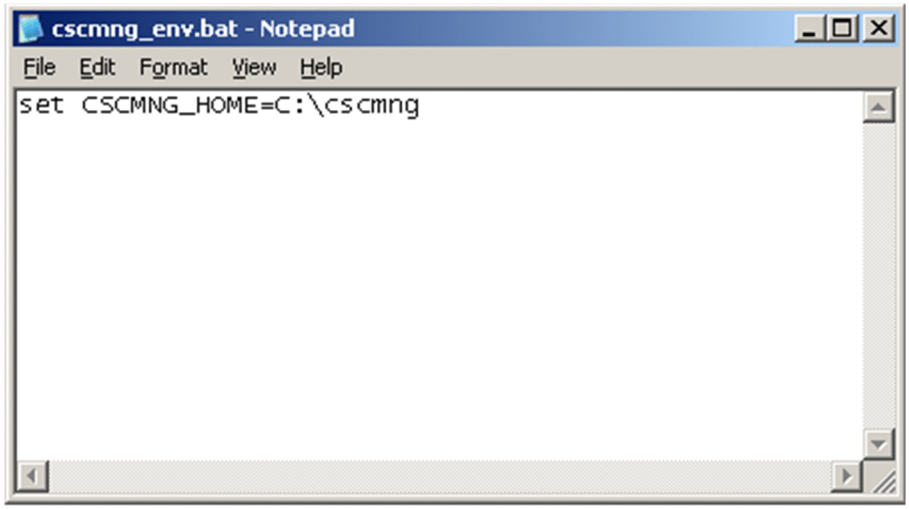
     The CSCMNG_HOME environment variable is enabled.

- **Example for setting short cut of command prompt**

  The following is the procedure for setting short cut to the command prompt:

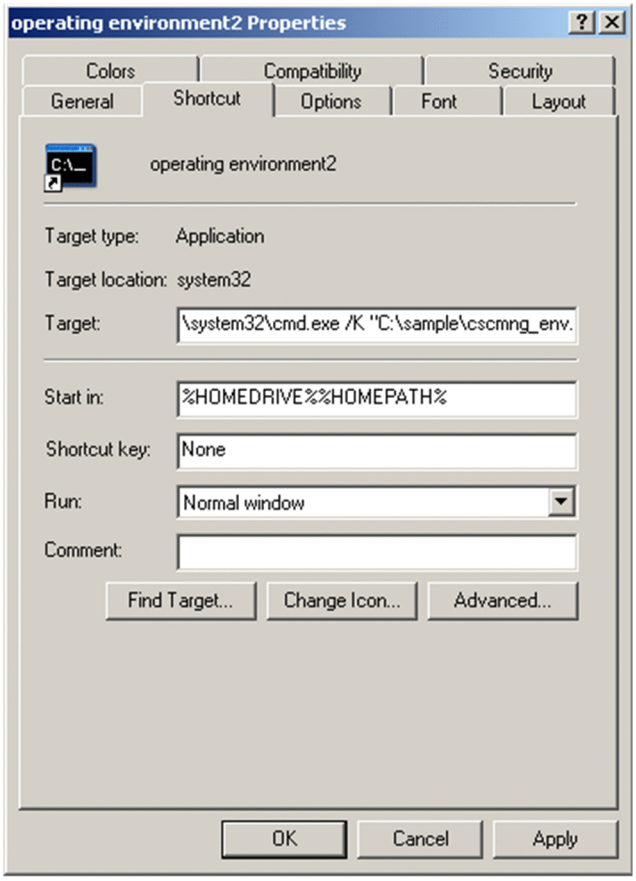
  1. Create the cscmng_env.bat file where the following contents are described, in an optional directory:

```
set CSCMNG_HOME=C:\cscmng
```



  2. Copy the short cut of the command prompt in the optional directory and change the property link destination as follows:

```
cmd.exe /K full-path-of-the-cscmng_env.bat-file-create-in-step1
```



(b) Examples for settings of CSCMNG_HOME environment variables (In UNIX)

The following is the example for setting `/home/user1/cscmng`:

- **Example for setting Bourne-shell**

  The following is the procedure for setting Bourne-shell:

  1. Create the `cscmng_env.bat` file where the following contents are described, in an optional directory:

     ```
     export CSCMNG_HOME=/home/user1/cscmng
     ```

  2. Execute shell by the following format:

     ```
     . cscmng.sh
     ```

     When shell is executed, `cscmng.sh` file is read and the `CSCMNG_HOME` environment variable is enabled.

- **Example for setting C shell**

  The following is the example for setting Cshell:

  1. Create the `cscmng.csh` file in which the following contents are described, in an optional directory:

     ```
     setenv CSCMNG_HOME /home/user1/cscmng
     ```

  2. Execute shell by the following format:

     ```
     source cscmng.csh
     ```

     When shell is executed, `cscmng.sh` file is read and the `CSCMNG_HOME` environment variable is enabled.

(2) Setting up the operating environment

When configuring multiple operating environments on one machine, you must see setup only the environments to be configured. For details about how to set up operating environment, see *2.4 Settings Related to the Operating Environment*.

The following are the precautions that you must take when changing the common definition of the HCSC-Manager command and the HCSC-Manager definition file from an initial value.

(a) Precautions when changing the HCSC-Manager definition file from initial value

- Create the `%CSCMNG_HOME%\config\manager` directory, and then after copying the following property file under the `%CSCMNG_HOME%\config\manager` directory you can use the property file.

  `Service Platform installation directory``\CSC\config\manager\templates\cscmng.properties`
- The HCSC-Manager definition file changes to `%CSCMNG_HOME%\config\manager\cscmng.properties` and not <*Service Platform installation directory*>`\CSC\config\manager\cscmng.properties`.
- Confirm if `%CSCMNG_HOME%\config\manager\cscmng.properties` exists when the HCSC-Manager definition file is not enabled. If the file exists, check if file correctly edited.

(b) Precaution when changing the common definition of HCSC-Manager commands from initial value

- Create the `%CSCMNG_HOME%\config\manager` directory, and then after copying the following property file under the `%CSCMNG_HOME%\config\manager` directory, you can use the property file.

  `Service Platform installation directory``\CSC\config\manager\templates\csccmd.properties`
- The common definition file of the HCSC-Manager command changes to `%CSCMNG_HOME%\config\manager\csccmd.properties` and not *Service Platform installation directory*`\CSC\config\manager\csccmd.properties`.
- Confirm if `%CSCMNG_HOME%\config\manager\csccmd.properties` exists when HCSC-Manager command common definition file is not enabled. If the file exists, check if the file is correctly edited.

(3) Setting up the HCSC server

For details about the HCSC server setups, see *3.1 Setting Up the System*.

(4) GUI start-up

After the HCSC server is setup, and when the operation is executed using the GUI of Eclipse, startup Eclipse when the `CSCMNG_HOME` environment variable is in an enabled state. For example, if the `CSCMNG_HOME` environment variable is enabled at the Command Prompt, startup `eclipse.exe` from the Command Prompt.

3 System Setup and Unsetup

This chapter describes system setup and unsetup, as well as HCSC server definitions. This chapter also describes the procedure for migrating from the test environment to the production environment.

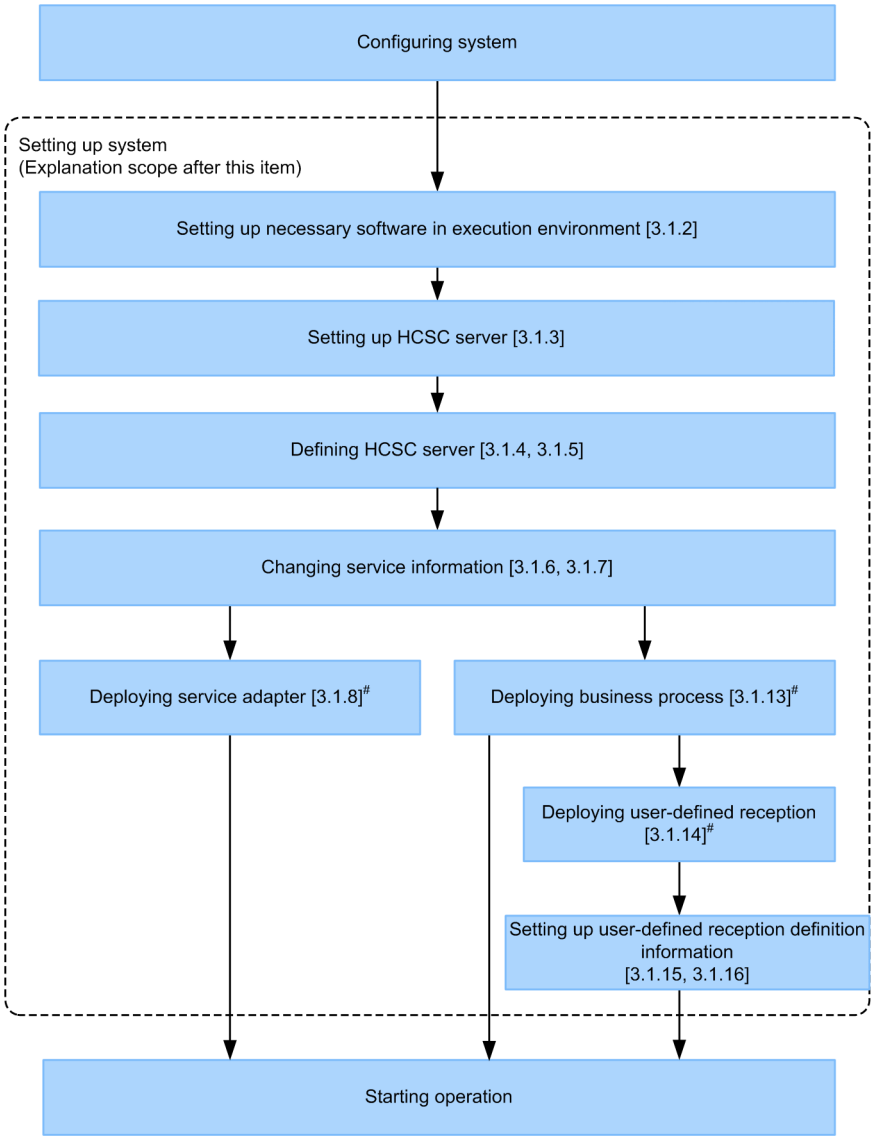
3.1 Setting Up the System

This section describes how to set up the system using a Service platform.

3.1.1 Flow of systemsetup

The following figure shows the flow of system setup. Note that to set up the system by using the Easy Setup functionality for the production environment, see "*3.5 Easy Setup of production environment*".

Figure 3–1: Figure Flow of system setup



Note#

You can also execute these operations in a batch. In this case, the packaging and deployment definition of the HCSC components is executed before the HCSC components are deployed, and the components are started after the HCSC components are deployed.

However, batch execution is performed during system development or from unit testing to integration testing. For details, see "7.5 Batch execution of the process for deploying HCSC components on the HCSC Server and then starting " in "Service Platform Basic Development Guide".

The following paragraphs describe the processes in the figure:

Important note

- Before deploying the service adapters, business processes, and user-defined receptions, make sure you import and refresh the repository.
- Depending on the flow of processing during operations and the measures to be taken when errors occur, you must specify some settings before the operations start. For details, see "2.7.1 Invoking service components of an HCSC server from TP1 using standard synchronous reception", and "*7.Troubleshooting*" in "Service Platform Overview".
- In UNIX and when the Component Container administrator is changed, unify the Service Coordinator administrator. For details, see "*Appendix A How to Change the Service Coordinator Administrator*".

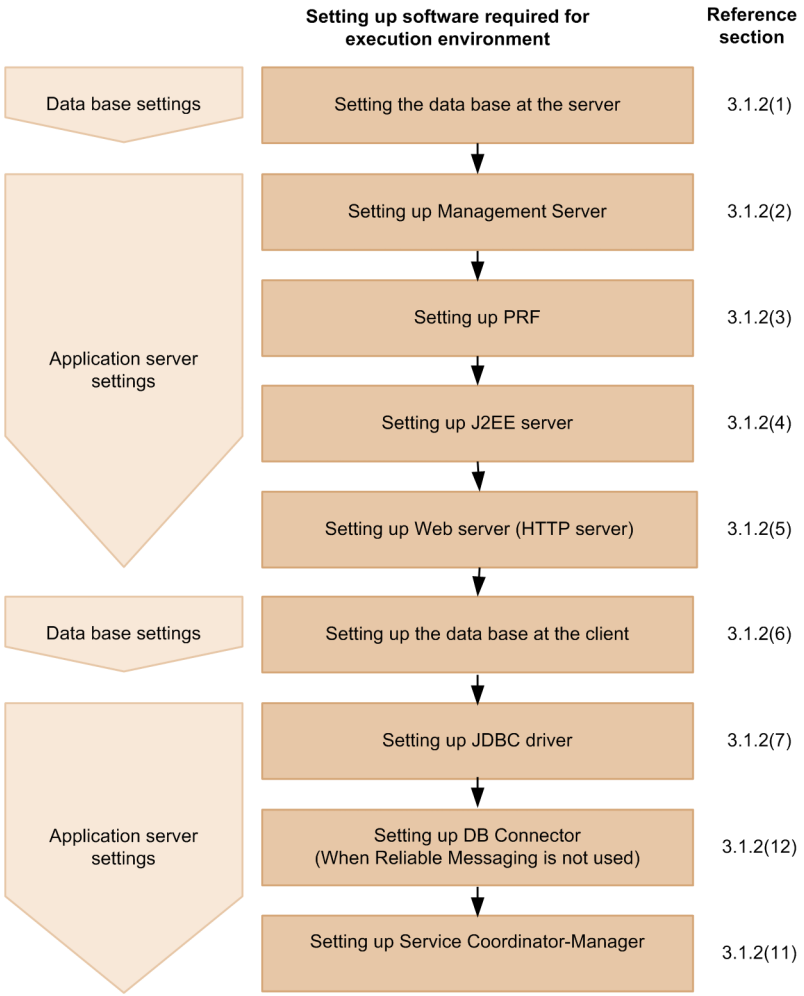
3.1.2 Setting up the software required for the execution environment

Before you set up the execution environment, you must set up the software required for the execution environment. The settings for the software required for the execution environment differ as follows depending on the usage of the database and Reliable Messaging:

- When database is used and Reliable Messaging is not used

  The following figure shows the flow of software settings required for the execution environment and their reference destinations.

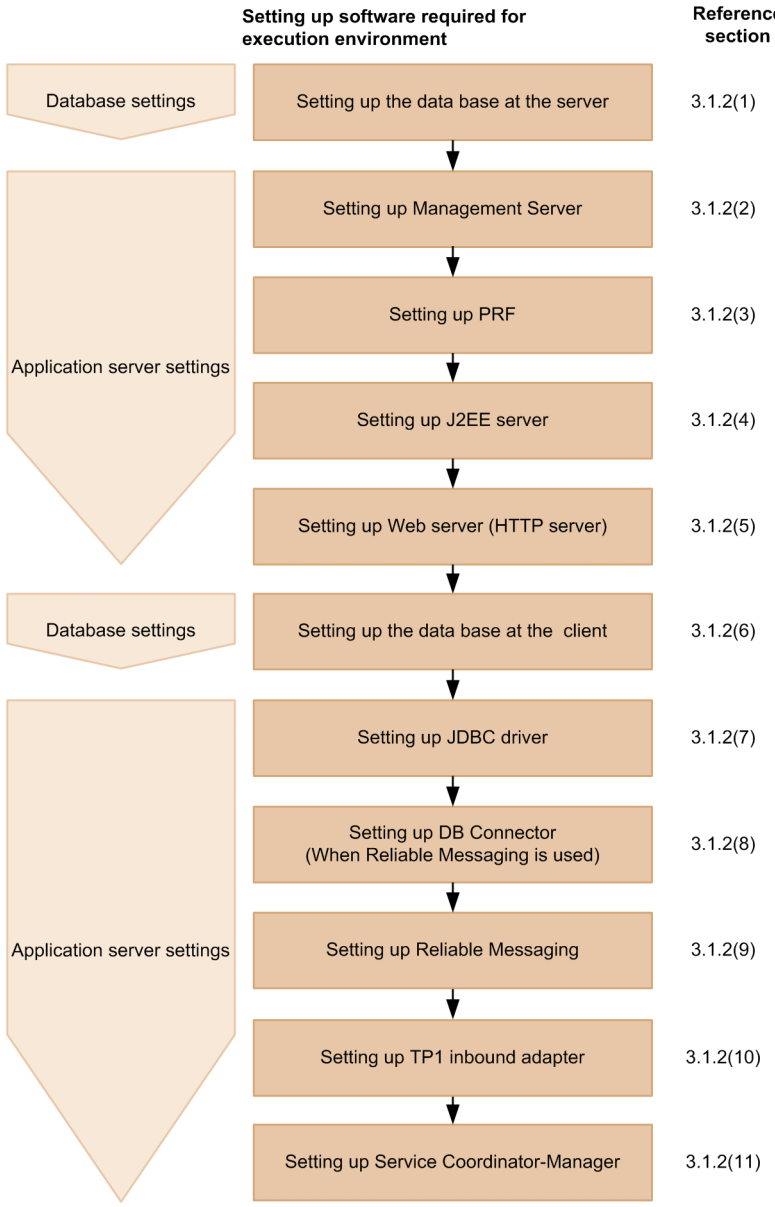
  Figure 3–2: Figure Software settings required for the execution environment (When database is used and Reliable Messaging is not used)



- When both database and Reliable Messaging are used

The following figure shows the flow of software settings required for the execution environment and their reference destinations.

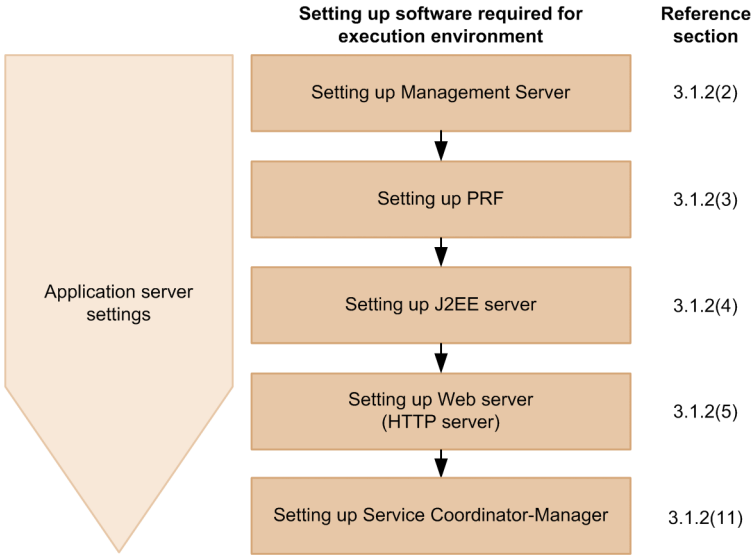
Figure 3–3: Figure Software settings required for the execution environment (When both database and Reliable Messaging are used)



- When both database and Reliable Messaging are not used

  The following figure shows the flow of software settings required for the execution environment and their reference destinations.

Figure 3–4: Figure Software settings required for the execution environment (When both database and Reliable Messaging are not used)



The following paragraphs describe the software settings to be implemented before you set up the execution environment:

(1) Setting up the database on the server

Set up both, DB server and DB client, during database setup.

(a) Settings on the DB server (In HiRDB)

Implement the following operations:

Setting up the character code for the HiRDB server

Specify any one of Shift JIS Kanji code, EUC Japanese Kanji code, UTF-8, or single-byte character code as the character code. For details on how to change the character code, see the description related to specifying or selecting character codes in "HiRDB System Installation and Design Guide".

Important note

When the HCSC server is operated in UNIX, the character codes on the HCSC server and HiRDB server must match.

Setting up the environment

For details on HiRDB environment settings, see "HiRDB System Installation and Design Guide".

Setting up the user permissions

First, decide the name of the connected user. Thereafter, to save the management information on HiRDB, set up permissions for the users who will be connecting to HiRDB. In HiRDB, a user is created by setting up the CONNECT permission for the user.

Permissions to be set up

- CONNECT permission

  This permission is required for using HiRDB. This permission enables the user to connect (CONNECT) to the database. An error occurs if a user who does not have the CONNECT permission attempts to use HiRDB.

- Define schema permission

  This permission is required for defining a schema. If you set up the define schema permission, you can define the schema, tables, view tables, indexes, and abstract data types. You can also register a stored procedure and stored function.

How to set up the permissions

Use the database definition utility (pddef) and SQL Executer to set up the permissions. For details on how to set up the permissions, see "HiRDB System Operation Guide". For details on how to use the database definition utility, see "HiRDB Command Reference".

Procedure to set up the permissions by using the database definition utility:

1. Set up the following environment variables:

   In Windows

```
SET PDHOST=<Host name or IP address of HiRDB server>
SET PDNAMEPORT=<Port number of HiRDB server>
SET PDUSER=<Name of the user who has DBA permissions>/<password>
```

   In UNIX (Bourne shell)

```
export PDHOST=<Host name or IP address of HiRDB server>
export PDNAMEPORT=<Port number of HiRDB server>
export PDUSER=<Name of the user who has DBA permissions>/<password>
```

2. Execute the database definition utility (pddef) with the following command:

```
pddef
```

3. Execute the following SQL statement:

```
GRANT CONNECT TO <user name># IDENTIFIED BY <password>;
GRANT SCHEMA TO <user name>#;
```

   Note#

   The user for whom the permissions are specified is the connected user that the messaging infrastructure uses. The value is the same as the PDUSER environment variable that is registered in the HiRDB client environment variable group.

   For details on the PDUSER environment variable, see "*Table 3-5 Table Environment variables set up in the environment variable group*".

4. To terminate the database definition utility (pddef) in Windows, press the [Ctrl] key + [Z] key, and then press the [Enter] key.

   To terminate the database definition utility (pddef) in UNIX, press the [Ctrl] key + [D] key, and then press the [Enter] key.

Defining a schema

Define the schema to store the management information on HiRDB.

How to define a schema

Use the database definition utility (pddef) and SQL Executer to define a schema. For details on how to define a schema, see "HiRDB SQL Reference". For details on how to use the database definition utility, see "HiRDB Command Reference".

Procedure to define a schema by using the database definition utility:

1. Set up the following environment variables:

   In Windows

```
SET PDHOST=<Host name or IP address of HiRDB server>
SET PDNAMEPORT=<Port number of HiRDB server>
SET PDUSER=<User name>#/<password>
```

   Note#

   The user name to be specified is the name of the user for whom permissions are set up.

   In UNIX (Bourne shell)

```
export PDHOST=<Host name or IP address of HiRDB server>
export PDNAMEPORT=<Port number of HiRDB server>
export PDUSER=<User name>#/<password>
```

   Note#

   The user name to be specified is the name of the user for whom permissions are set up.

2. Execute the database definition utility (pddef) with the following command:

```
pddef
```

3. Execute the following SQL statement:

```
CREATE SCHEMA;
```

4. To exit the database definition utility (pddef) in Windows, press the [Ctrl] key + [Z] key, and then press the [Enter] key.

   To exit the database definition utility (pddef) in UNIX, press the [Ctrl] key + [D] key, and then press the [Enter] key.

Preparing the RD area

To store the management information tables of the messaging infrastructure, create the RD area as and when required. For details on how to create an RD area, see "HiRDB System Operation Guide".

Setting up pd_max_users (number of concurrent users)

In the operand pd_max_users (number of concurrent users) of the HiRDB system common definition, specify the maximum number of DB connections to be used in the execution environment. For details on specifying this value, see "*Table 3-4 Table Number of database connections used in the execution environment*".

For details on pd_max_users, see "HiRDB Version 9 System Definition".

(b) Settings on the DB server (In Oracle)

Implement the following operations:

Setting up the environment

For details on the environment settings for Oracle, see the documentation published by the Oracle Corporation.

Creating the connected users and setting up permissions

To save the management information on Oracle, you must create the connected users for Oracle, and set up the permissions.

Setting up the permissions

Set up the following permissions as the system permissions:

- CREATE ANY INDEX system permission
- CREATE SESSION system permission
- CREATE TABLE system permission
- CREATE VIEW system permission
- FORCE ANY TRANSACTION system permission

Set up the following permissions as the object permissions:

- SELECT permission for SYS.DBA_PENDING_TRANSACTIONS
- EXECUTE permission for SYS.DBMS_SYSTEM

Furthermore, set up the following role:

- SELECT_CATALOG_ROLE

How to set up the connected users and permissions

Use the Oracle Enterprise Manager Console, or sqlplus to create the user and set up permissions. An example of settings when using Oracle Enterprise Manager Console and sqlplus is as follows:

Example of settings when the Oracle Enterprise Manager console is used

1. Connect to the database as a sys user.
2. On the navigator tree, click on [Security], then right click [User], and then select [Create].
3. Open the [General] tab, and enter the name and password.
4. Open the [Role] tab, delete the CONNECT role, and then add SELECT_CATALOG_ROLE.
5. Open the [System] tab and set up the system permissions.
6. Open the [Object] tab, select [SYS], [View], and [DBA_PENDING_TRANSACTIONS], and then set up the SELECT permission.
7. Select [SYS], [Package], and [DBMS_SYSTEM], and then set up the EXECUTE permission.

8. Open the [Limit allocation] tab and set up the allocation limit size for the table area.
9. Click the [Create] button.

Example of settings when sqlplus is used

1. Connect to the database as a sys user.
2. Issue the following SQL statement (The value specified for the QUOTA phrase is an example value).

```
CREATE USER <Name of the user who is granted permission> PROFILE "DEFAULT"
 IDENTIFIED BY <password> DEFAULT TABLESPACE "USERS"
 TEMPORARY TABLESPACE "TEMP"
 QUOTA 10 M ON "USERS"
 ACCOUNT UNLOCK;
GRANT CREATE ANY INDEX TO <Name of the user who is granted permission>;
GRANT CREATE SESSION TO <Name of the user who is granted permission>;
GRANT CREATE TABLE TO <Name of the user who is granted permission>;
GRANT CREATE VIEW TO <Name of the user who is granted permission>;
GRANT FORCE ANY TRANSACTION TO <Name of the user who is granted permission>;
GRANT SELECT ON "SYS"."DBA_PENDING_TRANSACTIONS"
TO <Name of the user who is granted permission>;
GRANT EXECUTE ON "SYS"."DBMS_SYSTEM" TO <Name of the user who is granted permission>;
GRANT SELECT_CATALOG_ROLE TO <Name of the user who is granted permission>;
```

(2) Setting up Management Server

Set up Management Server and specify the environment settings. For details, see the description related to the Management Server operating environment in "4.1.15 Information to be set up for using Management Server" in "Application Server System Setup and Operation Guide". For details on the settings for using HCSC-Manager, see "*2.1.6 Management Server settings for using HCSC-Manager*".

Note that Management Server and Administration Agent form the base for operating the HCSC server. Therefore, specify the settings so that Management Server and Administration Agent start automatically when the OS starts.

For details on how to set up the settings, see "mngautorun (Setting up and cancelling settings for autostart and auto-restart) " in "Application Server Command Reference Guide".

(3) Setting up PRF

Use the Smart Composer functionality or management portal functionality to set up PRF.

For details on setting up PRF by using the Smart Composer functionality, see "4.8 Setting up the system using other functionality" in "Application Server System Setup and Operation Guide".

For details on setting up PRF by using the management portal functionality, see "3. Configuration and Deletion of the System that executes J2EE Applications" in "Application Server Management Portal Operation Guide".

(4) Setting up a J2EE server

Implement the following operations:

(a) Setting up a J2EE server

Use the Smart Composer functionality or management portal functionality to set up a J2EE server.

For details on setting up a J2EE server by using the Smart Composer functionality, see "4.8 Setting up the system using other functionality" in "Application Server System Setup and Operation Guide".

For details on setting up a J2EE server by using the management portal functionality, see "3. Configuration and Deletion of the System that Executes J2EE Applications" in "Application Server Management Portal Operation Guide".

! Important note

During setup, make sure that the logical server name and real server name are the same. If the names are different, HCSC server setup might fail.

(b) Setting up the system environment variables for a J2EE server

For details on how to set up the system environment variables for a J2EE server, see the OS documentation. For details on the items to be checked when the system environment variables are set up, see "4.1.13 Items to be checked when the logical server environment variables are set up" in "Application Server System Setup and Operation Guide".

(c) Default settings for the SOAP Communication Infrastructure andJAX-WS engine

When using the SOAP1.1 mode, you must specify the default settings for the SOAP Communication Infrastructure. When using the SOAP 1.1/1.2 combined mode, you must specify the default settings for the JAX-WS engine. The procedure for specifying each of the default settings are as follows:

? Default settings for using the SOAP1.1 mode

When using the SOAP1.1 mode, specify the default settings for the SOAP Communication Infrastructure as follows:

1. To use WSDL4J that is distributed based on Common Public License Version 1.0, obtain the "wsdl4j.jar" file and copy the file to the following directory:

```
In <Service Platform installation directory>\c4web\lib
```

2. Specify the server definition file (c4websv.cfg).

   The following table lists and describes the contents to be specified in the server definition file for the SOAP Communication Infrastructure in a J2EE server operated by the HCSC server. For details on creating the server definition file, see "10.2 Setting up the server definition file" in "Application Server SOAP Application Development Guide".

   Table 3–1: TableSettings in the server definition file (SOAP Communication Infrastructure)

Settings	Key names	Set value (default)	Description
Multi-reference	c4web.common.<identifier>.do_multirefs	false	You cannot specify this property when using user-defined receptions. If true is specified, the operations are not guaranteed.
Data type definition	c4web.common.<identifier>.send_xsi_types	true	You cannot specify this property when using user-defined receptions. If false is specified, the operations are not guaranteed.
Character reference option	c4web.common.<identifier>.character_reference	false	You cannot specify this property when using user-defined receptions. If true is specified, the operations are not guaranteed.
Option for checking the qualified name of the SOAP Header	c4web.common.<identifier>.enable_soapheader_check	true	When using user-defined receptions, the option for checking the qualified name of the SOAP Header in the user-defined reception forcefully operates as false.
Maintaining an HTTP Session	c4web.application.<identifier>.app_maintainsession	false	You cannot specify this property when using user-defined receptions. If true is specified, the operations are not guaranteed.

Tip

The identifier in an HCSC server is a key used for obtaining the information about a running server from the server definition file. The key uses a name wherein the initial "/" is removed from the context root of the SOAP application deployed on the server. Therefore, in HCSC-Messaging, the key name is as follows:

Standard reception identifier: Cluster name

User-defined reception identifier: Reception ID of the user-defined reception

(Example) When the cluster name is "cluster1"

Standard reception identifier: "cluster1"

3. Specify the common definition file (c4webcom.cfg).

   The following table lists and describes the contents to be specified in the common definition file for the SOAP Communication Infrastructure in a J2EE server operated by the HCSC server. For details on creating the

common definition file, see "10.4 Setting up the common definition file" in "Application Server SOAP Application Development Guide".

Table 3–2: TableSettings in the common definition file (SOAP Communication Infrastructure)

Settings	Key names	Set value (default)	Description
Importance of trace file output	c4web.logger.log_level	WARN	Do not specify DEBUG in this property. If DEBUG is specified, a large amount of memory is consumed and throughput is affected as compared to the specification of another value.

●Default settings for using the SOAP1.1/1.2 combined mode

When using the SOAP1.1/1.2 combined mode, specify the default settings for the JAX-WS engine as follows:

1. Specify the common definition file (cjwconf.properties).

   The following table lists and describes the contents to be specified in the common definition file for the JAX-WS engine in a J2EE server operated by the HCSC server. For details on creating the common definition file, see "10.1.2 Settings in the common definition file" in "Application Server Web Service Development Guide".

   Table 3–3: TableSettings in the common definition file (JAX-WS engine)

Settings	Key names	Set value (default)	Description
Existence of maintenance of an HTTP Session	javax.xml.ws.session.maintain	false	The operations when true is specified are not guaranteed.

2. Specify the proxy settings for the servers.

   For details on how to specify the proxy settings, see "10.10 Connecting via a proxy server" in "Application Server Web Service Development Guide".

(d) Specific settings for setting up an HCSC server

Specify the following in the user property file for J2EE servers (usrconf.properties):

Property	Specified content
ejbserver.rmi.localinvocation.scope	Specify "app".
ejbserver.server.j2ee.feature	Specify "1.4".
ejbserver.jndi.global.enabled	Specify "false". For "true", "KDJE47722-W" is output in the Component Container message log, but Service Coordinator does not use (cannot use) the Portable Global JNDI name, so application startup continues and there is no problem.
ejbserver.distributedtx.XATransaction.enabled	Specify "true" or "false". Check whether the HCSC server accesses multiple resources (such as DB server), and specify "true" to disable and "false" to enable the light transaction functionality.

Note that not to specify "true" for ejbserver.DynamicStubLoading.Enabled.

(e) Setting up the container extension library

Specify the following settings for the container extension library. For details on how to set up the container extension library, see "14. Container Extension Library" in "Application Server Common Container Functionality Guide".

- **When the SOAP1.1 mode is used**

```
<Reliable Messaging installation directory>･lib･reliablemessaging-api.jar
<Service Platform installation directory>･c4web･lib･hitsaaj.jar
```

To disable cjjaxws.jar, comment out or delete the cjjaxws.jar line.

- **When the SOAP1.1/1.2 combined mode is used**

```
<Reliable Messaging installation directory>･lib･reliablemessaging-api.jar
<Service Platform installation directory>･jaxws･lib･cjjaxws.jar
```

To disable hitsaaj.jar, comment out or delete the hitsaaj.jar line.

At this time, specify in the format "add.class.path=<jar path>".

You can also specify this definition from the management portal. Specify the class path in the extension parameter on the [J2EE Container Settings] screen of the logical J2EE server specified in "Environment Settings of Logical Servers" in the management portal. The value set up here is applied to the option definition file for J2EE servers (usrconf.cfg).

For details on the option definition file for J2EE servers, see "2.3 usrconf.cfg (Option definition file for J2EE servers) " in "Application Server Definition Reference Guide". For details on the settings specified in the "Environment Settings of Logical Servers", see "10. Environment Settings of Logical Servers" in "Application Server Management Portal Operation Guide".

(5) Setting up a Web server (HTTP server)

There are two methods for setting up a Web server (HTTP server), the method of using the in-process HTTP server included in the J2EE server and the method of using HTTP Server.

(a) Method of using the in-process HTTP server

Implement the following operations:

Setting up the in-process HTTP server

For details on system setup, see "Application Server System Setup and Operation Guide".

Setting up the connection timeout value of the in-process HTTP server

If the connection pooling functionality is used in the SOAP Communication Infrastructure existing in the service requester, the time required for saving the connection in the service requester must be consistent with the connection timeout value in the HCSC-server operating machine.

To set up the connection timeout value:

1. From the management portal, select [Environment settings of logical servers].
2. From the server view, select [Logical J2EE server], [J2EE server], and then [<J2EE server name>].
3. In the [HTTP server] tab, select the [Communication or Thread Control] tab.
4. The [Communication or Thread Control Settings] screen is displayed.
5. In [Web Client Connection Settings], click on [Persistent Connection] and then [Timeout], and specify a value that is equal to or greater than the value specified in the c4web.common.connection_pool.timeout property of the common definition file for the SOAP Communication Infrastructure (Web Services). For example, if the c4web.common.connection_pool.timeout property is not specified, the default value 1800 (unit: seconds) is used for operations, so set up 3600, which is a multiple of this value, as the timeout value.

   Note that the timeout value can be specified in the range of 0 to 3600. Therefore, set up 0 if the value specified in the c4web.common.connection_pool.timeout property is greater than 1800.

(b) Method of using HTTP Server

Implement the following operations:

Setting up HTTP Server

For details on how to set up HTTP Server, see "HTTP Server".

Settings for integrating HTTP Server and J2EE server

To integrate HTTP Server with a J2EE server, you must set up the parameters for Web server integration in the Easy Setup definition file. For details on the parameters, see "4.13 Parameters that can be specified in a logical Web server" in "Application Server Definition Reference Guide".

Setting up the KeepAliveTimeout value of HTTP Server

If the connection pooling functionality is used in the SOAP Communication Infrastructure existing in the service requester, the time required for saving the connection in the service requester must be consistent with the KeepAliveTimeout value in the HCSC-server operating machine.

In KeepAliveTimeout of httpsd.conf, which is an HTTP Server configuration file, specify a value that is equal to or greater than a multiple of the value specified in the c4web.common.connection_pool.timeout property of the common definition file for the SOAP Communication Infrastructure (Web Services). For example, if the c4web.common.connection_pool.timeout property is not specified, the default value 1800 is used for operations, so set up 3600, which is a multiple of this value, in KeepAliveTimeout.

Note that the value can be specified in the range of 0 to 65535. For details, see "7.4.2 Settings related to connection pooling" in "Application Server SOAP Application Development Guide".

(6) Setting up the database client

(a) Settings in the DB client (In HiRDB)

Implement the following operations on the execution environment machine:

Setting up the environment variables

Set up the following environment variables in Windows:

In UNIX, set up the following environment variables as the environment variables to be used for starting the J2EE server operated by the HCSC server and for executing Management Server:

For details on how to set up the environment variables for starting a J2EE server operated by the HCSC server, see "10.9.24 Setting up the environment variables for J2EE servers" in "Application Server Management Portal Operation Guide".

For details on how to set up the environment variables for executing Management Server, see "10.9 mserverenv.cfg (Environment variable definition file for Management Server)" in "Application Server Definition Reference Guide".

PDXAMODE

Specify 1.

However, when the light transaction functionality is used, you need not set up PDXAMODE.

PDTXACANUM

Specify the maximum number of database connections to be used by Service Platform.

However, when the light transaction functionality is used, you need not set up PDTXACANUM.

The maximum value of DB connections must be estimated according to the execution environment to be used. The following table lists and describes the triggers at which the execution environment uses a DB connection and the number of database connections.

Table 3–4: Table Number of database connections used in the execution environment

Database connection usage destination	Database connection usage trigger	Number of database connections used
Messaging infrastructure	At startup	1
	When command is executed	1
	When a service component execution request is received	Number of concurrently executed service components
Business process infrastructure	When a business process execution request is received	Number of concurrently executed business processes
DB adapter	When a service component execution request is received	Number of concurrently executed service components
Reliable Messaging	See "3.4.1 DBMS settings (When HiRDB is used)" in "Reliable Messaging".	

The total number of DB connections used becomes the maximum value.

PDLANG or LANG

When the HCSC server is operated in UNIX, specify the same character code as the HiRDB server in PDLANG or LANG, depending on the HiRDB server character code. For details, see the contents related to PDLANG in "HiRDB UAP Development Guide".

When the HCSC server is operated in Windows, no settings need be specified.

LC_CTYPE

When the HCSC server is operated in UNIX, specify the same character code as the HiRDB server.

When the HCSC server is operated in Windows, no settings need be specified.

LD_LIBRARY_PATH

When the HCSC server is operated in Linux(R) or HP-UX (IPF), add the following path:

- <HiRDB operational directory>/client/lib
  Specify this path for installing HiRDB/Single Server, HiRDB/Parallel Server, or HiRDB Server.
- In <HiRDB installation directory>/client/lib
  Specify this path for installing HiRDB/Run Time, or HiRDB/Developer's Kit.

When the HCSC server is operated in Windows, no settings need be specified.

LIBPATH

When the HCSC server is operated in AIX, add the following path:

- <HiRDB operational directory>/client/lib
  Specify this path for installing HiRDB/Single Server, HiRDB/Parallel Server, or HiRDB Server.
- In <HiRDB installation directory>/client/lib
  Specify this path for installing HiRDB/Run Time, or HiRDB/Developer's Kit.

When the HCSC server is operated in Windows, no settings need be specified.

Setting up the environment variable group

To register the environment variable group:

In Windows

Select "System Group" with the tool for registering the HiRDB client environment variables, and register the environment variable group. In this case, specify the name of the environment variable group registered here in the DB Connector property definition.

In UNIX

Register the group in the configuration file of the HiRDB client environment variable group. In this case, specify the configuration file path of the environment variable group registered here in the DB Connector property definition.

For details on how to register the environment variable group, see the contents related to the registration of an environment variable group in "HiRDB UAP Development Guide".

For details on DB Connector properties, see "4.2.2 Defining DB Connector properties" in "Application Server Application Setup Guide".

The following lists and describes the environment variables set up in the environment variable group.

Table 3–5: Table Environment variables set up in the environment variable group

Name of the environment variable	Contents to be set up
PDHOST	Specify the database host name or IP address.
PDUSER	Specify the database user name and database password.
PDNAMEPORT	Specify the database port number.
PDSWAITTIME	Specify a value greater than the Component Container transaction timeout value#.
PDCWAITTIME	Specify a value greater than the Component Container transaction timeout value#.
PDSWATCHTIME	Specify 0.

Note#

Specify the transaction timeout value for Component Container in the user property file for J2EE servers. For details on the transaction timeout value for Component Container, see "8.6.4 Setting up a transaction timeout" in "Application Server System Design Guide".

(b) Settings in the DB client (In Oracle)

Set up Oracle JDBC Thin Driver. For details on the setup for Oracle JDBC Thin Driver, see "*3.1.2(7)(b) Setting up Oracle JDBC Thin Driver*".

(7) Setting up the JDBC driver

The JDBC driver to be used must be selected after considering the usage conditions.

The following table lists and describes how to select the JDBC driver to be used.

Table 3–6: Table JDBC drivers to be used

Used DBMS	Used JDBC driver	JDBC driver package
HiRDB (Version 8 or Version 9)#1	HiRDB TYPE4 JDBC Driver	JP.co.Hitachi.soft.HiRDB.JDBC.HiRDBDriver
Oracle	Oracle JDBC Thin Driver	• oracle.jdbc.driver.OracleDriver • oracle.jdbc.OracleDriver#2

Note#1

When DB Connector for HiRDB Type4 JDBC Driver is used

Note#2

When ORACLE11G is specified in the dbtype property of the HCSC server setup definition file

(a) Setting up HiRDB Type4 JDBC Driver

For details on setting up HiRDB Type4 JDBC Driver, see the contents related to HiRDB Type4 JDBC Driver in "HiRDB UAP Development Guide".

Note that you must specify the following settings in order to use the HCSC server:

1. Specify the JAR file for HiRDB Type4 JDBC Driver (pdjdbc2.jar) as the class path in <Service Platforminstallation directory>/manager/config/mserver.cfg file. At this time, specify the file in the "web.add.class.path=<Path of pdjdbc2.jar>" format.

   Example 1 (For HiRDB/Run Time)

   web.add.class.path=<HiRDB/Run Time installation directory>/client/lib/pdjdbc2.jar

   Example 2 (For HiRDB/Single Server)

   web.add.class.path=<HiRDB/Single Server installation directory>#/client/lib/pdjdbc2.jar

   Note#

   <HiRDB installation directory> is the directory named hirdb_s.

2. Specify the JAR file for HiRDB Type4 JDBC Driver (pdjdbc2.jar) as the class path in the option definition file for J2EE servers (usrconf.cfg). At this time, specify the file in the "add.class.path=<Path of pdjdbc2.jar>" format.

   Example 1 (For HiRDB/Run Time)

   add.class.path=<HiRDB/Run Time installation directory>/client/lib/pdjdbc2.jar

   Example 2 (For HiRDB/Single Server)

   add.class.path=<HiRDB/Single Server installation directory>#/client/lib/pdjdbc2.jar

   Note#

   <HiRDB installation directory> is the directory named hirdb_s.

   You can also specify this definition from the management portal. Specify the class path in the extension parameter on the [J2EE Container Settings] screen of the logical J2EE server specified in "Environment Settings of Logical Servers" in the management portal. The value set up here is applied to the option definition file for J2EE servers (usrconf.cfg).

   For details on the option definition file for J2EE servers, see "2.3 usrconf.cfg (Option definition file for J2EE servers)" in "Application Server Definition Reference Guide". For details on the settings specified in the "Environment Settings of Logical Servers", see "10. Environment Settings of Logical Servers" in "Application Server Management Portal Operation Guide".

3. Specify the JAR file for HiRDB Type4 JDBC Driver (pdjdbc2.jar) as the class path in the extension parameter on the [J2EE Container Settings] screen of the logical J2EE server specified in "Environment Settings of Logical Servers" in the management portal. At this time, specify in the "add.class.path=<Path of pdjdbc2.jar>" format.

   The value set up here is applied to the option definition file for J2EE servers (usrconf.cfg).

   For details on specifying settings in the "Environment Settings of Logical Servers", see "10. Environment Settings of Logical Servers" in "Application Server Management Portal Operation Guide".

   Example 1 (For HiRDB/Run Time)

   add.class.path=<HiRDB/Run Time installation directory>/client/lib/pdjdbc2.jar

   Example 2 (For HiRDB/Single Server)

   add.class.path=<HiRDB/Single Server installation directory>#/client/lib/pdjdbc2.jar

   Note#

   <HiRDB installation directory> is the directory named hirdb_s.

4. Specify the JAR file for HiRDB Type4 JDBC Driver (pdjdbc2.jar) as the class path in HCSC_ADDCLASSPATH of the HCSC-Messaging command definition file.

   For details on the HCSC-Messaging command definition file, see "HCSC-Messaging command definition file" in "Service Platform Reference Guide".

(b) Setting up Oracle JDBC Thin Driver

For details on setting up Oracle JDBC Thin Driver, see "4.1.7 Setting up the database connection environment (in Oracle)" in "Application Server System Setup and Operation Guide" or the manual for the database being used.

You must specify the following settings in order to use the HCSC server. Note that the type of Oracle JDBC Thin Driver differs depending on the Oracle version in use; therefore, take care when you specify the class path of the JAR file for Oracle JDBC Thin Driver.

1. Specify the JAR file for Oracle JDBC Thin Driver as the class path in <Service Platforminstallation directory>/manager/config/mserver.cfg file. At this time, specify the file in the "web.add.class.path=<Path of Oracle JDBC Thin Driver>" format.

   Example (For Oracle 11g (JDK6))

   web.add.class.path=<Oracle Client installation directory>/jdbc/lib/ojdbc6.jar

2. Specify the JAR file for Oracle JDBC Thin Driver as the class path in the option definition file for J2EE servers (usrconf.cfg). At this time, specify the file in the "add.class.path=<Path of Oracle JDBC Thin Driver>" format.

   Example (For Oracle 11g (JDK6))

   add.class.path=<Oracle Client installation directory>/jdbc/lib/ojdbc6.jar

   You can also specify this definition from the management portal. Specify the class path in the extension parameter on the [J2EE Container Settings] screen of the logical J2EE server specified in "Environment Settings of Logical Servers" in the management portal. The value set up here is applied to the option definition file for J2EE servers (usrconf.cfg).

   For details on the option definition file for J2EE servers, see "2.3 usrconf.cfg (Option definition file for J2EE servers)" in "Application Server Definition Reference Guide". For details on the settings specified in the "Environment Settings of Logical Servers", see "10. Environment Settings of Logical Servers" in "Application Server Management Portal Operation Guide".

3. Specify the JAR file for Oracle JDBC Thin Driver as the class path in the extension parameter on the [J2EE Container Settings] screen of the logical J2EE server specified in "Environment Settings of Logical Servers" in the management portal. At this time, specify in the "add.class.path=<Path of Oracle JDBC Thin Driver>" format.

   The value set up here is applied to the option definition file for J2EE servers (usrconf.cfg).

   For details on specifying settings in the "Environment Settings of Logical Servers", see "10. Environment Settings of Logical Servers" in "Application Server Management Portal Operation Guide".

   Example (For Oracle 11g (JDK6))

   add.class.path=<Oracle Client installation directory>/jdbc/lib/ojdbc6.jar

4. Specify the JAR file for Oracle JDBC Thin Driver as the class path in HCSC_ADDCLASSPATH of the HCSC-Messaging command definition file.

   For details on the HCSC-Messaging command definition file, see "HCSC-Messaging command definition file" in "Service Platform Reference Guide".

(8) Setting up DB Connector(When Reliable Messaging is used)

HCSC server uses DB Connector to connect to the database. There are cases in which database access is managed or not managed in the transaction depending on the processing timing and table types; therefore, you must prepare two DB Connectors, DB Connector whose transaction support type is XATransaction or LocalTransaction, and DB Connector whose transaction support type is NoTransaction.

Note that for DB Connector whose transaction support type is XATransaction or LocalTransaction, use DB Connector that can be integrated with Reliable Messaging in order to improve the processing performance.

Specify the display name for each DB Connector in "dbcon-xadisplayname" and "dbcon-nodisplayname" of the HCSC server setup definition file. For details on the HCSC server setup definition file, see "HCSC server setup definition file" in "Service Platform Reference Guide".

(a) Importing DB Connector

You must select the DB Connector to be imported after considering the usage conditions. The following table lists and describes how to select the RAR file to be imported.

Table 3–7: TableHow to select the RAR file to be imported (When Reliable Messaging is used)

Properties in the HCSC server setup definition file	Used database	Usage of light transaction functionality	
		Used	Not used
dbcon-xadisplayname	HiRDB (Version 8 or Version 9)#	DBConnector_HiRDB_Type4_CP_Cosminexus_RM.rar	DBConnector_HiRDB_Type4_XA_Cosminexus_RM.rar
	Oracle	DBConnector_Oracle_CP_Cosminexus_RM.rar	DBConnector_Oracle_XA_Cosminexus_RM.rar
dbcon-nodisplayname	HiRDB (Version 8 or Version 9)#	DBConnector_HiRDB_Type4_CP.rar	
	Oracle	DBConnector_Oracle_CP.rar	

Note#

When HiRDB Type4 JDBC Driver is used as the JDBC driver.

For details on how to import DB Connector, see "4.2 Settings for connecting to the database" in "Application Server Application Setup Guide". For the property definitions, see "4.1 Connector property file" in "Application Server Application and Resource Definition Reference Guide".

For details on the light transaction functionality, see "3.14.5 Light transaction" in "Application Server Common Container Functionality Guide". For details on how to set up the functionality, see "10.9.7 Setting up a transaction" in "Application Server Management Portal Operation Guide".

When a DB adapter is used, import DB Connector that is used by the DB adapter. The following table lists and describes how to select the RAR file to be imported.

Table 3–8: Table How to select the RAR file to be imported (When a DB adapter is used)

Used JDBC driver	Used database	Usage of light transaction functionality	
		Used	Not used
HiRDB TYPE4 JDBC Driver	HiRDB (Version 8 or Version 9)	DBConnector_HiRDB_Type4_CP.rar	DBConnector_HiRDB_Type4_XA.rar
Oracle JDBC Thin Driver	Oracle	DBConnector_Oracle_CP.rar	DBConnector_Oracle_XA.rar

(b) Defining properties

After you import DB Connector, see "4.1 Connector Property File" in "Application Server Application and Resource Definition Reference Guide" to define the properties. However, you must specify the contents listed in the following table in the properties.

Important note

The transaction support type (value specified in the <transaction-support> tag) must be the same in DB Connector that can be integrated with Reliable Messaging and DB Connector used with the DB adapter.

The value specified in the <transaction-support> tag differs as follows depending on whether a light transaction or global transaction is applied:

- When a light transaction is applied to the J2EE server
  LocalTransaction
- When a global transaction is applied to the J2EE server
  XATransaction

Table 3–9: Table DB Connector property file settings to be specified in dbcon-xadisplayname (Oracle)

Settings	Set value
<display-name> tag	DB Connector display name
databaseName property specified in the <config-property> tag	Database name#1
bufSize property specified in the <config-property> tag	Value greater than the maximum message length used in the system#2
<transaction-support> tag	XATransaction#3
	LocalTransaction#4

Note#1

The set value differs depending on DB Connector to be used. For details on the set values, see "4.1 Connector Property File" in "Application Server Application and Resource Definition Reference Guide". You must also set up the information required for connecting to the database together with this value.

Note#2

The DB Connectors to be used are as follows. Specify these DB Connectors when REAL is specified in the LONGVARBINARY_Access property.

・DBConnector_DABJ_XA_Cosminexus_RM.rar

・DBConnector_DABJ_CP_Cosminexus_RM.rar

Note#3

When the light transaction functionality is not used, specify this value for the following DB Connectors:

・DBConnector_DABJ_XA_Cosminexus_RM.rar

・DBConnector_Oracle_XA_Cosminexus_RM.rar

Note#4

When the light transaction functionality is used, specify this value for the following DB Connectors:

・DBConnector_DABJ_CP_Cosminexus_RM.rar

・DBConnector_Oracle_CP_Cosminexus_RM.rar

Table 3–10: Table DB Connector property file settings to be specified in dbcon-xadisplayname (HiRDB Type4)

Settings	Set value
<display-name> tag	DB Connector display name
maxBinarySize property specified in the <config-property> tag	Value greater than the maximum message length used in the system#1
<transaction-support> tag	XATransaction#2
	LocalTransaction#3

Note#1

Specify this value when REAL is specified in the LONGVARBINARY_Access property. Make sure you specify a value other than 0.

Note#2

When the light transaction functionality is not used, specify this value for the following DB Connectors:

・DBConnector_HiRDB_Type4_XA_Cosminexus_RM.rar

Note#3

When the light transaction functionality is used, specify this value for the following DB Connectors:

・DBConnector_HiRDB_Type4_CP_Cosminexus_RM.rar

Note

Set up the information required for connecting to the database. For details on the set values, see "4.1 Connector Property File" in "Application Server Application and Resource Definition Reference Guide".

Table 3–11: Table DB Connector property file settings to be specified in dbcon-nodisplayname (Oracle)

Settings	Set value
<display-name> tag	DB Connector display name
databaseName property specified in the <config-property> tag	Database name#1
bufSize property specified in the <config-property> tag	Value greater than the maximum message length used in the system#2
<transaction-support> tag	NoTransaction#3

Note#1

The set value differs depending on database to be used. For details on the set values, see "4.1 Connector Property File" in "Application Server Application and Resource Definition Reference Guide". You must also set up the information required for connecting to the database together with this value.

Note#2

The DB Connectors to be used are as follows. Specify these DB Connectors when REAL is specified in the LONGVARBINARY_Access property.

・DBConnector_DABJ_CP.rar

Note#3

Specify this value when the following DB Connectors are used:

・DBConnector_DABJ_CP.rar

・DBConnector_Oracle_CP.rar

Table 3–12: Table DB Connector property file settings to be specified in dbcon-nodisplayname (HiRDB Type4)

Settings	Set value
<display-name> tag	DB Connector display name
maxBinarySize property specified in the <config-property> tag	Value greater than the maximum message length used in the system#1
<transaction-support> tag	NoTransaction#2

Note#1

Specify this value when REAL is specified in the LONGVARBINARY_Access property. Make sure you specify a value other than 0.

Note#2

Specify this value when the following DB Connectors are used:

・DBConnector_HiRDB_Type4_CP.rar

Note

Set up the information required for connecting to the database. For details on the set values, see "4.1 Connector Property File" in "Application Server Application and Resource Definition Reference Guide".

Table 3–13: Table Connector property file settings to be specified when a DB adapter is used

Settings	Set value
<display-name> tag	DB Connector display name#1

Settings	Set value
databaseName property specified in the <config-property> tag	Database name#2
<transaction-support> tag	XATransaction
	LocalTransaction

Note#1

You can also set up this value in the <linked-to> tag of the HITACHI Application Integrated Property File of the DB adapter. For details on the HITACHI Application Integrated Property File, see "3.3.5 Defining a DB adapter" in "Service Platform Reception and Adapter Definition Guide".

Note#2

The set value differs depending on DB Connector to be used. For details on the set values, see "4.1 Connector Property File" in "Application Server Application and Resource Definition Reference Guide".

(9) Setting up Reliable Messaging

Set up Reliable Messaging. For details on the operations, see "3. System Setup" in "Reliable Messaging". To customize the properties among the setup operations, use the following methods:

(a) Setting up the configuration properties for Reliable Messaging

The following table lists and describes the configuration properties to be set up and the values to be specified. In the authentication information (User and Password), specify the user name and password of the connected user to be used by Reliable Messaging for accessing HiRDB or Oracle.

Table 3–14: Table Configuration properties to be set up and the values to be specified

Property name	Specified content	Set value
RMSystemName	System name	Specify a system name that is unique in the entire system to be integrated.
RMLinkedDBConnectorName	Display Name of DB Connector to be integrated	Specify the display Name of DB Connector to be integrated.
RMSHConnectFlag	Existence of a shared queue for reception to be used when applications are integrated between multiple systems by using a shared queue	When you use standard asynchronous reception (MDB (DB queue)), specify "true". When you do not use standard asynchronous reception (MDB (DB queue)), or when you are using a database in which a DB queue cannot be used, specify "false".
RMTRConnectFlag	Usage of transmit between queues	Specify "true".
RMMaxDeliveryNum	Maximum delivery count	Set up a value other than 0 (1 to 512) (recommended value: 10)
RMDeadMessageQueueName	Name of dead message queue	Set up an identifier from 1 to 20 characters. Make sure you use the dead message queue. Use the dead message queue as the local queue.

(b) Points to be considered

- Do not change the value of the configuration property "RMWaitRestoration". Operate the property with the default value "true" for Reliable Messaging.
- The dead message queue specified in the dead message queue name "RMDeadMessageQueueName" is a special queue to which the messages, where the delivery count has reached the maximum value and the service components are not invoked, are moved when you use asynchronous standard receptions (MDB (WS-R) and MDB (DB queue)) and asynchronous service adapters (MDB (WS-R) adapter and MDB (DB queue) adapter).

If the dead message queue name is not specified and the dead message queue is not created, note that the processing for invoking the service components is re-executed infinitely.

Create the queue to be used as the dead message queue after Reliable Messaging is set up and starts for the first time.

- When you use Oracle as the database, you cannot use asynchronous standard reception (MDB (DB queue)) and asynchronous MDB (DB queue) adapter.

(10) Setting up the TP1 inbound adapter

When using TP1/ RPC reception, set up the TP1 inbound adapter. If the J2EE server has been set up, you can set up the adapter at any time.

For details on the set up of TP1 inbound adapter, see "4.12.2 Setting up a resource adapter" in "Application Server Common Container Functionality Guide". Note that to set up the TP1 inbound adapter, you must set up the HITACHI Connector property definition file.

(11) Setting up Service Coordinator-Manager

As and when required, see "*2.4 Settings Related to the Operating Environment*" to set up Service Coordinator-Manager.

(12) Setting up DB Connector (When Reliable Messaging is not used)

HCSC server uses DB Connector to connect to the database. There are cases in which database access is managed or not managed in the transaction depending on the processing timing and table types; therefore, you must prepare two DB Connectors, DB Connector whose transaction support type is XATransaction or LocalTransaction, and DB Connector whose transaction support type is NoTransaction.

Note that for DB Connector whose transaction support type is XATransaction or LocalTransaction; use DB Connector that can be integrated with Reliable Messaging in order to improve the processing performance.

Specify the display name for each DB Connector in "dbcon-xadisplayname" and "dbcon-nodisplayname" of the HCSC server setup definition file. For details on the HCSC server setup definition file, see "HCSC server setup definition file" in "Service Platform Reference Guide".

(a) Importing DB Connector

You must select the DB Connector to be imported after considering the usage conditions. The following table lists and describes how to select the RAR file to be imported.

Table 3–15: Table How to select the RAR file to be imported (When database is used and Reliable Messaging is not used)

Properties in the HCSC server setup definition file	Used database	RAR files to be imported
dbcon-xadisplayname	HiRDB (Version 8 or Version 9)#	• When the light transaction functionality is used DBConnector_HiRDB_Type4_CP.rar • When the light transaction functionality is not used DBConnector_HiRDB_Type4_XA.rar
	Oracle	• When the light transaction functionality is used DBConnector_Oracle_CP.rar • When the light transaction functionality is not used DBConnector_Oracle_XA.rar
dbcon-nodisplayname	HiRDB (Version 8 or Version 9)#	DBConnector_HiRDB_Type4_CP.rar
	Oracle	DBConnector_Oracle_CP.rar

Note#

When using HiRDB Type4 JDBC Driver in JDBC Driver.

When a DB adapter is used, import DB Connector that is used by the DB adapter. The following table lists and describes how to select the RAR file to be imported.

Table 3–16: Table How to select the RAR file to be imported (When a DB adapter is used)

Used JDBC driver	Used database	RAR files to be imported
HiRDB TYPE4 JDBC Driver	HiRDB (Version 8 or Version 9)	• When the light transaction functionality is used DBConnector_HiRDB_Type4_CP.rar • When the light transaction functionality is not used DBConnector_HiRDB_Type4_XA.rar
Oracle JDBC Thin Driver	Oracle	• When the light transaction functionality is used DBConnector_Oracle_CP.rar • When the light transaction functionality is not used DBConnector_Oracle_XA.rar

For details on how to import DB Connector, see "4.2 Settings for connecting to the database" in "Application Server Application Setup Guide". For the property definitions, see "4.1 Connector property file" in "Application Server Application and Resource Definition Reference Guide".

For details on the light transaction functionality, see "3.14.5 Light transaction" in "Application Server Common Container Functionality Guide". For details on how to set up the functionality, see "10.9.7 Setting up a transaction" in "Application Server Management Portal Operation Guide".

(b) Defining properties

After you import DB Connector, see "4.1 Connector Property File" in "Application Server Application and Resource Definition Reference Guide" to define the properties. However, you must specify the contents listed in the following table in the properties.

Table 3–17: Table DB Connector property file settings to be specified in dbcon-xadisplayname (Oracle)

Settings		Set value
<display-name> tag		DB Connector display name
databaseName property specified in the <config-property> tag		Database name[#1]
bufSize property specified in the <config-property> tag		Value greater than the maximum message length used in the system[#2]
<transaction-support> tag	When the light transaction functionality is not used	XATransaction[#3]
	When the light transaction functionality is used	LocalTransaction[#4]

Note#1

The set value differs depending on DB Connector to be used. For details on the set values, see "4.1 Connector Property File" in "Application Server Application and Resource Definition Reference Guide". You must also set up the information required for connecting to the database together with this value.

Note#2

Use the following DB Connectors. Specify these DB Connectors when REAL is specified in the LONGVARBINARY_Access property.

・DBConnector_DABJ_XA.rar

・DBConnector_DABJ_CP.rar

Note#3

Specify this value for the following DB Connectors:

・DBConnector_DABJ_XA.rar

・DBConnector_Oracle_XA.rar

Note#4

Specify this value for the following DB Connectors:

・DBConnector_DABJ_CP.rar

・DBConnector_Oracle_CP.rar

Table 3–18: Table DB Connector property file settings to be specified in dbcon-xadisplayname (HiRDB Type4)

Settings		Set value
<display-name> tag		DB Connector display name
maxBinarySize property specified in the <config-property> tag		Value greater than the maximum message length used in the system[#1]
<transaction-support> tag	When the light transaction functionality is not used	XATransaction[#2]
	When the light transaction functionality is used	LocalTransaction[#3]

Note#1

Specify this value when REAL is specified in the LONGVARBINARY_Access property. Make sure you specify a value other than 0.

Note#2

Specify this value for the following DB Connector:

・DBConnector_HiRDB_Type4_XA.rar

Note#3

Specify this value for the following DB Connector:

・DBConnector_HiRDB_Type4_CP.rar

Note

Set up the information required for connecting to the database. For details on the set values, see "4.1 Connector Property File" in "Application Server Application and Resource Definition Reference Guide".

Table 3–19: Table DB Connector property file settings to be specified in dbcon-nodisplayname (Oracle)

Settings	Set value
<display-name> tag	DB Connector display name
databaseName property specified in the <config-property> tag	Database name[#1]
bufSize property specified in the <config-property> tag	Value greater than the maximum message length used in the system[#2]
<transaction-support> tag	NoTransaction[#3]

Note#1

The set value differs depending on database to be used. For details on the set values, see "4.1 Connector Property File" in "Application Server Application and Resource Definition Reference Guide". You must also set up the information required for connecting to the database together with this value.

Note#2

Use the following DB Connectors. Specify these DB Connectors when REAL is specified in the LONGVARBINARY_Access property.

・DBConnector_DABJ_CP.rar

Note#3

Specify this value when the following DB Connectors are used:

・DBConnector_DABJ_CP.rar

・DBConnector_Oracle_CP.rar

Table 3–20: Table DB Connector property file settings to be specified in dbcon-nodisplayname (HiRDB Type4)

Settings	Set value
<display-name> tag	DB Connector display name
maxBinarySize property specified in the <config-property> tag	Value greater than the maximum message length used in the system#1
<transaction-support> tag	NoTransaction#2

Note#1

Specify this value when REAL is specified in the LONGVARBINARY_Access property. Make sure you specify a value other than 0.

Note#2

Specify this value when the following DB Connectors are used:

・DBConnector_HiRDB_Type4_CP.rar

Note

Set up the information required for connecting to the database. For details on the set values, see "4.1 Connector Property File" in "Application Server Application and Resource Definition Reference Guide".

Table 3–21: Table Connector property file settings to be specified when a DB adapter is used

Settings	Set value
<display-name> tag	DB Connector display name#1
databaseName property specified in the <config-property> tag	Database name#2
<transaction-support> tag	XATransaction
	LocalTransaction

Note#1

You can also set up this value in the <linked-to> tag of the HITACHI Application Integrated Property File of the DB adapter. For details on the HITACHI Application Integrated Property File, see "3.3.5 Defining a DB adapter" in "Service Platform Reception and Adapter Definition Guide".

Note#2

The set value differs depending on DB Connector to be used. For details on the set values, see "4.1 Connector Property File" in "Application Server Application and Resource Definition Reference Guide".

3.1.3 Setting up an HCSC server

To deploy the service adapters, business processes, and user-defined receptions to the HCSC server and set up the execution environment, you must first set up the HCSC server. When you set up the HCSC server, you can also set up the cluster.

This subsection describes the preconditions for setting up the HCSC server and explains how to perform the setup.

Reference note

It is recommended that you specify the HCSC server definition information after you set up the HCSC server and before you start the HCSC server. For details on how to define the HCSC server, see "*3.1.4 Setting up the HCSC server definition information*".

(1) Preconditions

The following conditions must be satisfied to set up the HCSC server:

- The following processes are running on the execution environment machine where the HCSC server will be set up:
  - Administration Agent

- Management Server
- J2EE server
- PRF
- HTTP Server

For details on how to start Administration Agent, Management Server, J2EE server, and PRF, see "Application Server System Setup and Operation Guide". For details on how to start HTTP Server, see "*5.3.5 Starting HTTP Server*".

- Reliable Messaging, DB Connector, and DB client are set up and running on the execution environment machine where the HCSC server will be set up.
- The usage of database and Reliable Messaging in the same cluster is identical.
- The SOAP modes of all the HCSC servers in the same repository are identical.
- The HCSC server configuration definition file and HCSC server setup definition file are created.

  For details on how to create the HCSC server configuration definition file, see "*2.3.1 Setting HCSC server configuration definition file*", and for details on the file contents, see "HCSC server configuration definition file" in "Service Platform Reference Guide".

  For details on how to create the HCSC server setup definition file, see "*2.3.2 Setting HCSC server setup definition file*", and for details on the file contents, see "*HCSC server setup definition file*" in "Service Platform Reference Guide".
- When configuring a cluster in the HCSC server to be set up and the HCSC server that is already set up, the same settings are specified for the items that must have the same settings in the HCSC server configuration definition file and HCSC server setup definition file.

  For details on the items in the HCSC server configuration definition file and HCSC server setup definition file that must have the same settings between the HCSC servers configuring the cluster, see "*2.5.1(1) Setting up an execution environment*" for a load-balancing cluster configuration, and see "*2.6.1(1) Setting up an execution environment (executing node and standby node)*" for a high availability cluster configuration.
- The J2EE server is restarted to reset up the HCSC server after the server is unset up.

! Important note

If a queue with the same name as the following queue names used in asynchronous receptions exists in the J2EE server where the HCSC server is set up, the setup fails. After the setup fails, the queue with the same name is deleted.

- For an independent configuration and load-balancing cluster
  CSC<HCSC server name>ACPT_RCVQ
  CSC<HCSC server name>ACPT_DBQ
- For an HA cluster
  CSC<cluster name>ACPT_RCVQ
  CSC<cluster name>ACPT_DBQ

Therefore, make sure that these queues with the queue names used in asynchronous receptions do not exist and then implement setup.

---

(2) How to perform the setup

To set up the HCSC server, execute the cscsvsetup command in the operating environment.

For details on the cscsvsetup command, see "cscsvsetup (Setting up the HCSC server) " in "Service Platform Reference Guide".

The contents to be set up differ depending on whether a single HCSC server is set up, or whether the server is set up to configure a cluster with an already set up HCSC server.

! Important note

- If a communication failure or timeout occurs during the execution of the command, the processing might be concluded in the execution environment. Therefore, obtain the HCSC server setup information and re-execute the cscsvsetup command according to the obtained information. For details on how to obtain the HCSC server setup information, see "*5.3.14 Checking the HCSC server setup information*". Note that when obtaining the HCSC server setup information, you must use the -host option in the cscutil command. For details on the cscutil command, see "cscutil (Various operations) " in "Service Platform Reference Guide".

- The cluster name and HCSC server name are not case sensitive, so specify a unique name. However, you can omit the cluster name when you set up the HCSC server.
- When using a database for setup, do not execute cscsvsetup command (setting up the HCSC server) or cscsvunsetup command (unsetting up the HCSC server) on multiple machines at the same time even if the operating environment repositories are different.

(a) When setting up an independent HCSC server

Specify the cluster name in the -cluster option. However, this server is an independent HCSC server, so a configuration of clusters is not formed at this stage. When you set up other HCSC servers, you can configure a cluster by specifying and setting up the cluster names specified here.

```
cscsvsetup -user <login user ID> -pass <login password> -csc <HCSC server name> -cluster
<cluster name> -propfile <Name of HCSC server configuration definition file>
```

Note that if you omit the cluster name, the HCSC server name specified in the -csc option is set up as the cluster name.

```
cscsvsetup -user <login user ID> -pass <login password> -csc <HCSC server name> -propfile
<Name of HCSC server configuration definition file>
```

(b) To configure a cluster with an already set up HCSC server

In the -cluster option, specify the cluster name for adding the HCSC server.

```
cscsvsetup -user <login user ID> -pass <login password> -csc <HCSC server name> -cluster
<Cluster name for adding the HSCS server> -propfile <Name of HCSC server configuration
definition file>
```

(3) Adding and changing the setup information

If you re-execute the setup described in "*(2) How to perform the setup*" for the HCSC server that is already set up, you can add or change the set up information.

To add or change the HCSC server setup information, the HCSC server, service adapters, business processes, and user-defined receptions must be stopped already.

For details on how to check the status of the HCSC server, service adapters, business processes, and user-defined receptions, see "*5.3.15 Checking the HCSC server information*", "*5.3.17 Checking the service adapter information*", "*5.3.18 Checking the business process information*", and "*5.3.19 Checking the information of user-defined reception*" respectively.

The information that you can add or change is as follows:

Information that can be added

- Types of standard reception

  You can add and set up the synchronous (Web service/ SessionBean), and asynchronous (MDB (WS-R)/ MDB and (DB queue)) standard receptions. To change or delete the information of the already set up standard reception types, execute unsetup and then reset up.

Information that can be changed

- Location information for the synchronous standard reception (Web service)

  This is the Web server location information used for the synchronous standard reception (Web service). You can change the Web server IP address, port number, and protocol.
- Location information for the asynchronous (MDB (WS-R)) standard reception

  This is the Web server location information used for the asynchronous (MDB (WS-R)) standard reception. You can change the Web server IP address, port number, and protocol.
- Location information for the synchronous (SessionBean) standard reception

  This is the NameServer location information used for the synchronous (SessionBean) standard reception. You can change the NameServer IP address and port number.
- Managerlocation information

You can change the IP address and port number for accessing Manager.

Important note

To add or change information other than that mentioned above, you must execute unsetup and resetup of the HCSC server. If you add or change other information without executing HCSC server unsetup, and then implement setup, the additions and changes are ignored.

3.1.4 Setting up the HCSC server definition information

This subsection describes the preconditions for setting up the HCSC server definition information, specified in the HCSC server runtime definition file, and explains how to set up the information.

(1) Preconditions

- HCSC server is stopped or running

  For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".
- HCSC server runtime definition file has been created

  For details on how to create the HCSC server runtime definition file, see "*2.3.3 Setting HCSC server runtime definition file*", and for details on the file contents, see "HCSC server runtime definition file" in "Service Platform Reference Guide".

(2) How to set up the information

To set up the HCSC server definition information that is specified in the HCSC server runtime definition file, execute the cscsvconfig command in the operating environment.

For details on the cscsvconfig command, see "cscsvconfig (HCSC server runtime definition) " in "Service Platform Reference Guide".

The execution format of the cscsvconfig command is as follows:

To set up the definitions for the HCSC servers in a cluster in a batch

Specify the cluster name and execute the command.

The contents of the definition file specified in the -propfile option are set up for the HCSC servers in the cluster specified in the -cluster option.

```
cscsvconfig -user <login user ID> -pass <login password> -cluster <cluster name> -operation
set -propfile <Name of the HCSC server runtime definition file>
```

To set up the definitions for the specified HCSC server

Specify the HCSC server name and execute the command.

The contents of the definition file specified in the -propfile option are set up for the HCSC server specified in the -csc option.

```
cscsvconfig -user <login user ID> -pass <login password> -csc <HCSC server name> -operation
set -propfile <Name of the HCSC server runtime definition file>
```

Important note

The set up definition information is applied when the HCSC server is restarted. Note that the reception-related definition information is applied when the reception starts.

3.1.5 Checking the contents defined in the HCSC server

This subsection describes the preconditions for checking the definition contents set in the HCSC server, and explains how to check the contents.

(1) Preconditions

The HCSC server must be stopped or running.

For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".

(2) How to check the contents

To check the contents defined in the HCSC server, execute the cscsvconfig command in the operating environment.

For details on the cscsvconfig command, see "cscsvconfig (HCSC server runtime definition) " in "Service Platform Reference Guide".

The execution format of cscsvconfig command is as follows:

```
cscsvconfig -user <login user ID> -pass <login password> -csc <HCSC server name> -operation
get
```

The defined contents set up in the HCSC server are output to standard output. As and when required, redirect the output contents to a file.

3.1.6 Changing the service information

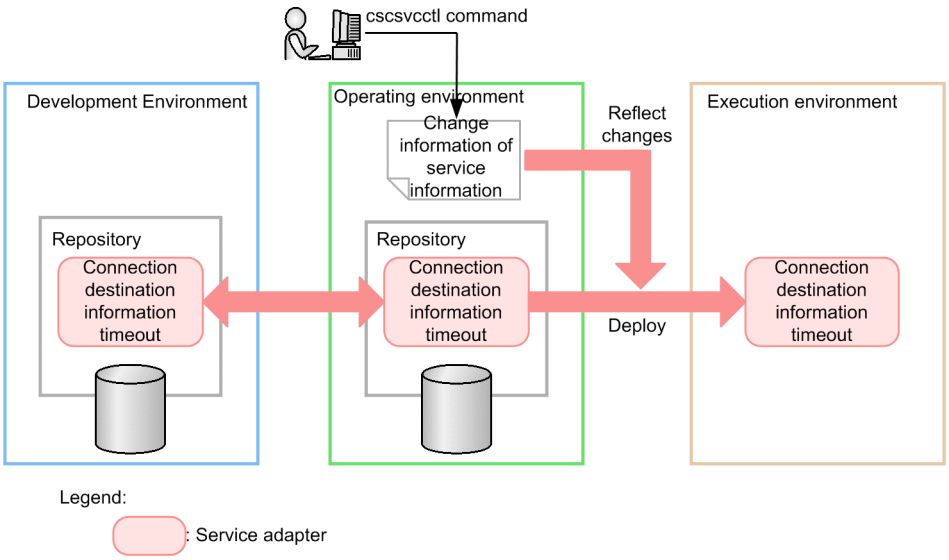
When a service adapter is developed in the development environment, you set up the connection destination information, timeout values, and so on for the service adapter. In the operating environment, these set values are considered as the **service information** and you can change the values to environment-appropriate values.

The changed service information is not applied to the repository. The changed service information is stored in the operating environment, and is applied when the service adapter is deployed in the execution environment. Therefore, you can manage the service information independent of the development environment.

Note that the service information set up in the operating environment is valid as long as the service information is not deleted. Even if the service adapter information is changed in the development environment, unless you delete the service information set up in the operating environment, the service information set up in the operating environment is applied to the service adapter.

The following figure shows the handling of the service information in each environment.

Figure 3–5: Figure Flow from the set up to the changing of the service information



This subsection describes the preconditions for changing the service information and explains how to change the information.

(1) Preconditions

To change the service information, the following conditions must be satisfied:

- The repository is not shared
- In all the HCSC servers in the cluster, the service adapter that changes the service information is in an un-deployed state

(2) How to change the information

To change the service information, execute the cscsvcctl command in the operating environment.

For details on the cscsvcctl command, see "cscsvcctl (Managing the service information) " in "Service Platform Reference Guide".

The execution format of the command differs depending on whether the service information is changed in a batch or whether the specified service information is changed individually.

(a) To change the service information in a batch

To change the service information in a batch:

1. In the -getfile option, specify the file name (any) to output the service information and then execute the command.

```
cscsvcctl -user <login user ID> -pass <login password> -getfile <name of the service-
information change definition file>
```

2. Define the change contents in the obtained service-information change definition file.

   The values set for the proxy server user ID/ password, and basic authentication user ID/ password are output to the obtained service-information change definition file, as follows:

   - If the values are specified: The value has already been set.
   - If the values are not specified: Blank

   Note that if you do not want to change the proxy server user ID/password and basic authentication user ID/ password, define the obtained value as is in the -getfile option. To use basic authentication, set up all the basic authentication-related parameters (usability, user name, and password).

   For details on the service-information change definition file, see "Service-information change definition file" in "Service Platform Reference Guide".

3. Specify the service-information change definition file in the -setfile option and execute the command.

```
cscsvcctl -user <login user ID> -pass <login password> -setfile <name of the service-
information change definition file>
```

(b) To change the specified service information individually

To change the specified service information individually, specify the service information you want to change in the -props option, and then execute the command.

```
cscsvcctl -user <login user ID> -pass <login password> -cluster <cluster name> -name
<Service ID of the service adapter> -props <Property>
```

To use basic authentication, set up all the basic authentication-related parameters (usability, user name, and password) of the service-information change definition file.

For details on the service-information change definition file, see "Service-information change definition file" in "Service Platform Reference Guide".

(3) Deleting the service information

The service information changed with the cscsvcctl command is deleted in the following cases:

- When a line is commented out by coding "#" at the beginning of the service information line to be deleted, and then the service information is overwritten by specifying the -setfile option in the cscsvcctl command
- When all the HCSC servers in the cluster are unset

- When the service adapter that changed the service information with the cscsvcctl command is deleted or set to private# in the development environment, and imported into the operating environment

  However, the service information is not deleted if a service adapter, which has the same service ID and type as the service adapter deleted in the development environment, is imported.

  Note#

  Means that the HCSC components are deleted (deployment definition is deleted) from the HCSC server, and the system configuration definition is updated.

3.1.7 Checking the service information

This subsection describes the preconditions for checking the service information, and explains how to check the information.

(1) Preconditions

The repository is not shared

(2) How to check the information

To check the changed service information, execute the cscsvcls command in the operating environment.

For details on the cscsvcls command, see "cscsvcls (Displaying the service information) " in "Service Platform Reference Guide".

To check the service information that is currently valid, execute the cscsvcls command without specifying an option.

```
cscsvcls -user <login user ID> -pass <login password>
```

To check the changed service information and the service information set in the development environment, execute the cscsvcls command by specifying the -detail option.

```
cscsvcls -user <login user ID> -pass <login password> -detail
```

Note that, if the user proxy server user ID/ password, and basic authentication user ID/ password are set up, "The value has already been set." is displayed as the set value when the service information is output.

3.1.8 Deploying a service adapter

This subsection describes the preconditions for deploying the service adapter in the execution environment, and explains how to deploy the service adapter.

Note that the series of processing to deploy and start the HCSC components in the HCSC server, can also be executed in the development environment in a batch. However, batch execution is performed during system development or from unit testing to integration testing. For details, see " 7.5 Batch execution of the processing for deploying and starting the HCSC components on the HCSC server" in "Service Platform Basic Development Guide".

(1) Preconditions

To deploy the service adapter, the following conditions must be satisfied:

- The HCSC server in the deployment-destination execution environment is running

  For details on how to check the status of the HCSC server, see "5.3.15 Checking the HCSC server information".

- In the following cases, the HCSC server is restarted before deployment
  - When the service component type (MDB (WS-R) adapter or MDB and (DB queue) adapter) of the service adapter to be deployed is changed while retaining the same name as the service ID of the deleted MDB (WS-R) adapter or MDB and (DB queue) adapter

- When the queue information (JMS message type, maximum number of messages, and RD area of the transmit queue creation destination) of the service adapter to be deployed is changed while retaining the same name as the service ID of the deleted MDB (WS-R) adapter
- When the service adapter with a service ID that only has a case difference with the service ID of the is deleted MDB (WS-R) adapter or MDB and (DB queue) adapter, is deployed

If the service adapter is deployed without restarting the HCSC server, the information defined in the newly deployed service adapter is ignored and the operations might not be normal.

(2) How to deploy the service adapter

To deploy the service adapter, execute the csccompodeploy command in the operating environment.

For details on the csccompodeploy command, see "csccompodeploy (Deploying the HCSC components) " in "Service Platform Reference Guide".

The execution format of the command differs depending on whether all the service adapters are deployed in a batch, or whether only the specified service adapter is deployed.

! Important note

When the service adapter is deployed, do not use the service ID of the service adapter that only has a difference of case with the service ID of the deployed service adapter and business process, or the reception ID of the user-defined reception. If such a name is used, the service adapter cannot be deployed.

(a) To deploy all the service adapters in a batch

Deploy all the service adapters on the HCSC server or cluster in a batch.

The execution format of the command differs depending on whether the service adapter deployment destination is a single HCSC server, or all the HCSC servers configuring the cluster.

To deploy all the service adapters on a single HCSC server

Execute the command by specifying the name of the HCSC server and the -all option.

All the service adapters, which are not deployed, are deployed on the HCSC server specified in the -csc option (all the business processes and user-defined receptions that are not deployed are also deployed at the same time).

```
csccompodeploy -user <login user ID> -pass <login password> -csc <HCSC server name> -all
```

To deploy all the service adapters on all the HCSC servers in the cluster

Execute the command by specifying the cluster name and the -all option.

All the service adapters, which are not deployed, are deployed on all the HCSC servers in the cluster specified in the -cluster option (all the business processes and user-defined receptions that are not deployed are also deployed at the same time).

```
csccompodeploy -user <login user ID> -pass <login password> -cluster <cluster name> -all
```

! Important note

If the service adapters, business processes, and user-defined receptions cannot be deployed because the -all option was specified, even if un-deployed service adapters, business processes, and user-defined receptions exist, they are ignored and the command terminates. After executing the command, use the cscrepls command to check the deployment status.

For details on the cscrepls command, see "cscrepls (Displaying the repository information) " in "Service Platform Reference Guide".

(b) To deploy the specified service adapter only

Deploy only the specified service adapter on the HCSC server or cluster.

The execution format of the command differs depending on whether the service adapter deployment destination is a single HCSC server, or all the HCSC servers configuring the cluster.

To deploy the specified service adapter on a single HCSC server

Execute the command by specifying the name of the HCSC server and the service ID of the service adapter.

The service adapter specified in the -name option is deployed on the HCSC server specified in the -csc option.

```
csccompodeploy -user <login user ID> -pass <login password> -csc <HCSC server name> -name
<Service ID of the service adapter>
```

With the cscrepls command, you can check the HCSC server name and service ID of the service adapter specified in the csccompodeploy command. For details on the cscrepls command, see "cscrepls (Displaying the repository information)" in "Service Platform Reference Guide".

To deploy the specified service adapter on all the HCSC servers in the cluster

Execute the command by specifying the cluster name and the service ID of the service adapter.

The specified service adapter is deployed on all the HCSC servers in the cluster specified in the -cluster option.

```
csccompodeploy -user <login user ID> -pass <login password> -cluster <cluster name> -name
<Service ID of the service adapter>
```

3.1.9 Obtaining the service adapter definition files in the operating environment

This subsection describes how to obtain the definition files of the following service adapters in the operating environment, with the -operation get option of the csccmctl command:

- DB adapter
- TP1 adapter
- File adapter
- Object Access adapter
- Message Queue adapter
- FTP adapter
- File operations adapter
- Mail adapter
- HTTP adapter
- Custom adapter

This option is used by the operators to obtain the definition files in the operating environment after the developers develop these service adapters and perform the deployment definition.

Note that the definition files are not set up in the operating environment the moment the files are obtained. To set up the definition files in the operating environment, you must use the -operation set option after obtaining the files. For details on how to set up the definition files, see "*3.1.10 Setting and updating the service adapter definition files in the operating environment*".

(1) Examples of command usage

The following is an example of using the command for obtaining the definition files. For details on the csccmctl command, see "csccmctl (Managing the definition files) " in "Service Platform Reference Guide".

Example 1

To obtain the definition file "csccustomadapter.properties" with cluster name "CLS1" and service ID "ADP1" in the directory beneath "C:\tmp":

```
csccmctl -cluster CLS1 -name ADP1 -targetfilename csccustomadapter.properties -basedir C:
\tmp -operation get
```

Example 2

To obtain the communication definition file "adptp1_config.xml", which is set in the TP1 adapter and has the cluster name "CLS1" and service ID "ADP1", in the directory beneath "C:\tmp"

```
csccmctl -cluster CLS1 -name ADP1 -targetfilename adptp1_config.xml -basedir C:\tmp -
operation get
```

(2) Points to be considered

- If the definition file with the same specified file name already exists in the directory, the file in the directory is overwritten.
- In the following cases, the command terminates abnormally:
  - If the directory specified in the -basedir option does not exist
  - If a directory with the same name as the specified file name exists
  - If writing to the file fails

3.1.10 Setting and updating the service adapter definition files in the operating environment

The definition files obtained in the operating environment are set up in the operating environment with the -operation set option of the cscmctl command. If the definition files are already set up, the set contents are updated by re-executing the -operation set option.

This subsection describes how to set up and update the definition files of the following service adapters with the -operation set option of the cscmctl command:

- DB adapter
- TP1 adapter
- File adapter
- Object Access adapter
- Message Queue adapter
- FTP adapter
- File operations adapter
- Mail adapter
- HTTP adapter
- Custom adapter

Note that the definition files set up with this option are only enabled in the operating environment.

(1) Example of command usage

The following is an example of using the command for setting and updating the service adapter definition files. For details on the cscmctl command, see "cscmctl (Managing the definition files) " in "Service Platform Reference Guide".

Example 1

To set or update the definition file "csccustomadapter.properties", which is allocated to a directory beneath "C:\tmp" and has the cluster name "CLS1" and service ID "ADP1", in the operating environment

```
cscmctl -cluster CLS1 -name ADP1 -targetfilename csccustomadapter.properties -basedir C:
\tmp -operation set
```

Example 2

To set or update the communication definition file "adptp1_config.xml", which is set in the TP1 adapter allocated to a directory beneath "C:\tmp" and has the cluster name "CLS1" and service ID "ADP1", in the operating environment

```
cscmctl -cluster CLS1 -name ADP1 -targetfilename adptp1_config.xml -basedir C:\tmp -
operation set
```

Note that the set up and updated definition contents are deleted in one of the following cases:

- When the definition file is deleted with the -operation reset option

- When all the HCSC servers in the cluster are unset
- When the service adapter that set the definition file in the development environment is deleted, and a repository changed to another HCSC component is imported

(2) Points to be considered

- Execute the -operation set option before deploying the HCSC components.
- When you want to import the repository of a service adapter that has the same service ID, but different type as the service adapter that has the set and updated definition files and which was deleted by the csccompoundeploy command, you must use the -operation reset option to delete the definition file of the service adapter with the target service ID.
- If the directory [-cluster specified value]-[-name specified value] does not exist beneath <repository root>/manager/custom, the directory is created internally in the command.
- An error occurs in the following cases:
  - If the file specified in the -targetfilename option does not exist
  - If the directory up to the specified file does not exist
  - If an attempt to read the file set in the -targetfilename option fails
  - If the definition file contains a definition that is inappropriate for the contents to be defined in the operating environment

3.1.11 Deleting the service adapter definition files from the operating environment

This subsection describes how to delete the definition files of the following service adapters with the -operation reset option of the csccmctl command:

- DB adapter
- TP1 adapter
- File adapter
- Object Access adapter
- Message Queue adapter
- FTP adapter
- File operations adapter
- Mail adapter
- HTTP adapter
- Custom adapter

(1) Example of command usage

The following is an example of using the command for deleting the service adapter definition files. For details on the csccmctl command, see "csccmctl (Managing the definition files) " in "Service Platform Reference Guide".

Example 1: To delete the definition file "csccustomadapter.properties" with cluster name "CLS1" and service ID "ADP1" from the operating environment

```
csccmctl -cluster CLS1 -name ADP1 -targetfilename csccustomadapter.properties -operation
reset
```

Example 2: To delete the communication-configuration definition file "adptp1_config.xml", which is set in the TP1 adapter and has cluster name "CLS1" and service ID "ADP1", from the operating environment

```
csccmctl -cluster CLS1 -name ADP1 -targetfilename adptp1_config.xml -operation reset
```

(a) Points to be considered

- Execute the -operation reset option before the HCSC components are deployed.
- An error occurs in the following cases:
  - If the file specified in the -targetfilename option does not exist
  - If the file specified in the -targetfilename option cannot be deleted

3.1.12 Checking the status of the operating environment definition file

You can check a changed definition file by using the cscsvcls command.

(1) Example of command usage

The following is an example of using the command for checking the changed definition file. For details on the cscsvcls command, see "cscsvcls (Displaying the service information)" in "Service Platform Reference Guide".

To check the service information that is currently valid

Execute the cscsvcls command without specifying the -detail option.

```
cscsvcls -user <login user ID> -pass <login password>
```

To check the changed service information and the service information set in the development environment

Execute the cscsvcls command by specifying the -detail option.

```
cscsvcls -user <login user ID> -pass <login password> -detail
```

Note that if the proxy server user ID/ password, and basic authentication user ID/ password are set up, "The value has already been set." is displayed as the set value when the service information is output.

3.1.13 Deploying a business process

This subsection describes the preconditions for deploying a business process in the execution environment, and explains how to deploy the business process.

Note that the series of processing to deploy and start the HCSC components in the HCSC server, can also be executed in the development environment in a batch. However, batch execution is performed during system development or from unit testing to integration testing. For details, see "7.5 Batch execution of processes for deploying HCSC components on the HCSC Server and then starting " in "Service Platform Basic Development Guide".

(1) Preconditions

To deploy a business process, the HCSC server in the deployment-destination execution environment must be in a running state.

For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".

(2) How to deploy a business process

To deploy a business process, execute the csccompodeploy command in the operating environment.

For details on the csccompodeploy command, see "csccompodeploy (Deploying the HCSC components)" in "Service Platform Reference Guide".

The execution format of the command differs depending on whether all the business processes are deployed in a batch, or only a specified business process is deployed.

! Important note

When a business process is deployed, do not use the service ID of the business process that only has a difference of case with the service ID of the deployed service adapter and business process, or the reception ID of the user-defined reception. If such a name is used, the business process cannot be deployed.

(a) To deploy all the business processes in a batch

Deploy all the business processes on the HCSC server or cluster in a batch.

The execution format of the command differs depending on whether the business process deployment destination is a single HCSC server, or all the HCSC servers configuring the cluster.

To deploy all the business processes on a single HCSC server

Execute the command by specifying the name of the HCSC server and the -all option.

All the business processes, which are not deployed, are deployed on the HCSC server specified in the -csc option (all the service adapters and user-defined receptions that are not deployed are also deployed at the same time).

```
csccompodeploy -user <login user ID> -pass <login password> -csc <HCSC server name> -all
```

To deploy all the business processes on all the HCSC servers in the cluster

Execute the command by specifying the cluster name and the -all option.

All the business processes, which are not deployed, are deployed on all the HCSC servers in the cluster specified in the -cluster option (all the service adapters and user-defined receptions that are not deployed are also deployed at the same time).

```
csccompodeploy -user <login user ID> -pass <login password> -cluster <cluster name> -all
```

! Important note

If the service adapters, business processes, and user-defined receptions cannot be deployed because the -all option was specified, even if un-deployed service adapters, business processes, and user-defined receptions exist, they are ignored and the command terminates. After executing the command, use the cscrepls command to check the deployment status.

For details on the cscrepls command, see "cscrepls (Displaying the repository information) " in "Service Platform Reference Guide".

(b) To deploy the specified business process only

Deploy only the specified business process on the HCSC server or cluster.

The execution format of the command differs depending on whether the business process deployment destination is a single HCSC server, or all the HCSC servers configuring the cluster.

To deploy the specified business process on a single HCSC server

Execute the command by specifying the name of the HCSC server and the service ID of the business process.

The business process specified in the -name option is deployed on the HCSC server specified in the -csc option.

```
csccompodeploy -user <login user ID> -pass <login password> -csc <HCSC server name> -name
<business process service ID>
```

With the cscrepls command, you can check the HCSC server name and service ID of the business process specified in the csccompodeploy command. For details on the cscrepls command, see "cscrepls (Displaying the repository information)" in "Service Platform Reference Guide".

To deploy the specified business process on all the HCSC servers in the cluster

Execute the command by specifying the cluster name and the service ID of the business process.

The specified business process is deployed on all the HCSC servers in the cluster specified in the -cluster option.

```
csccompodeploy -user <login user ID> -pass <login password> -cluster <cluster name> -name
<business process service ID>
```

3.1.14 Deploying a user-defined reception

This subsection describes the preconditions for deploying a user-defined reception in the execution environment, and explains how to deploy the user-defined reception.

Note that the series of processing to deploy and start the HCSC components in the HCSC server, can also be executed in the development environment in a batch. However, batch execution is performed during system development or from unit testing to integration testing. For details, see "7.5 Batch execution of processes for deploying HCSC components on the HCSC Server and then starting in "Service Platform Basic Development Guide".

(1) Preconditions

To deploy a user-defined reception, the HCSC server in the deployment-destination execution environment must be in a running state.

For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".

(2) How to deploy a user-defined receptions

To deploy a user-defined reception, execute the csccompodeploy command in the operating environment.

For details on the csccompodeploy command, see "csccompodeploy (Deploying the HCSC components) " in "Service Platform Reference Guide".

The execution format of the command differs depending on whether all the user-defined receptions are deployed in a batch, or only a specified user-defined receptions is deployed.

! Important note

When a user-defined reception is deployed, do not use the reception ID of the user-defined reception that only has a difference of case with the service ID of the deployed service adapter and business process, or the reception ID of the user-defined reception. If such a name is used, the user-defined reception cannot be deployed.

(a) To deploy all the user-defined receptions in a batch

Deploy all the user-defined receptions in the HCSC server or cluster in a batch.

The execution format of the command differs depending on whether the deployment destination of the user-defined reception is a single HCSC server, or all the HCSC servers configuring the cluster.

To deploy all the user-defined receptions on a single HCSC server

Execute the command by specifying the name of the HCSC server and the -all option.

All the user-defined receptions, which are not deployed, are deployed on the HCSC server specified in the -csc option (all the service adapters and business processes that are not deployed are also deployed at the same time).

```
csccompodeploy -user <login user ID> -pass <login password> -csc <HCSC server name> -all
```

To deploy all the user-defined receptions on all the HCSC servers in the cluster

Execute the command by specifying the cluster name and the -all option.

All the user-defined reception, which are not deployed, are deployed on all the HCSC servers in the cluster specified in the -cluster option (all the service adapters and business processes that are not deployed are also deployed at the same time).

```
csccompodeploy -user <login user ID> -pass <login password> -cluster <cluster name> -all
```

! Important note

If the service adapters, business processes, and user-defined receptions cannot be deployed because the -all option was specified, even if un-deployed service adapters, business processes, and user-defined receptions exist, they are ignored and the command terminates. After executing the command, use the cscrepls command to check the deployment status.

For details on the cscrepls command, see "cscrepls (Displaying the repository information) " in "Service Platform Reference Guide".

(b) To deploy the specified user-defined reception only

Deploy only the specified user-defined reception in the HCSC server or cluster.

The execution format of the command differs depending on whether the deployment destination of the user-defined reception is a single HCSC server, or all the HCSC servers configuring the cluster.

To deploy the specified user-defined reception on a single HCSC server

Execute the command by specifying the name of the HCSC server and the reception ID of the user-defined reception.

The user-defined reception specified in the -name option is deployed on the HCSC server specified in the -csc option.

```
csccompodeploy -user <login user ID> -pass <login password> -csc <HCSC server name> -name
<reception ID of the user-defined reception>
```

With the cscrepls command, you can check the HCSC server name and reception ID of the user-defined reception specified in the csccompodeploy command. For details on the cscrepls command, see "cscrepls (Displaying the repository information) " in "Service Platform Reference Guide".

To deploy the specified user-defined reception on all the HCSC servers in the cluster

Execute the command by specifying the cluster name and the reception ID of the user-defined reception.

The specified user-defined reception is deployed on all the HCSC servers in the cluster specified in the -cluster option.

```
csccompodeploy -user <login user ID> -pass <login password> -cluster <cluster name> -name
<reception ID of the user-defined reception>
```

3.1.15 Setting the definition information for user-defined receptions

Among the user-defined receptions, you can set up the following definition information in the SOAP receptions:

- Maximum number of concurrent executions
- Number of dedicated threads
- Size of pending queue

This subsection describes the preconditions for setting up the definition information, and explains how to set up the information.

! Important note

If the user-defined reception and the business process using that user-defined reception are deleted, the definition information set up here is disabled. When you re-deploy the user-defined reception, and the business process using that user-defined reception thereafter, make sure that you re-specify the definition information for the user-defined reception.

(1) Preconditions

To set up the definition information for the SOAP reception, the HCSC server must be in a running state.

For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".

(2) How to set up the information

To set up the definition information for a SOAP reception, first create the user-defined reception runtime definition file. The template file of the user-defined reception runtime definition file is stored in the following directory with the file name "cscurcptnconfig.properties":

```
<Service Platform installation directory>·CSC·config·manager·templates·
cscurcptnconfig.properties
```

Copy the template file to any location, edit the definition information, and then create the user-defined reception runtime definition file. For details on the user-defined reception runtime definition file, see "User-defined reception runtime definition file" in "Service Platform Reference Guide".

When the user-defined reception runtime definition file is created, execute the csccompoconfig command in the operating environment to set up the definition information. The set up definition information is applied when the HCSC components are restarted. For details on the csccompoconfig command, see "csccompoconfig (Defining HCSC components) " in "Service Platform Reference Guide".

The execution format of the command differs depending on whether the definition information is set for the SOAP reception deployed on the HCSC server, or whether the definition information is set for the SOAP reception deployed on the HCSC server in a cluster.

To set the definition information for the SOAP reception deployed on the HCSC server

Execute the command by specifying the name of the HCSC server and reception ID of the SOAP reception.

The definition information specified in the user-defined reception runtime definition file is set up for the SOAP reception on the specified HCSC server.

```
csccompoconfig -user <login user ID> -pass <login password> -operation set -propfile <user-
defined reception runtime definition file > -csc <HCSC server name> -name <reception ID>
```

To set the definition information for the SOAP reception deployed on the HCSC server in a cluster

Execute the command by specifying the cluster name and the reception ID of the SOAP reception.

The definition information specified in the user-defined reception runtime definition file is set up for the SOAP reception deployed in the specified cluster.

```
csccompoconfig -user <login user ID> -pass <login password> -operation set -propfile <user-
defined reception runtime definition file > -cluster <cluster name> -name <reception ID>
```

3.1.16 Checking the definition information of the user-defined receptions

This subsection describes the preconditions for checking the definition information of the user-defined receptions, and explains how to check the information.

(1) Preconditions

To check the definition information of the user-defined receptions, the HCSC server must be in a running state.

For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".

(2) How to check the information

To check the set up definition information of the user-defined receptions, execute the csccompoconfig command in the operating environment specifying "get" in the -operation option, the HCSC server name in the -csc option, and the reception ID of the user-defined reception in the -name option.

For details on the csccompoconfig command, see "csccompoconfig (Defining HCSC components)" in "Service Platform Reference Guide".

The execution format of the csccompoconfig command is as follows:

```
csccompoconfig -user <login user ID> -pass <login password> -operation get -csc <HCSC
server name> -name <reception ID>
```

3.1.17 Checking or changing the set contents

For details on how to check the contents set up for the HCSC servers, service adapters, business processes, and user-defined receptions, see the following locations:

To check the setup information for HCSC servers

See "*5.3.14 Checking the HCSC server setup information*" and "*5.3.15 Checking the HCSC server information*".

To check the deployment information for service adapters

See "*5.3.17 Checking the service adapter information*".

To check the deployment information for business processes

See "*5.3.18 Checking the business process information*".

To check the deployment information for user-defined receptions

See "*5.3.19 Checking the information of user-defined reception*".

When you check the setup information and want to change the already setup contents, execute unsetup and then resetup. For details on how to execute unsetup, see "*3.3 Cancelling System Setup*".

Important note

To add or change the setup information for an HCSC server, you can add or change some contents without unsetting up the HCSC server. For details on adding or changing the HCSC server setup, see "*3.1.3 (3) Adding and changing the setup information*".

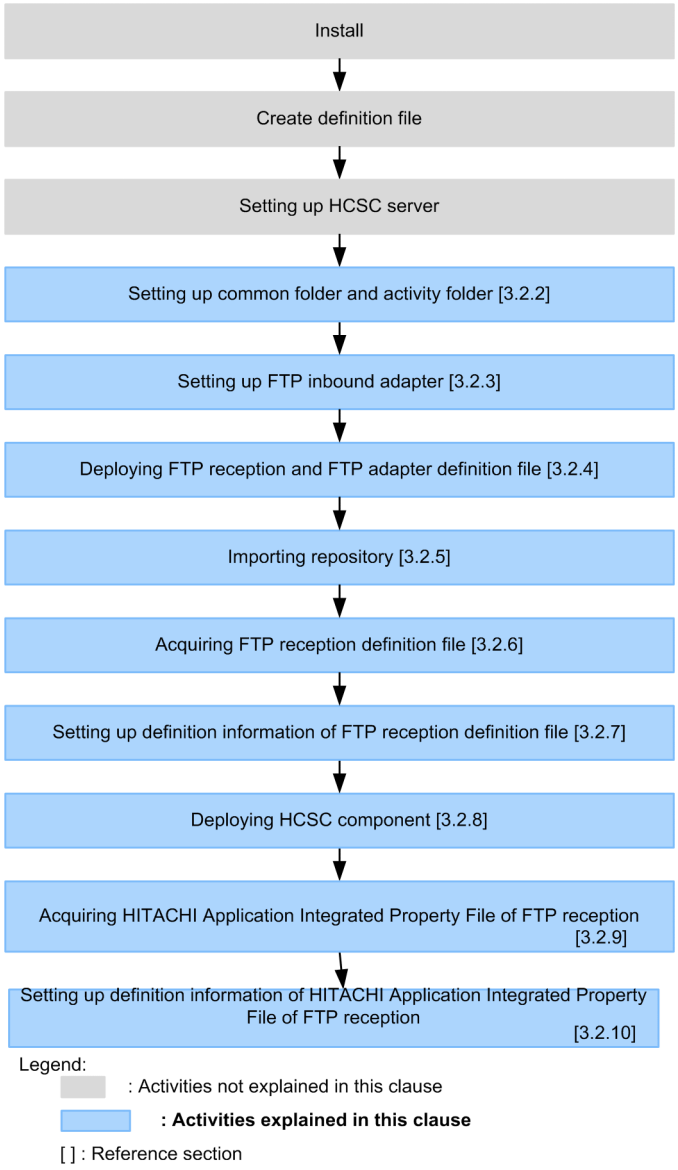
3.2 System setup (For FTP integration)

This section describes the flow and procedure of setting up a system for FTP integration.

3.2.1 Flow of setup for an FTP-integrated system

The following figure shows the flow of setup for an FTP-integrated system.

Figure 3–6: Figure Flow of setup for an FTP-integrated system



3.2.2 Setting up the common folders and work folders

To use an FTP-integrated system, you must set up the path of the common folders and work folders in the HCSC server runtime definition file.

For details on the properties to be set up in the HCSC server runtime definition file, see "HCSC server runtime definition file" in "Service Platform Reference Guide".

The execution format for setting up the HCSC server runtime definition file on an HCSC server in a cluster is as follows:

```
cscsvconfig -user <login user ID> -pass <login password> -cluster <cluster name> -operation
set -propfile <Name of the HCSC server runtime definition file>
```

For details on the cscsvconfig command, see "cscsvconfig (HCSC server runtime definition) " in "Service Platform Reference Guide".

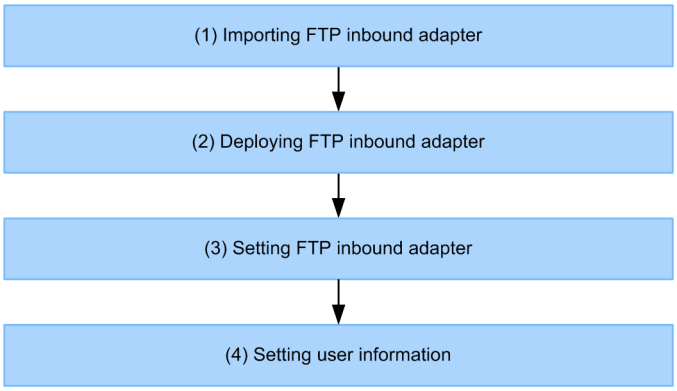
3.2.3 Setting up the FTP inbound adapter

To set up the FTP inbound adapter, the HCSC server must be in a running state.

For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".

The following figure shows flow of setup for an FTP inbound adapter.

Figure 3–7: Figure Flow of setup for an FTP inbound adapter



(1) Importing the FTP inbound adapter

The execution format for importing the FTP inbound adapter is as follows:

```
<Service Platform installation directory>·CC·admin·bin·cjimportres <J2EE server name> -type
rar -f "<Service Platform installation directory>·CSC·inbound-adapter·ftp·rar·
ftp_inbound_adapter.rar"
```

For details on the cjimportres command, see "2.4 Resource operation commands used in the J2EE server" in "Application Server Command Reference Guide".

(2) Deploying the FTP inbound adapter

The execution format for deploying the FTP inbound adapter is as follows:

```
<Service Platform installation directory>·CC·admin·bin·cjdeployrar <J2EE server name> -
resname FTP_Inbound_Resource_Adapter
```

For details on the cjdeployrar command, see "2.4 Resource operation commands used in the J2EE server" in "Application Server Command Reference Guide".

(3) Setting up the FTP inbound adapter

The procedure for setting up the FTP inbound adapter, and the contents of the property file are as follows.

Reference note

To operate the FTP-integrated system with the default settings, you can omit the settings described here.

(a) Setup procedure

1. Obtain the attributes from the RAR file of the FTP inbound adapter, and create the property file.
   The execution format for creating the property file from the RAR file of the FTP inbound adapter is as follows:

```
<Service Platform installation directory>･CC･admin･bin･jgetrarprop <J2EE server name> -
resname FTP_Inbound_Resource_Adapter -c <file path of the property file>
```

   For details on the cjgetrarprop command, see "2.4 Resource operation commands used in the J2EE server" in "Application Server Command Reference Guide".

2. Edit the property file.
   For details on the property file, see " *(b) Contents of the property file*".

3. The values specified in the property file in which the definition items were edited, are applied to the RAR file of the FTP inbound adapter.
   The execution format for applying the property file to the FTP inbound adapter is as follows:

```
<Service Platform installation directory>･CC･admin･bin･cjsetrarprop <J2EE server name> -
resname FTP_Inbound_Resource_Adapter -c <file path of the property file>
```

For details on the cjsetrarprop command, see "2.4 Resource operation commands used in the J2EE server" in "Application Server Command Reference Guide".

(b) Contents of the property file

Property file definitions

The definition tags in the property file are as follows:

```
<hitachi-connector-property>
 <resourceadapter>
 <config-property>
 <config-property-name> : Definition name
 <config-property-type> : Definition type
 <config-property-value> : Definition value
 </config-property>
 <config-property>
 <config-property-name> : Definition name
 <config-property-type> : Definition type
 <config-property-value> : Definition value
 </config-property>
 :
(Repeated for the existing number of definitions)
 :
```

To edit a definition, search for the "Definition name" you want to edit, and rewrite the corresponding "Definition value". For details on the items that can be edited, see "*Property file definition items*".

Note the following when you edit the property file:

- Rewrite only the values of the definition items listed in the "definition items". Do not change the other items and values.
- Do not specify the contents of the property file in the application property file (cosminexus.xml).
- Do not change the resource adapter name in the <display-name> tag existing in the property file.
- In the log output related settings, if you change the file size per log file, and the number of backup log files for each type of log, make a backup of the log files before you start the FTP inbound adapter.

Property file definition locations

The following figure shows the definition locations for the property files.

Figure 3–8: Figure Locations where the property file contents and definitions are set up

```
<?xml version="1.0" encoding="MS932"?>
                :
                :
<hitachi-connector-property>
<display-name>FTP_Inbound_Resource_Adapter</display-name>
 <vendor-name>Hitachi, Ltd.</vendor-name>
 <eis-type>FTP_Client</eis-type>
 <resourceadapter-version>XX-XX</resourceadapter-version>
                :
                :
<resourceadapter>
   <resourceadapter-class>com.cosminexus.ftp.resourceadapter.FTPInboundResourceAdapter</
resourceadapter-class>
   <config-property>
     <description xml:lang="en"></description>
     <config-property-name>server_resourceAdapterName</config-property-name>
     <config-property-type>java.lang.String</config-property-type>
     <config-property-value>FTP_Inbound_Resource_Adapter</config-property-value>
   </config-property>
   <config-property>
     <description xml:lang="en"></description>
     <config-property-name>nioListener_port</config-property-name>
     <config-property-type>java.lang.Integer</config-property-type>
     <config-property-value>21</config-property-value>
   </config-property>          Overwrite point
   <config-property>
     <description xml:lang="en"></description>
     <config-property-name>nioListener_localAddress</config-property-name>
     <config-property-type>java.lang.String</config-property-type>
     <config-property-value>10.209.12.111</config-property-value>
   </config-property>                  Overwrite point
   <config-property>
     <description xml:lang="en"></description>
     <config-property-name>xxx</config-property-name>
     <config-property-type>xxx</config-property-type>
     <config-property-value>xxx</config-property-value>
   </config-property>            Overwrite point
                                        :
                                        :
   <inbound-resourceadapter>
                                        :
                                        :
   </inbound-resourceadapter>
  </resourceadapter>

  <resourceadapter-runtime>
                                        :
                                        :
  </resourceadapter-runtime>

</hitachi-connector-property>
```

Legend:
Line of " : " : Abbreviation of description

Property file definition items

The following table describes and lists the property file definition items for each setup content.

Table 3–22: Table Lists of property file definition items (Settings related to transmit control)

Definition items	Definition name	Range of values	Default value	Supplementary information
Maximum number of concurrent connections	server_maxLogins	1 to 1024	10	--
Use of character set UTF-8	server_charset_UTF8	ON or OFF	ON	If ON is specified, UTF-8 is used as the character code. If OFF is specified, MS932 is used as the character code. Note that if the character set is specified with the FTP

Definition items	Definition name	Range of values	Default value	Supplementary information
Use of character set UTF-8	server_charset_UTF8	ON or OFF	ON	command, that setting is enabled.
Compatibility of FTP response termination character	server_endOfLineCompatible	true or false	false (CRLF becomes the default termination code)	If true is specified, an OS-dependent linefeed code (In Windows: CRLF, In UNIX: LF) is used as the FTP response termination character. If false is specified, CRLF is used as the FTP response termination character.
Local IP address	nioListener_localAddress	0.0.0.0 to 255.255.255.255	All available (If the host executing the FTP inbound adapter has multiple IP addresses, the requests from the FTP client are received on all the IP addresses)	You can only specify the IPv4 IP address. IPv6 is not supported.
Port number	nioListener_port	1 to 65535	21	--
Local IP address when the data connection is established	nioListener_dataConnection_active_localAddress	0.0.0.0 to 255.255.255.255	Any available (If the host executing the FTP inbound adapter has multiple IP addresses, the system automatically allocates any IP address)	You can only specify the IPv4 IP address. IPv6 is not supported.
Port number when the data connection is established	nioListener_dataConnection_active_localPort	1 to 65535	Any available (The port number that is free in the host executing the FTP inbound adapter is allocated)	Do not specify a port number that is already in use. If specified, the data connection cannot be established.
Listen backlog count	nioListener_listenBacklog	1 to 2147483647	50	--
Data connection buffer size	nioListener_dataConnection_socketBufferSize	1 to 65536	16384	(Unit: bytes)

Legend:
-: None in particular

Table 3–23: Table List of property file definition items (Settings related to timeout)

Definition items	Definition name	Range of values	Default value	Supplementary information
Idle timeout	nioListener_idleTimeout	0 to 7200	300	If 0 is specified, the timeout is not monitored. (Unit: seconds)

Definition items	Definition name	Range of values	Default value	Supplementary information
Data connection retry count	nioListener_dataConnection_active_connectRetryCount	0 to 50	5	If 0 is specified, connection is not retried.
Data connection monitoring time	nioListener_dataConnection_active_connectRetryInterval	0 to 1800	10	If 0 is specified, the timeout is not monitored. (Unit: seconds)
Data sending and data receiving timeout	nioListener_dataConnection_idleTimeout	0 to 1800	10	If 0 is specified, the timeout is not monitored. (Unit: seconds)

For the FTPS-related settings in the property file definition items, see "Appendix H.3 Property file definition items during setup (FTP inbound adapter)" in "Service Platform Reception and Adapter Definition Guide".

Table 3–24: Table List of property file definition items (Settings related to log output)

Classification	Definition items	Definition name	Range of values	default value	Supplementary information
Message log	Output level	server_message_logLevel	debug, or info	info	info: This level outputs information that is used for normal operations and is necessary for operations. debug: This level is used for investigation when test or error occurs, and outputs the debug information in addition to the information output in "info".
	Size per log file	server_message_maxFileSize	1MB to 2048MB	10MB	Specify the character string for the unit as well. (Unit: MB)
	Number of backup log files	server_message_maxBackupIndex	1 to 16	4	--
Maintenance log	Log output level	server_maintenance_logLevel	debug, or info	info	The meaning of "info" and "debug" is the same as the "log output level" of the message log.
	Size per log file	server_maintenance_maxFileSize	1MB to 2048MB	5MB	Specify the character string for the unit as well. (Unit: MB)
	Number of backup log files	server_maintenance_maxBackupIndex	1 to 16	4	--
Protocol trace log	Log output level	server_protocol_logLevel	debug, or info	info	The meaning of "info" and "debug" is the same as the "log output level" of the message log.

Classification	Definition items	Definition name	Range of values	default value	Supplementary information
Protocol trace log	Size per log file	server_protocol_maxFileSize	1MB to 2048MB	20MB	Specify the character string for the unit as well. (Unit: MB)
	Number of backup log files	server_protocol_maxBackupIndex	1 to 16	4	--
Transmit history log	Log output level	server_history_logLevel	debug, or info	info	The meaning of "info" and "debug" is the same as the "log output level" of the message log.
	Size per log file	server_history_maxFileSize	1MB to 2048MB	12MB	Specify the character string for the unit as well. (Unit: MB)
	Number of backup log files	server_history_maxBackupIndex	1	1	--
Common log between resource adapters	Log output level	server_common_logLevel	debug, or info	info	The meaning of "info" and "debug" is the same as the "log output level" of the message log.
	Size per log file	server_common_maxFileSize	1MB to 2048MB	5MB	Specify the character string for the unit as well. (Unit: MB)
	Number of backup log files	server_common_maxBackupIndex	1 to 16	4	--

Legend:
--: None in particular

(4) Setting up the user information

The user information is managed as a file by the FTP inbound adapter. The Administrator who has the administrator permission can register, update, delete, and display the authentication information file by executing the operation commands.

(a) Operation commands for authentication information

The following table describes the operation commands for authentication information.

Table 3–25: Table Operation commands for authentication information

Operation commands	Contents
csmftpaddusr (Command for registering or updating a user in the FTP inbound adapter)	Registers a user. Also, updates the password of a user that is already registered.
csmftpdelusr (Command for deleting a user in the FTP inbound adapter)	Deletes the authentication information of the registered users.
csmftplsusr (Command for displaying the users of the FTP inbound adapter)	Displays the authentication information of the registered users.

For details on the operation commands, see the description in "5. Commands (Operating Environment and Execution Environment)" in "Service Platform Reference Guide".

Note the following when you execute the operation commands:

- Execute the operation commands when the FTP inbound adapter is in a stopped state.
- While an operation command is being executed, you cannot execute another operation command. Execute the other operation command after the operation command executed first terminates.

The execution format of operation commands is as follows:

- **Registering or updating users in the FTP inbound adapter**
  The execution format for registering or updating a user in the FTP inbound adapter is as follows:

```
csmftpaddusr -usr <user name> -pass <password of the user>
```

  For details, see "csmftpaddusr (Registering or updating users in the FTP inbound adapter) " in "Service Platform Reference Guide".

- **Deleting users in the FTP inbound adapter**
  The execution format for deleting users in the FTP inbound adapter is as follows:

```
csmftpdelusr -usr <user name>
```

  For details, see "csmftpdelusr (Deleting users in the FTP inbound adapter) " in "Service Platform Reference Guide".

- **Displaying the users of the FTP inbound adapter**
  The execution format for displaying the users of the FTP inbound adapter is as follows:

```
csmftplsusr
```

  For details, see "csmftplsusr (Displaying the users of the FTP inbound adapter) " in "Service Platform Reference Guide".

(b) Permission to access the authentication information

To grant the permission to access the authentication information, before the operations start, the operator must set up the update or reference permission for the authentication information file only for the Administrator who executes the operation commands.

Note that if the access permission is set up for the Administrator, the Administrator becomes the owner of the authentication information file.

3.2.4 Allocating the definition files for the FTP reception, FTP adapter, and File operations adapter

The following table lists and describes the storage destinations of various definition files for the FTP reception, FTP adapter, and File operations adapter.

Table 3–26: Storage destinations of various definition files for the FTP reception, FTP adapter, and File operations adapter

Components used for definition	Definition file name	Storage destination
FTP reception	FTP reception configuration file	`<Service Platform installation directory>\CSC\config\ftprecp\<service ID>.properties`
	FTP execution permission list definition file	Any location[#1]
	List command option definition file	Any location[#1]
	FTP command permission list definition file (for FTP receptions)	Any location[#1]

Components used for definition	Definition file name	Storage destination
FTP adapter	FTP command permission list definition file (for FTP adapters)	Any location#2
	FTP adapter execution environment property file	<Service Platform installation directory>\CSC\custom-adapter\FTP\config\<service ID>.properties
	FTP adapter account definition file	Any location#2
File operations adapter	File operations adapter execution environment property file	<Service Platform installation directory>\CSC\config\adpfop\<service ID>.properties

Note#1

Reference from FTP reception configuration file.

Note#2

Reference from FTP adapter execution environment property file.

3.2.5 Importing a repository

To use an FTP reception, which was created in the development environment, in the operating environment, import the repository information stored in the ZIP file format into a repository.

To import the repository information into a repository, execute the cscrepctl command.

The execution format for importing the repository information into a repository is as follows:

```
cscrepctl -user <login user ID> -pass <login password> -import <file name>
```

For details, see "cscrepctl (Importing and exporting) " in "Service Platform Reference Guide".

3.2.6 Obtaining the FTP reception definition file

This subsection describes the preconditions for obtaining the FTP reception definition file set up in the development environment, and explains how to obtain the file.

(1) Preconditions

To obtain the FTP reception definition file, the HCSC server must be in a running state.

For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".

(2) How to obtain the file

To obtain the FTP reception definition file set up in the development environment, execute the csccmctl command in the operating environment.

The execution format for obtaining the FTP reception definition file is as follows:

```
csccmctl -user <login user ID> -pass <login password> -cluster <cluster name> -name
<reception ID of the FTP reception> -targetfilename cscurecpftp.properties -basedir <file
path of the directory where cscurecpftp.properties is stored> -operation get
```

For details, see "csccmctl (Managing the definition files) " in "Service Platform Reference Guide".

3.2.7 Setting up the definition information of the FTP reception definition file

This subsection describes the preconditions for setting the definition information of the obtained FTP reception definition file in the operating environment, and explains how to set up the information.

(1) Preconditions

To set up the definition information of the FTP reception definition file, the following conditions must be satisfied:

- The HCSC server is running
- The command for setting up the definition information of the FTP reception definition file is executed before the HCSC components are deployed

For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".

(2) How to set up the information

To set up the definition information of the FTP reception definition file, execute the csccmctl command in the operating environment.

The execution format for setting up the definition information of the FTP reception definition file is as follows:

```
csccmctl -user <login user ID> -pass <login password> -cluster <cluster name> -name
<reception ID of the FTP reception> -targetfilename cscurecpftp.properties -basedir <file
path of the directory where cscurecpftp.properties is stored> -operation set
```

For details, see "csccmctl (Managing the definition files) " in "Service Platform Reference Guide".

3.2.8 Deploying the HCSC components

This subsection describes the preconditions for deploying the HCSC components in the execution environment, and explains how to deploy the components.

(1) Preconditions

To deploy the HCSC components in an already set up HCSC server, the HCSC server in the deployment-destination execution environment must be in a running state.

For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".

(2) How to deploy the components

To deploy the HCSC components in an already set up HCSC server, execute the csccompodeploy command in the operating environment.

The execution format for deploying the HCSC components is as follows:

```
csccompodeploy -user <login user ID> -pass <login password> -cluster <cluster name> -all
```

For details, see "csccompodeploy (Deploying HCSC components)" in "Service Platform Reference Guide".

3.2.9 Obtaining the HITACHI Application Integrated Property File for FTP receptions

This subsection describes the preconditions for obtaining the HITACHI Application Integrated Property File for FTP receptions, and explains how to obtain the file.

(1) Preconditions

To obtain the HITACHI Application Integrated Property File for FTP receptions, the HCSC server must be in a running state.

For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".

(2) How to obtain the file

To obtain the HITACHI Application Integrated Property File for FTP receptions, execute the csccompoconfig command in the operating environment.

The execution format for obtaining the HITACHI Application Integrated Property File for FTP receptions is as follows:

```
csccompoconfig -user <login user ID> -pass <login password> -csc <HCSC server name> -name
<reception ID of the FTP reception> -operation get
```

For details, see "csccompoconfig (Defining HCSC components) " in "Service Platform Reference Guide".

3.2.10 Setting up the definition information of the HITACHI Application Integrated Property File for FTP receptions

This subsection describes the preconditions for setting up the definition information of the HITACHI Application Integrated Property File for FTP receptions, and explains how to set up the information.

(1) Preconditions

To set up the definition information of the HITACHI Application Integrated Property File for FTP receptions, the HCSC server must be in the running state and the state of the FTP reception must be deployed. However, an error occurs if the FTP reception is running.

Furthermore, if the following conditions are satisfied, the same value must be set up for the maximum number of instances specified in the HITACHI Application Integrated Property File, and the maximum number of threads used for monitoring the FTP reception timeout to be set up in the FTP reception configuration file.

- A timeout value is set up for FTP reception
- The maximum number of instances is changed with the csccompoconfig command

For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".

(2) How to set up the information

To set up the definition information of the HITACHI Application Integrated Property File for FTP receptions, execute the csccompoconfig command in the operating environment.

The execution format for setting up the definition information of the HITACHI Application Integrated Property File for FTP receptions is as follows:

```
csccompoconfig -user <login user ID> -pass <login password> -csc <HCSC server name> -name
<reception ID of the FTP reception> -operation set
```

For details, see "csccompoconfig (Defining HCSC components) " in "Service Platform Reference Guide".

3.3 Cancelling System Setup

This section describes how to cancel the system setup that was performed using a Service platform.

3.3.1 Deleting a service adapter

This subsection describes the preconditions for deleting a service adapter deployed in the execution environment, and explains how to delete the service adapter.

Note that the series of processing to stop and delete the HCSC components from the HCSC server can also be executed in the development environment in a batch. However, batch execution is performed during system development or from unit testing to integration testing. For details, see "7.6 Batch execution of processes for stopping HCSC components and deleting them from the HCSC server" in "Service Platform Basic Development Guide".

(1) Preconditions

To delete a service adapter, the following conditions must be satisfied:

- The HCSC server is running

  For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".
- The service adapter is in a stopped state

  For details on how to check the status of the service adapter, see "*5.3.17 Checking the service adapter information*".

(2) How to delete a service adapter

To delete a service adapter, execute the csccompoundeploy command in the operating environment.

For details on the csccompoundeploy command, see "csccompoundeploy (Deleting the deployed HCSC components) " in "Service Platform Reference Guide".

The execution format of the command differs depending on whether all the service adapters are deleted in a batch, or whether only the specified service adapter is deleted.

! Important note

If the service adapter cannot be deleted, eliminate the cause of the error, and then delete again.

(a) To delete all the service adapters in a batch

Delete all the service adapters on the HCSC server or cluster in a batch.

The execution format of the command differs depending on whether the service adapter is deleted from a single HCSC server, or all the HCSC servers configuring the cluster.

To delete all the service adapters from a single HCSC server

Execute the command by specifying the name of the HCSC server and the -all option.

All the service adapters deployed on the HCSC server specified in the -csc option are deleted (all the undeleted business processes and user-defined receptions are also deleted at the same time).

```
csccompoundeploy -user <login user ID> -pass <login password> -csc <HCSC server name> -all
```

To delete all the service adapters from all the HCSC servers configuring the cluster

Execute the command by specifying the cluster name and the -all option.

All the service adapters deployed on all the HCSC servers in the cluster specified in the -cluster option are deleted (all the undeleted business processes and user-defined receptions are also deleted at the same time).

```
csccompoundeploy -user <login user ID> -pass <login password> -cluster <cluster name> -all
```

(b) To delete the specified service adapter only

Among the service adapters deployed on the HCSC server or cluster, only the specified service adapter is deleted.

The execution format of the command differs depending on whether the service adapter is deleted from a single HCSC server, or all the HCSC servers configuring the cluster.

To delete only the specified service adapter from a single HCSC server

Execute the command by specifying the name of the HCSC server and the service ID of the service adapter.

The service adapter specified in the -name option is deleted, from among the service adapters deployed on the HCSC server specified in the -csc option.

```
csccompoundeploy -user <login user ID> -pass <login password> -csc <HCSC server name> -name
<Service ID of the service adapter>
```

To delete only the specified service adapter from all the HCSC servers configuring the cluster

Execute the command by specifying the cluster name and the service ID of the service adapter.

Only the specified service adapter is deleted, from among the service adapters deployed on all the HCSC servers in the cluster specified in the -cluster option.

```
csccompoundeploy -user <login user ID> -pass <login password> -cluster <cluster name> -name
<Service ID of the service adapter>
```

! Important note

If in-process requests exist, the service adapter is not deleted.

To destroy the in-process requests, and to delete the service adapter forcefully, execute the csccompoundeploy command by specifying the -force option.

The following are the examples of forced deletion:

- To delete all the service adapters of the HCSC server "HCSC" forcefully

```
csccompoundeploy -user admin -pass admin -csc HCSC -all -force
```

- To delete the service adapter "Adapter1" of the HCSC server "HCSC" forcefully

```
csccompoundeploy -user admin -pass admin -csc HCSC -name Adapter1 -force
```

3.3.2 Deleting a business process

This subsection describes the preconditions for deleting a business process deployed in the execution environment, and explains how to delete the business process.

Note that the series of processing to stop and delete the HCSC components from the HCSC server, can also be executed in the development environment in a batch. However, batch execution is performed during system development or from unit testing to integration testing. For details, see "7.6 Batch execution of processes for stopping HCSC components and deleting them from the HCSC server" in "Service Platform Basic Development Guide".

(1) Preconditions

To delete a business process, the following conditions must be satisfied:

- The HCSC server is running

  For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".
- The business process is in a stopped state

  For details on how to check the status of the business process, see "*5.3.18 Checking the business process information*".

(2) How to delete

To delete a business process, execute the csccompoundeploy command in the operating environment.

For details on the csccompoundeploy command, see "csccompoundeploy (Deleting the deployed HCSC components)" in "Service Platform Reference Guide".

The execution format of the command differs depending on whether all the business processes are deleted in a batch, or whether only the specified business process is deleted.

! Important note

If the business process cannot be deleted, eliminate the cause of the error, and then delete again.

(a) To delete all the business processes in a batch

Delete all the business processes on the HCSC server or cluster in a batch.

The execution format of the command differs depending on whether the business process is deleted from a single HCSC server, or all the HCSC servers configuring the cluster.

To delete all the business processes from a single HCSC server

Execute the command by specifying the name of the HCSC server and the -all option.

All the business processes deployed on the HCSC server specified in the -csc option are deleted (all the undeleted service adapters and user-defined receptions are also deleted at the same time).

```
csccompoundeploy -user <login user ID> -pass <login password> -csc <HCSC server name> -all
```

To delete all the business processes from all the HCSC servers configuring the cluster

Execute the command by specifying the cluster name and the -all option.

All the business processes deployed on all the HCSC servers in the cluster specified in the -cluster option is deleted (all the undeleted service adapters and user-defined receptions are also deleted at the same time).

```
csccompoundeploy -user <login user ID> -pass <login password> -cluster <cluster name> -all
```

(b) To delete the specified business process only

Among the business processes deployed on the HCSC server or cluster, only the specified business process is deleted.

The execution format of the command differs depending on whether the business process is deleted from a single HCSC server, or all the HCSC servers configuring the cluster.

To delete only the specified business process from a single HCSC server

Execute the command by specifying the name of the HCSC server and the service ID of the business process.

The business process specified in the -name option is deleted, from among the business processes deployed on the HCSC server specified in the -csc option.

```
csccompoundeploy -user <login user ID> -pass <login password> -csc <HCSC server name> -name
<business process service ID>
```

To delete only the specified business process from all the HCSC servers configuring the cluster

Execute the command by specifying the cluster name and the service ID of the business process.

Only the specified business process is deleted, from among the business processes deployed on all the HCSC servers in the cluster specified in the -cluster option.

```
csccompoundeploy -user <login user ID> -pass <login password> -cluster <cluster name> -name
<business process service ID>
```

3.3.3 Deleting a user-defined reception

This subsection describes the preconditions for deleting a user-defined reception deployed in the execution environment, and explains how to delete the user-defined reception.

Note that the series of processing to stop and delete the HCSC components from the HCSC server can also be executed in the development environment in a batch. However, batch execution is performed during system development or from unit testing to integration testing. For details, see "7.6 Batch execution of processes for stopping HCSC components and deleting them from the HCSC server" in "Service Platform Basic Development Guide".

(1) Preconditions

To delete a user-defined reception, the following conditions must be satisfied:

- The HCSC server is running
  For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".
- The user-defined reception is in a stopped state
  For details on how to check the status of the user-defined reception, see "*5.3.19 Checking the information of user-defined reception*".

(2) How to delete

To delete a user-defined reception, execute the csccompoundeploy command in the operating environment.

For details on the csccompoundeploy command, see "csccompoundeploy (Deleting the deployed HCSC components) " in "Service Platform Reference Guide".

The execution format of the command differs depending on whether all the user-defined receptions are deleted in a batch, or whether only the specified user-defined reception is deleted.

! Important note

If the user-defined reception cannot be deleted, eliminate the cause of the error, and then delete again.

(a) To delete all the user-defined receptions in a batch

Delete all the user-defined receptions on the HCSC server or cluster in a batch.

The execution format of the command differs depending on whether the user-defined reception is deleted from a single HCSC server, or all the HCSC servers configuring the cluster.

To delete all the user-defined receptions from a single HCSC server

Execute the command by specifying the name of the HCSC server and the -all option.

All the user-defined receptions deployed on the HCSC server specified in the -csc option are deleted (all the undeleted service adapters and business processes are also deleted at the same time).

```
csccompoundeploy -user <login user ID> -pass <login password> -csc <HCSC server name> -all
```

To delete all the user-defined receptions from all the HCSC servers configuring the cluster

Execute the command by specifying the cluster name and the -all option.

All the user-defined receptions deployed on all the HCSC servers in the cluster specified in the -cluster option are deleted (all the undeleted service adapters and business processes are also deleted at the same time).

```
csccompoundeploy -user <login user ID> -pass <login password> -cluster <cluster name> -all
```

(b) To delete the specified user-defined reception only

Among the user-defined receptions deployed on the HCSC server or cluster, only the specified user-defined reception is deleted.

The execution format of the command differs depending on whether the user-defined reception is deleted from a single HCSC server, or all the HCSC servers configuring the cluster.

To delete only the specified user-defined reception from a single HCSC server

Execute the command by specifying the name of the HCSC server and the reception ID of the user-defined reception.

The user-defined reception specified in the -name option is deleted, from among the user-defined receptions deployed on the HCSC server specified in the -csc option.

```
csccompoundeploy -user <login user ID> -pass <login password> -csc <HCSC server name> -name
<reception ID of the user-defined reception>
```

To delete only the specified user-defined reception from all the HCSC servers configuring the cluster

Execute the command by specifying the cluster name and the reception ID of the user-defined reception.

Only the specified user-defined reception is deleted, from among the user-defined receptions deployed on all the HCSC servers in the cluster specified in the -cluster option.

```
csccompoundeploy -user <login user ID> -pass <login password> -cluster <cluster name> -name
<reception ID of the user-defined reception>
```

3.3.4 Unsetting up an FTP-integrated system

(1) Deleting a service adapter

For details on how to delete the service adapters, including the FTP adapter and file operations adapter, deployed in the execution environment, see "*3.3.1 Deleting a service adapter*".

(2) Deleting a business process

For details on how to delete the business processes deployed in the execution environment, see "*3.3.2 Deleting a business process*".

(3) Deleting a user-defined reception

For details on how to delete the user-defined receptions, including the FTP receptions, deployed in the execution environment, see "*3.3.3 Deleting a user-defined reception*".

(4) Deleting an FTP inbound adapter

This subsection describes the preconditions for deleting an FTP inbound adapter, and explains how to delete the adapter.

(a) Preconditions

To delete an FTP inbound adapter, the following conditions must be satisfied:

- The HCSC server is running
  For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".
- The FTP inbound adapter is in a stopped state
  For details on how to check the status of the FTP inbound adapter, see "4.6 Referencing the list of resource adapters" in "Application Server Application Setup Guide".

(b) How to delete the adapter

Implement the following operations:

●Canceling the settings for the FTP inbound adapter

The execution format for deleting all the user information (user name and password) registered in the FTP inbound adapter is as follows:

```
<Service Platform installation directory>·CSC·bin·csmftpdelusr -usr <user name>
```

For the command details, see "csmftpdelusr (Deleting users in the FTP inbound adapter) " in "Service Platform Reference Guide".

! Important note

If the log output destination directory for executing operation commands is set up in the environment variable (CSCFTP_CMD_LOG), cancel the settings.

●Un-deploying the FTP inbound adapter

The execution format for un-deploying the FTP inbound adapter is as follows:

```
<Service Platform installation directory>·CC·admin·bin·cjundeployrar <J2EE server name> -
resname <display name of resource adapter>
```

For details on the cjundeployrar command, see "2.4 Resource operation commands used in the J2EE serve" in "Application Server Command Reference Guide".

●Deleting the FTP inbound adapter

The execution format for deleting the FTP inbound adapter is as follows:

```
<Service Platform installation directory>･CC･admin･bin･cjdeleteres <J2EE server name> -type
rar -resname <display name>
```

For details on the cjdeleteres command, see "2.4 Resource operation commands used in the J2EE server" in "Application Server Command Reference Guide".

3.3.5 Unsetting up an HCSC server

If you unset up an HCSC server, all the set up information is cancelled. If an unset up HCSC server forms a cluster with other HCSC servers, that server is deleted from the cluster.

During the unsetup operation, the repository information just before the unsetup operation is backed up. You can import the backed up repository information into the development environment as and when required. The backup is stored in the following directory with the file name "repository.zip":

```
<Service Platform installation directory>\CSC\spool\manager\unsetup_bk
\repository.zip
```

Note that as a consequence of the HCSC server unsetup, if the HCSC server set up in the repository no longer exists, all the service information is deleted.

This subsection describes the preconditions for the HCSC server unsetup operation, and explains how to execute unsetup.

(1) Preconditions

To unset up an HCSC server, the following conditions must be satisfied:

- The HCSC server to be unset up is in a stopped state

  For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".
- All the service adapters, business processes, and user-defined receptions are in a pre-deployment state

  For details on how to check the status of the service adapters, business processes, and user-defined receptions, see "*5.3.17 Checking the service adapter information*", "*5.3.18 Checking the business process information*", and "*5.3.19 Checking the information of user-defined reception*".
- The backup file (<Service Platform installation directory>･CSC･spool･manager･unsetup_bk･repository.zip) is not accessed

  If the backup file is being accessed, HCSC server unsetup might fail.
- Other commands are not being executed at the same time

(2) How to perform an unsetup

To unset up an HCSC server, execute the cscsvunsetup command in the operating environment. For a test environment that was set up by using the HCSC Easy Setup functionality, use the HCSC Easy Setup functionality to perform unsetup.

For details on the cscsvunsetup command, see "cscsvunsetup (Unsetting up the HCSC server) " in "Service Platform Reference Guide".

The execution format of the cscsvunsetup command is as follows:

```
cscsvunsetup -user <login user ID> -pass <login password> -csc <HCSC server name>
```

! Important note

- If the types of standard receptions for each of the HCSC servers configuring the cluster are different, first unset up the HCSC server for which the specified standard reception types are few.
- If the HCSC server cannot be unset up, eliminate the cause of the error, and then re-execute the unsetup operation.

- As a consequence of unsetting up the HCSC server, if the HCSC server set up in the repository no longer exists, the repository information is deleted along with the business processes and service adapters. To continue to develop the business processes and service adapters before deletion, import the backup file (repository.zip) into the HCSC development environment, and continue development.
- When you perform unsetup by using a database, do not execute the cscsvsetup command (Setting up the HCSC server) and cscsvunsetup command (Unsetting up the HCSC server) on multiple machines at the same time even if the operating environment repositories are assumed to be different.

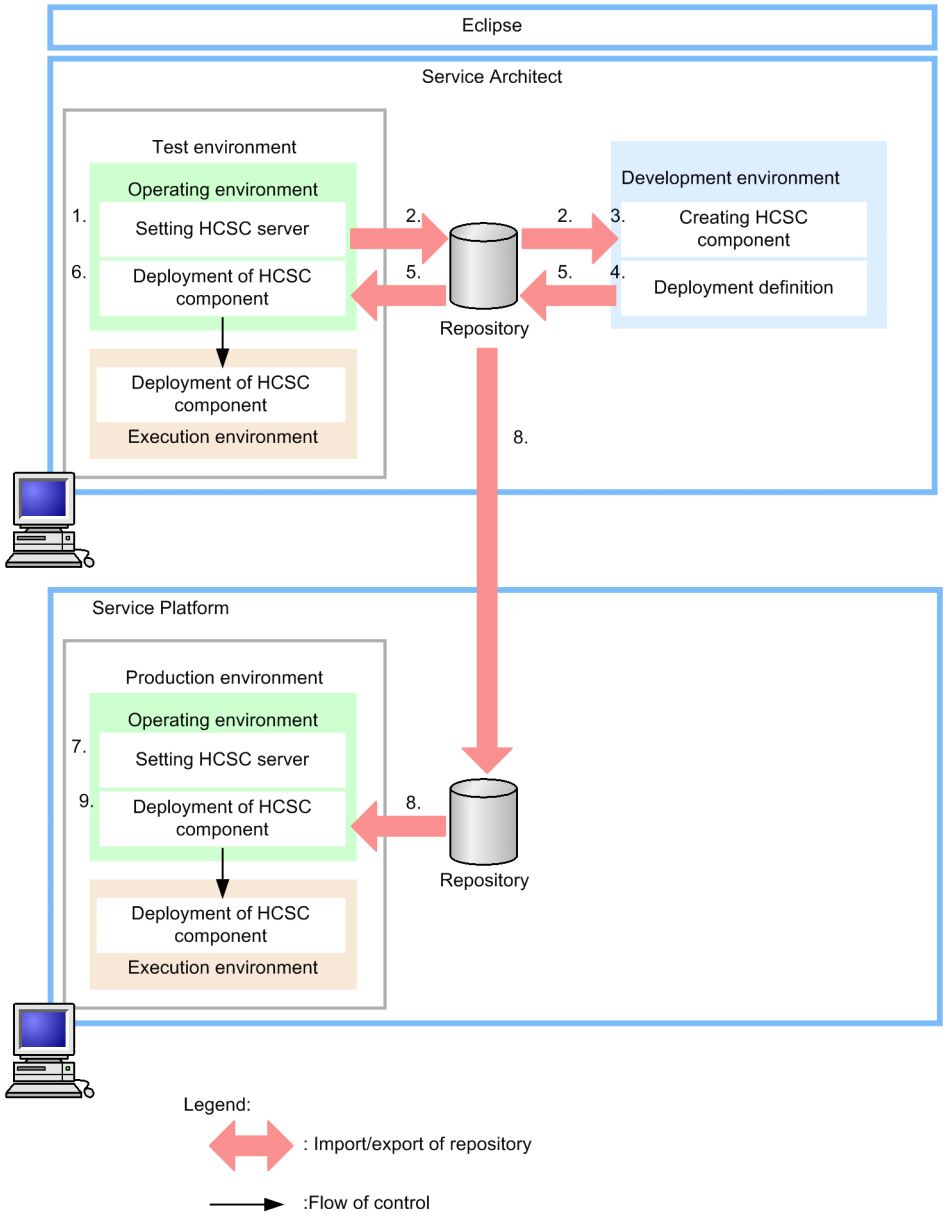
3.4 Procedure for Moving from Test Environment to Production Environment

This section describes the procedure for moving from the test environment to the production environment.

3.4.1 Procedure of migration when the existence of usage of the database and Reliable Messaging in the test and production environments is the same

The following figure shows the migration procedure when the existence of usage of the database and Reliable Messaging in the test environment and production environment are the same. For an overview of migration, see "*1.3(1) Case 1: When configuring with the same settings of the database and Reliable Messaging, in the test environment and the production environment*".

Figure 3–9: Procedure of migration (When the existence of usage of database and Reliable Messaging is the same in the test environment and production environment)



1. Set up the HCSC server in the test environment, and define the system configuration.
   You can set up the HCSC server and define the system configuration by using the HCSC Easy Setup functionality.
2. Export the repository from the operating environment, and import the system configuration definition, specified in the test environment, into the development environment.
3. Create the HCSC components in the development environment.
4. Based on the system configuration definition specified in the test environment, define and update where to deploy the HCSC components in the system configuration (deployment definition).
5. Export the repository containing the deployment definition, specified in the development environment, and import the repository into the operating environment.
6. Based on the deployment definition specified in the development environment, deploy the HCSC components into the test environment.
7. Set up the HCSC server in the production environment, and define the system configuration.

Specify the same settings for the existence of usage of the database and Reliable Messaging in the test environment and production environment.

Also, specify the same SOAP mode in the test environment and production environment.

8. Export the repository containing the deployment definition, specified in the development environment, and import the repository into the operating environment.

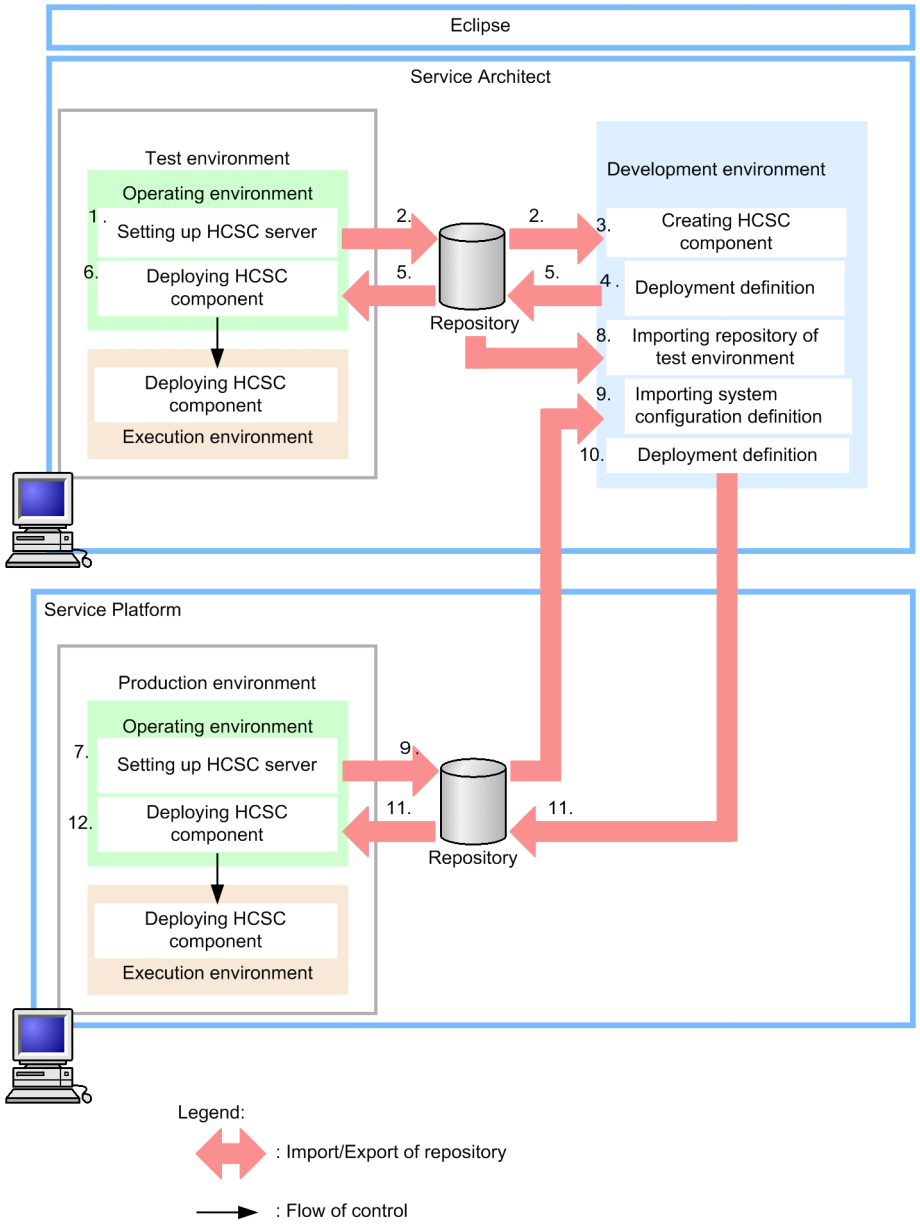
   If standard import is used, you can migrate the test environment repository into the production environment as is, even if the HCSC server name or IP address are different.

9. Based on the deployment definition specified in the development environment, deploy the HCSC components into the production environment.

3.4.2 Procedure of migration from an environment where both database and Reliable Messaging are used to an environment where both are not used

The following figure shows the migration procedure when both database and Reliable Messaging are used in the test environment, and both database and Reliable Messaging are not used in the production environment. For an overview of migration, see "*1.3(3) Case 3: When configuring with the different settings of the database and Reliable Messaging, in the test environment and in the production environment (When re-creating a repository)*".

Figure 3–10: Figure Procedure of migration (When migrating from an environment where both database and Reliable Messaging are used to an environment where both are not used)



1. Set up the HCSC server in the test environment, and define the system configuration.

   You can set up the HCSC server and define the system configuration by using the HCSC Easy Setup functionality. When setting up the HCSC server by using the HCSC Easy Setup functionality, select the model with DB/RM.

2. Export the repository from the operating environment, and import the system configuration definition, specified in the test environment, into the development environment.
3. Create the HCSC components in the development environment.
4. Based on the system configuration definition specified in the test environment, define and update where to deploy the HCSC components in the system configuration (deployment definition).

   At this time, the system configuration definition that forms the base of the deployment definition specifies settings for using both database and Reliable Messaging.

5. Export the repository containing the deployment definition, specified in the development environment, and import the repository into the operating environment.

6. Based on the deployment definition specified in the development environment, deploy the HCSC components into the test environment.
7. Set up the HCSC server in the production environment, and define the system configuration.

   In the HCSC server setup definition file, specify "OFF" for the db-use property and "OFF" for the rm-use property.

   Also, specify the same SOAP mode in the test environment and production environment.
8. Import the system configuration definition and service definition specified in the test environment into the development environment.
9. Export the repository from the operating environment of the production environment, and import the system configuration definition specified in the production environment into the development environment.
10. Based on the system configuration definition specified in the production environment, define and update where to deploy the system configuration definition in the system configuration (deployment definition).

    At this time, the system configuration definition that forms the base of the deployment definition specifies settings for not using both database and Reliable Messaging.

    Note that an error occurs if a deployment definition is specified for the asynchronous receptions, asynchronous service adapters, and persistent business processes.
11. Export the repository containing the deployment definition, specified in the development environment, and import the repository into the operating environment.

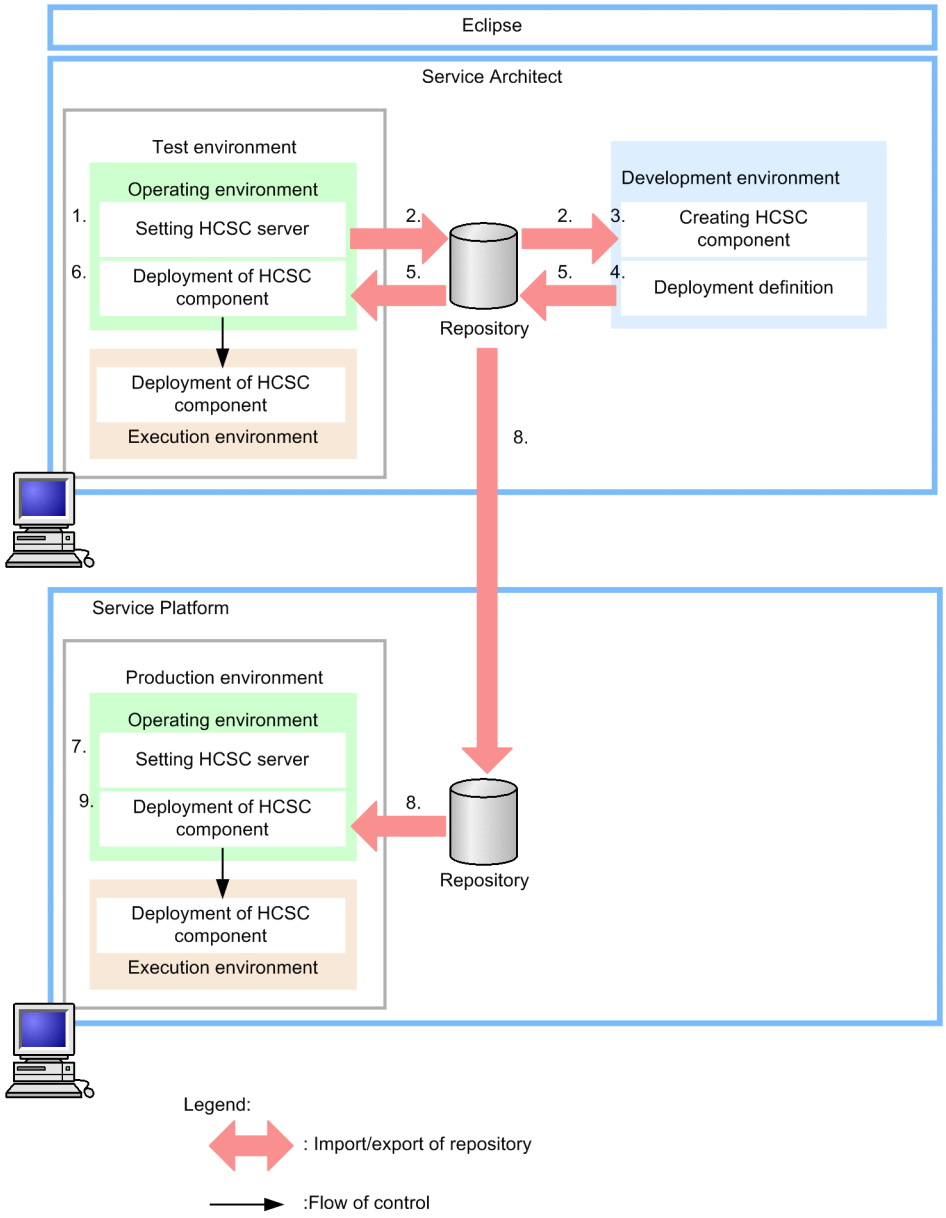
    For the test environment repository (repository imported in 8.), migrate the repository (repository imported in 9.) in which the system configuration definition for the production environment is specified, into the production environment.
12. Based on the deployment definition specified in the development environment, deploy the HCSC components into the production environment.

    The HCSC components are deployed in the production environment with a configuration for not using both database and Reliable Messaging.

3.4.3 Procedure of migration from an environment where both database and Reliable Messaging are not used to an environment where both are used

The following figure shows the migration procedure when both database and Reliable Messaging are not used in the test environment, and both database and Reliable Messaging are used in the production environment. For an overview of migration, see "*1.3(2) Case 2: When configuring with different settings of the database and Reliable Messaging, in the test environment and the production environment (When repository can be moved as it is)*".

Figure 3–11: Figure Procedure of migration (When migrating from an environment where both database and Reliable Messaging are not used to an environment where both are used)



1. Set up the HCSC server in the test environment, and define the system configuration.

   You can set up the HCSC server and define the system configuration by using the HCSC Easy Setup functionality. When setting up the HCSC server by using the HCSC Easy Setup functionality, select the model without DB/RM.

2. Export the repository from the operating environment, and import the system configuration definition, specified in the test environment, into the development environment.
3. Create the HCSC components in the development environment.
4. Based on the system configuration definition specified in the test environment, define and update where to deploy the HCSC components in the system configuration (deployment definition).

   At this time, the system configuration definition that forms the base of the deployment definition specifies settings for not using both database and Reliable Messaging.

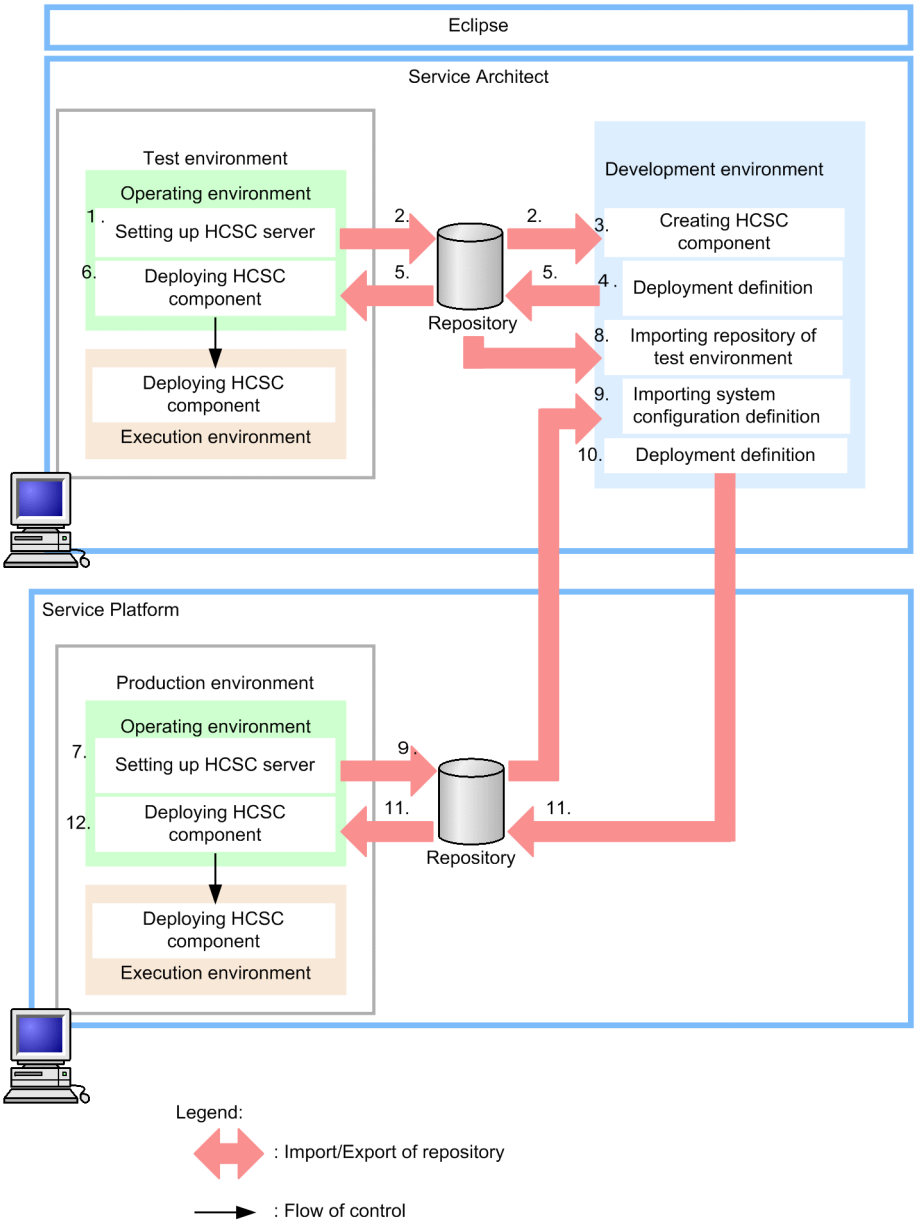
5. Export the repository containing the deployment definition, specified in the development environment, and import the repository into the operating environment.
6. Based on the deployment definition specified in the development environment, deploy the HCSC components into the test environment.

7. Set up the HCSC server in the production environment, and define the system configuration.
   In the HCSC server setup definition file, specify "ON" for the db-use property, and "ON" for the rm-use property.
   Also, specify the same SOAP mode in the test environment and production environment.
8. Export the repository containing the deployment definition, specified in the development environment, and import the repository into the operating environment.
   If standard import is used, you can migrate the test environment repository into the production environment as is, even if the HCSC server name or IP address are different.
9. Based on the deployment definition specified in the development environment, deploy the HCSC components into the production environment.
   The system configuration defined in 7 takes priority in the production environment, so the HCSC components are deployed with the configuration for using both database and Reliable Messaging.

3.4.4 Procedure of migration from an environment where both database and Reliable Messaging are used to an environment where database is used and Reliable Messaging is not used

The following figure shows the migration procedure when both database and Reliable Messaging are used in the test environment, and database is used and Reliable Messaging is not used in the production environment. For an overview of migration, see "*1.3(3) Case 3: When configuring with the different settings of the database and Reliable Messaging, in the test environment and in the production environment (When re-creating a repository)*".

Figure 3–12: Figure Procedure of migration (When migrating from an environment where both database and Reliable Messaging are used to an environment where database is used and Reliable Messaging is not used)



1. Set up the HCSC server in the test environment, and define the system configuration.

   You can set up the HCSC server and define the system configuration by using the HCSC Easy Setup functionality. When setting up the HCSC server by using the HCSC Easy Setup functionality, select the model with DB/RM. When the execution log is not used, you can also select the model without DB/RM. For the migration procedure when the model without DB/RM is selected, see "*3.4.5 Procedure of migration from an environment where both database and Reliable Messaging are not used to an environment where database is used and Reliable Messaging is not used*".

2. Export the repository from the operating environment, and import the system configuration definition, specified in the test environment, into the development environment.
3. Create the HCSC components in the development environment.
4. Based on the system configuration definition specified in the test environment, define and update where to deploy the HCSC components in the system configuration (deployment definition).

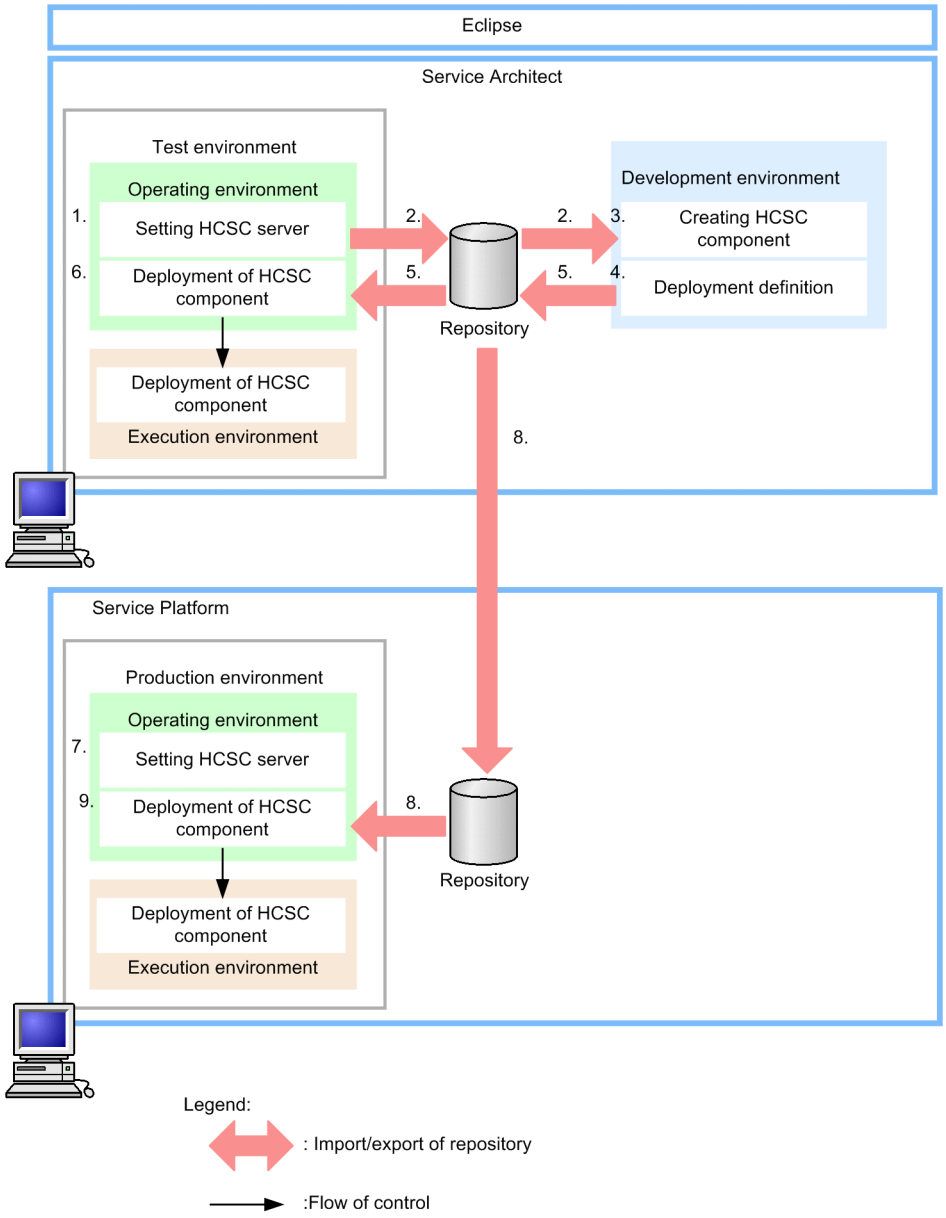
At this time, the system configuration definition that forms the base of the deployment definition specifies settings for using both database and Reliable Messaging.

5. Export the repository containing the deployment definition, specified in the development environment, and import the repository into the operating environment.
6. Based on the deployment definition specified in the development environment, deploy the HCSC components into the test environment.
7. Set up the HCSC server in the production environment, and define the system configuration.
   In the HCSC server setup definition file, specify "ON" for the db-use property and "OFF" for the rm-use property.
   Also, specify the same SOAP mode in the test environment and production environment.
8. Import the system configuration definition and service definition specified in the test environment into the development environment.
9. Export the repository from the operating environment of the production environment, and import the system configuration definition specified in the production environment into the development environment.
10. Based on the system configuration definition specified in the production environment, define and update where to deploy the system configuration definition in the system configuration (deployment definition).
    At this time, the system configuration definition that forms the base of the deployment definition specifies settings for using the database and not using Reliable Messaging.
    Note that an error occurs if a deployment definition is specified for the asynchronous receptions, asynchronous service adapters, and persistent business processes.
11. Export the repository containing the deployment definition, specified in the development environment, and import the repository into the operating environment.
    For the test environment repository (repository imported in 8.), migrate the repository (repository imported in 9.) in which the system configuration definition for the production environment is specified, into the production environment.
12. Based on the deployment definition specified in the development environment, deploy the HCSC components into the production environment.
    The HCSC components are deployed in the production environment with a configuration for using the database and not using Reliable Messaging.

3.4.5 " INDEXITEM="procedure of migration [when migrating from environment where both database and Reliable Messaging are not used to environment where database is used and Reliable Messaging is not used]">Procedure of migration from an environment where both database and Reliable Messaging are not used to an environment where database is used and Reliable Messaging is not used

The following figure shows the migration procedure when both database and Reliable Messaging are not used in the test environment, and the database is used and Reliable Messaging is not used in the production environment. For an overview of migration, see "*1.3(2) Case 2: When configuring with different settings of the database and Reliable Messaging, in the test environment and the production environment (When repository can be moved as it is)*".

Figure 3–13: Figure Procedure of migration (When migrating from an environment where both database and Reliable Messaging are not used to an environment where database is used and Reliable Messaging is not used)



1. Set up the HCSC server in the test environment, and define the system configuration.

   You can set up the HCSC server and define the system configuration by using the HCSC Easy Setup functionality. When setting up the HCSC server by using the HCSC Easy Setup functionality, select the model with DB/RM.

2. Export the repository from the operating environment, and import the system configuration definition, specified in the test environment, into the development environment.
3. Create the HCSC components in the development environment.
4. Based on the system configuration definition specified in the test environment, define and update where to deploy the HCSC components in the system configuration (deployment definition).

   At this time, the system configuration definition that forms the base of the deployment definition specifies settings for not using both database and Reliable Messaging.

5. Export the repository containing the deployment definition, specified in the development environment, and import the repository into the operating environment.

6. Based on the deployment definition specified in the development environment, deploy the HCSC components into the test environment.
7. Set up the HCSC server in the production environment, and define the system configuration.

   In the HCSC server setup definition file, specify "ON" for the db-use property and "OFF" for the rm-use property.

   Also, specify the same SOAP mode in the test environment and production environment.
8. Export the repository containing the deployment definition, specified in the development environment, and import the repository into the operating environment.

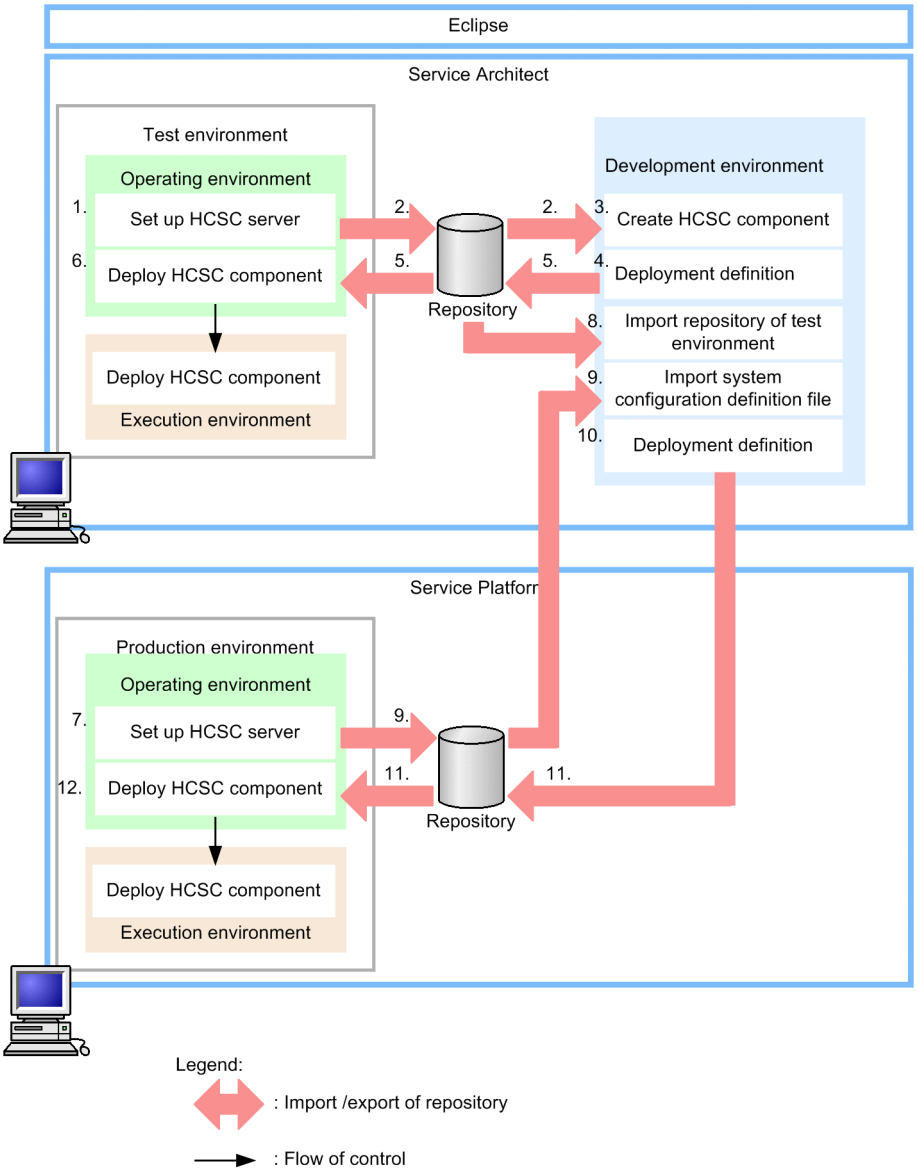
   If standard import is used, you can migrate the test environment repository into the production environment as is, even if the HCSC server name or IP address are different.
9. Based on the deployment definition specified in the development environment, deploy the HCSC components into the production environment.

   The system configuration defined in 7 takes priority in the production environment, so the HCSC components are deployed with the configuration for using the database and not using Reliable Messaging.

3.4.6 Procedure of migration from an environment where database is used and Reliable Messaging is not used to an environment where both are not used

The following figure shows the migration procedure when database is used and Reliable Messaging is not used in the test environment, and both database and Reliable Messaging are not used in the production environment. For an overview of migration, see "*1.3(3) Case 3: When configuring with the different settings of the database and Reliable Messaging, in the test environment and in the production environment (When re-creating a repository)*".

Figure 3–14: Figure Procedure of migration (when migrating from an environment where database is used and Reliable Messaging is not used to an environment where both are not used)



1. Set up the HCSC server in the test environment, and define the system configuration.

   You can set up the HCSC server and define the system configuration by using the HCSC Easy Setup functionality. When setting up the HCSC server by using the HCSC Easy Setup functionality, select a model with DB and without RM.

2. Export the repository from the operating environment, and import the system configuration definition, specified in the test environment, into the development environment.
3. Create the HCSC components in the development environment.
4. Based on the system configuration definition specified in the test environment, define and update where to deploy the HCSC components in the system configuration (deployment definition).

   At this time, the system configuration definition that forms the base of the deployment definition specifies settings for using the database and not using Reliable Messaging.

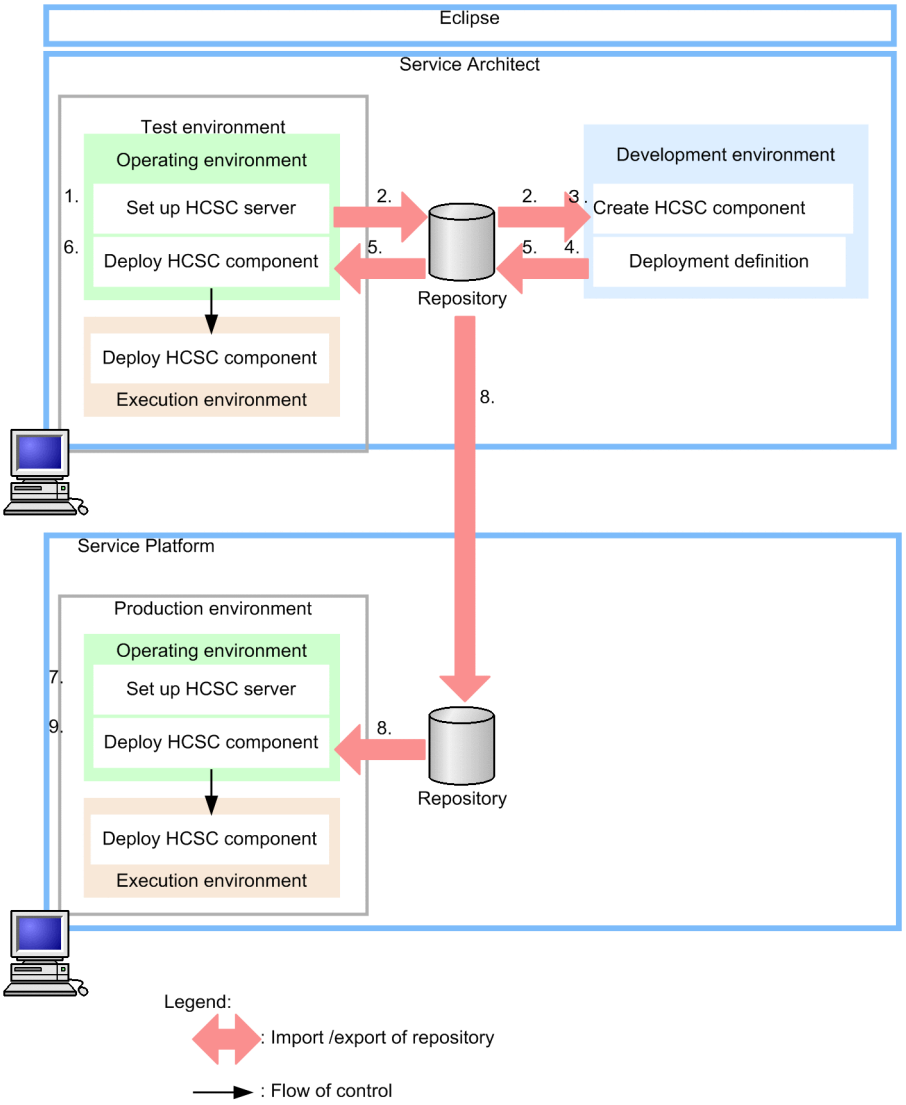
5. Export the repository containing the deployment definition, specified in the development environment, and import the repository into the operating environment.
6. Based on the deployment definition specified in the development environment, deploy the HCSC components into the test environment.

7. Set up the HCSC server in the production environment, and define the system configuration.
   In the HCSC server setup definition file, specify "OFF" for the db-use property and "OFF" for the rm-use property.
   Also, specify the same SOAP mode in the test environment and production environment.
8. Import the system configuration definition and service definition specified in the test environment into the development environment.
9. Export the repository from the operating environment of the production environment, and import the system configuration definition specified in the production environment into the development environment.
10. Based on the system configuration definition specified in the production environment, define and update where to deploy the system configuration definition in the system configuration (deployment definition).
    At this time, the system configuration definition that forms the base of the deployment definition specifies settings for not using both database and Reliable Messaging.
    Note that an error occurs if a deployment definition is specified for the asynchronous service adapters, and persistent business processes.
11. Export the repository containing the deployment definition, specified in the development environment, and import the repository into the operating environment.
    For the test environment repository (repository imported in 8.), migrate the repository (repository imported in 9.) in which the system configuration definition for the production environment is specified, into the production environment.
12. Based on the deployment definition specified in the development environment, deploy the HCSC components into the production environment.
    The HCSC components are deployed in the production environment with a configuration for not using both database and Reliable Messaging.

3.4.7 Procedure of migration from an environment where the database is used and Reliable Messaging is not used to an environment where both are used

The following figure shows the migration procedure when database is used and Reliable Messaging is not used in the test environment, and both database and Reliable Messaging are used in the production environment. For an overview of migration, see "*1.3(2) Case 2: When configuring with different settings of the database and Reliable Messaging, in the test environment and the production environment (When repository can be moved as it is)*".

Figure 3–15: Figure Procedure of migration (when migrating from an environment where the database is used and Reliable Messaging is not used to an environment where both are used)



1. Set up the HCSC server in the test environment, and define the system configuration.

   You can set up the HCSC server and define the system configuration by using the HCSC Easy Setup functionality. When setting up the HCSC server by using the HCSC Easy Setup functionality, select a model with DB and without RM.

2. Export the repository from the operating environment, and import the system configuration definition, specified in the test environment, into the development environment.
3. Create the HCSC components in the development environment.
4. Based on the system configuration definition specified in the test environment, define and update where to deploy the HCSC components in the system configuration (deployment definition).

   At this time, the system configuration definition that forms the base of the deployment definition specifies settings for using the database and not using Reliable Messaging.

5. Export the repository containing the deployment definition, specified in the development environment, and import the repository into the operating environment.
6. Based on the deployment definition specified in the development environment, deploy the HCSC components into the test environment.
7. Set up the HCSC server in the production environment, and define the system configuration.

   In the HCSC server setup definition file, specify "ON" for the db-use property and "ON" for the rm-use property.

Also, specify the same SOAP mode in the test environment and production environment.

8. Export the repository containing the deployment definition, specified in the development environment, and import the repository into the operating environment.

   If standard import is used, you can migrate the test environment repository into the production environment as is, even if the HCSC server name or IP address are different.

9. Based on the deployment definition specified in the development environment, deploy the HCSC components into the production environment.

   The system configuration defined in 7 takes priority in the production environment, so the HCSC components are deployed with the configuration for using both database and Reliable Messaging.

3.5 Easy Setup of production environment

With the HCSC production environment Easy Setup functionality, various information required for the production environment can be auto set. Also, the information set by the HCSC production environment Easy Setup functionality can be easily changed and the automatic un-setup of the production environment that is set up with the HCSC production Easy Setup functionality can be performed.

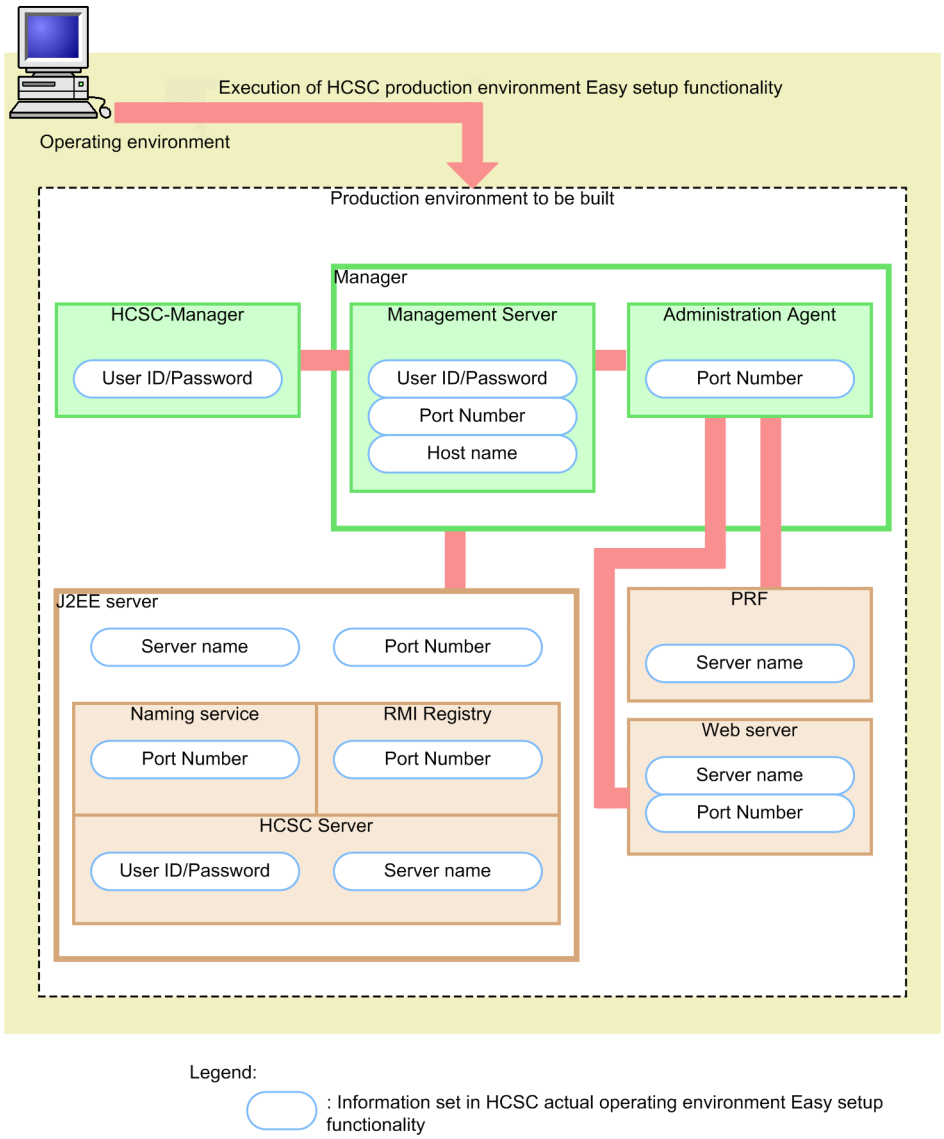
You need not be aware of the various commands required in the production environment setup when performing batch setup using the HCSC production environment Easy Setup functionality. Also, you can perform execution without being aware of the commands when validating or changing the information that is set with the HCSC production Easy Setup functionality or also when unsetting up the production environment set up using the HCSC actual environment Easy Setup functionality.

This section describes the outline and methods to use the HCSC production environment Easy Setup functionality.

3.5.1 Environment that can be set up with the Easy Setup functionality for the HCSC production environment

The configuration of the production environment that is set up by using the environment functionality that can be set up with the Easy Setup functionality for the HCSC production environment is as shown in the following figure. You cannot set up the processes other than those shown in the following figure by using the Easy Setup functionality for the HCSC production environment. To use processes other than those shown in the following figure in the production environment, specify the settings with a method that does not use the Easy Setup functionality for the HCSC production environment (hereafter, normal method).

Figure 3–16: Figure Production environment configuration set up by using the Easy Setup functionality for the HCSC production environment



When you use the Easy Setup functionality for the HCSC production environment, you can automatically set up information such as the user ID, password, port number, and host name for each production environment process shown in Figure 3-16. For details on the information set up in the production environment when Easy Setup functionality for the HCSC production environment is used, see "*3.5.4 Operating the production environment that was set up with the Easy Setup functionality for the HCSC production environment*".

Note the following points when you set up the environment by using the Easy Setup functionality for the HCSC production environment:

- You cannot set up a remote execution environment with Easy Setup functionality for the HCSC production environment.
- You cannot use the Easy Setup functionality for the HCSC production environment and the HCSC Easy Setup functionality (setup of test environment) together. To use one setup functionality in an environment that is already set up by using another functionality, unset up the environment, and then set up the environment by using another setup functionality.
- You can set up only one HCSC server in an environment set up by using the Easy Setup functionality for the HCSC production environment. Do not set up the second HCSC server.

- An environment set up by using the Easy Setup functionality for the HCSC production environment cannot be operated from another machine. To perform operations from another machine, use the cscsvsetup command to perform the setup. For details on how to perform the setup using the cscsvsetup command, see "*3.1.3 Setting up an HCSC server*".
- If setup or unsetup is performed by using the Easy Setup functionality for the HCSC production environment, and if the setup or unsetup does not terminate normally, you cannot upgrade the version.

Note the following additional points in UNIX:

- When changing Component Container Administrator during update installation, change the file attributes beneath the following directory in the same manner as Component Container Administrator:
  - Directories beneath the repository root
  - Directories beneath the log directory
  - Directories beneath the response message output directory
  - Directories beneath the system management information directory
  - Directory of the SQL script file
  - Directory of the SOAP fault operation definition file
  - User message trace directory

  For details on how to change the file attributes, see "*Appendix A How to Change the Service Coordinator Administrator*".

  Set up permissions for the directories and the files in the directories as follows:

  Above directories and files in the directories

  Grant write permission to all the users.

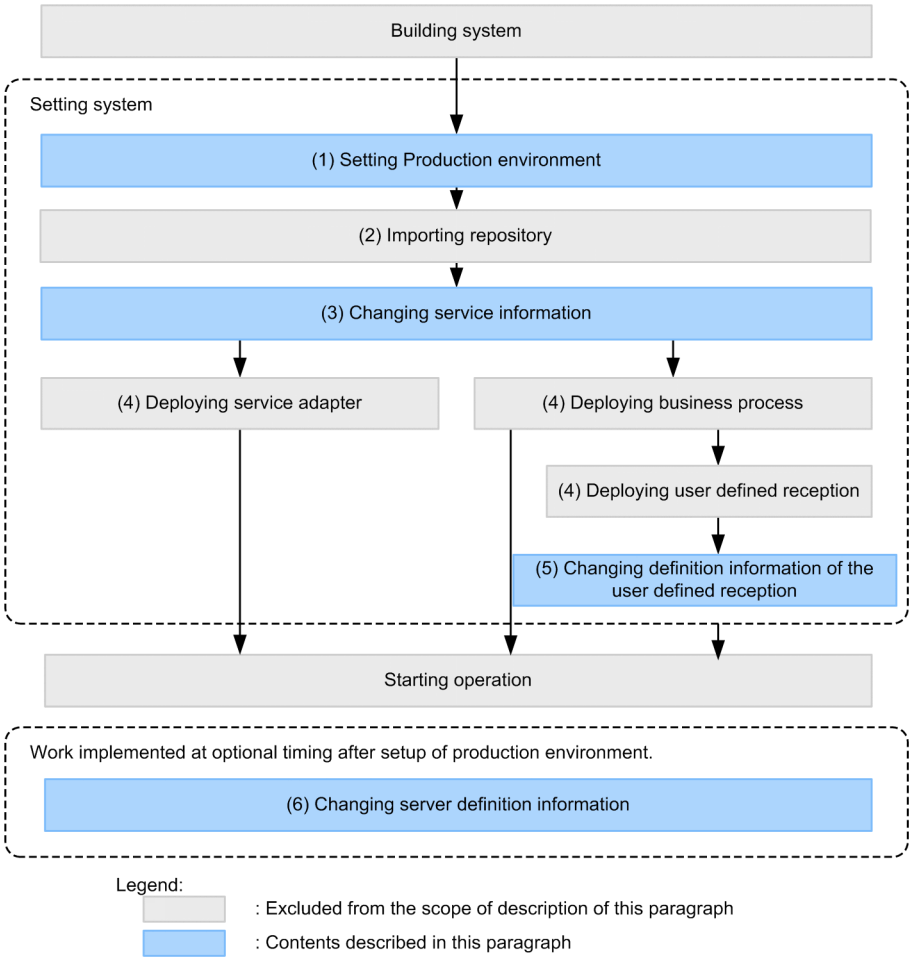
  Parent directories of the above directories

  Grant execution permission. However, if the above directories are not changed from their default values, execution permission need not be granted.
- When changing to Component Container Administrator that does not have the root permission, specify 1024 or higher port number.

3.5.2 Flow of system setup using Easy Setup functionality for the HCSC production environment

The following figure shows the flow of system setup using Easy Setup functionality for the HCSC production environment.

Figure 3–17: Figure Flow of setup (When the Easy Setup functionality for the HCSC production environment is used)



Important note

Specify settings so that Management Server and Administration Agent start automatically when the OS starts.

The following paragraphs describe the operations for setting up a system by using the Easy Setup functionality for the HCSC production environment.

(1) Setting up the production environment

Set up the production environment by using the Easy Setup functionality for the HCSC production environment. To setup the production environment by using the Easy Setup functionality for the HCSC production environment, you must create the definition file by using the template file. For the setup of the production environment, see "*3.5.3(1) Setting up the production environment* ".

(2) Importing the repository

Import the repository created in the development environment into the operating environment. For details on importing the repository, "*4.3 Importing a repository*".

(3) Changing the service information

Change the service information set up by using the Easy Setup functionality for the HCSC production environment. For details on changing the set up service information, see "*3.5.3(2) Changing the setup information*".

(4) Deploying a service adapters, business processes, and user-defined receptions

Deploy the service adapters, business processes, and user-defined receptions in the execution environment. For details on deploying the service adapters, business processes, and user-defined receptions, see "*3.1.8 Deploying a service adapter*", "*3.1.13 Deploying a business process*", and "*3.1.14 Deploying a user-defined reception*".

(5) Changing the definition information of the user-defined reception

Change the definition information of the user-defined reception set up by using the Easy Setup functionality for the HCSC production environment. For details on changing the definition information of the set up user-defined reception, see "*3.5.3(2) Changing the setup information*".

(6) Changing the server definition information

Change the definition information for the server at any time after setting up the production environment. For details on changing the server definition information, see "*3.5.3(2) Changing the setup information*".

3.5.3 Executing the Easy Setup functionality for the HCSC production environment

This subsection describes the procedure for setting up the production environment, changing the setup information, and performing unsetup by using the Easy Setup functionality for the HCSC production environment.

(1) Setting up the production environment

This subsection describes the preconditions for setting up the production environment by using the Easy Setup functionality for the HCSC production environment, and explains the procedure of setup.

(a) Preconditions

The preconditions for setting up the production environment are as follows:

Status of the system when the Easy Setup functionality for the HCSC production environment is used

When you set up the production environment by using the Easy Setup functionality for the HCSC production environment, the system must be in one of the following states:

- Service Platform has just been installed
- If the production environment was set up once by using the Easy Setup functionality for the HCSC production environment, the environment was unset up by using the Easy Setup functionality for the HCSC production environment
- If the test environment was set up once by using the Easy Setup functionality for the test environment, the environment was unset up by using the Easy Setup functionality for the test environment

Setting up the environment variables

To set up the production environment by using the Easy Setup functionality for the HCSC production environment, the environment variable must be specified. For details on the environment variables, see "4.1.13 Items to be checked when the logical server environment variables are set up" in "Application Server System Setup and Operation Guide".

(b) Setup procedure

To set up the production environment by using the Easy Setup functionality for the HCSC production environment, you must use the template file to create the definition file. The following shows the setup procedure in the production environment:

1. Copy the template file to any directory (preparation environment).
   For details on the template file to be copied and the storage location of the template file, see "*3.5.5 Definition files used with the Easy Setup functionality for the HCSC production environment*".
2. Edit the template file and create the definition file.

For details on the template file to be edited, see "*3.5.5 Definition files used with the Easy Setup functionality for the HCSC production environment*".

3. Copy the definition file created in 2 from the preparation environment to any directory in the production environment.
4. Execute the cscsetup command to set up the production environment.
   Specify the storage destination directory for the definition file in the -setup option and then execute the command.

```
cscsetup -setup <storage destination directory for the definition file>
```

For details on the cscsetup command, see "cscsetup (Easy setup of the production environment) " in "Service Platform Reference Guide".

5. Change the HTTP Server definition file.
   For details on the definition file to be changed, see "*3.5.5 Definition files used with the Easy Setup functionality for the HCSC production environment*".

(2) Changing the setup information

You can change the information that was set up by using the Easy Setup functionality for the HCSC production environment. You can change the following information:

- Service information
- Definition information for user-defined receptions
- Definition information for servers

This subsection describes the preconditions for changing the information that was set up by using the Easy Setup functionality for the HCSC production environment, and explains the change procedure.

(a) Preconditions

The preconditions for changing the information that was set up by using the Easy Setup functionality for the HCSC production environment are as follows:

- The production environment was set up by using the Easy Setup functionality for the HCSC production environment.
- All the logical servers are in a stopped state.

Furthermore, if the information to be changed is the service information or definition information for user-defined receptions, the following conditions must be satisfied:

When changing the service information

- The repository is imported from the development environment.
- The HCSC components are in an un-deployed state.

When changing the definition information for user-defined receptions

- The HCSC components are in a deployed state.

(b) Change procedure

To change the information that was set up by using the Easy Setup functionality for the HCSC production environment:

1. Apply the information to be changed in the definition files created in the preparation environment at setup, and change the definition files.
   The definition files to be changed differ as follows depending on the information to be changed:
   - Service information: service-information change definition file (cscadpconfig.properties)
   - Definition information for user-defined receptions: User-defined reception runtime definition file (cscurcptnconfig_id.properties)
   - Definition information for servers: Easy Setup definition file (SOA.xml)

For details on the definition files to be changed, see "*3.5.5 Definition files used with the Easy Setup functionality for the HCSC production environment*".

2. Copy the definition file changed in 1 from the preparation environment to the production environment.

   Copy the directory where the definition file is stored.

3. Execute the cscsetup command to change the information set up in the production environment.

   Specify the storage destination directory for the definition file in the -change option and then execute the command.

```
cscsetup -change <storage destination directory for the definition file>
```

For details on the cscsetup command, see "cscsetup (Easy setup of the production environment) " in "Service Platform Reference Guide".

(3) Unsetting up production environment

This subsection describes the preconditions for unsetting up the production environment that was set up by using the Easy Setup functionality for the HCSC production environment, and explains how to perform unsetup.

! Important note

To unset up the production environment that was set up by using the Easy Setup functionality for the HCSC production environment, the state of the files other than snapshotlog.conf, snapshotlog2.conf, c4websv.cfg, and c4webcom.cfg returns to the one during installation. Therefore, make a backup for the files that were manually changed by the user, and then perform unsetup.

(a) Preconditions

The preconditions for unsetting up the production environment that was set up by using the Easy Setup functionality for the HCSC production environment are as follows:

- The production environment is in the state as the one immediately after setup was executed by using the Easy Setup functionality for the HCSC production environment (the HCSC components are in an un-deployed state).
- Management Server and Administration Agent are running.

(b) How to perform unsetup

To unset up the production environment that was set up by using the Easy Setup functionality for the HCSC production environment, execute the cscsetup command by specifying the -unsetup option.

```
cscsetup -unsetup
```

For details on the cscsetup command, see "cscsetup (Easy setup of the production environment) " in "Service Platform Reference Guide".

(4) Points to be considered when changing or unsetting up the information of the set up production environment

The notes on changing or unsetting up the information of the set up production environment are as follows:

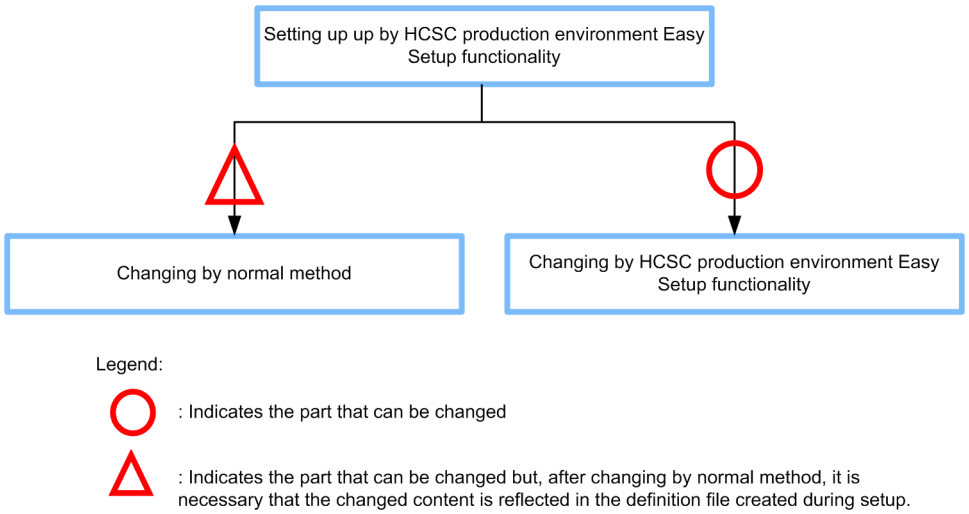
(a) Points to be considered when performing setup by using the Easy Setup functionality for the HCSC production environment

When an error occurs or when a sudden problem must be handled, the production environment that was set up by using the Easy Setup functionality for the HCSC production environment is sometimes changed or unset up with a normal method. The following paragraphs describe the relationship with the normal method for changing and unsetting up the information that was set up by using the Easy Setup functionality for the HCSC production environment:

Changing the information that was set up by using the Easy Setup functionality for the HCSC production environment

The following figure shows the changing of the information that was set up by using the Easy Setup functionality for the HCSC production environment.

Figure 3–18: Figure Changing of the information that was set up by using the Easy Setup functionality for the HCSC production environment



If the information that was set up by using the Easy Setup functionality for the HCSC production environment is changed with the normal method, you must apply the changed contents to the definition file created during setup, and then change the definition information of the production environment. However, the information of the following Service Platform-related definition files need not be changed:

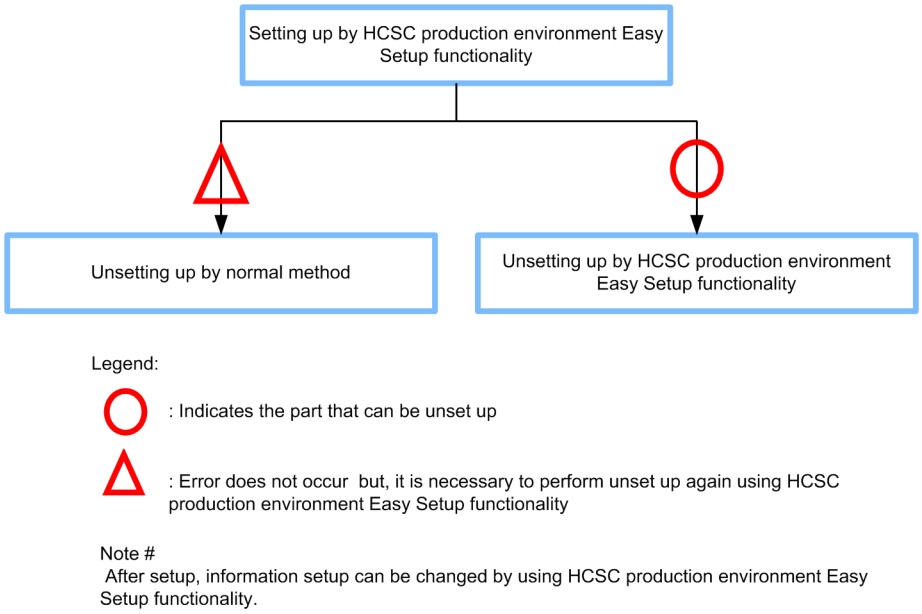
- HCSC-Manager definition file (cscmng.properties)
- HCSC-Manager command definition file (csccmd.properties)
- HCSC server configuration definition file (cscsvsetup.xml)
- HCSC server setup definition file (cscsvsetup.properties)
- Server runtime definition file (cscsvconfig.properties)
- User-defined reception runtime definition file (cscurcptnconfig_id.properties)
- Service-information change definition file (cscadpconfig.properties)

For details on how to change the definition information, see "*(2) Changing the setup information*".

Unsetting up production environment that was set up by using the Easy Setup functionality for the HCSC production environment

The following figure shows the unset up of production environment that was set up by using the Easy Setup functionality for the HCSC production environment.

Figure 3–19: Figure **Unsetting up production environment that was set up by using the Easy Setup functionality for the HCSC production environment**



If a production environment that was set up by using the Easy Setup functionality for the HCSC production environment is unset up with the normal method, the unsetup operation must be performed again by using the Easy Setup functionality for the HCSC production environment as follows:

1. After performing unsetup with the normal method, re-execute setup with the normal method, and return the production environment to the state when the environment was set up by using the Easy Setup functionality for the HCSC production environment.
2. Perform unsetup by using the Easy Setup functionality for the HCSC production environment.

(b) Points to be considered when performing setup without using the Easy Setup functionality for the HCSC production environment

A production environment that was set up without using the Easy Setup functionality for the HCSC production environment cannot be changed and unset up by using the Easy Setup functionality for the HCSC production environment.

3.5.4 Operating the production environment that was set up with the Easy Setup functionality for the HCSC production environment

This subsection describes how to operate the production environment that was set up by using the Easy Setup functionality for the HCSC production environment, and the information required for operations.

(1) Starting and stopping the production environment

The following table lists and describes how to start and stop the production environment.

Table 3–27: Table How to start and stop the production environment

Start and stop target	Start and stop method
• Management Server • Administration Agent	Start automatically when the production environment machine starts. Stop automatically when the production environment machine stops.
• Performance Tracer • J2EE server • HCSC server	Execute the following command at the command prompt: When starting:

Start and stop target	Start and stop method
• Performance Tracer • J2EE server • HCSC server	<Service Platform installation directory>\CSC\bin\cscsvstart.bat -system When stopping: <Service Platform installation directory>\CSC\bin\cscsvstop.bat -system For details on how to start, stop, and operate the Performance Tracer and J2EE server, see "Application Server System Setup and Operation Guide". For details on how to start, stop, and operate the HCSC server, see "*5.3.4 Starting HCSC server*" and "*5.3.33 Terminating the HCSC Server*".

(2) Information required for the production environment operations

If you perform setup by using the Easy Setup functionality for the HCSC production environment, the information required for the production environment operations is automatically set up. The following paragraphs describe the information specified in the production environment that was set up by using the Easy Setup functionality for the HCSC production environment. Note that the items for which fixed values are specified cannot be changed with the Easy Setup functionality for the HCSC production environment.

(a) User ID and password information

The following table lists and describes the user ID and password information specified in the production environment that was set up with the Easy Setup functionality for the HCSC production environment.

Table 3–28: Table User ID and password set up in the production environment

Setup destination	Set up user ID or password	Fixed value	Description
Management Server	Management User ID	admin	Management User ID for logging in to Management Server
	Password	admin	Password for logging in to Management Server
HCSC-Manager	HCSC-Manager login user ID	admin	User ID for logging in to HCSC-Manager
	HCSC-Manager login password	admin	Password for logging in to HCSC-Manager

(b) Port number information

The following table lists and describes the port number information specified in the production environment that was set up with the Easy Setup functionality for the HCSC production environment.

Table 3–29: Table Port number set up in the production environment

Setup destination	Set up port number	Default value	Description
Management Server	Port number for operating the HCSC server	28099	Port number used for accessing Management Server from HCSC-Manager
	Port number for operating the logical server	28080	Port number used for accessing Management Server from Smart Composer or management portal screen
	Port number for receiving the termination requests	28005	Port number used for internal management by Management Server
	Port number for internal communication	28009	Port number used for internal management by Management Server
	Port number for in-process naming service	28900	Port number used for internal management by Management Server

Setup destination	Set up port number	Default value	Description
Administration Agent	Port number for connecting to Agent	20295	Port number for internal management, used to access Administration Agent from Management Server
J2EE server	Port number for receiving SessionBeans	900	Port number used for accessing HCSC server from Management Server, or for accessing a standard reception (SessionBean) from a service requester
	Port number for checking operations	23152	Port number used for internal management by HCSC server
	Port number for simple web server	8080	Port number used for internal management by HCSC server
Web server	Port number for receiving requests	80	Port number that receives requests

(c) Name information

The following table lists and describes the information, such as the host name and server name, specified in the production environment that was set up with the Easy Setup functionality for the HCSC production environment. For names other than those listed in the table, see the values specified in each template file.

Table 3–30: Table Names specified in the production environment

Setup destination	Set up name	Fixed value	Description
Management Server	Host name	localhost	Management Server host name
HCSC-Manager	Manager name	Manager	HCSC-Manager specific distinguished name used by HCSC-Manager to identify Manager
PRF	Server name	PRF	Name for identifying the logical server or cluster
J2EE server	Server name	J2EEServer	Name of the J2EE server that sets up the HCSC server
Cluster	Cluster name	Cluster	Cluster name
HCSC server	HCSC server name	HCSC	HCSC server name
Web server	Server name	WebServer	Name used for identifying the logical server or cluster

(d) Reception information

The following table lists and describes the reception information specified in the production environment that was set up with the Easy Setup functionality for the HCSC production environment.

Table 3–31: Table Reception information specified in the production environment

Reception information	Fixed value
Standard synchronous reception (SessionBean)	OFF
Standard synchronous reception (Web service)	ON
Standard asynchronous reception (MDB (WS-R))	OFF
Standard asynchronous reception (MDB and (DB queue))	OFF
User-defined reception	ON

3.5.5 Definition files used with the Easy Setup functionality for the HCSC production environment

When performing setup by using the Easy Setup functionality for the HCSC production environment, use the template files to create the definition files. Also, when changing the set up information, change the created definition file. Note that the template files are stored in the following directory:

```
<Service Platform installation directory>\CSC\config\manager\templates\hsetup
\esb
```

The following table describes whether the definition files and template files to be used with the Easy Setup functionality for the HCSC production environment are provided. Note that this subsection describes the items that are edited when the definition files are created or changed, and the items for which values different from default values are set up in the Easy Setup functionality for the HCSC production environment. For details on the items and definition files other than those described here, see the manual description locations listed in the "Reference manual" and "Reference section" columns in the table.

Table 3–32: Table Provision of definition files and template files used with the Easy Setup functionality for the HCSC production environment

No.	Definition file name	Creatability during setup	Changea bility	Existence of template file	Reference manual	Reference section
1	Manager configuration file (manager.cfg)	M	--	Yes	Application Server Definition Reference Guide	10.10
2	Administration Agent property file (adminagent.properties)	M	--	Yes		10.2
3	Management Server environment configuration file (mserver.properties)	M	--	Yes		10.7
4	Client common settings property file (cmxclient.properties)	M	--	Yes		4.4
5	Client common definition file (mngsvrutilcl.properties)	M	--	Yes		10.17
6	snapshot log primary delivery target definition file (snapshotlog.conf)	Y	--	No		12.2
7	snapshot log secondary delivery target definition file (snapshotlog.2.conf)	Y	--	No		12.2
8	Server definition file (SOAP Communication Infrastructure) (c4websv.cfg)	M	--	Yes	Application Server SOAP Application Development Guide	10.2
9	Common definition file (SOAP Communication Infrastructure) (c4webcom.cfg)	M	--	Yes		10.4
10	HCSC-Manager definition file (cscmng.properties)	M	--	Yes	Service Platform Reference Guide	HCSC-Manager definition file
11	HCSC-Manager command definition file (csccmd.properties)	M	--	Yes		HCSC-Manager command definition file
12	HCSC server configuration definition file (cscsvsetup.xml)	M	--	Yes		HCSC server configuration definition file

No.	Definition file name	Creatability during setup	Changeability	Existence of template file	Reference manual	Reference section
13	HCSC server setup definition file (cscsvsetup.properties)	M	--	Yes	Service Platform Reference Guide	HCSC server setup definition file
14	HCSC server runtime definition file (cscsvconfig.properties)	M	--	Yes		HCSC server runtime definition file
15	User-defined reception runtime definition file (cscurcptnconfig_id.properties)	A	Y#	Yes		user-defined reception runtime definition file
16	Service-information change definition file (cscadpconfig.properties)	A	Y#	Yes		Service-information change definition file
17	Easy Setup definition file (SOA.xml)	M	Y#	Yes	Application Server Definition Reference Guide	4.6
18	HTTP Server definition file (httpsd.conf)	A	x	No	HTTP Server	Specific location not applicable.
19	cscsetup command definition file (cscsetup.properties)	Y	--	Yes	Service Platform Reference Guide	cscsetup command definition file

Legend:

M: Necessarily created.

Y: Created and changed as and when required.

A: Need not be created. Ignore even if created.

x: An error occurs if this file exists. Delete the file.

-: Do not change.

Yes: Template file is provided.

No: Template file is not provided.

Note#

The following table describes the mapping between the definition file to be changed and the information to be changed:

Information to be changed	Definition file to be changed
Service information	Service-information change definition file (cscadpconfig.properties)
Definition information for user-defined receptions	User-defined reception runtime definition file (cscurcptnconfig_id.properties)
Definition information for servers	Easy Setup definition file (SOA.xml)

Important note

Do not change the name of the definition file, excluding the user-defined reception runtime definition file (cscurcptnconfig_id.properties).

(1) Description format of the definition files

The format for describing the definition files in this subsection is as follows:

File name

Specifies the name of the definition file.

Description

Specifies the description of the definition file.

File storage destination

Specifies the storage destination of the definition file.

Items to be edited #

Specifies the items to be edited when the definition file is created and changed.

Items for which values different from default values are specified#

Specifies the items for which values different from default values are specified when the setup is performed by using the Easy Setup functionality for the HCSC production environment.

Note#

The table contents of these items are as follows:

Category

The items in the definition file are categorized.

Item name

Specifies the names of items to be edited when the definition file is created or changed, and the items for which values different from default values are specified in the Easy Setup functionality for the HCSC production environment.

Parameters to be specified (or specified) in <param-name>

Specifies parameters to be specified or that are specified in the <param-name> tag. Applicable only to the Easy Setup definition file (SOA.xml).

Default value

Specifies the default values for the definition file. If the value of an item is omitted, the default value is assumed.

Values specified in the Easy Setup functionality for the HCSC production environment

Specifies the values specified in the definition file when the setup is performed by using the Easy Setup functionality for the HCSC production environment.

Description

Specifies the description of the item.

Content specified in <param-value>

Specifies the contents to be set up in the <param-value> tag. Applicable only to the Easy Setup definition file (SOA.xml).

(2) Manager configuration file

File name

manager.cfg

Description

Specifies the common settings for the components and commands to be operated in Management Server and Administration Agent respectively.

Items to be edited

Item name	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Description
com.cosminexus.manager.log.dir #	<Manager installation directory>・log	--	Specifies the Manager log output directory.

Legend:

-: None

Note#

There are items to be edited during setup.

Items for which values different from default values are specified

Item name	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Description
com.cosminexus.manager.log.compatible	true	false	Specifies the upward compatibility of Manager log.

(3) Administration Agent property file

File name

adminagent.properties

Description

Specifies the settings related to Administration Agent.

Items to be edited

Item name	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Description
adminagent.adapter.port#	20295	20295	Specifies the port number used by Administration Agent. Must match the value of <agent-port> under <host> in the Easy Setup definition file (SOA.xml).
adminagent.snapshotlog.log_dir#	<directory specified in com.cosminexus.manager.log.dir of manager.cfg >・snapshot	--	Specifies the snapshot log output destination directory as a character string.
adminagent.j2ee.watch.interval	10	10	Specifies the operation confirmation interval for J2EE servers in seconds.
adminagent.hws.watch.interval	10	10	Specifies the operation confirmation interval for HTTP Server in seconds.
adminagent.j2ee.watch.retry_count	1	1	Specifies the retry count when the operation confirmation processing fails during the confirmation of J2EE server operations.

Item name	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Description
adminagent.hws.watch.retry_count	1	1	Specifies the retry count when the operation confirmation processing fails during the confirmation of HTTP Server operations.
adminagent.j2ee.watch.start_time	45	45	Specifies the time period from the execution of the start command to the start of operation confirmation when the J2EE server is started, in seconds.
adminagent.hws.watch.start_time	0	0	Specifies the time period from the execution of the start command to the start of operation confirmation when HTTP Server is started, in seconds.
adminagent.j2ee.watch.timeout	60	60	Specifies the time until timeout during the confirmation of J2EE server operations, in seconds.
adminagent.hws.watch.timeout	60	60	Specifies the time until timeout during the confirmation of HTTP Server operations, in seconds.

Legend:
-: None

Note#
There are items to be edited during setup.

Items for which values different from default values are specified

Item name	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Description
adminagent.adapter.allowedHosts	--	localhost	Specifies the host name or IP address that is allowed access to the server.
adminagent.adapter.bind_host	localhost	--	Specifies the host name or IP address to be used for communication with Administration Agent.
adminagent.hws.watch.method	HEAD	OPTIONS	Specifies the HTTP method for confirming the HTTP Server operations when 2 is specified in adminagent.hws.watch.level.
adminagent.snapshotlog.num_snapshots	10	4	Specifies the number of snapshot log files for each logical server, collected as primary data.
adminagent.snapshotlog.listfile.2.num_snapshots	10	4	Specifies the number of snapshot log files for each logical server, collected as secondary data.
adminagent.j2ee.process.console_log.enabled	false	true	Specifies whether to output the console output information of a J2EE server to the console log.

Legend:
-: None

(4) Management Server environment configuration file

File name

mserver.properties

Description

Specifies the settings for the port number used by Management Server, and the operations of commands for detecting errors.

Items to be edited

Category	Item name	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Description
Settings for the port number used by Management Server	webserver.connector.ajp13.port#	--	28009	Specifies the port number for internal communication of Management Server.
	webserver.connector.http.port#	--	28080	Specifies the HTTP port number for Management Server connection. This value must match the value of cmx.connect.host in the client common settings property file (cmxclient.properties), and the value of mngsvrutil.connect.host in the client common definition file (mngsvrutilcl.properties).
	webserver.shutdown.port#	--	28005	Specifies the port number for receiving the Management Server termination requests.
	ejbserver.naming.port#	28900	28900	Specifies the port number to be used for internal management by Management Server.
	webserver.connector.http.permitted.hosts#	When not defined: * When not set up: localhost	*	Specifies the host that is allowed to access Management Server and IP address or host name of the Administration Agent operating host.
Settings for operations of error detection commands	com.cosminexus.mngsvr.management.port#	28099	28099	Specifies the external connection port number for the Management Server remote management function.
	com.cosminexus.mngsvr.management.listen.port#	0	0	Specifies the port number for client connection, which is created during an external connection to the Management Server remote management function.
Settings for the HCSC operation mode	ejbserver.server.edition.settingforce	Smart	--	Specifies whether Management Server is to be used from HCSC-Manager. • Smart Management Server is not used from HCSC-Manager. • <Not specified> Management Server is used from HCSC-Manager.

Category	Item name	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Description
Settings for the HCSC operation mode	ejbserver.server.edition .settingforce	Smart	--	If "Smart" is specified, the settings for ejbserver.naming.port are ignored.

Legend:
-: None

Note#
There are items to be edited during setup.

Items for which values different from default values are specified

Category	Item name	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Description
Settings for operations of error detection commands	com.cosminexus.mngsvr.management.enabled	false	true	Specifies whether to enable the Management Server remote management function.
	com.cosminexus.mngsvr.management.connector.enabled	false	true	Specifies whether to enable the external connection to the Management Server remote management function.
	com.cosminexus.mngsvr.management.host	--	localhost	Specifies the host name or IP address when fixing the host of the external connection to the Management Server remote management function.
	java.rmi.server.hostname	--	localhost	Specifies the host name or IP address when fixing the host of the external connection to the Management Server remote management function.

Legend:
-: None

(5) Client common settings property file

File name

cmxclient.properties

Description

Specifies the default values for the common arguments of the commands provided with the Smart Composer functionality. This file is used to set up common default values for all the clients.

Items to be edited

Item name	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Description
cmx.apply_user#	--	SYSTEM, Administrator	Specify the user ID of the OS for the client that applies this file.
cmx.connect.host#	--	localhost: 28080	Specifies the host name and port number that is assumed when the -m option of the common arguments is omitted. This value must match the value of webserver.connector.http.port in the

Item name	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Description
cmx.connect.host#	--	localhost: 28080	Management Server environment configuration file (mserver.properties), and the value of mngsvrutil.connect.host in the client common definition file (mngsvrutilcl.properties).

Legend:
-: None

Note#
There are items to be edited during setup.

Items for which values different from default values are specified

Item name	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Description
cmx.connect.userid	--	admin	Specifies the user ID that is assumed when the -u option of the common arguments is omitted.
cmx.connect.passwd	--	admin	Specifies the password that is assumed when the -p option of the common arguments is omitted.
cmx.verbose	false	true	Specify true to set the -verbose option of the common arguments as the default, and specify false to set the -noverbose option as the default.
cmx.websystem.name	--	SOA	Specifies the Web system name used when the -s option of the following commands is omitted: • cmx_build_system • cmx_define_application • cmx_define_resource • cmx_delete_serverref • cmx_delete_system • cmx_deploy_application • cmx_deploy_resource • cmx_list_model • cmx_list_status • cmx_resume_lb • cmx_start_application • cmx_s

Legend:
-: None

(6) Client common definition file

File name

mngsvrutilcl.properties

Description

Specifies the default values of the options for the mngsvrutil command as the common definition.

Items to be edited

Item name	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Description
mngsvrutil.apply_user#	--	SYSTEM,Administrator	Specifies the user who applies the client common definition file in the OS user when executing the mngsvrutil command or adapter command.
mngsvrutil.connect.host#	--	localhost: 28080	Specifies the host name and port number of Management Server specified in the -m option of the mngsvrutil command. This value must match the value of webserver.connector.http.port in the Management Server environment configuration file (mserver.properties), and the value of cmx.connect.host in the client common settings property file (cmxclient.properties).

Legend:

-: None

Note#

There are items to be edited during setup.

Items for which values different from default values are specified

Item name	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Description
mngsvrutil.connect.password	--	admin	Specifies the password to be specified in the -p option of the mngsvrutil command.
mngsvrutil.connect.userid	--	admin	Specifies the user ID to be specified in the -u option of the mngsvrutil command.
mngsvrutil.target_name	--	J2EEServer	Specifies the logical server name or host name to be specified in the -t option of the mngsvrutil command.

Legend:

-: None

(7) Snapshot log primary delivery target definition file

File name

snapshotlog.conf

Description

Defines the target file of primarily sent data for collecting the snapshot log. No template file is provided for this file.

File storage destination

<Service Platform installation directory>・manager・config

Items to be edited

Category	Item name	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Description
Directory to be collected	%val%#	--	--	Specifies the output destination of the HCSC-Manager log file.

Category	Item name	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Description
Directory to be collected	%val%#	--	--	If cscmng.log.dir is customized in cscmng.properties, the following two values must be added. If cscmng.log.dir is not customized, the log file output destination is already specified, so the values need not be added. • Value with "/.+" added to the definition value in cscmng.log.dir • Value with "/mmap/.+" added to the definition value in cscmng.log.dir **(Example of settings)** If cscmng.log.dir is D:/Home/log/Manager/HCSCManager • D:/Home/log/Manager/HCSCManager/.+ • D:/Home/log/Manager/HCSCManager/mmap/.+

Legend:

-: None

Note#

There are items to be edited during setup.

Items for which values different from default values are specified

None

(8) Snapshot log secondary delivery target definition file

File name

snapshotlog.2.conf

Description

Defines the target file of secondarily sent data for collecting the snapshot log. No template file is provided for this file.

File storage destination

<Service Platform installation directory>・manager・config

Items to be edited

Category	Item name	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Description
Directory for collection	%val%#	--	--	Specifies the output destination for the backup file of HCSC-Manager. If cscmng.backup.dir is customized in cscmng.properties, the following two values must be added. If cscmng.backup.dir is not customized, the backup file output destination is already specified, so the values need not be added. • Value with "/.+" added to the definition value in cscmng.backup.dir **(Example of settings)** If cscmng.backup.dir is D:/Home/log/Manager/HCSCManager/backup

Category	Item name	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Description
Directory for collection	%val%#	--	--	• D:/Home/log/Manager/HCSCManager/backup/.+
	%val%#	--	--	Specifies the location for allocating the repository. If cscmng.repository.dir is customized in cscmng.properties, the following three values must be added. If cscmng.repository.dir is not customized, the repository allocation location is already specified, so the values need not be added. • Value with "/.+" added to the definition value in cscmng.repository.dir • Value with "/.+/.+" added to the definition value in cscmng.repository.dir • Value with "/.+/.+/.+" added to the definition value in cscmng.repository.dir **(Example of settings)** If cscmng.repository.dir is D:/Home/work/Manager/HCSCManager/repository • D:/Home/work/Manager/HCSCManager/repository/.+ • D:/Home/work/Manager/HCSCManager/repository/.+/.+ • D:/Home/work/Manager/HCSCManager/repository/.+/.+/.+

Legend:

-: None

Note#

There are items to be edited during setup.

Items for which values different from default values are specified

None

(9) Server definition file (SOAP Communication Infrastructure)

File name

c4websv.cfg

Description

Specifies the information required for server-side operations on SOAP Communication Infrastructure.

Items to be edited

None

Items for which values different from default values are specified

None

(10) Common definition file (SOAP Communication Infrastructure)

File name

c4webcom.cfg

Description

Specifies the information required for the common server and client operations on SOAP Communication Infrastructure.

Items to be edited

None

Items for which values different from default values are specified

Category	Item name	default value	Values specified in the Easy Setup functionality for the HCSC production environment	Description
Log settings	c4web.logger.aplog_error_record	NONE	ALL	Specifies the settings for the output of application log when an error occurs.

(11) HCSC-Manager definition file

File name

cscmng.properties

Description

Specifies the information required for HCSC-Manager operations.

Items to be edited

Category	Item name	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Description
Repository settings	cscmng.repository.root#	<Service Platform installation directory>・CSC・repository	--	Specifies the root directory of the repository with the absolute path.
Log settings	cscmng.log.dir#	<Service Platform installation directory>・CSC・log・manager	--	Specifies the log output destination directory with the absolute path.
Environment backup	cscmng.envbackup.dir#	Current directory	--	Specifies the output destination directory for the environment backup file when the environment is backed up with cscenvbackup.

Legend:

-: None

Note#

There are items to be edited during setup.

Items for which values different from default values are specified

Category	Item name	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Description
Settings for HCSC server operation	cscmng.server.HCSC.system	--	WebServer,PRF	Specifies the logical servers to be managed in the HCSC system.

Legend:
-: None

(12) HCSC-Manager command definition file

File name

csccmd.properties

Description

Specifies the default values for the command options used with Service Platform.

Items to be edited

None

Items for which values different from default values are specified

Category	Item name	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Description
Common command definitions	csc.all.user	--	admin	Specifies the default values for the arguments common to all the commands.
	csc.all.pass	--	admin	
csccompoconfig common definitions	csc.compoconfig.operation	--	get	
	csc.compoconfig.csc	--	HCSC	
csccompodeploy common definitions	csc.compodeploy.csc	--	HCSC	
csccompostart common definitions	csc.compostart.csc	--	HCSC	
csccompostop common definitions	csc.compostop.csc	--	HCSC	
csccompoundeploy common definitions	csc.compoundeploy.csc	--	HCSC	
cscrcptnstart common definitions	csc.rcptnstart.csc	--	HCSC	
cscrcptnstop common definitions	csc.rcptnstop.csc	--	HCSC	
cscresinfo common definitions	csc.resinfo.csc	--	HCSC	
cscstatus common definitions	csc.status.csc	--	HCSC	
	csc.status.type	--	system	
cscsvconfig common definitions	csc.svconfig.operation	--	get	
	csc.svconfig.csc	--	HCSC	
cscsvstart common definitions	csc.svstart.csc	--	HCSC	
cscsvstop common definitions	csc.svstop.csc	--	HCSC	
	csc.svstop.force	--	Not set up	

Legend:
-: None

(13) HCSC server configuration definition file

File name

cscsvsetup.xml

Description

Specifies the configuration information for the HCSC server.

Items to be edited

Category	Item name	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Description
Definition of manager	<port>port number of Manager</port>[#]	28099	28099	Specifies the port number for connecting to the remote management function of Manager. This value must match the value of com.cosminexus.mngsvr.management.port in Management Server environment configuration file (mserver.properties).

Note#

There are items to be edited during setup.

Items for which values different from default values are specified

Category	Item name	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Description
Definition of cluster	<name>Cluster name</name>	--	Cluster	Specifies the cluster name.
Definition of manager	<name>Manager name</name>	--	Manager	Specifies the HCSC-Manager-specific distinguished name used by HCSC-Manager to identify Manager.
	<ip-address>IP address of Manager</ip-address>	--	localhost	Specifies the IP address where Management Server is started.
	<id>Management User ID of Manager</id>	--	admin	Specifies the Management User ID of Management Server.
	<password>Management User password of Management Server</password>	--	admin	Specifies the Management User password of Management Server.
Definition of csc-server	<name>HCSC server name</name>	--	HCSC	Specifies the HCSC server name.
	<j2ee-server-name>Name of J2EE server that sets up the HCSC server </j2ee-server-name>	--	J2EEServer	Specifies the name of the J2EE server where HCSC server is set up.
	<setup-properties>HCSC server setup definition file name</setup-properties>	--	cscsvsetup.properties	Specifies the name of the HCSC server setup definition file with the relative path, or absolute path.
Definition of soap-reception	<ip-address> IP address of %Web server</ip-address>	--	localhost	Specifies the IP address where the Web server is running.
	<port>Port number of %Web server</port>	--	80	Specifies the reception port number of the Web server.

Category	Item name	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Description
Definition of soap-reception	<protocol>Protocol type</protocol>	--	http	Specifies the Web server reception protocol.

Legend:
-: None

(14) HCSC server setup definition file

File name

cscsvsetup.properties

Description

Specifies the contents that can be set up when the HCSC server is set up.

Items to be edited

None

Items for which values different from default values are specified

Category	Item name	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Description
Related to setup configuration	db-use	--	OFF	Specifies whether to use a database with HCSC server.
	rm-use	--	OFF	Specifies whether to use Reliable Messaging with HCSC server.
Related to standard receptions	request-ejb	--	OFF	Specifies whether to use the standard synchronous reception (SessionBean).
	request-soap	--	ON	Specifies whether to use the standard synchronous reception (Web service).
	request-jms	--	OFF	Specifies whether to use the standard asynchronous reception (MDB (WS-R)).
	request-dbq	--	OFF	Specifies whether to use the standard asynchronous reception (MDB and (DB queue)).
Related to user-defined receptions	request-userdef-soap	--	ON	Specifies whether to use SOAP receptions.

Legend:
-: None

(15) HCSC server runtime definition file

File name

cscsvconfig.properties

Description

Specifies the post-setup HCSC server definition information from HCSC-Manager.

Items to be edited

None

Items for which values different from default values are specified

Category	Item name	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Description
Data transformation	xmltelegram-namespace-complement	--	ON	Specifies whether to complement the name space declaration corresponding to the name space prefix specified for the attribute values in an XML message for the XML messages flowing in the HCSC server.

Legend:
-: None

(16) User-defined reception runtime definition file

File name

cscurcptnconfig_id.properties

Description

Specifies the SOAP reception information.

When using the user-defined reception runtime definition file, change the file name to "cscurcptnconfig_<reception ID>.properties" and then execute the file. If the reception ID is "rcp1", change the file name to "cscurcptnconfig_rcp1.properties" and then execute. Note that if you want to change multiple SOAP receptions, create multiple files for each SOAP reception.

Items to be edited

Item name	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Description
user-defined-reception-soap.threads.maximum#	10	20	Specifies the maximum number of concurrent executions of the SOAP reception.
user-defined-reception-soap.exclusive.threads#	0	0	Specifies the number of dedicated threads of the SOAP reception.
user-defined-reception-soap.queue-size#	8192	10	Specifies the pending queue size of the SOAP reception.

Note#
Items to be edited during tuning.

Items for which values different from default values are specified

None

(17) Service-information change definition file

File name

cscadpconfig.properties

Description

Specifies the changes in the service information for the service adapter.

Items to be edited

Category	Item name	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Description
Service information of the SOAP adapter	Cluster.<service ID>.WebService.url[#1]	Value specified during service adapter development	--	Specifies the URL to be used for invoking a service component.
	Cluster.<service ID>.WebService.c4web.application.socket_read_timeout[#2]	300	--	Specifies the read timeout value for the service adapter socket in seconds.

Legend:

-: None

Note#1

There are items to be edited during setup.

Note#2

Items to be edited during tuning.

Items for which values different from default values are specified

None

(18) Easy Setup definition file

File name

SOA.xml

Description

Defines the Web system.

Items to be edited

Category	Parameters to be specified in <param-name>	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Content specified in <param-value>
Service unit definition/ HTTP Server definition/ common configuration definitions for logical servers	mstartup.force.watchtime	60	60	Specifies the forced-stop monitoring time for the logical servers in seconds.
	mstartup.restartcnt	1	1	Specifies the auto-restart count for the logical servers.
	mstartup.retrywait	60	60	Specifies the auto-restart retry interval for logical servers in seconds.
	mstartup.start.watchtime	60	60	Specifies the start monitoring time for logical servers in seconds.
	mstartup.watchtime	60	60	Specifies the stop monitoring time for logical servers in seconds.
Service unit definition/ HTTP Server definition/ configuration definition for HTTP Server/ Web server definitions	Listen[#1]	--	80	Specifies the IP address and port number that receives the request.

Category	Parameters to be specified in <param-name>	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Content specified in <param-value>
Service unit definition/ HTTP Server definition/ configuration definition for HTTP Server/ Web server definitions	ThreadsPerChild[#2]	40	50	Specifies the number of server threads to be started.Specify this definition only in Windows.
Service unit definition/ HTTP Server definition/ configuration definition for HTTP Server/ redirector operation definition for HTTP Server	JkLogFileDir[#1]	logs	--	Specifies the log file output destination directory. In Windows, use "･" as the path separation character. Note that forward slash (/) cannot be specified.
	JkTraceLogFileDir[#1]	logs	--	Specifies the output destination directory for maintenance trace log files. In Windows, use "･" as the path separation character. Note that forward slash (/) cannot be specified.
Service unit definition/ HTTP Server definition/ configuration definition for HTTP Server/ worker definition	worker.default.cachesize[#2]	64	40	Specifies the number of worker connections that are reused by the redirector. Specify this definition only in Windows.
	worker.default.port[#1]	--	8007	Specifies the worker port number. This value must match the value of webserver.connector.ajp13.port in the Easy Setup definition file (SOA.xml).
	worker.default.receive_timeout[#2]	3600	3600	Specifies the communication timeout value in seconds.
Service unit definition/ HTTP Server definition/ configuration definition for HTTP Server/ HTTP Server log output definition	CustomDivideFileNum[#1]	8	8	Specifies the number of divided log files.
	HttpsdLogFileDir[#1]	logs	--	Specifies the output destination directory for the log output by the Web server. In Windows, use "･" as the path separation character. Note that forward slash (/) cannot be specified.
Service unit definition/ J2EE server definition/ common configuration definitions for logical servers	mstartup.force.watchtime	--	60	Specifies the forced-stop monitoring time of the logical server in seconds.
	mstartup.restartcnt	--	1	Specifies the auto-restart count of the logical server.
	mstartup.retrywait	--	60	Specifies the auto-restart retry interval of the logical server in seconds.
	mstartup.start.watchtime	--	600	Specifies the start monitoring time for logical servers in seconds.
	mstartup.watchtime	--	60	Specifies the stop monitoring time of the logical servers in seconds.
	user.env.variable	--	Not set	Specifies the environment variables for starting the server.
	JAVACOREDIR=%val%[#1]	--	--	Specifies the output destination for the JavaVM thread dump. In Windows, use "･" as the path separation character. Note that forward slash (/) cannot be specified.

Category	Parameters to be specified in <param-name>	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Content specified in <param-value>
Service unit definition/ J2EE server definition/ J2EE server configuration definition/ user properties/ parameters beginning with ejbserver.http	ejbserver.http.port[#1]	8080	8080	Specifies the port number of the simple web server.
Service unit definition/ J2EE server definition/ J2EE server configuration definition/ user properties/ parameters beginning with ejbserver.management	ejbserver.management.JVM.stats_monitor.FullGCCount.interval	600	600	Specifies the threshold value monitoring interval, in the monitoring of the full garbage collection frequency, in seconds.
	ejbserver.management.JVM.stats_monitor.FullGCCount.threshold	10	10	Specifies the frequency that forms the threshold value, in the monitoring of the full garbage collection frequency.
	ejbserver.management.statistics.interval	60	60	Specifies the statistics collection interval in seconds.
	ejbserver.management.stats_file.dir[#1]	<work directory>・ejb・<server name>・stats	--	Specifies the output destination directory of the statistics file. In Windows, use "・" as the path separation character. Note that forward slash (/) cannot be specified.
	ejbserver.management.stats_file.num[#1]	7	8	Specifies the number of statistics files.
Service unit definition/ J2EE server definition/ J2EE server configuration definition/ user properties/ parameters beginning with ejbserver.naming	ejbserver.naming.port[#1]	900	900	Specifies the port of the CORBA Naming Service that the J2EE server uses as a naming service.
Service unit definition/ J2EE server definition/ J2EE server configuration definition/ user properties/ parameters beginning with ejbserver.rmi	ejbserver.rmi.naming.port[#1]	23152	23152	Specifies the port number of the RMI registry used by the J2EE server.
	ejbserver.rmi.remote.listener.port[#1]	0	0	Specifies the port for receiving requests when statistics is collected by a JMX client (such as Administration Agent, JP1/Performance Management - Agent Option for uCosminexus Application Server).
Service unit definition/ J2EE server definition/ J2EE server configuration definition/ user properties/ parameters beginning with ejbserver.watch	ejbserver.watch.defaultRequestQueue.threshold	80	80	Specifies the threshold value that outputs an alert message.
Service unit definition/ J2EE server definition/ J2EE server configuration definition/user property/ parameters beginning with vbroker	vbroker.se.iiop_tp.scm.iiop_tp.listener.port[#1]	0	0	Specifies the communication port to be set up for each J2EE server.
Service unit definition/ J2EE server definition/ J2EE server configuration definition/ user properties/	webserver.connector.ajp13.max_threads[#2]	10	20	Specifies the number of concurrent executions for the Web container to process requests.

Category	Parameters to be specified in <param-name>	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Content specified in <param-value>
parameters beginning with webserver.connector	webserver.connector.ajp13.port#1	8007	8007	Specifies the port number to be used for communication with the Web server. This value must match the value of worker.default.port in Easy Setup definition file (SOA.xml).
Service unit definition/ J2EE server definition/ J2EE server configuration definition/ JavaVM option definition	-Xms%val%#2	256m	1024m	Specifies the initial Java heap size.
	-Xmx%val%#2	512m	1024m	Specifies the maximum Java heap size.
	XX:PermSize=%val%#2	128m	128m	Specifies the initial size of Permanent area.
	XX:MaxPermSize=%val%#2	128m	128m	Specifies the maximum size of Permanent area.
	ejb.public.directory#1	<work directory>・ejb・<server name>・logs	--	Specifies the work directory of the J2EE server. The J2EE server is started, considering the specified directory as the work directory. In Windows, use "・" as the path separation character. Note that forward slash (/) cannot be specified.
	ejb.server.log.directory#1	<work directory>・ejb・<server name>・logs	--	Specifies the log file output destination directory. In Windows, use "・" as the path separation character. Note that forward slash (/) cannot be specified.
Service unit definition/ PRF definition/ common configuration definitions for logical servers	mstartup.force.watchtime	600	60	Specifies the forced-stop monitoring time for logical servers in seconds.
	mstartup.restartcnt	1	1	Specifies the auto-restart count for logical servers.
	mstartup.retrywait	0	0	Specifies the auto-restart retry interval for logical servers in seconds.
	mstartup.start.watchtime	60	60	Specifies the start monitoring time for logical servers in seconds.
	mstartup.watchtime	600	600	Specifies the stop monitoring time for logical servers in seconds.
Service unit definition/ PRF definition/ PRF configuration definition	prfspool#1	&{cosminexus.home}/PRF/spool	--	Specifies the PRF trace output directory. In Windows, use "・" as the path separation character. Note that forward slash (/) cannot be specified.
Host definition	--	20295	20295	Specifies the Administration Agent port number in <agent-port>#1#3 under <host>. This value must match the value of adminagent.adapter.port in the Administration Agent property file (adminagent.properties).

Legend:

-: None

Note#1

There are items to be edited during setup.

Note#2

Items to be edited during tuning.

Note#3

Specified in the tag mentioned in the table and not in <param-value>.

Items for which values different from default values are specified

Category	Parameters specified in <param-name>	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Content specified in <param-value>
Web system definition	--	--	SOA	Specifies the name for identifying the Web system in <name>[#] under <web-system>.
Physical tier definition	--	--	combined-tier	Specifies the type of physical tier in <tier-type>[#] under <tier>.
Service unit definition	--	--	Unit	Specifies the name for identifying the service unit, in <name>[#] under <unit>.
	--	--	localhost	Specifies the host name set in <name-name> in the host definition, the host name defined in the already set up Web system, or @myhost, in <host-ref>[#] under <unit>.
	--	--	combined-tier	Specifies the type of physical tier to which the host specified in <host-ref> belongs, in <hosts-for>[#] under <unit>.
Service unit definition/ HTTP Server definition	--	cmx_<Web system name>_<service unit name>_<type>_<serial number>	WebServer	Specifies the name for identifying the logical server or cluster, in <logical-server-name>[#] under <define-server>.
	--	--	web-server	Specifies the type of logical server defining the configuration, in <logical-server-type>[#] under <define-server>.
Service unit definition/ HTTP Server definition/ configuration definition for HTTP Server/ Web server definitions	KeepAliveTimeout	15	3	Specifies the request waiting time for a KeepAlive connection in seconds.
Service unit definition/ HTTP Server definition/ configuration definition for HTTP Server/ redirector operation definition for HTTP Server	JkMount	/* [J2EE server name] (for combined-tier and http-tier)	/* default	Specifies the URL pattern which is to be transmitted to the Web container server, during a request to HTTP Server.
Service unit definition/ HTTP Server definition/ configuration definition for HTTP Server/ worker definition	worker.default.type	--	ajp13	Specifies the worker type.
	worker.default.host	--	localhost	Specifies the host name or IP address of the worker.
	worker.list	--	default	Specifies the list of worker names.
Service unit definition/ HTTP Server definition/ configuration definition for	HttpsdErrorMethod	Div	Wrap	Specifies the error log output format.

Category	Parameters specified in <param-name>	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Content specified in <param-value>
HTTP Server/ HTTP Server log output definition	HttpsdRequestMethod	Div	Wrap	Specifies the request log output format.
Service unit definition/ J2EE server definition	--	cmx_<Web system name>_<service unit name>_<type>_<serial number>	J2EEServer	Specifies the name for identifying the logical server or cluster in <logical-server-name>[#] under <define-server>.
	--	--	j2ee-server	Specifies the type of logical server defining the configuration, in <logical-server-type>[#] under <define-server>.
Service unit definition/ J2EE server definition/ common configuration definitions for logical servers	mstartup.no	--	80	Specifies an integer as the order for starting the servers during a batch start operation.
Service unit definition/ J2EE server definition/ J2EE server configuration definition/ user properties/ parameters beginning with ejbserver.ext	ejbserver.ext.method_observation.interval	--	10	Specifies whether to use the functionality for monitoring the business application execution time. Also, specifies the time interval for monitoring whether a running request has timed out, and the time interval for canceling a timed out request (method), in seconds.
Service unit definition/ J2EE server definition/ J2EE server configuration definition/ user properties/ parameters beginning with ejbserver.jndi	ejbserver.jndi.global.enabled	true	false	Specifies whether to register an object with the Portable Global JNDI name for the naming service, when the application starts.
Service unit definition/ J2EE server definition/ J2EE server configuration definition/ user properties/ parameters beginning with ejbserver.manager	ejbserver.manager.agent.MEventAgent.enabled	true	false	Specifies whether to enable the Management event issuing functionality.
Service unit definition/ J2EE server definition/ J2EE server configuration definition/ user properties/ parameters beginning with ejbserver.rmi	ejbserver.rmi.naming.host	--	localhost	Specifies the host name or IP address of the RMI registry to be used as the service provider by J2EE server, in a multi-homed host environment.
Service unit definition/ J2EE server definition/ J2EE server configuration definition/ user properties/ parameters beginning with ejbserver.server	ejbserver.server.threaddump.filenum	256	4	Specifies the maximum number of thread dump files to be used when the J2EE server detects an error and voluntarily outputs a thread dump.
Service unit definition/ J2EE server definition/ J2EE server configuration definition/ user properties/ parameters beginning with webserver.connector	webserver.connector.ajp13.bind_host	--	localhost	Specifies the IP address or host name to be used for Web server integration.

Category	Parameters specified in <param-name>	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Content specified in <param-value>
Service unit definition/ J2EE server definition/ J2EE server configuration definition/ JavaVM option definition	add.jvm.arg	--	+	Specifies the output format of the extended verbosegc information in -XX:%val%HitachiCommaVerboseGC.
		--	+	Specifies whether to use the Explicit Memory Management functionality in -XX:%val%HitachiUseExplicitMemory.
Service unit definition/ J2EE server definition/ J2EE server configuration definition/ JavaVMsystem property	ejbserver.container.security.disabled	false	true	Specifies whether to enable the Enterprise Bean access control functionality.
	ejbserver.ctm.enabled	true	false	Specifies whether to use the CTM functionality.
	ejbserver.rmi.stateless.unique_id.enabled	false	true	Specifies whether invocation is not needed for the invocation of the remove method of Stateless Session Bean.
Service unit definition/ J2EE server definition/ J2EE server configuration definition/ Extension parameter of J2EE container	add.class.path	--	<cosminexus.home>･c4web･lib･hitsaaj.jar	Specifies the SOAP Communication Infrastructure as the communication base.
Service unit definition/ J2EE server definition/ J2EE server configuration definition/ SecurityManager	use.security	true	false	Specifies whether to use SecurityManager in the J2EE server startup options.
Service unit definition/ PRF definition	--	cmx_<Web system name>_<service unit name>_<type>_<serial number>	PRF	Specifies the name for identifying the logical server or cluster, in <logical-server-name>[#] under <define-server>.
	--	--	performance-tracer	Specifies the type of logical server defining the configuration, in <logical-server-type>[#] under <define-server>.
Service unit definition/ PRF definition/ common configuration definitions for logical servers	mstartup.no	0	0	Specifies the order for starting the servers during a batch start operation.
Service unit definition/ PRF definition/ PRF configuration definition	PrfTraceLevel	STANDARD	00030000	Specifies the trace collection level of the performance tracer.
Host definition	--	--	localhost	Specifies the name or IP address for identifying the server, in <host-name>[#] under <host>.
	--	Value specified in <host-name>	localhost	Specifies the host name or IP address of Administration Agent in <agent-host>[#] under <host>.

Legend:
-: None

Note#

Specified in the tag mentioned in the table and not in <param-value>.

(19) HTTP Server definition file

File name

httpsd.conf

Description

Specifies the information required for HTTP Server operations. After performing setup by using the Easy Setup functionality for the HCSC production environment, change the file directly, as and when required before you start HTTP Server.

File storage destination

<Service Platform installation directory>・httpsd・servers・HWS_WebServer・conf

Items to be edited

Category	Item name	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Description
Host that is permitted to connect to Web server	<Location %val%>[#]	--	/	Specified to define a directive for the requests to a location indicated by a specific URL.
	Order %val%[#]	--	deny,allow	Specifies the evaluation order for setting up the Allow directive and Deny directive.
	Deny from %val%[#]	--	all	Specified to control the clients that can access the Web server.
	Allow from %val%[#]	--	localhost	Specified to control the clients that can access the Web server.

Legend:

-: None

Note#

There are items to be edited during setup.

Items for which values different from default values are specified

None

(20) cscsetup command definition file

File name

cscsetup.properties

Description

Specifies the information required for the operations of the cscsetup command. This definition file is only enabled in UNIX.

Items to be edited

Item name	Default value	Values specified in the Easy Setup functionality for the HCSC production environment	Description
owner[#1#2]	Superuser	--	Specifies the owner to be set up in Component Container Administrator.
group[#1#2]	Superuser	--	Specifies the group to be set up in Component Container Administrator.

Legend:

-: None

Note#1

There are items to be edited during setup.

Note#2

If the owner and group values are not specified, execute setup and unsetup with the following information.

Table 3–33: Table Set values when the owner and group values are not specified

OS	File owner	Group name
Linux	root	root
HP-UX	root	sys
AIX	root	system

4 Repository Management

This chapter describes how to set, import, export, and reference repository information.

4.1 Overview of a repository

Repository is a directory used for storing information shared between developments and operating environments.

The system configuration information created in an operating environment is used in a development environment. The definition information created in a development environment is used in an operating environment.

(1) Repository information

The information shared in a repository is called as repository information. It consists of the following items:

- System configuration
- A service adapter or a business process, which is generated
- Mapping definition
- Format definition
- Deployment information

(2) Directory used as repository

If you install Service Platform, the following standard directory is set for the repository:

```
<Installation directory of Service Platform>\CSC\repository
```

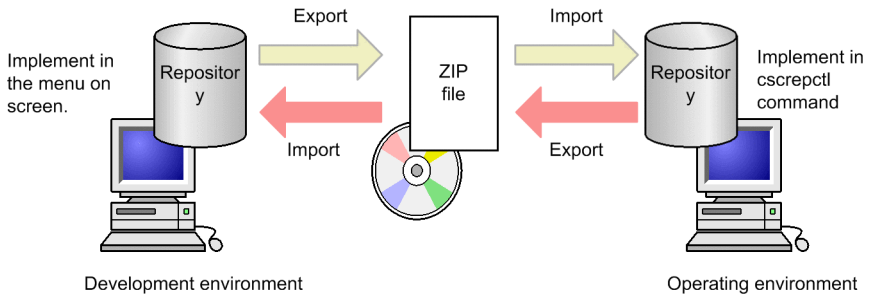
You can also change the directory, which is to be set as a repository. Change it in the HCSC-Manager definition file. For details on how to change the directory, see "*2.4.1 Customizing operating environment*".

When you are setting up multiple operating and execution environments (setting the environment variable CSCMNG_HOME) on 1 machine, the repository is set in the following root directory:

```
%CSCMNG_HOME%\repository
```

To share information in development and operating environments, export (save) the repository information to the media in ZIP file format and import (read) that information to the repository of another environment. The following figure shows import and export of a repository:

Figure 4–1: FigureExport and import of a repository



Here, for details on saving the repository information of an operating environment, see "*4.2 Exporting Repository Information*". For details on expanding the repository information to an operating environment, see "*4.3 Importing a repository*". Moreover, for details on saving the repository information of a development environment and expanding the repository information in a development environment, see "3.2 Managing a Repository" in "Service Platform Basic Development Guide".

! Important note

In 07-60 onwards versions, you cannot share 1 repository between development and operating environments. If you share a repository in a previous version, create separate repositories in development and operating environments and migrate these repositories. For migration procedure, see "Appendix A.3 Migrating procedure when a repository is shared between development environment and operating environment in earlier version" in "Service Platform Basic Development Guide".

(3) Repository exclusion

During operation involving updating of a repository, the repository might get locked and the operation might not be possible. There are 2 types of locks, namely **exclusive lock** and **shared lock**. There are following restrictions during an operation:

- You cannot perform operations, which are meant for exclusive lock or shared lock during exclusive lock.
- You cannot perform operations, which are meant for another shared lock at the same time during shared lock.

The following table describes the lock types and target operations:

Table 4–1: TableLock types and target operations

Lock type	Target operation	Explanation
Exclusive lock	Operation to be performed using update based command	The following commands will be targeted: • csccompodeploy command • csccompoundeploy command • cscpasswd command • cscrepctl command • cscsvcctl command • cscsvsetup command • cscsvunsetup command
Shared lock	Operation to be performed using reference based command	The following commands will be targeted: • cscpidelete command • cscpireexec command • cscpiselect command • cscrepdiff command • cscrepls command • cscstatus command • cscsvcls command • cscsvconfig command • cscutil command • cscresinfo command
	Operation to be performed on the screen of an operating environment	-

Legend:
-: Not applicable.

(4) Points to be considered

- You cannot use a repository, which is created in the development environment of a different version.
- Do not access any file or directory present in the directory used as a repository. If you access, various commands might fail.

4.2 Exporting Repository Information

In the development environment, to use information created in the operating environment, use the `cscrepctl` command to export repository information in ZIP file format. The contents of the created ZIP file cannot be changed.

Enter the following command:

```
cscrepctl -user login-user-ID -pass login-password -export file-name
```

For details about the `cscrepctl` command, see *cscrepctl (Importing/Exporting)* in the *uCosminexus Service Platform Reference Guide*.

4.3 Importing a repository

When using the contents created in a development environment in an operating environment, use the cscrepctl command and import the repository information saved in ZIP file format to the repository.

(1) Import method

Enter the following command:

```
cscrepctl -user <Login-user ID> -pass <Login password> -import <File name>
```

When importing a repository, you must first confirm that any directory or file present in the directory, which is set in the repository, is not being referenced. Then execute the cscrepctl command.

For details on the cscrepctl command, see "cscrepctl (import/export) " in "Service Platform Reference Guide".

(a) Import method

2 types of the import method are as follows:

Standard import

Generally use standard import. Import HCSC components of another repository in the HCSC server configuration information of the current operating environment. The HCSC components existing prior to the import operation are destroyed.

If you want to check whether the configuration information of the HCSC server is same in the repository information of the current operating environment and the repository information to be imported, specify -check option in the cscrepctl command.

Component import

Use this type of import method when you want to add HCSC components of the specified repository ZIP file to the repository of an operating environment. The HCSC components existing prior to the import operation remain. To perform component import, specify the -compo option in the cscrepctl command.

For details on the component import, see "*4.6 Adding, updating, and deleting a repository using component as a unit*".

(b) Method of expanding the repository information

From the following 2 expansion methods, you can select the contents to be expanded in a repository within the repository information saved in ZIP file format:

Difference expansion

Only the changed HCSC components are to be expanded in the repository of an operating environment. The HCSC components, which are not changed, are not expanded in the repository of an operating environment. The HCSC components of the current repository of the operating environment remain as are.

Whole expansion

All the ZIP files to be imported including the HCSC components, which are not changed, are to be extracted in the repository of an operating environment. To perform overall expansion, specify the-overwrite option in the cscrepctl command.

(c) Restrictions on import

You cannot import the repository information in any one of the following cases:

1. If the HCSC server is not set up (in case of standard import)
2. If the HCSC server configuration is different in the current repository information of the operating environment and the repository information to be imported
3. If the currently deployed business process or the service adapter is deleted in the repository information to be imported
4. If information of the currently deployed business process or the service adapter is updated in the repository information to be imported

5. If setting related to the option of whether to use database and Reliable Messaging is different in the current repository information of the operating environment and the repository information to be imported#
6. If SOAP mode of the current repository information of the operating environment and that of the repository information to be imported are different

For 3. and 4, import the repository after deleting the corresponding business process or the service adapter from the execution environment.

Note#

Even if setting related to the option of whether to use database and Reliable Messaging is different in the current repository information of the operating environment and the repository information to be imported, you can perform the import operation for some cases. The following table describes the settings to be performed when import is possible and when import is not possible:

Table 4–2: TableSettings to be performed when import is possible and when import is not possible

Settings to be performed in the repository information to be imported	Settings to be performed in the current repository information of the operating environment		
	Use database as well as Reliable Messaging	Use database and do not use Reliable Messaging	Do not use database as well as Reliable Messaging
Use database as well as Reliable Messaging	Y	N	N
Use database and do not use Reliable Messaging	Y	Y	N
Do not use database as well as Reliable Messaging	Y	Y	Y

Legend:

Y: Can be imported.

N: Cannot be imported.

(2) Auto-backup at the time of import

When importing a repository, auto-backup of the repository information prior to import is to be performed in ZIP file format. The backup file is output to the following directory with cscimport.zip as the file name.

```
<Installation directory of Service Platform>\CSC\spool\manager
```

You can change the output destination directory of the backup file using cscmng.envbackup.dir parameter or cscmng.envbackup.dir.import parameter of HCSC-Manager definition file.

Moreover, you can set the option of whether to perform auto-backup using cscmng.envbackup.autoget parameter or cscmng.envbackup.autoget.off parameter of HCSC-Manager definition file.

For details on HCSC-Manager definition file, see "HCSC-Manager definition file" in "Service Platform Reference Guide".

For details on how to restore an operating environment from the backup file, see "*7.9.3(2) Restoring the operating environment*".

(3) Import at the time of version upgrade

If you import repository information whose version is newer than the current repository information, the version of the repository is automatically upgraded at the time of import.

If the business process or the service adapter, which is currently deployed, is deleted in the repository information to be imported, an error occurs in the import operation at the time of version upgrade. If an error occurs, export the current repository from the operating environment and import it in the development environment. After that, export the repository whose version is upgraded in the development environment from the development environment and import it in the operating environment.

For details on version upgrade, see "*Appendix G. Migration from an Old Version*".

4.4 Referencing the repository information

You can verify the information in a repository using a command. When you deploy not deployed business process or a service adapter, if a failure occurs while deploying multiple business processes or service adapters, there is no post-processing. Therefore use the cscrepls command and verify the deployment status.

Moreover, private components can be displayed by specifying -private option in the cscrepls command. If private components are present in the repository of an operating environment, the service ID might be duplicated and component import might not be possible. When using component import functionality, specify -private option, verify the private components and take appropriate action.

An example of executing the command is as follows:

- When displaying the repository information

```
cscrepls -user <Login user ID> -pass <Login password> -repfile <ZIP file name of the exported repository>
```

- When displaying the repository information including private components

```
cscrepls -user < Login user ID > -pass <Login password> -repfile <ZIP file name of the exported repository> -private
```

For details on the cscrepls command, see "cscrepls (displaying the repository information)" in "Service Platform Reference Guide".

4.5 Referencing difference information of repositories

You can check the difference between the current repository information of the operating environment and the specified repository information using the cscrepdiff command. You can check the information of the business process or the service adapter, which is added, changed, and deleted.

(1) Preconditions

The following conditions must be met to display the difference in the repository information:

- Current repository information of the operating environment and the repository information whose difference is to be displayed must have a single cluster configuration
- The setting related to the option of whether to use the database and Reliable Messaging must be same in the current repository information of the operating environment and the repository information whose difference is to be displayed.#
- The SOAP mode must be same in the current repository information of the operating environment and the repository information whose difference is to be displayed

Note#

Even if the setting related to the option of whether to use the database and Reliable Messaging is different in the current repository information and the repository information whose difference is to be displayed, difference in the repository information can be displayed for some cases. The following table describes the settings to be performed when the difference in the repository information can be displayed and when it cannot be displayed:

Table 4–3: TableSettings to be performed when the difference in the repository information can be displayed and when it cannot be displayed

Settings to be performed in the current repository information of the operating environment	Settings to be performed in the repository information whose difference is to be displayed		
	Use database as well as Reliable Messaging	Use database and do not use Reliable Messaging	Do not use database as well as Reliable Messaging
Use database as well as Reliable Messaging	Y	N	N
Use database and do not use Reliable Messaging	Y	Y	Y
Do not use database as well as Reliable Messaging	Y	Y	N

Legend:

Y: The difference can be displayed.

N: The difference cannot be displayed.

(2) Display method

Execute the cscrepdiff command and display the difference information of repositories. Execution format of the command is as follows:

- **When displaying the difference in the repository information (at the time of standard import)**

```
cscrepdiff -user <Login user ID> -pass <Login password> -repfile <Repository ZIP file name>
```

- **When displaying the entire repository information (at the time of standard import)**

```
cscrepdiff -user <Login user ID> -pass <Login password> -repfile <Repository ZIP file name> -allinfo
```

- **When displaying the difference in the repository information (at the time of component import)**

```
cscrepdiff -user <Login user ID> -pass <Login password> -repfile <Repository ZIP file name> -compo
```

- **When displaying the entire repository information (at the time of component import)**

```
cscrepdiff -user < Login user ID> -pass <Login password> -repfile <Repository ZIP file name> -compo -allinfo
```

For details on the cscrepdiff command, see "cscrepdiff (displaying the difference in the repository information)" in "Service Platform Reference Guide".

(3) Display contents of the difference

The display contents of the difference in the repository information differ in standard import and component import. The following table describes the display contents in each case:

Table 4–4: TableDisplay contents of the difference (at the time of standard import)

Repository in the operating environment	Repository ZIP file		
	With HCSC components		Without HCSC components
	With change	Without change	
With HCSC components	change	no change#	delete
Without HCSC components	add	-	N

Legend:

N: The contents are not displayed.

-: The contents are not displayed since the corresponding condition does not occur.

Note#

The contents are displayed only when -allinfo option is specified. If -allinfo option is not specified, the contents are not displayed.

Table 4–5: TableDisplay contents of the difference (at the time of component import)

Repository in the operating environment	Repository ZIP file		
	With HCSC components		Without HCSC components#1
	With change	Without change	
With HCSC components	change	no change#2	no change#2
Without HCSC components	add	-	N

Legend:

N: The contents are not displayed.

-: The contents are not displayed since the corresponding condition does not occur.

Note#1

An error occurs, if the HCSC component of the service ID specified in -name option of the cscrepdiff command does not exist in the repository ZIP file.

Note#2

The contents are displayed only when -allinfo option is specified. If -allinfo option is not specified, the contents are not displayed.

An example of display contents of the difference is as follows:

Status of import source and import destination

Contents of the repository ZIP file to be imported

- Business process 1 (bp1): With change
- Business process 2 (bp2): Without change
- Business process 4 (bp4): Other than import target

Contents of the repository of the operating environment to be imported

- Business process 1 (bp1)

- Business process 2 (bp2)
- Business process 3 (bp3)

- **When displaying the difference in the repository information (at the time of standard import)**

```
cscrepdiff -repfile repository.zip
KEOS52129-I cscrepdiff will now start.
Command Edit Time: YYYY/MM/DD hh:mm:ss.SSS
[BusinessProcess]
change:
< Cluster/bp1 YYYY/MM/DD hh:mm:ss
> Cluster/bp1 YYYY/MM/DD hh:mm:ss
delete:
< Cluster/bp3 YYYY/MM/DD hh:mm:ss
add:
> Cluster/bp4 YYYY/MM/DD hh:mm:ss
KEOS52130-I cscrepdiff ended normally.
```

- **When displaying the entire repository information (at the time of standard import)**

```
cscrepdiff -repfile repository.zip -allinfo
KEOS52129-I cscrepdiff will now start.
Command Edit Time: YYYY/MM/DD hh:mm:ss.SSS
[Business Process]
no change:
Cluster/bp2 YYYY/MM/DD hh:mm:ss
change:
< Cluster/bp1 YYYY/MM/DD hh:mm:ss
> Cluster/bp1 YYYY/MM/DD hh:mm:ss
delete:
< Cluster/bp3 YYYY/MM/DD hh:mm:ss
add:
> Cluster/bp4 YYYY/MM/DD hh:mm:ss
KEOS52130-I cscrepdiff ended normally.
```

- **When displaying the difference in the repository information (at the time of component import)**

```
cscrepdiff -repfile repository.zip -compo
KEOS52129-I cscrepdiff will now start.
Command Edit Time: YYYY/MM/DD hh:mm:ss.SSS

[BusinessProcess]
change:
< Cluster/bp1 YYYY/MM/DD hh:mm:ss
> Cluster/bp1 YYYY/MM/DD hh:mm:ss
add:
> Cluster/bp4 YYYY/MM/DD hh:mm:ss
KEOS52130-I cscrepdiff ended normally.
```

- **When displaying the entire repository information (at the time of component import)**

```
cscrepdiff -repfile repository.zip -compo -allinfo
KEOS52129-I cscrepdiff will now start.
Command Edit Time: YYYY/MM/DD hh:mm:ss.SSS
[BusinessProcess]
no change:
Cluster/bp2 YYYY/MM/DD hh:mm:ss
Cluster/bp3 YYYY/MM/DD hh:mm:ss
```

```
change:
< Cluster/bp1 YYYY/MM/DD hh:mm:ss
> Cluster/bp1 YYYY/MM/DD hh:mm:ss
add:
> Cluster/bp4 YYYY/MM/DD hh:mm:ss
KEOS52130-I cscrepdiff ended normally.
```

4.6 Adding, updating, and deleting a repository using component as a unit

By using component import functionality, you can edit the HCSC components within the repository developed in multiple development environments using the cscrepctl command in the repository of the operating environment.

The HCSC components, which do not exist in the repository ZIP file to be imported, are to be deleted from the repository of the operating environment in standard import. By using the component import functionality, you can add and update only the specific HCSC components within the repository ZIP file without deleting them from the repository of the operating environment.

The following activities can be performed using the component import functionality:

Activity name	Activity contents	Option to be specified in the cscrepctl command
Adding HCSC components	You can add a new HCSC component while keeping the HCSC components present in the repository of the operating environment as are.	-import
Updating HCSC components	The HCSC component present in the repository of the operating environment is replaced.	-import, -overwrite
Deleting HCSC components	You can delete the HCSC component present in the repository of the operating environment.	-delete

The possibility of execution of the component import functionality differs as per the conditions mentioned in the following table:

Table 4–6: TablePossibility of execution of the component import functionality

Condition	Adding HCSC components (Specify the -import option)	Updating HCSC components (Specify the -import, -overwrite options)	Deleting HCSC components (Specify the -delete option)
When the version of the repositories is same	Y	Y	-
If there is 1 cluster in the repository	Y	Y	Y
If the HCSC component whose either of the following information is matching, does not exist: • Service ID • Service name • Reception ID	Y	-	-
If the HCSC component whose context root is not matching, does not exist	Y	Y	-
If the HCSC component whose entire following information is matching, exist: • Service ID • Service name • Component type • Service adapter type	-	Y	-
If the HCSC component to be imported in the operating environment releases a service in the development environment	Y	Y	-
If the target HCSC component is not deployed	-	Y	Y

Legend:
Y: Can be executed.
-: Cannot be executed.

4.6.1 Adding and updating a repository using component as a unit

Execute the cscrepctl command by specifying the -import option to add (import) or update a repository using component as a unit. You can validate whether the HCSC components within the specified repository ZIP file can be imported in the repository of the operating environment by executing the cscrepcheck command prior to import operation.

(1) Validation of possibility of import prior to import operation (cscrepcheck command)

Use the cscrepcheck command to check information of the HCSC components of the repository of the operating environment and status of these components, to validate the following contents and display the validation result. For details on the cscrepcheck command, see "cscrepcheck (validation of possibility of import) " in "Service Platform Reference Guide".

- Whether it is possible to import the repository ZIP file
- Whether it is possible to import the HCSC components within the repository ZIP file using component as a unit

The repository is not imported when you use the cscrepcheck command. Execute the cscrepctl command to import the repository.

(a) Cases in which the possibility of import cannot be validated

The possibility of importing the repository information cannot be validated in the following cases:

- If the current repository information of the operating environment and the repository information to be validated do not have a single cluster configuration
- If the SOAP mode is different in the current repository information of the operating environment and the repository information to be validated
- If the settings related to the option of whether to use the database and Reliable Messaging are different
  The following table describes the possibility of validating import when the settings are different:

  Table 4–7: TableSettings to be performed when the possibility of import can be validated and when it cannot be validated

Settings to be performed in the current repository information of the operating environment	Settings to be performed in the repository information to be validated		
	Use database as well as Reliable Messaging	Use database and do not use Reliable Messaging	Do not use database as well as Reliable Messaging
Use database as well as Reliable Messaging	Y	Y	Y
Use database and do not use Reliable Messaging	N	Y	Y
Do not use database as well as Reliable Messaging	N	N	Y

Legend:
Y: The possibility of import can be validated.
N: The possibility of import cannot be validated.

(b) Validating the possibility of import

An example of validating the possibility of importing the specified repository by executing the cscrepcheck command is as follows. In this example, it is a prerequisite that the user ID and password of HCSC-Manager are defined in HCSC-Manager command definition file.

- Example 1 of command execution

The possibility of importing the entire repository.zip is to be validated.

```
cscrepcheck -repfile D:\tmp\repository.zip
```

- Example 2 of command execution
  The possibility of importing repository.zip using component as a unit is to be validated.

```
cscrepcheck -repfile D:\tmp\repository.zip -compo
```

- Example 3 of command execution
  The possibility of importing service ID "1" in repository.zip is to be validated.

```
cscrepcheck -repfile D:\tmp\repository.zip -compo -name 1
```

(c) Result of validating the possibility of import

An example of validation result displayed by executing the cscrepcheck command is as follows:

- When import is possible
  Messages indicating start and end of validation are displayed and the command ends successfully.

```
KEOS52322-I cscrepcheck will now start.
Command Edit Time: YYYY/MM/DD hh:mm:ss.SSS
KEOS50237-I Verification of the repository to be imported will now be started.
KEOS50238-I Verification of the repository to be imported has ended successfully.
KEOS52323-I cscrepcheck ended normally.
```

- When import is not possible
  After a message indicating start of validation is displayed, all the HCSC components which cannot be imported and their causes are displayed and the message KEOS50239-E indicating an error in validation is output. After that, the command ends successfully.

```
KEOS52322-I cscrepcheck will now start.
Command Edit Time: YYYY/MM/DD hh:mm:ss.SSS
KEOS50237-I Verification of the repository to be imported will now be started.
...
<Display an error message for each HCSC component>
...
KEOS50239-E Verification of the repository to be imported has ended with errors.
KEOS52323-I cscrepcheck ended normally.
```

If any other error occurs, the command ends successfully without showing the error message KEOS50239-E as an output.

(2) Importing a repository using component as a unit (cscrepctl command)

An example of importing a repository with component as a unit by using the cscrepctl command is as follows. In this example, it is a prerequisite that the user ID and password of HCSC-Manager are defined in HCSC-Manager command definition file.

- Example 1 of command execution
  Only the HCSC component having service ID "1" from repository.zip is imported in the repository of the operating environment.

```
cscrepctl -import repository.zip -compo -name 1
```

- Example 2 of command execution
  If the -name option is not specified as shown below, all the HCSC components from repository.zip are imported in the repository of the operating environment.

```
cscrepctl -import repository.zip -compo
```

- Example 3 of command execution

  From among the HCSC components present in repository.zip, the HCSC components specified in HCSC component-specification file "hcsccomponent.txt"# are imported in a batch in the repository of the operating environment.

```
cscrepctl -import repository.zip -compo -namelist hcsccomponent.txt
```

Note#

For HCSC component-specification file, see "HCSC component-specification file" in "Service Platform Reference Guide".

For the cscrepctl command, see "cscrepctl (import/export) in "Service Platform Reference Guide".

4.6.2 Deleting a repository using component as a unit

In the component import functionality, you must first delete the HCSC components, which are duplicated, since the import operation fails, if the repository information is duplicated in the repository.

Execute the cscrepctl command by specifying the -delete option to delete the repository using component as a unit. The repository is deleted from the operating environment irrespective of whether the HCSC components are released.

- Example 1 of command execution

  An example of deleting the HCSC component having service ID "1" from the repository of the operating environment using the cscrepctl command is as follows. In this example, it is assumed that the user ID and password of HCSC-Manager are using HCSC-Manager command definition file.

```
cscrepctl -delete -name 1
```

- Example 2 of command execution

  From among the HCSC components present in the repository of the operating environment, the HCSC components specified in HCSC component-specification file "hcsccomponent.txt"# are deleted in a batch.

```
cscrepctl -delete -namelist hcsccomponent.txt
```

Note#

For HCSC component-specification file, see "HCSC component-specification file" in "Service Platform Reference Guide".

For the cscrepctl command, see "cscrepctl (import/export)" in "Service Platform Reference Guide".

5 System Operations

This chapter describes how to log in and out, as well as HCSC server operations.

5.1 Preparation for HCSC server operations

To begin operating the HCSC server, you must log in to HCSC-Manager. This section describes how to log in and out.

5.1.1 Logging In

This subsection describes how to log in to the HCSC server.

(1) Using windows

To log in to the HCSC server using windows in the operating environment:

1. Start Eclipse.
2. From the menu, choose HCSC-Manager, then Log in.
   If the current perspective is the HCSC-Manager perspective (if the tree view is displayed), a dialog box to enter the user ID and password is displayed.
   If the current perspective is not the HCSC-Manager perspective (if the tree view is not displayed), a dialog box to confirm whether you want to switch the perspective is displayed. To switch the perspective, choose Yes. If you do not want to switch the perspective, choose No. After this, the dialog box to enter the user ID and password is displayed.
3. Enter the user ID and password and then click the OK button.
   Once the login procedure has been completed successfully, the configuration and status of the server and HCSC components are displayed in the tree view.
   You can use the `cscpasswd` command to set and change a user ID and password. For details about how to set and change user IDs and passwords, see *2.4.2 Setting user information*. For details about the `cscpasswd` command, see *cscpasswd (Managing users)* in the *uCosminexus Service Platform Reference Guide*.

(2) Using commands

If you specify the login user name and password in the following parameters in the HCSC-Manager command definition file beforehand, there is no need to specify the login user ID and password when you execute the HCSC-Manager commands:

- `csc.all.user`=*HCSC-Manager login-user-name*
- `csc.all.pass`=*HCSC-Manager login-password*

(3) Notes about login

During execution of any of the commands listed below, the repository used by these commands is locked. Therefore, you cannot log in using windows or commands. In this case, log in after command execution terminates.

- `csccompodeploy` (deploys HCSC components)
- `csccompoundeploy` (deletes HCSC components)
- `cscenvrestore` (restores HCSC-Manager environment)
- `cscpasswd` (manages users)
- `cscrepctl` (imports/exports)
- `cscsvcctl` (manages service information)
- `cscsvsetup` (sets up an HCSC server)
- `cscsvunsetup` (cancels HCSC server setup)

5.1.2 Logging Out

This subsection describes how to log out from the HCSC server.

(1) Using windows

To log out from the HCSC server using windows in the operating environment:

1. From the menu, choose HCSC-Manager, then Log out.
   A dialog box confirming logout is displayed.
2. Click the OK button.
   Once the logout procedure has been successfully completed, the window returns to the initial status.

(2) Using commands

You can log out from the HCSC server after the HCSC-Manager command terminates.

5.2 Points to be noted at the timeofsystem operations

The following are the notes at the time of system operations:

- Service Coordinator creates and uses Reliable Messaging queue. If you operate this queue with commands of Reliable Messaging, the status of the HCSC server becomes invalid. Therefore, do not operate the queue.
- You cannot access the network drive from Service Coordinator. Do not specify a path on a network drive in arguments and various definitions of commands.
- In Windows, execute all HCSC server operations with users belonging to the "Administrators" group.
- In Windows, the active /passive status of the menu of HCSC-Manager Plug-in is not reflected immediately and a menu that cannot be executed might be activated in some cases. To set to an appropriate status, select a view different from the view that is currently in active status.
- In Windows, when you use HCSC-Manager, do not execute [Window]-[New Window] from the Eclipse menu.
- In Windows, it is recommended that you use HCSC-Manager Plug-in functionality other than login in the HCSC-Manager perspective.
- Warning message KDCCE0605-W is output during HCSC server operations, but you need not take any action.
- At the time of using HCSC server, you cannot use SSL/TLS communication using RSA BSAFE SSL-J.
- If the stub has been generated from WSDL of the old version, re-generate the stub based on WSDL of a new version.
- When you send and receive an XML message, characters within the message are converted to character references and entity references depending on the contents of the message and your system configuration. The notation system for character references and entity references are "& # x61" and "& lt". For details on character references and entity references, see the description related to character references and entity references in the XML 1.0 document.
- The timing for committing transactions of business processes has been changed in 09-00.For details, see "3.4 Business process transactions " in "Service Platform Overview".
- You cannot use parser switching function in the HCSC server. For the parser switching function, see "3.7 Parser switching functionality" in "Application Server XML Processor User Guide".
- The root application information is displayed in the message text of the KDEC00001-E and KDEC60002-E messages in the version 08-00 or later of this product.

5.3 HCSC Server Operations

This section describes how to operate the system that has been set up using the operating environment on a Service platform.

5.3.1 Flow of operations

This subsection describes the flow of operations in the following cases:

- Preparation before starting operations
- When you start operations
- When you operate the system during operations
- When you end operations

The following paragraph describes the prerequisites and procedure for the required operations in each case:

(1) Preparation before starting operations

It is recommended that you implement the following activities prior to operation.

(a) Registering a logical server

To enable logical server operations (referencing batch start and stop, and status with the HCSC server), change the parameters of the HCSC-Manager definition file, as follows:

```
cscmng.server.<HCSC server name>.system=logical server name
```

(b) Controlling the access to repositories

For security purpose, ensure that the repository is not accessed.

Set such that the following repository is not accessed, if the root directory of the repository is not changed:

```
<Installation directory of Service Platform>\CSC\repository
```

When you change the root directory of the repository, implement access control in the changed repository. If you have built multiple operating environments on one machine (set the environment variable CSCMNG_HOME), implement access control to the next repository.

```
%CSCMNG_HOME%\repository
```

(c) Backup

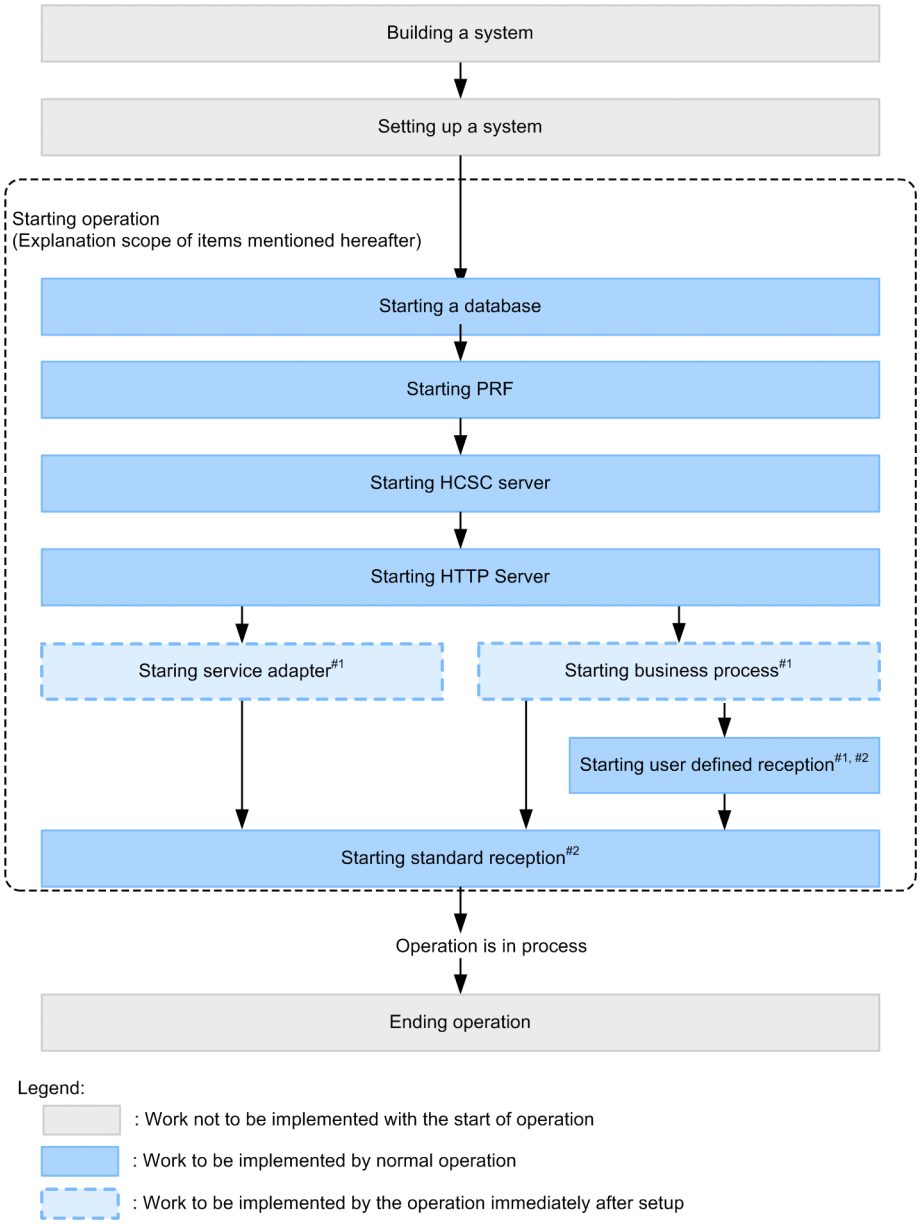
Take a backup of the information of operating environment, as a preparation for failure at the time of operation. By managing the backup information on a machine other than the operating environment, you can recover the operating environment after a failure occurrence. Take backup by executing the cscenvbackup command.

For details on the cscenvbackup command, see"cscenvbackup (backup of the HCSC-Manager environement) " in"Service Platfom Reference Guide".

(2) When you start operations

To start operations by starting the system, you must perform activities according to the flow shown in the following figure:

Figure 5–1: Flow of activities when you start operations



#1

You can also execute these activities in a batch. The packaging, deployment definition, and deployment of HCSC components are executed before the start of HCSC components.

However, batch execution is performed at the time of system development, or at the time of integration test from unit test.For details, see "7.5 Batch execution of processes started by deploying HCSC components to the HCSC server" in "BPM/ESB Service Platform Basic Development Guide ".

#2

You can also start concurrently by using the cscrcptnstart command.

(3) When you operate the system during system operations

You can perform the following operations as and when required, during system operations.

(a) Referencing the status and information

You can reference each of following status and information as and when required.. The reference methods are described in the paragraph subsequent to "*5.3.10 Checking the Database Status*".

- Database status
- PRF status
- HTTP Server status (when you use HTTP Server)
- Manager status
- HCSC server setup information
- HCSC server information
- Service adapter information
- Business process information
- Information of User-defined reception

Furthermore, you must check the following configuration components of the execution environment and status of HCSC servers on a regular basis.

- DatabasesStart up status
- PRF start up status
- HTTP server start up status (when you use HTTP Server)
- Manager start up status
- Start up status and starting status of HCSC server

(b) Cache of the definition information

You can cache the definition information of business processes as and when required. For the description on how to perform cache, see "*5.3.20 Performing cache of the definition information of the business process*".

(c) Changes in definitions and configuration

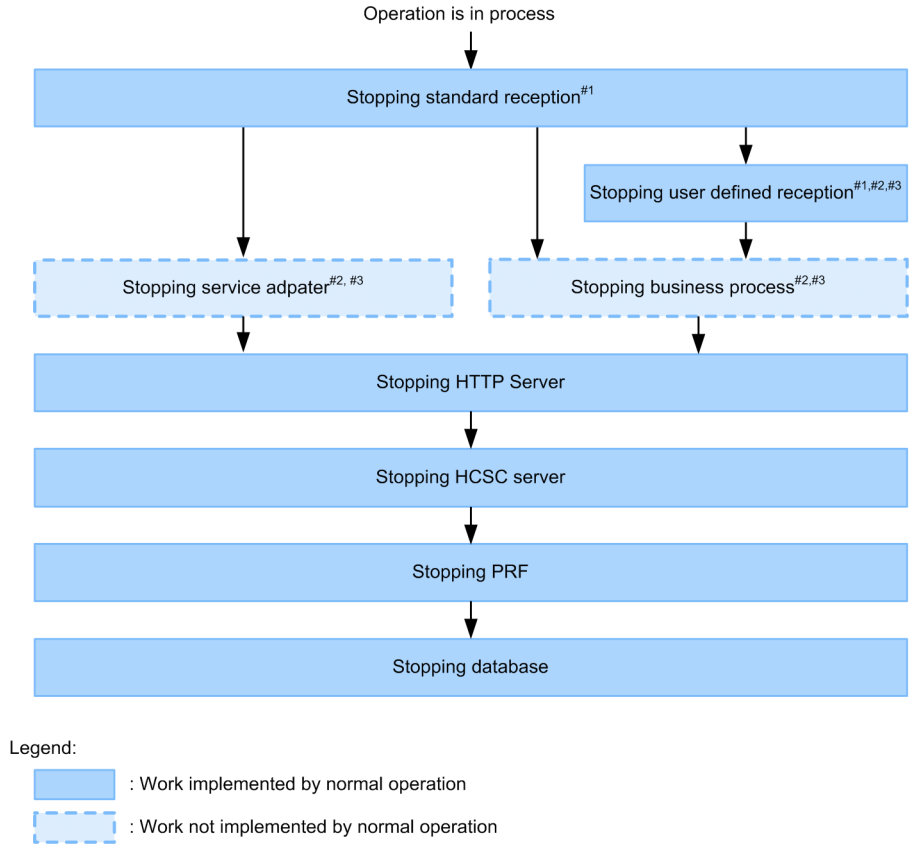
You can change the following definitions and configuration as and when required. The method to change is described in the paragraph subsequent to "*5.3.21 Changing HCSC Server Definitions*".

- HCSC server definition
- Definition information of the user-defined reception
- Configuration of HCSC components
- Connection destination of service components
- Flow-volume control value
- Communication timeout value
- Changing resource adapter properties

(4) When you end operations

To end the operation by stopping the system, you must perform activities according to the flow shown in the following figure. The method to stop is described in the paragraph subsequent to "*5.3.28 Terminating the Standard Reception*".

Figure 5–2: Flow of activities when you end operations



#1

You can also stop concurrently by using the cscrcptnstop command.

#2

Implement to disable the reception of service components execution requests.

#3

You can execute these activities in a batch. Furthermore, after stopping, HCSC components are deleted from the HCSC server. However, batch execution is performed at the time of system development, or at the time of the integration test from the unit test.For details, see "7.6 Batch execution of the process of deleting HCSC components from HCSC processes by stopping HCSC components" in "BPM/ESB Service Platform Basic Development Guide".

5.3.2 Starting a Database

This subsection explains about how to start a database.

(1) In the case of HiRDB

To start HiRDB, execute the `pdstart` command on the database server.

For details about the `pdstart` command, see the manual *HiRDB command reference*.

(2) In the case of Oracle

For details on how to start Oracle, see the documentation published by Oracle Corporation.

5.3.3 Starting PRF

To start PRF, execute the `cscsvstart` command in the operating environment. Specify the logical server name for PRF with the `-logical` option and execute the command.

For details about the `cscsvstart` command, see *cscsvstart (Starting the HCSC server)* in the manual *Cosminexus Service Platform Reference*.

The execution format of the `cscsvstart` command is described below:

```
cscsvstart -user login-user-ID -pass login-password -csc HCSC-server-name -logical
logical-server-name-of-PRF
```

5.3.4 Starting HCSC server

This subsection describes the prerequisites and method to start HCSC servers.

(1) Prerequisites

When you start a HCSC server, if the HCSC server, the service adapter, or the business process fails to start, the service adapter and the business process as well as the user-defined reception and standard reception might change to the stopped status. In such cases, you need to remove the cause of the error and restart the service adapter and the business process as well as the user-defined reception and the standard reception.

For details on how to start the service adapter and business process, see "*5.3.6 Starting Service Adapters*", or "*5.3.7 Starting Business Processes*". For details on how to start the receptions, see "*5.3.8 Starting user-defined receptions*", and "*5.3.9 Starting standard receptions*".

(2) Starting method

The methods to start the HCSC server are as follows:

(a) When using screens

Procedure to start the HCSC server by using screens in the operating environment is as follows:

1. In the tree view, double-click the HCSC server to be started.
   Information on the selected HCSC server is displayed in the editor area.
2. In the editor area, select the [Operations] tab.
   The Operations page displays information on operations of the HCSC server you selected in step 1.
   For details on the Operations page of an HCSC server, see "4.4 Operations page" in "Service Platform Reference Guide".
3. Check the contents displayed in the Operations page, and click the [Start] button of "HCSC-Server".
   A dialog box confirming startup of the HCSC server is displayed.
4. Check the information displayed in the dialog, and click the [OK] button.
   HCSC server startup processing begins. Log information during startup processing is output in the console view.
   If you click the [Cancel] button, the system returns to the Operations page without executing startup processing.
   When HCSC server startup processing is completed, a dialog indicating the execution result is displayed.
5. Check the dialog that displays the execution result.

   If startup processing is successful:

   Click the [OK] button to return to the Operations page.

   On the Operations page, the operating status of HCSC server changes to. [Start status]. Also, the [Start] button is disabled and the [Stop] button is enabled.

   If startup processing fails

   The contents of error are displayed in the dialog. Take appropriate action by referencing the message ID displayed in the detail information.

(b) When using commands

To start the HCSC server, execute the cscsvstart command or the cscutil command in the operating environment. To start HCSC servers in the cluster as a batch, or to start a logical server, execute the cscsvstart command.

Use the cscsvstart and cscutil commands in the following cases:

- cscsvstart command
  To start the HCSC server in the operating environment in which the corresponding repository exists
- cscutil command
  To start the HCSC server in an environment (for example, execution environment directly operating in JP1) in which the cscutil command can be used and the corresponding repository does not exist.

The method of executing each command is as follows:

●In case of the cscsvstart command

Execute the cscsvstart command in the operating environment.

For details on the cscsvstart command, see "cscsvstart (starting HCSC servers) " in "Service Platform Reference Guide".

The execution format of the cscsvstart command is as follows:

To start all HCSC servers in the cluster in a batch

Execute the command by specifying the cluster name. All HCSC servers in the cluster specified in the -cluster option are started in a batch (the logical server does not start).

```
cscsvstart -user <login-user-ID> -pass < login-password > -cluster <cluster-name >
```

To start logical servers concurrently with HCSC servers in the cluster, specify the -system option. However, logical servers must be registered in the HCSC-Manager definition files.

For details on registering logical servers, see, "*5.3.1 (1) Preparation before starting operations*".

```
cscsvstart -user <login-user-ID> -pass <login password> -cluster <cluster name> -system
```

Furthermore, if you want to start only the logical server without starting the HCSC server, specify the -logical option.

```
cscsvstart -user <login user ID> -pass <login password> -cluster <cluster name> -logical
<logicalservername>
```

To start each HCSC server one by one

Execute the command by specifying the HCSC server name. The HCSC server specified with the -csc option is started (the logical server is not started).

```
cscsvstart -user <login user ID> -pass <login password> -csc <HCSC server name>
```

To start the HCSC server and the logical server at the same time, specify the -system option.

```
cscsvstart -user <login user ID> -pass <login password> -csc <HCSC server name> -system
```

Furthermore, if you want to start only the logical server without starting the HCSC server, specify the -logical option.

```
cscsvstart -user <login user ID> -pass <login password> -csc <HCSC server name> -logical
<logicalservername>
```

●In case of the cscutil command

Execute the cscutil command in the operating environment. Specify server in the -target option and start in the -operation option.

For details on the cscutil command, see "cscutil (various operations) " in "Service Platform Reference Guide".

The execution format of the cscutil command depends on whether you use the property definition file.

When you do not use the property definition file

In the -props option, specify the HCSC server name and J2EE server name.

```
cscutil -user <login user ID> -pass <login password> -mng <Manager name> -target server -
operation start -props "CSCSrvName=<HCSC server name>, J2EESrvName=<J2EE server name>"
```

You can use the cscrepls command to check the Manager name, the HCSC server name, and the J2EE server name that are specified in the cscutil command. For details on the cscrepls command, see "cscrepls (displaying the repository information) " in "Service Platform Reference Guide".

When using the property definition file

Specify the name of the property definition file in the -propfile option. The property definition file must be created beforehand in the J2SE property file format.

```
cscutil -user <login user ID> -pass <login password> -mng <Manager name> -target server -
operation start -propfile <proeprtydefinitionfilename>
```

5.3.5 Starting HTTP Server

To start HTTP Server, execute the `cscsvstart` command in the operating environment. Specify the logical server name of HTTP Server with the `-logical` option and execute the command.

For details about the `cscsvstart` command, see *cscsvstart (Starting the HCSC server)* in the manual *Cosminexus Service Platform Reference*.

The execution format of the `cscsvstart` command is described below:

```
cscsvstart -user login-user-ID -pass login-password -csc HCSC-server-name -logical
logical-server-name-of-HTTP-Server
```

5.3.6 Starting Service Adapters

This subsection describes the prerequisites for starting a service adapter, and how to start it.

(1) Prerequisites

Before you start a service adapter, the HCSC server must be in active status.

For details about how to check HCSC server status, see *5.3.15 Checking the HCSC server information*.

(2) How to start a service adapter

This subsection describes how to start a service adapter.

(a) Using windows

To start a service adapter using windows in the operating environment:

1. In the tree view, double-click the service adapter to be started.
   Information about the double-clicked service adapter is displayed on the Operations page in the editor area.
   For details about the Operations page for service adapters, see *4.4 Operations page* in the manual *Cosminexus Service Platform Reference*.
2. Check the information displayed in the Operations page, and then click the Start button.
   A dialog box confirming startup of the service adapter is displayed.
3. Check the information displayed in the dialog box and then click the OK button.
   The service adapter startup processing begins. Log information during startup processing is displayed in the console view.
   If the **Cancel** button is clicked, the system returns to the Operations page without executing startup processing.
   When service adapter startup processing is completed, a dialog box indicating the execution result is displayed.
4. Check the dialog box indicating the execution result.
   If startup processing was successful:
   Click the **OK** button to return to the Operations page.

On the Operations page, the service adapter status is set to active. Also, the **Start** button is disabled and the **Stop** button is enabled.

If startup processing failed:

The dialog box displays the nature of the error. Check the message ID provided in the detailed information, and then take appropriate action.

(b) Using commands

To start a service adapter, execute the `csccompostart` command or `cscutil` command in the operating environment.

Use the `csccompostart` and `cscutil` command in the following cases:

- `csccompostart` command

  To start a service adapter in an operating environment where the corresponding repository exists.

- `cscutil` command

  To start the service adapter in an environment (for example, execution environment directly operating in JP1) where the `cscutil` command can be used and where the corresponding repository does not exist.

The following describes how to execute the above commands:

Using the `csccompostart` command

Execute the `csccompostart` command in the operating environment.

For details about the `csccompostart` command, see *csccompostart (Starting HCSC components)* in the manual *Service Platform Reference*.

The execution format of the `csccompostart` command is described below:

To start the service adapters deployed on all the HCSC servers in a cluster, in a batch (for each cluster)

Specify the cluster-name and the `-all` option and execute the command.

The service adapters deployed on all the HCSC servers in the cluster specified with the `-cluster` option are started in a batch (all the business processes and user-defined receptions that are not running, are also started at the same time).

```
csccompostart -user login-user-ID -pass login-password -cluster cluster-name -
all
```

If you want to start only the service adapter without starting the business process and user-defined reception, specify the service ID of the service adapter.

```
csccompostart -user login-user-ID -pass login-password -cluster cluster-name -
name service-ID-of-the-service-adapter
```

To start all the service adapters deployed on the HCSC server in a batch (for each HCSC server)

Specify the HCSC server name and the `-all` option and execute the command.

The service adapters deployed on the HCSC server specified with the `-csc` option are started (all the business processes and user-defined receptions that are not running, start at the same time).

```
csccompostart -user login-user-ID -pass login-password -csc HCSC-server-name -
all
```

If you want to start only the service adapter without starting the business process and user-defined reception, specify the service ID of the service adapter.

```
csccompostart -user login-user-ID -pass login-password -csc HCSC-server-name -
name service-ID-of-the-service-adapter
```

Using the `cscutil` command

Execute the `cscutil` command in the operating environment. Specify `compo` in the `-target` option and `start` in the `-operation` option.

For details about the `cscutil` command, see *cscutil (Various operations)* in the manual *Cosminexus Service Platform Reference*.

The execution format of the `cscutil` command depends on whether or not a property definition file is used.

When a property definition file is not used

In the `-props` option, specify the service adapter's service ID, HCSC server name, J2EE server name, and type.

```
cscutil -user login-user-ID -pass login-password -mng manager-name -target
compo -operation start -props "AdapterName=service-ID-of-the-service-adapter,
CSCSrvName=HCSC-server-name, J2EESrvName=J2EE-server-name,
ServiceKind=serviceAdapter"
```

You can use the `cscrepls` command to check the Manager name, service adapter's service ID, HCSC server name, and J2EE server name that are specified in the `cscutil` command. For details about the `cscrepls` command, see *cscrepls (Displaying the repository information)* in the manual *Service Platform Reference*.

When a property definition file is used

Specify the name of the property definition file name in the `-propfile` option. The property definition file must be created beforehand in the J2SE property file format.

```
cscutil -user login-user-ID -pass login-password -mng manager-name -target
compo -operation start -propfile property-definition-file-name
```

5.3.7 Starting Business Processes

This subsection describes the prerequisites for starting a business process and how to start it.

(1) Prerequisites

Before you start a business process, the HCSC server must be in active status.

For details about how to check HCSC server status, see *5.3.15 Checking the HCSC server information*.

(2) How to start a service adapter

This subsection describes how to start a business process.

(a) Using windows

To start a business process using windows in the operating environment:

1. In the tree view, double-click the business process to be started.
   Information about the double-clicked business process is displayed in the editor area.
2. In the editor area, choose the Operations page.
   Information about operations of the business process you chose in step 1 is displayed.
   For details about the Operations page for business processes, see *4.4 Operations page* in the manual *Cosminexus Service Platform Reference*.
3. Check the information displayed in the Operations page, and then click the Start button.
   A dialog box confirming startup of the business process is displayed.
4. Check the information displayed in the dialog box and then click the OK button.
   Business process startup processing begins. Log information during startup processing is displayed in the console view.
   If the **Cancel** button is clicked, the system returns to the Operations page without executing startup processing.
   When business process startup processing is completed, a dialog box indicating the execution result is displayed.
5. Check the dialog box indicating the execution result.
   If startup processing was successful:
   Click the **OK** button to return to the Operations page.
   On the Operations page, the business process status is set to active. Also, the **Start** button is disabled and the **Stop** button is enabled.

If startup processing failed:

The dialog box displays the nature of the error. Check the message ID provided in the detailed information, and then take appropriate action.

(b) Using commands

To start a business process, execute the `csccompostart` command or `cscutil` command in the operating environment.

Use the `csccompostart` and `cscutil` command in the following cases:

- `csccompostart` command

  To start a business process in the operating environment where the corresponding repository exists.

- `cscutil` command

  To start a business process in an environment (for example, the execution environment operating directly in JP1) where the `cscutil` command can be used and where the corresponding repository does not exist.

The following describes how to execute the above commands:

Using the `csccompostart` command

Execute the `csccompostart` command in the operating environment.

For details about the `csccompostart` command, see *csccompostart (Starting HCSC components)* in the manual *Cosminexus Service Platform Reference*.

The execution format of the `csccompostart` command is described below:

To start the business processes deployed on all the HCSC servers in the cluster, in a batch (for each cluster)

Specify the cluster-name and the `-all` option and execute the command.

The business processes deployed on all the HCSC servers in the cluster specified with the `-cluster` option are started in a batch (all the service adapters and user-defined receptions that are not running, are started at the same time).

```
csccompostart -user login-user-ID -pass login-password -cluster cluster-name -
all
```

If you want to start only the business process without starting the service adapter and user-defined reception, specify the service ID of the business process.

```
csccompostart -user login-user-ID -pass login-password -cluster cluster-name -
name service-ID-of-the-business-process
```

To start all the business processes deployed on the HCSC server in a batch (for each HCSC server)

Specify the HCSC server name and the `-all` option and execute the command.

The business processes deployed on the HCSC server specified with the `-csc` option are started (all the service adapters and user-defined receptions that are not running, start at the same time).

```
csccompostart -user login-user-ID -pass login-password -csc HCSC-server-name -
all
```

If you want to start only the business process without starting the service adapter and user-defined reception, specify the service ID of the business process.

```
csccompostart -user login-user-ID -pass login-password -csc HCSC-server-name -
name service-ID-of-the-business-process
```

Using the `cscutil` command

Execute the `cscutil` command in the operating environment. Specify `compo` in the `-target` option and `start` in the `-operation` option.

For details about the `cscutil` command, see *cscutil (Various operations)* in the manual *Cosminexus Service Platform Reference*.

The execution format of the `cscutil` command depends on whether or not a property definition file is used.

When a property definition file is not used

In the `-props` option, specify the business process's service ID, HCSC server name, J2EE server name, and type.

```
cscutil -user login-user-ID -pass login-password -mng manager-name -target
compo -operation start -props "AdapterName=service-ID-of-the-business-process,
CSCSrvName=HCSC-server-name, J2EESrvName=J2EE-server-name, ServiceKind=bp"
```

You can use the `cscrepls` command to check the Manager name, business process's service ID, HCSC server name, and J2EE server name that are specified in the `cscutil` command. For details about the `cscrepls` command, see *cscrepls (Displaying the repository information)* in the manual *Cosminexus Service Platform Reference*.

When a property definition file is used

Specify the name of the property definition file name in the `-propfile` option. The property definition file must be created beforehand in the J2SE property file format.

```
cscutil -user login-user-ID -pass login-password -mng manager-name -target
compo -operation start -propfile property-definition-file-name
```

5.3.8 Starting user-defined receptions

This subsection describes the prerequisites and methods for starting the user-defined reception.

(1) Prerequisites

To start the user-defined reception, the following conditions must be fulfilled:

- The HCSC server is in active status.
- The business process in which the user-defined reception is defined is in running status.

For details on how to check HCSC server status, see "*5.3.15 Checking the HCSC server information*".

(2) Starting methods

You can start the user-defined reception, by the following methods:

(a) When using screens

The procedure for starting the user-defined reception by using the operating environment screen is as follows:

1. In the tree view, double click the user-defined reception to be started.

   The information of the double clicked user-defined reception is displayed in the Operations page of the editor area.

   For details on the the Operations page of the user-defined reception, see "4.4 Operations page" in "Service Platform Reference Guide".

2. Check the contents displayed in the Operations page, and click the [Start] button.

   A dialog confirming the start of the user-defined reception is displayed.

3. Check the contents displayed in the dialog, and click the [OK] button.

   The process for starting the user-defined reception is initiated. Log during startup process is displayed in the console view.

   If you click the [Cancel] button, the system returns to the Operations page without executing startup process.

   When the process for starting the user-defined reception is complete, a dialog showing the execution result is displayed.

4. Check the dialog showing the execution result.

   If the start process is successful:

   Click the [OK] button to return to the Operations page.

In the Operations page, the status of user-defined reception changes to [Start] status. Also, the [Start] button is disabled and the [Stop] button is enabled.

If the start process fails:

Contents of the error are displayed in the dialog. Take appropriate action, by checking the message ID provided in the detail information.

(b) When using commands

To start a user-defined reception, execute the cscrcptnstart command or csccompostart command in the operating environment.

Use the cscrcptnstart and csccompostart commands in the following cases:

- cscrcptnstart command
  - Use this command to start receptions in a batch.
  - Use this command to start all user-defined receptions deployed on the HCSC server in a batch.
    You can also start the user-defined receptions of each cluster in a batch. Note that you cannot start only a specific user-defined reception.
  - Use this command to start the user-defined reception in the operating environment in which the corresponding repository exists.
- Csccompostart command
  - Use this command to start service adapters, business processes, and user-defined receptions in a batch.
    You cannot start only user-defined receptions in a batch.
  - Use this command to start a specific user-defined reception deployed on the HCSC server.
    You can also start a specific user-defined reception for each cluster.
  - Use this command to start the user-defined reception in the operating environment in which the corresponding repository exists.

The description of how to execute each command is as follows:

●When using the cscrcptnstart command

Execute the cscrcptnstart command in the operating environment.

For details on the cscrcptnstart command, see "cscrcptnstart (starting the standard reception and user-defined reception) " in "Service Platform Reference Guide ".

Execution format of the cscrcptnstart command is as follows:

To start the user-defined receptions deployed on all HCSC servers within the cluster, in a batch (for each cluster)

Execute the command by specifying the cluster name.

The user-defined receptions deployed on all HCSC servers within the cluster specified in the -cluster option are started in a batch (even all the non-started standard receptions are concurrently started).

```
cscrcptnstart -user <login user ID> -pass <login password> -cluster <cluster name>
```

If you want to start only the user-defined reception without starting the standard reception, specify the -userdef option.

```
cscrcptnstart -user <login user ID> -pass <login password> -cluster <cluster name> -userdef
```

To start user-defined receptions deployed on the HCSC server in a batch (for each HCSC server)

Execute this command by specifying the HCSC server name.

The user-defined receptions deployed on the HCSC server, specified in the -csc option are started (non-started standard receptions are also started concurrently).

```
cscrcptnstart -user <login user ID> -pass <login password> -csc <HCSC server name>
```

If you want to start only the user-defined reception without starting the standard reception, specify the -userdef option.

```
cscrcptnstart -user <login user ID> -pass <login password> -csc <HCSC server name> -userdef
```

●When using the csccompostart command

Execute the csccompostart command in the operating environment.

For details on the csccompostart command, see "csccompostart (starting HCSC components) " in "Service Platform Reference Guide".

Execution format of the csccompostart command is as follows:

To start user-defined receptions deployed on all HCSC servers within the cluster, in a batch (for each cluster)

Execute the command by specifying the cluster-name and the -all option.

The user-defined receptions deployed on all HCSC servers within the cluster, specified in the -cluster option are started in a batch (all the non-started service adapters and business processes are also started concurrently).

```
csccompostart -user <login user ID> -pass <login password> -cluster <cluster name> -all
```

To start user-defined receptions deployed on the HCSC server in a batch (for each HCSC server)

Execute this command by specifying the HCSC server name and the -all option.

The user-defined receptions deployed on the HCSC server specified in the -csc option are started (all the non-started service adapters and business processes are also started concurrently).

```
csccompostart -user <login user ID> -pass <login password> -csc <HCSC server name> -all
```

To start a specific user-defined reception deployed on all HCSC servers within the cluster

Execute the command by specifying the cluster-name and the reception ID of the user-defined reception.

```
csccompostart -user <login user ID> -pass <login password> -cluster <cluster name> -name
<reception ID of the user-defined reception>
```

To start a specific user-defined reception deployed on the HCSC server

Execute the command by specifying the HCSC server name and the reception ID of user-defined reception.

```
csccompostart -user <login user ID> -pass <login password> -csc <HCSC server name> -name
<reception ID of the user-defined reception >
```

5.3.9 Starting standard receptions

This subsection describes the prerequisites and methods for starting the standard reception.

(1) Prerequisites

To start the standard reception, the HCSC server must be in running status.

For details on how to check HCSC server status, see "*5.3.15Checking the HCSC server information*".

(2) Starting method

This subsection describes how to start the standard reception.

! Important note

If startup of the standard reception fails, eliminate the cause of the error, and forcibly stop the standard reception. Once the standard reception is in stopped status, start it again and then restart operations. For details on how to forcibly stop the standard reception, see "*5.3.28 Terminating the Standard Reception*".

(a) When using screens

The procedure of starting the standard reception by using screens in the operating environment is as follows:

1. In the Tree view, double-click the HCSC server on which the standard reception is to be started.
   Information of the double-clicked HCSC server is displayed in the editor area.
2. In the editor area, select the [Operations] tab.
   The Operations page displays information on operations of the HCSC server you selected in step 1.

For details on the Operations page for an HCSC server, see "4.4 Operations page" in "Service Platform Reference Guide".

3. Check the contents displayed in the Operations page, and, click the [Start] button of "Standard reception".
   A dialog confirming startup of the standard reception is displayed.
4. Check the contents displayed in the dialog, and click the [OK] button.
   The process to standard reception is initiated A Log during startup process is displayed in the console view.
   If you click the [Cancel] button, the system returns to the Operations page without executing startup process.
   When the process of starting the standard reception is complete, a dialog showing the execution result is displayed.
5. Check the dialog showing the execution result.
   If startup process is successful:
   Click the [OK] button to return to the Operations page.
   On the Operations page, the operating status of the standard reception changes to "Started status". Also, the [Start] button is disabled and the [Normal Stop] and [Planned Stop] buttons are enabled.
   If startup process fails:
   Contents of the error are displayed in a dialog. Take appropriate actions, by checking the message ID displayed in the detail information.

(b) When using commands

To start the standard reception, execute the cscrcptnstart command or cscutil command in the operating environment.

Use the cscrcptnstart command and the cscutil command in the following cases:

- Cscrcptnstart command
  To start the standard reception in the operating environment in which the corresponding repository exists
- Cscutil command
  To start the standard reception in an environment (for example, execution environment directly operating in JP1) in which you can use the cscutil command and the corresponding repository does not exist.

The description of how to execute each command is as follows:

●When using the cscrcptnstart command

Execute the cscrcptnstart command in the operating environment.

For details on the cscrcptnstart command, see "cscrcptnstart (starting standard reception and user-definition reception) " in "Service Platform Reference Guide"

Execution format of the cscrcptnstart command is as follows:

To start standard receptions of all HCSC servers in the cluster in a batch (for each cluster)

Execute the command by specifying the cluster name.

The standard receptions of all HCSC servers within the cluster specified in the -cluster option are started in a batch (all the non-started user-defined receptions are also started concurrently).

```
cscrcptnstart -user <login user ID> -pass <login password> -cluster <cluster name>
```

If you want to start only the standard reception without starting the user-defined reception, specify the -standard option.

```
cscrcptnstart -user <login user ID> -pass <login password> -cluster <cluster name> -standard
```

To start standard receptions for the HCSC server in a batch (for each HCSC server)

Execute the command by specifying the HCSC server name.

The standard reception for the HCSC server specified in the -csc option is started (all the non-started user-defined receptions are also started concurrently).

```
cscrcptnstart -user <login user ID> -pass <login password> -csc <HCSC server name>
```

If you want to start only the standard reception without starting the user-defined reception, specify the -standard option.

```
cscrcptnstart -user <login user ID> -pass <login password> -csc <HCSC server name> -standard
```

●When using the cscutil command

Execute the cscutil command in the operating environment. Also, specify request_service in the -target option and specify start in the -operation option.

For details on the cscutil command, see "cscutil (various operations) " in "Service Platform Reference Guide".

Execution format of the cscutil command differs depending on whether you use the property definition file.

When you do not use the property definition file

In the -props option, specify the HCSC server name and the J2EE server name.

```
cscutil -user <login user ID> -pass <login password> -mng <Manager name> -target
request_service -operation start -props "CSCSrvName=<HCSC server name>, J2EESrvName=<J2EE
server name>"
```

You can use the cscrepls command to check the Manager name, the HCSC server name, and the J2EE server name specified in the cscutil command. For details on the cscrepls command, see "cscrepls (displaying repository information) " in "Service Platform Reference Guide"

When you use the property definition file

Specify the name of the property definition file name in the -propfile option. You must create the property definition file beforehand in the J2SE property file format.

```
cscutil -user <login user ID> -pass <login password> -mng <Manager name> -target
request_service -operation start -propfile <property definition file name>
```

5.3.10 Checking the Database Status

This subsection explains how to view the database status.

(1) How to view

The following points explain how to view the database status:

(a) In the case of HiRDB

To view the HiRDB status, execute the `pdls` command in the database server.

For details on the `pdls` command, see the manual *HiRDB Command Reference*.

(b) In the case of Oracle

For details about how to view the Oracle status, see the documentation published by Oracle Corporation.

5.3.11 Checking the PRF Status

This subsection explains the prerequisites for viewing the PRF status and how to view the status.

(1) Prerequisites

To view the PRF status, PRF needs be registered in the HCSC-Manager definition file. For details, see the contents related to logical server registration in *5.3.1(1) Preparation before starting operations*.

(2) How to view

To view the PRF status, execute the `cscstatus` command in the operating environment. Specify `system` with the `-type` option and execute the command.

For details about the `cscstatus` command, see *cscstatus (Displaying the status)* in the manual *Cosminexus Service Platform Reference*.

The following shows the execution format of the `cscstatus` command.

```
cscstatus -user login-user-ID -pass login-password -csc HCSC-server-name -type system
```

5.3.12 Checking the HTTP Server Status

This subsection explains the prerequisites for viewing the status of HTTP Server and how to view the status.

(1) Prerequisites

To view the status of HTTP Server, HTTP Server must be registered in the HCSC-Manager definition file. For details, see the contents related to logical server registration in *5.3.1(1) Preparation before starting operations*.

(2) How to view

To view the HTTP Server status, execute the `cscstatus` command in the operating environment. Specify `system` with the `-type` option and execute the command.

For details about the `cscstatus` command, see *cscstatus (Displaying the status)* in the manual *Cosminexus Service Platform Reference*.

The following shows the execution format of the `cscstatus` command.

```
cscstatus -user login-user-ID -pass login-password -csc HCSC-server-name -type system
```

5.3.13 Checking the Manager status

The *Manager* contains two processes, namely Management Server and Administration Agent. This subsection explains how to view the status:

(1) How to view

(a) Viewing Management Server status

To view the status of the Management Server, execute the `mngsvrutil` command on the machine on which the J2EE server is running.

For details on the `mngsvrutil` command, see *mngsvrutil (Management Server management command)* in the manual *Cosminexus Application Server Commands*.

(b) Viewing Administration Agent status

To view the status of Administration Agent, execute the `adminagentcheck` command on the machine on which the J2EE server is running.

For details on the `adminagentcheck` command, see *adminagentcheck (Checking the Administration Agent operations)* in the manual *Application Server Commands*.

5.3.14 Checking the HCSC server setup information

This subsection describes the prerequisites and method for referencing the HCSC server setup information.

(1) Prerequisites

To reference the HCSC server setup information, the HCSC server must be in a stopped or running state.

For details on how to check HCSC server status, see "*5.3.15 Checking the HCSC server information*".

(2) Reference method

To reference HCSC server setup information, execute the cscutil command in the operating environment. Specify server in the -target option and specify get_setup_info in the -operation option. When you execute the cscutil command, the contents of the HCSC server setup definition file are displayed.

For details on the HCSC server setup definition file, see "HCSC server setup definition file" in "Service Platform Reference Guide".

For details on the cscutil command, see "cscutil (various operations) " in "Service Platform Reference Guide".

The execution format of the cscutil command differs depending on whether you use the property definition file.

When you do not use the property definition file

In the -props option, specify the HCSC server name.

```
cscutil -user <login user ID> -pass <login password> -mng <Manager name> -target server -
operation get_setup_info -props "CSCSrvName=<HCSC server name>"
```

You can use the cscrepls command to check the Manager name and the HCSC server name specified in the cscutil command. For details on the cscrepls command, see "cscrepls (displaying the repository information) " in "Service Platform Reference Guide".

When you use the property definition file

Specify the name of the property definition file name in the -propfile option. You must create the property definition file beforehand in the J2SE property file format.

```
cscutil -user <login user ID> -pass <login password> -mng <Manager name> -target server -
operation get_setup_info -propfile <property definition file name>
```

5.3.15 Checking the HCSC server information

The HCSC server information that you can reference differs in case of windows and commands. For details on the information that you can reference, see the contents of corresponding screens and commands in "Service Platform Reference Guide".

This subsection describes the prerequisites and methods for referencing the HCSC server information.

(1) Prerequisites

You can reference the HCSC server information only when the HCSC server is already configured.

(2) Reference method

The methods for referencing HCSC server information are as follows:

(a) When using screens

In the Tree view, double-click the HCSC server information of which you want to reference. Information of the double-clicked HCSC server is displayed in the editor area. You can check the HCSC server information by displaying the Basic information page and the Operations page in the editor area.

For details on the Basic information page and Operations page for HCSC server, see "4.2 Basic information page" in "Service Platform Reference Guide". For details on the Operating page of the HCSC server, see "4.4 Operations page" in "Service Platform Reference Guide"..

Furthermore, you can also check the operating status of the HCSC server by using icons displayed in the Tree view. For details on the icons displayed, see "4.1 Screen configuration (operating environment) " in "Service Platform Reference Guide".

(b) When using commands

To view the HCSC server information, execute the cscstatus command or cscutil command.

You can execute the cscstatus and cscutil commands from the operating environment. Use the respective commands in the following cases:

- cscstatus command
  Use this command to reference the dynamic information (running state) of the HCSC server.
- Cscutil command
  Use this command to reference the static information (definition information set up in the HCSC server setup definition file and HCSC server runtime definition file) for the HCSC server. The information that is reflected in the actual operation is displayed as the definition information. The information set by the user is reflected at the time of starting the HCSC server or at the time of starting receptions. In either of the following cases, the information set when you had started the HCSC server and the reception last time, is displayed:
  - If the definition information is set when the HCSC server is running, and the HCSC server is not restarted after setting the information
  - If the definition information is set when the reception is running and the reception is not restarted after setting this information

The description of how to execute each command is as follows:

●Using the cscstatus command

In the operating environment, execute the cscstatus command.

For details on the cscstatus command, see "cscstatus (status display) " in "Service Platform Reference Guide".

Execution format of the cscstatus command is as follows:

To view the information of all HCSC servers

Execute the command without specifying any option.

```
cscstatus -user <login user ID> -pass <login password>
```

To view logical server information of a specific HCSC server

Execute the command by specifying the -csc and -type options. Specify "system" in the -type option.

```
cscstatus -user <login user ID> -pass <login password> -csc <HCSC server name> -type system
```

To reference the reception information of a specific HCSC server

Execute the command by specifying the -csc and -type options. Specify "reception" in the -type option.

```
cscstatus -user <login user ID> -pass <login password> -csc <HCSC server name> -type
reception
```

To reference the HCSC component information of a specific HCSC server

Execute the command by specifying the -csc and -type options. In the -type option, specify "compo".

```
cscstatus -user <login user ID> -pass <login password> -csc <HCSC server name> -type compo
```

●When using the cscutil command

Execute the cscutil command in the operating environment. Specify server in the -target option and specify get_info in the -operation option.

For details on the cscutil command, see "cscutil (various operations) " in "Service Platform Reference Guide".

The execution format of the cscutil command differs depending on whether you use the property definition file.

When you use the property definition file

In the -props option, specify the HCSC server name.

```
cscutil -user <login user ID> -pass <login password> -mng <Manager server> -target server -
operation get_info -props "CSCSrvName=<HCSC server name>"
```

You can use the cscrepls command to check the Manager name and the HCSC server name specified in the cscutil command. For details on the cscrepls command, see "cscrepls (displaying the repository information) " in "Service Platform Reference Guide".

When you do not use the property definition file

Specify the name of the property definition file name in the -propfile option. You must create the property definition file beforehand in the J2SE property file format.

```
cscutil -user <login user ID> -pass <login password> -mng <Manager name> -target server -
operation get_info -propfile <property definition file name>
```

Information output during command execution

The following table lists and describes the output information during command execution. The output information that is not listed in this table is the maintenance information for troubleshooting.

Table 5–1: TableInformation output by the command for referencing the HCSC server information

Output item	Output information
server-status	Displays the HCSC server status: • active (active status) • inactive (inactive status)# • starting (during startup processing) • stopping (during termination processing)
request-service-status	Displays the standard reception status. If the HCSC server is not running, this information is not displayed. • active (active status) • inactive (inactive status) • starting (during startup process) • startfailed (start failure status) • stopping (during stopping process) • stopfailed (stop failure status)

#

When the time required to acquire the status of the HCSC server exceeds the command timeout duration set in the csc-command-timeout of the HCSC server runtime definition file, output is performed in inactive status.

5.3.16 Checking Resource Operation Information of the HCSC Server

You can reference the information related to the resource statistics information on the HCSC server using windows and commands. The information that can be referenced using the windows and commands are the same. For details about the information that you can reference, see the description of the relevant windows and commands in the manual *Service Platform Reference*.

By checking the statistics information of the resources, you can check whether the resources are used within the defined scope. Moreover, you can also check whether you can safely terminate the resources before terminating the HCSC component, standard reception, and user-defined reception.

The statistics information is notified to HCSC server from the execution environment after every 60 seconds which is the default value. If the statistics information is notified to the HCSC server, the information displayed by windows and commands is updated. If you want to change the time interval when the statistics information is notified to the HCSC server, see the following manual:

To change the interval from the operating environment portal

For details, see *10.9.17 Settings for monitoring information (J2EE server)* in the manual *Application Server Management Portal Operation Guide*.

When the interval is changed using the Smart Composer functionality

See *3.3 Functionality to output the information file* and *3.4 Functionality for issuing events* in the manual *Application Server Function Guide - Operation, Monitoring, and Linkage*.

Note that you can reference resource statistics as statistics information. For details about how to reference the statistics information of the resource statistics, see appendix *Appendix E Statistical Information of Resource Statistics for HCSC Server*.

This subsection describes the prerequisites for checking resource operation information of HCSC server and how to check.

(1) Prerequisites

To check the resource statistics for HCSC server, the HCSC server must be in active status.

For details about how to check HCSC server status, see *5.3.15 Checking the HCSC server information*.

(2) How to view

The following describes how to check resource operation information of the HCSC server.

(a) Using windows

In the tree view, double-click the HCSC server on which you will check resource operation information. Information about the double-clicked HCSC server is displayed in the editor area. In the editor area, choose the `statistics confirmation` tab. The information related to the resource statistics for HCSC server is displayed.

For details about the `statistics confirmation` tab for the HCSC server, see *4.5 Resource information page* in the manual *Service Platform Reference*.

(b) Using commands

To check resource operation information of the HCSC server, execute the `cscresinfo` command in the operating environment.

For details about the `cscresinfo` command, see *cscresinfo (Displaying resource information)* in the manual *Service Platform Reference*.

5.3.17 Checking the service adapter information

The server adapter information that you can reference differs in case of screens and commands. For details on the information that you can reference, see the contents of corresponding screens and commands in "Service Platform Reference Guide".

This subsection describes the prerequisites and methods for referencing the service adapter information.

(1) Prerequisites

You can reference the server adapter information only when the HCSC server is in running state.

For details on how to check HCSC server status, see "5.3.15 Checking the HCSC server information".

(2) Reference method

The methods for referencing server adapter information are as follows:

(a) When using screens

In the Tree view, double-click the service adapter. Information on the double-clicked service adapter is displayed in the editor area. You can reference the service adapter information on the Operations page in the editor area.

For details on the Operations page for service adapters, see "4.4 Operations page" in "Service Platform Reference Guide".

You can also check the operating status of service adapter by icons displayed in the Tree view. For details on the icons displayed, see "4.1 Screen configuration (operating environment) " in "Service Platform Reference Guide".

(b) When using commands

To reference the service adapter information, execute the cscstatus command or cscutil command.

You can execute the cscstatus and cscutil commands from the operating environment. Use respective commands in the following cases:

- cscstatus command

  Use this command to reference the service adapter dynamic information (running status), service ID, and update time.
- cscutil command

  Use this command to reference the service adapter static information (definition information).

The description of how to execute each command is as follows:

●When using cscstatus command

Execute the cscstatus command in the operating environment. Execute the command by specifying the -csc and -type options. In the −type option, specify "compo".

For details on the cscstatus command, see "cscstatus (status display) " in "Service Platform Reference Guide".

The execution format of the cscstatus command is as follows:

```
cscstatus -user <login user ID> -pass <login password> -csc <HCSC server name> -type compo
```

●When using cscutil command

Execute the cscutil command in the operating environment. Specify compo in the -target option and specify get_adapter_info in the -operation option.

For details on the cscutil command, see the "cscutil (various operations)" in "Service Platform Reference Guide".

The execution format of the cscutil command differs depending on whether you use property definition file.

When you do not use property definition file

In the −props option, specify the HCSC server name and the service ID of the service adapter.

```
cscutil -user <login user ID> -pass <login password> -mng <Manager name> -target compo -
operation get_adapter_info -props "CSCSrvName=<HCSC server name>, AdapterName=<Service ID
of the service adapter>"
```

You can use the cscrepls command to check the Manager name, HCSC server name, and the service ID of the service adapter specified in the cscutil command. For details on the cscrepls command, see "cscrepls(displaying the repository information)" in "Service Platform Reference Guide".

When you use the property definition file

Specify the name of the property definition file name in the -propfile option. You must create the property definition file beforehand in the J2SE property file format.

```
cscutil -user <login user ID> -pass <login password> -mng <Manager name> -target compo -
operation get_adapter_info -propfile <property definition file name>
```

! Important note

- If you acquire information of an undeployed service adapter, the character string "null" is displayed.
- If you execute the cscutil command without the specifying the service ID of the service adapter, information of all the service adapters managed by the HCSC server is output.

Information output during command execution

The following table lists and describes the output information during command execution. The output information that is not listed in this table is the maintenance information for troubleshooting.

Table 5–2: TableInformation output by the command for referencing service adapter information

Output item	Output information
serviceName.<serial number>	Outputs Service component name.
adapterName. <serial number>	Displays the adapter distinguished name.
cscServerName. <serial number>	Displays the HCSC server name.
ownerCluster name. <serial number>	Displays the cluster name.
serviceKind. <serial number>	Outputs the HCSC component type. In the case of a service adapter, outputs "ServiceAdapter".
serviceProtocolKind. <serial number>	Outputs the protocol of the service component: • WebService (synchronous service (Web Services) call) • SessionBean (synchronous service (SessionBean) call) • MDB_WSR (asynchronous service (MDB (WS-R) call) • MDB_DBQ (asynchronous service (MDB (database queue) call)

Output item	Output information
serviceProtocolKind. <serial number>	• Custom (service adapters other than those mentioned above)
serviceStatus. <serial number>	Outputs the service adapter status: • active (active status) • inactive (inactive status) • starting (during startup processing) • startfailed (startup error) • stopping (during stop processing) • stopfailed (stopping error) • deleting (during deletion processing) • null (undeployed)
entryTime. <serial number>	Outputs the time at which the service adapter is deployed.
adapterQueueName. <serial number>	Outputs the queue name. The service adapter type is output only in case of MDB(WS-R) or MDB ((DB queue).
modifiedTime. <serial number>	Outputs the time at which the service adapter is updated (total time in milliseconds since 1970-01-01 at 00:00:00).
lcVersion. <serial number>	Outputs the location version number.
lcRevision. <serial number>	Outputs the location revision number.

5.3.18 Checking the business process information

The business process information that you can reference differs in case of using windows and commands. For details on the information that you can reference, see the contents of the corresponding screens and commands in "Service Platform Reference Guide".

This subsection describes the prerequisites and method for referencing the business process information.

(1) Prerequisites

You can reference business process information only when the HCSC server is in the running status.

For details on how to check HCSC server status, see "*5.3.15 Checking the HCSC server information*".

(2) Reference method

The methods for referencing the business process information are as follows:

(a) When using screens

In the Tree view, double-click the business process. Information of the double-clicked business process is displayed in the editor area. You can reference business process information on the Operations page in the editor area.

For details on the Operations page for business processes, see "4.4 Operations page" in "Service Platform Reference Guide".

You can also check the icon displayed in the Tree view to determine the operating status of the business process. For details on icons displayed, see "4.1 Screen configuration (operating environment) " in "Service Platform Reference Guide".

(b) When using commands

To view information about business processes, execute the `cscstatus` or `cscutil` command from the operating environment. Use the respective commands in the following cases:

- cscstatus command

Use this command to reference the business process dynamic information (running status), service ID, and modification time.

- cscutil command

  Use this command to reference the business process static information (definition information).

The description of how to execute each command is as follows:

●When using the cscstatus command

Execute the cscstatus command in the operating environment. Execute the command by specifying the -csc and -type options. In the −type option, specify "compo".

For details on the cscstatus command, see "cscstatus (status display)" in "Service Platform Reference Guide".

Execution format of the cscstatus command is as follows:

```
cscstatus -user <login user ID> -pass <login password> -csc <HCSC server name> -type compo
```

●Using the cscutil command

Execute the cscutil command in the operating environment. Specify compo in the -target option and specify get_bp_info in the -operation option.

For details on the cscutil command, see the "cscutil (various operations) " in "Service Platform Reference Guide".

The execution format of the cscutil command depends on whether you use the property definition file.

When you do not use the property definition file

In the -props option, specify the HCSC server name and the service ID of the business process.

```
cscutil -user <login user ID> -pass <login password> -mng <Manager name> -target compo -
operation get_bp_info -props "CSCSrvName=<HCSC server name>, AdapterName=<service ID of the
business process>"
```

You can use the cscrepls command to check the Manager name, the HCSC server name, and the service ID of the business process specified in the cscutil command. For details on the cscrepls command, see "cscrepls (displaying the repository information)" in "Service Platform Reference Guide".

When you use the property definition file

Specify the name of the property definition file in the -propfile option. You must create the property definition file beforehand in the J2SE property file format.

```
cscutil -user <login user ID> -pass <login password> -mng <Manager name> -target compo -
operation get_bp_info -propfile <property definition file name>
```

Important note

- If you acquire information of an undeployed business process, the character string "null" is displayed.
- If you execute the cscutil command without specifying the service ID of the business process, information on all the business processes managed by the HCSC server is displayed.

Information output during command execution

The following table lists and describes the output information during command execution. The output information that is not listed in this table is the maintenance information for troubleshooting.

Table 5–3: TableInformation output by the command for referencing business process information

Output item	Output information
serviceName.<serial number>	Displays the service component name.
adapterName.<serial number>	Displays the service ID of the business process.
cscServerName.<serial number>	Displays the HCSC server name.
ownerCluster name.<serial number>	Displays the cluster name.
serviceKind.<serial number>	Displays the HCSC component type. In the case of the business process, displays "BusinessProcess".
serviceStatus.<serial number>	Displays the business process status:

Output item	Output information
serviceStatus.<serial number>	• active (active status) • inactive (inactive status) • starting (during startup processing) • startfailed (startup error) • stopping (during stop processing) • stopfailed (stop error) • deleting (during deletion processing) • null (undeployed)
modifiedTime.<serial number>	Displays the time at which the business process is updated (total time in milliseconds since 1970-01-01 at 00:00:00).
entryTime.<serial number>	Displays the time at which the business process is deployed.
lcVersion.<serial number>	Displays the location version number.
lcRevision.<serial number>	Displays the location revision number.

5.3.19 Checking the information of user-defined reception

This subsection describes the prerequisites and method for referencing the user-defined reception information.

(1) Prerequisites

To reference the user-defined reception information, the HCSC server must be in a running state.

For details on the method check the HCSC server status, see "*5.3.15 Checking the HCSC server information*".

(2) Reference method

To reference the user-defined reception information, execute the cscstatus command or cscutil command from the operating environment. Use the cscstatus and cscutil commands respectively in the following cases:

- cscstatus command

  Use this command to reference the user-defined reception dynamic information (running status), reception ID, and modification time.

- cscutil command

  Use this command to reference the static information (definition information set in the user-defined reception runtime definition file) of the user-defined reception.

  The information reflected in actual operations is output as the definition information. The information set by the user is reflected in at the time of starting the HCSC server or at the time of starting the standard reception or user-defined reception.

  In either of the following cases, the information set when you started the HCSC server last, or when you started the standard reception or user-defined reception is displayed:

  - If you set the definition information when the HCSC server is running and you do not restart the HCSC server after setting the information
  - If you set the definition information when the standard reception or user-defined reception is running, and you do not restart the standard reception or user-defined reception after setting this information

The description of how to execute each command is as follows:

●When using cscstatus command

Execute the cscstatus command in the operating environment. Execute the command by specifying the -csc and -type options. In the -type option, specify "compo".

For details on the cscstatus command, see "cscstatus (status display) " in "Service Platform Reference Guide".

Execution format of the cscstatus command is as follows:

```
cscstatus -user <login user ID> -pass <login password> -csc <HCSC server name> -type compo
```

●When using cscutil command

Execute the cscutil command in the operating environment. Specify compo_urecp in the -target option and specify get_info in the -operation option.

For details on the cscutil command, see"

cscutil (various operations) "in "Service Platform Reference Guide".

The execution format of the cscutil command differs depends on whether you use the property definition file.

When you do not use the property definition file

Specify the HCSC server name in the -props option.

```
cscutil -user <login user ID> -pass <login password> -mng <Manager name> -target
compo_urecp -operation get_info -props "CSCSrvName=<HCSC server name>"
```

You can use the cscrepls command to check the Manager name and HCSC server name specified in the cscutil command. For details on the cscrepls command, see the "cscrepls (displaying the repository information) " in "Service Platform Reference Guide".

When you use the property definition file

Specify the name of the property definition file in the -propfile option. You must create the property definition file beforehand in the J2SE property file format.

```
cscutil -user <login user ID> -pass <login password> -mng <Manager name> -target
compo_urecp -operation get_info -propfile <property definition file name>
```

! Important note

- If you acquire information on an undeployed user-defined reception, the "null" character string is displayed.
- If you execute the cscutil command without specifying the reception ID of the user-defined reception, the information of all user-defined receptions managed by the HCSC server is displayed.

Information output during command execution

The following table lists and describes the output information during command execution. The output information that is not listed in this table is the maintenance information for troubleshooting.

Table 5–4: Information output by the command for referencing the user-defined reception information

Output item	Output information
receptionName.<Serial number>	Displays the reception name of the user-defined reception.
receptionID.<Serial number>	Displays the reception ID of the user-defined reception.
cscServerName.<Serial number>	Displays the HCSC server name.
ownerCluster name.<Serial number>	Displays the cluster name.
serviceName.<Serial number>	Displays the service name related to the user-defined reception
receptionKind.<Serial number>	Displays the reception (HCSC component) type using the user-defined reception. • bp (business process)
receptionProtocolKind.<Serial number>	Displays the user-defined reception protocol. • WebService (synchronous service (Web Services) call)
receptionStatus.<Serial number>	• active (active status) • inactive (inactive status) • starting (during startup processing) • startfailed (startup error) • stopping (during stop processing) • stopfailed (stop error) • deleting (during deletion processing)

Output item	Output information
receptionStatus.<Serial number>	• null (undeployed)
entryTime.<Serial number>	Displays the time when the user-defined reception is defined in the YYYY/MM/DD hh:mm:ss.SSS format. • YYYY: Year • MM: Month • DD: Date • hh: Hour • mm: Minute • ss: Second • SSS: Milliseconds
modifiedTime.<Serial number>	Displays the time at which the user-defined reception is updated (total milliseconds from January 1, 1970 00:00:00).
lcVersion.<Serial number>	Displays the location version number.
lcRevision.<Serial number>	Displays the location revision number.
runtime.user-defined-reception-soap.threads.maximum.<Serial number>	Outputs the maximum number of concurrent executions for the user-defined reception. If the maximum number of concurrent executions is not set in the user-defined reception runtime definition file, the default value (10) is output.
runtime.user-defined-reception-soap.exclusive.threads.<Serial number>	Outputs the number of dedicated threads for the user-defined reception. If the number of dedicated threads is not set in the user-defined reception runtime definition file, the default value (0) is output.
runtime.user-defined-reception-soap.queue-size.<Serial number>	Outputs the pending queue size for the user-defined reception. If the pending queue size is not set in the user-defined reception runtime definition file, the default value (8192) is output.

5.3.20 Performing cache of the definition information of the business process

This subsection describes the cache of the format definition of the business process and the definition information of the data transformation definition.

(1) Prerequisites

To perform the cache business processes, the HCSC server must be in a running state.

For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".

(2) Performing cache

To perform cache of the format definition of the business process and the definition information of the data transformation definition, execute the cscprecache command in the operating environment. If you have not executed the cscprecache command, since the format definition and data transformation definition are not analyzed until the request processing time, it is recommended that you execute the cscprecache command.

You can execute the following processes with the cscprecache command:

- Send analysis requests to business processes running on HCSC servers in a batch
- Send analysis requests to specific business processes

  When you send the analysis request to multiple business processes, threads are generated in the command, and parallel processing is executed.

For details on the cscprecachecommand, see "cscprecache (advance cache of the format definition and data transformation definition) " in "Service Platform Reference Guide".

The execution format of the cscprecache command is as follows:

- **When you send analysis requests to business processes running on the HCSC server in a batch**

```
cscprecache -csc <HCSC server name>
```

- **When you send analysis requests for specific business processes**

```
cscprecache -csc <HCSC server name> -name <Service ID>
```

The following table describes the execution result of the cscprecache command that differs depending on whether you send analysis requests after the execution of the command:

Table 5–5: Execution results of the cscprecache command

Operations after executing the command	Execution results of cscprecache command
If the command returns the command execution results without sending analysis requests	• If the specified HCSC server is not running , • The command ends abnormally without sending the analysis request. • If you do not specify the -name option, • If the business process that is running does not exist, the command terminates successfully. • If you specify the -name option • If the business process specified with the -name option is not running, the command terminates abnormally. • Furthermore, if you specify components that are not business processes, the command terminates abnormally.
If the command returns the command execution results after sending analysis requests	• Each time the execution result of one business process is returned, execution results are output to the standard output or the standard error output. • If error occurs in the analysis process after all execution results are returned, the command terminates abnormally. If you succeed in performing all analysis processes and caches, the command terminates successfully. • If you execute the command for a cached business process, the command terminates successfully without executing the analysis process.

5.3.21 Changing HCSC Server Definitions

To change the HCSC server definition information, use the same method as that for setting the HCSC server definition information. For details about how to set up the HCSC server definition information, see *3.1.4 Setting up the HCSC server definition information*.

5.3.22 Changing the definition information of user-defined reception

This subsection describes the prerequisites and methods for changing the definition information for user-defined reception.

(1) Prerequisites

To change the definition information for user-defined reception, the HCSC server must be in running status.

For details on how to check HCSC server status, see "*5.3.15 Checking the HCSC server information*".

(2) Changing method

The procedure for changing the definition information of user-defined reception is as follows:

1. Check the definition information for user-defined reception.
   Execute the cscutil command for checking from the operating environment.

For details on how to check the definition information for user-defined reception, see "*3.1.16 Checking the definition information of the user-defined receptions*".

2. Stop the user-defined reception.

   For details on how to stop the user-defined reception, see "*5.3.29 Stopping the user -defined reception*".

3. Acquire the definition information for user-defined reception.

   Specify get in the -operation option of the csccompoconfig command to acquire the definition information for user-defined receptions.

   For details on the csccompoconfig command, see "csccompoconfig (HCSC component definition) " in "Service Platform Reference Guide".

4. Change the definition information acquired for user-defined reception.

   Change the parameter values in the user-defined reception runtime definition file and change the definition information for user-defined reception.

   For details on the user-defined reception runtime definition file, see "User-defined reception runtime definition file" in "Service Platform Reference Guide".

5. Specify the definition information for user-defined reception.

   For details on how to specify the definition information for user-defined reception, see "*3.1.15 Setting the definition information for user-defined receptions*".

6. Check the definition information for user-defined reception.

   For details on how to check the definition information for the user-defined reception, see "*3.1.16 Checking the definition information of the user-defined receptions*".

7. Start the user-defined reception.

   For details on how to start the user-defined reception, see "*5.3.8 Starting user-defined receptions*".

8. Check the user-defined reception information.

   Execute the cscutil command for checking from the operating environment.

   For details on how to check the definition information for user-defined reception, see "*5.3.19 Checking the information of user-defined reception*".

5.3.23 Changing the configuration of HCSC components

When the definition of the HCSC components is changed in the development environment, the changed definition is passed to the operating environment by using the repository. In the operating environment, change the configuration of HCSC components according to the definition information changed in the development environment.

This subsection describes the prerequisites and method for changing the configuration of the HCSC components:

(1) Prerequisites

To change the configuration of HCSC components, the following conditions must be fulfilled:

- The HCSC server is running.

  For details on how to check HCSC server status, see "*5.3.15 Checking the HCSC server information*".
- Management Server is in running state
- For details on how to check the Management Server status, see "*5.3.13 Checking the Manager status*".
- Administration Agent is in running state
- For details on how to check the Administration Agent status, see "*5.3.13 Checking the Manager status*".
- Database is in running state

  For details on how to check the database status, see "*5.3.10 Checking the Database Status*".

(2) Changing method

The procedure for changing the configuration of HCSC components is as follows:

1. Check the differences in the repository information.

For details on how to check the differences in the repository information, see "*4.5 Referencing difference information of repositories*".

2. Stop HCSC components.

   Specify the -cluster option in the csccompostop command, to stop HCSC components deployed on all HCSC servers within the cluster, in a batch.

   For details on how to stop HCSC components, see "*5.3.29 Stopping the user -defined reception*", "*5.3.30 Terminating the Service Adapter*", and "*5.3.31 Terminating the Business Process*".

3. Delete HCSC components.

   Specify the -cluster option in the csccompoundeploy command, to delete HCSC components deployed on all HCSC servers within the cluster, in a batch.

   For details on how to delete HCSC components, see "*3.3.1 Deleting a service adapter*", "*3.3.2 Deleting a business process*", and "*3.3.3 Deleting a user-defined reception*".

4. Import the repository.

5. For details on how to import the repository, see "*4.3 Importing a repository*".

6. Deploy HCSC components.

   Specify the -cluster option in the csccompodeploy command, to deploy the undeployed HCSC components on all HCSC servers within the cluster, in a batch.

   For details on how to deploy HCSC components, see "*3.1.8 Deploying a service adapter*", "*3.1.13 Deploying a business process*", and "*3.1.14 Deploying a user-defined reception*".

7. Start HCSC components.

   Specify the -cluster option in the csccompostart command, to start HCSC components deployed on all HCSC servers within the cluster, in a batch.

   For details on how to start HCSC components, see "*5.3.6 Starting Service Adapters*","*5.3.7 Starting Business Processes*", and "*5.3.8 Starting user-defined receptions*".

(3) Method for adding, updating, and deleting multiple HCSC components

The procedure for adding, updating, and deleting multiple HCSC components is as follows:

First, create a list of the target HCSC components with the following procedure:

1. Upgrade the version of new repository.

```
cscrepupdate -inputfile <zip file name> -outputfile <zip file name of the output
destination>
```

2. Acquire the change information of the current repository and the new repository. Create a list of the target HCSC components with any one of the following methods:

   - Output the HCSC component-specification file by specifying the -compo option in the cscrepdiff command.

```
cscrepdiff -repfile <repository zip file name> -compo -listfile <HCSC component-
specification file name of the output destination>
```

   - Create HCSC component-specification file manually.

The procedure for adding, updating, and deleting multiple HCSC components by specifying the created HCSC component-specification file in the -namelist option is as follows:

(a) Adding multiple HCSC components

The following is the procedure for adding multiple HCSC components. Use this procedure to add HCSC components of the distributed development.

1. Import repositories.

```
cscrepctl -import <repository zip file name> -compo -namelist <HCSC component-specification
file name>
```

2. Deploy HCSC components.

```
csccompodeploy -namelist <HCSC component-specification file name>
```

3. Start HCSC components.

```
csccompostart -namelist <HCSC component-specification file>
```

(b) Updating multiple HCSC components

The procedure for updating multiple HCSC components is as follows. Use this procedure to update HCSC components of the distributed development.

1. Stop HCSC components.

```
csccompostop -namelist <HCSC component-specification file name>
```

2. Undeploy HCSC components.

```
csccompoundeploy -namelist <HCSC component-specification file name>
```

3. Import repositories.

```
cscrepctl -import <repository zip file name> -compo -namelist <HCSC component-specification
file name>
```

4. Update the service information. Execution of this step is optional.

```
cscsvcctl -setfile < service-information change definition file>
```

5. Deploy HCSC components.

```
csccompodeploy -namelist <HCSC component-specification file name>
```

6. Start HCSC components.

```
csccompostart -namelist <HCSC component-specification file name>
```

(c) Deleting multiple HCSC components

The procedure for deleting multiple HCSC components is as follows:

1. Stop HCSC components.

```
csccompostop -namelist < component-specification file name >
```

2. Undeploy HCSC components.

```
csccompoundeploy -namelist <HCSC component-specification file name >
```

3. Delete the component information from respositories.execution of this step is optional.

```
cscrepctl -delete -namelist <HCSC component-specification file name >
```

(d) Adding, updating, and deleting multiple HCSC components

The procedure for concurrently adding, updating, and deleting multiple components is as follows. Use this procedure to switch HCSC components.

1. Stop HCSC components. (updating and deleting HCSC components).

```
csccompostop -namelist <HCSC component-specification file name>
```

2. Undeploy HCSC components.(updating and deleting HCSC components).

```
csccompoundeploy -namelist <HCSC component-specification file name>
```

3. Perform normal import of repositories.

```
cscrepctl -import <repository zip file name>
```

4. Update the service information. Execution of this step is optional.

```
cscsvcctl -setfile <service-information change definition file >
```

5. Deploy HCSC components. (updating and deleting HCSC components).

```
csccompodeploy -namelist <HCSC component-specification file name>
```

6. Star HCSC components. (updating and deleting HCSC components).

```
csccompostart -namelist <HCSC component-specification file name>
```

5.3.24 Changing the Component Service Connection Point

In the operating environment, you can change the information about the service adapter connection point.

This subsection explains the prerequisites for changing the service module connection point and how to change the connection point.

(1) Prerequisites

To change the service module connection point, the following conditions must be met:

- The HCSC server is running.
  For details about how to check HCSC server status, see *5.3.15 Checking the HCSC server information*.

(2) Change Procedures

The procedure for changing the service module connection point is explained below:

1. The service adapter will now stop.
   Specify the `-cluster` option with the `csccompostop` command and terminate the service adapters deployed on all the HCSC servers in the cluster, in a batch.
   For details about how to terminate service adapters, see *5.3.30 Terminating the Service Adapter*.
2. Delete the service adapter.
   Specify the `-cluster` option with the `csccompoundeploy` command and delete the service adapters deployed on all the HCSC servers in the cluster, in a batch.
   For details about how to delete service adapters, see *3.3.1 Deleting a service adapter*.
3. Collect and update the service information and change the service connection point.
   For details about how to collect and update the service information, see *3.1.6 Changing the service information*.
   Note that when you change the service module connection point, in the service information update, change the values of the following parameters in the service information change definition file. For details about the service information change definition file, see *Service information change definition file* in the manual *Cosminexus Service Platform Reference*.

   In the case of the service adapter for Web service

   ```
   cluster-name.service-ID.WebService.url=URL-used-to-invoke-service-components
   ```

   In the case of the service adapter for SessionBean

   ```
   cluster-name.service-ID.SessionBean.url=URL-used-to-invoke-service-components
   cluster-name.service-ID.SessionBean.lookupName=lookup-name
   ```

   In the case of the service adapter for MDB (WS-R)

   ```
   cluster name.service ID.MDB_WSR.url=message-destination-URL-of-the-service-
   adapter
   cluster-name.service-ID.MDB_WSR.queue_name=queue-name-associated-to-the-service-
   component
   ```

   In the case of the service adapter for MDB (DB queue)

   ```
   Cluster-name.service-ID.MDB_DBQ.queue_name=queue-name-associated-to-the-service-
   component
   ```

4. Deploy the service adapter.
   Specify the `-cluster` option with the `csccompodeploy` command and deploy the service adapters on all the HCSC servers in the cluster in a batch.
   For details about how to deploy service adapters, see *3.1.8 Deploying a service adapter*.
5. The service adapter will now start.
   Specify the `-cluster` option with the `csccompostart` command and start the service adapters deployed on all the HCSC servers in the cluster, in a batch.
   For details about how to start service adapters, see *5.3.6 Starting Service Adapters*.

5.3.25 Changing the Flow Control Value

In the operating environment, you can change the flow control value of the standard reception (synchronous reception (Web service)) and user-defined reception.

This subsection explains the prerequisites for changing the flow control value of the standard reception (synchronous reception (Web service)) and user-defined reception and how to change the value.

(1) Prerequisites

To change the flow control value of the standard reception (synchronous reception (Web service)) and user-defined reception, the following conditions must be met:

- Management Server is active
  For details about how to check the Management Server status, see *5.3.13 Checking the Manager status*.
- Administration Agent is active
  For details about how to check the Administration Agent status, see *5.3.13 Checking the Manager status*.

(2) Change Procedures

The procedure for changing the flow control value of the standard reception (synchronous reception (Web service)) and user-defined reception is explained below:

(a) To change the flow control value of the standard reception (synchronous reception (Web service))

The procedure for changing the flow control value of the standard reception (synchronous reception (Web service)) is explained below:

1. Update the HCSC server runtime definition file and change the flow control value.
   When you want to change the flow control value, change the following property values in the HCSC server runtime definition file. For details about the HCSC server runtime definition file, see *HCSC server runtime definition file* in the manual *Cosminexus Service Platform Reference*.
   - In SOAP 1.1

```
request-soap.instance.maximum=maximum-number-of-concurrent-executions-of-
standard-synchronous-reception-(Web-Service-or-SOAP-1.1) request-
soap.exclusive.threads=number-of-dedicated-threads-of-standard-synchronous-
reception-(Web-Service-or-SOAP-1.1) request-soap.queue-size=pending-queue-size-
of-standard-synchronous-reception-(Web-Service-or-SOAP-1.1)
```

   - In SOAP 1.2

```
request-soap1_2.instance.maximum=maximum-number-of-concurrent-executions-of-
standard-synchronous-reception-(Web-Service-or-SOAP-1.2)
request-soap1_2.exclusive.threads=number-of-dedicated-threads-of-standard-
synchronous-reception-(Web-Service-or-SOAP-1.2)
request-soap1_2.queue-size=pending-queue-size-of-standard-synchronous-reception-
(Web-Service-or-SOAP-1.2)
```

2. Specify the HCSC server runtime definition file.
   For details about how to specify the HCSC server runtime definition files, see *3.1.4 Setting up the HCSC server definition information*.

Important note

The specified information is reflected when the standard reception starts.

(b) To change the flow control value of the user-defined reception

The process of changing the flow control value of the user-defined reception is similar to the process for changing the definition information for user-defined reception. For details about how to change the definition information for user-defined reception, see *5.3.22 Changing the definition information of user-defined reception*.

Note that when you want to change the flow control value, change the following parameter values in the user-defined reception runtime definition file. For details about the user-defined reception runtime definition file, see *User-defined reception runtime definition file* in the manual *Cosminexus Service Platform Reference*.

```
user-defined-reception-soap.threads.maximum=maximum-number-of-concurrent-executions
user-defined-reception-soap.exclusive.threads=number-of-dedicated-threads
user-defined-reception-soap.queue-size=pending-queue-size
```

Important note

The specified information is reflected when the user-defined reception starts.

5.3.26 Changing the Communication Timeout Value for Invoking Service Modules

In the operating environment, you can change the communication timeout value for invoking the service modules of the service adapters of Web services and SessionBeans.

This subsection explains the prerequisites for changing the communication timeout value for invoking the service modules of the service adapters for Web services and SessionBeans and how to change the value.

(1) Prerequisites

To change the communication timeout value for invoking the service modules of the service adapter for Web service and service adapter for SessionBean, the following conditions must be met:

- The HCSC server is running.
  For details about how to check HCSC server status, see *5.3.15 Checking the HCSC server information*.

(2) Change Procedures

The following describes how to change the communication timeout value:

1. The service adapter will now stop.
   Specify the `-cluster` option with the `csccompostop` command and terminate the service adapters deployed on all the HCSC servers in the cluster, in a batch.
   For details about how to terminate service adapters, see *5.3.30 Terminating the Service Adapter*.
2. Delete the service adapter.
   Specify the `-cluster` option with the `csccompoundeploy` command and delete the service adapters deployed on all the HCSC servers in the cluster, in a batch.
   For details about how to delete service adapters, see *3.3.1 Deleting a service adapter*.
3. Collect and update the service information and change the communication timeout value for invoking the service.
   For details about how to collect and update the service information, see *3.1.6 Changing the service information*.
   Note that when you want to change the communication timeout value for invoking the service module, update the service information and change the following parameter values in the service information change definition file. For details about the service information change definition file, see *Service information change definition file* in the manual *Cosminexus Service Platform Reference*.

In the case of the service adapter for Web service (SOAP 1.1 mode)

```
Cluster-name.service-ID.WebService.c4web.application.socket_read_timeout=read-
timeout-value
Cluster-name.service-
ID.WebService.c4web.application.socket_connect_timeout=connect-timeout-value
Cluster-name. Service-
ID.WebService.c4web.application.socket_write_timeout=write-timeout-value
```

In the case of the service adapter for Web Services (SOAP 1.1/ 1.2 combined mode)

```
Cluster-name.service-ID.WebService.com.cosminexus.csc.request.timeout=read-
timeout-value
Cluster-name.service-
ID.WebService.com.cosminexus.csc.connect.timeout=connection-timeout-value
```

In the case of the service adapter for SessionBean

```
Cluster-name.service-ID.SessionBean.c4web.application.ejb_timeout=invoke-
timeout-value
```

4. Deploy the service adapter.

   Specify the `-cluster` option with the `csccompodeploy` command and deploy the service adapters on all the HCSC servers in the cluster in a batch.

   For details about how to deploy service adapters, see *3.1.8 Deploying a service adapter*.

5. The service adapter will now start.

   Specify the `-cluster` option with the `csccompostart` command and start the service adapters deployed on all the HCSC servers in the cluster, in a batch.

   For details about how to start service adapters, see *5.3.6 Starting Service Adapters*.

5.3.27 Changing resource adapter properties

This subsection describes the prerequisites and method to change properties of resource adapters being used by the HCSC server:

(1) Prerequisites

To change resource adapter properties, the following conditions must be fulfilled.

- Management server is in running state

  For details on how to check the status of Management Server, see"5.3.13(1)(a)Method to reference Management Server".

- Administration Agent is in running state

  For details on how to check the status of Administration Agent, see "5.3.13(1)(b)Viewing Administration Agent status".

(2) Method for changing

The following is the procedure for changing properties of the resource adapter. For details on how to acquire and set the Connector property file as mentioned in the procedure, see"4.4.2 Defining resource adapter properties (for Connector 1.0) "or "4.4.3 Defining resource adapter properties (for Connector 1.5) " in "Application Server Application Setup Guide".

1. Stopping the HCSC server and the logical server concurrently in a batch

   When the HCSC server is in a running status, specify -system option in the cscsvstop command, to concurrently stop the HCSC server and the logical server in a batch.

   For details on how to check the status of HCSC server, "5.3.15 Checking the HCSC server information".

   For details on how to stop the HCSC server and the logical server, see "5.3.33 Terminating the HCSC Server".

   Execution format of the cscsvstop command is as follows:

```
cscsvstop -user <login user ID> -pass <login password> -csc <HCSC server name> -system
```

2. Starting the J2EE server without starting J2EE applications.

   To start the J2EE server without starting J2EE applications, specify the -logical option in the cscsvstart command.

   For details on how to start the J2EE server, "*5.3.4 Starting HCSC server*".

   Execution format of the cscsvstart command is as follows:

```
cscsvstart -user <login user ID> -pass <login password> -csc <HCSC server name> -logical
<J2EE server name>
```

3. Stopping the resource adapter.

   Execute the cjstoprar command, to stop the resource adapter that is being used by the HCSC server.

   For details on how to stop resource adapters, see "4.4.7 Stopping J2EE resource adapters" in "Application Server Application Setup Guide"

   Execution format of the cjstoprar command is as follows:

```
cjstoprar <J2EE server name> [-nameserver <providerURL>]-resname <display name of the
resource adapter>
```

! Important note

When you stop DB Connector for Reliable Messaging, Reliable Messaging must be in a stopped state.

4. Acquiring the Connector property file of the resource adapter.

   Execute the cjgetrarprop command As and when required to acquire the Connector property file of the resource adapter being used the HCSC server.

   The execution format of the cjgetrarprop command is as follows:

```
cjgetrarprop <server name> [-nameserver <provider URL>] -resname <display name of the
resource adapter> -c <Connector property file path>
```

5. Editing the Connector property file of the resource adapter.

   For the setup value of the Connector property file of the resource adapter that is being used by the HCSC server, see "3.1.2 Setting up the software required for the execution environment".

6. Specifying the value of the Connector property file in the resource adapter.

   By executing the cjsetrarprop command, the value of the Connector property file is reflected in the resource adapter that is being used by the HCSC server.

   Execution format of the cjsetrarprop command is as follows:

```
cjsetrarprop <server name> [-nameserver <provider URL>] -resname <display name of the
resource adapter -c <Connector property file path>
```

7. Performing the Connection Test of the resource adapter.

   Execute the cjtestrescommand, and validate whether the information set in the resource adapter is correct, with the connection test.

   For the Connection test of resource adapters, see "4.4.5 Connection test of J2EE resource adapters" in "Application Server Application Setup Guide".

   Execution format of the cjtestres command is as follows:

```
cjtestres [<server name>] [-nameserver <provider URL>] -type rar -resname <display name of
the resource adapter
```

! Important note

To perform the connection test of Reliable Messaging, you must start DB Connector for Reliable Messaging. Also, to perform the connection test of DB Connector for Reliable Messaging, Reliable Messaging must be already started.

8. Starting the resource adapter.

   Execute the cjstartrar command to start the resource adapter being used by the HCSC server.

   For details on how to start the resource adapter, see "4.4.6 Starting J2EE resource adapters" in "Application Server Application Setup Guide".

   Execution format of the cjstartrar command is as follows:

```
cjstartrar 。e<server name>。f 。e-nameserver <provider URL>。f -resname <display name of the
resource adapter
```

Important note

When you start Reliable Messaging, DB Connector for Reliable Messaging must be already started.

9. Stopping the J2EE server.

   To stop the J2EE server, specify the -logical option in the cscsvstop command.

   For details on how to stop the J2EE server, see "5.3.33 Terminating the HCSC Server".

   Execution format of the cscsvstop command is as follows:

```
cscsvstop -user <login user ID> -pass <login password> -csc <HCSC server name> -logical
<J2EE server name>
```

10. Starting the HCSC server and the logical server concurrently in a batch

    Specify -system option in the cscsvstart command, to start the HCSC server and the logical server in a batch concurrently.

    For details on how to start the HCSC server and the logical server, see "*5.3.4 Starting HCSC server*".

    The execution format of the cscsvstart command is as follows:

```
cscsvstart -user <login user ID> -pass <login password> -csc <HCSC server name> -system
```

5.3.28 Terminating the Standard Reception

The supported methods for terminating standard receptions are normal termination, planned termination, and forced termination.

Normal termination

For synchronous acceptance

The system processes the current execution request and then terminates the standard reception.

For asynchronous acceptance

The system places an execution request from the service requester in unaccepted status, processes the current execution request, and then terminates the standard reception. Accepted execution requests remain unprocessed in the queue.

When the standard reception is restarted after normal termination, processing begins with the execution requests remaining in the queue.

If HCSC server setup is cancelled after normal termination, the execution requests remaining in the queue are discarded.

Planned termination

This termination method is used to cancel HCSC server setup after terminating the standard reception. When planned termination is executed, the standard reception is terminated as follows:

For synchronous acceptance

The system processes the current execution request and then terminates the standard reception.

For asynchronous acceptance

The system places an execution request from the service requester in unaccepted status, processes all the execution requests remaining in the queue, and then terminates the standard reception.

Forced termination

Forced termination can be achieved by commands only. This termination method can forcibly terminate the standard reception even when another command is executing or when the standard reception termination error has occurred.

This subsection describes the prerequisites for terminating the standard reception and how to terminate it.

(1) Prerequisites

To terminate the standard reception, the following conditions must be met:

- The HCSC server is running.

- The standard reception is in active status.

For details about how to check the status of the HCSC server and standard reception, see *5.3.15 Checking the HCSC server information*.

(2) Termination method

This subsection describes how to terminate the standard reception.

! Important note

If termination of the standard reception fails, eliminate the cause of the error and then forcibly terminate the standard reception. Once the standard reception is in inactive status, start it again to restart operations. For details about how to start the standard reception, see *5.3.9 Starting standard receptions*.

(a) Using windows

To terminate the standard reception using windows in the operating environment:

1. In the tree view, double-click the HCSC server on which you wish to terminate the standard reception.
   Information about the double-clicked HCSC server is displayed in the editor area.
2. In the editor area, choose the Operations tab.
   The Operations page displays information about operations of the HCSC server you chose in step 1.
   For details about the Operations page for an HCSC server, see *4.4 Operations page* in the manual *Cosminexus Service Platform Reference*.
3. Check the information displayed in the Operations page, and under Request reception, click the Normal Stop or Planned Stop button.
   A dialog box confirming termination of the standard reception is displayed.
4. Check the information displayed in the dialog box and then click the OK button.
   Standard reception termination processing begins. Log information during termination processing is displayed in the console view.
   If the **Cancel** button is clicked, the system returns to the Operations page without executing termination processing.
   When standard reception termination processing is finished, a dialog box indicating the execution result is displayed.
5. Check the dialog box indicating the execution result.
   If termination processing was successful:
   Click the **OK** button to return to the Operations page.
   On the Operations page, the standard reception status is set to inactive. Also, the **Normal Stop** and **Planned Stop** buttons are disabled and the **Start** button is enabled.
   If termination processing failed:
   The dialog box displays the nature of the error. Check the message ID provided in the detailed information, and then take appropriate action.

(b) Using commands

To terminate the standard reception, execute the `cscrcptnstop` command or `cscutil` command in the operating environment.

Use the `cscrcptnstop` command and `cscutil` command in the following cases:

- `cscrcptnstop` command
  To terminate the standard reception in the operating environment where the corresponding repository exists.
- `cscutil` command
  To terminate the standard reception in an environment (for example, execution environment operating directly in JP1) where the `cscutil` command can be used and where the corresponding repository does not exist.

The following describes how to execute the above commands:

Using the cscrcptnstop command

Execute the cscrcptnstop command in the operating environment.

For details about the cscrcptnstop command, see *cscrcptnstop (Stopping the standard and user-defined receptions)* in the manual *Cosminexus Service Platform Reference*.

The execution format of the cscrcptnstop command is explained below:

To terminate the standard receptions of all the HCSC servers in the cluster, in a batch (for each cluster)

Specify the cluster name and execute the command.

The standard receptions of all the HCSC servers in the cluster specified with the -cluster option are terminated in a batch (all the user-defined receptions that are not terminated are also terminated at the same time).

```
cscrcptnstop -user login-user-ID -pass login-password -cluster cluster-name
```

If you want to terminate only the standard reception without terminating the user-defined reception, specify the -standard option.

```
cscrcptnstop -user login-user-ID -pass login-password -cluster cluster-name -
standard
```

To terminate the standard reception for the HCSC server in a batch (For each HCSC server)

Specify the HCSC server name and execute the command.

The standard reception for the HCSC server specified with the -csc option is terminated (all the user-defined receptions that are not terminated are also terminated at the same time).

```
cscrcptnstop -user login-user-ID -pass login-password -csc HCSC-server-name
```

If you want to terminate only the standard reception without terminating the user-defined reception, specify the -standard option.

```
cscrcptnstop -user login-user-ID -pass login-password -csc HCSC-server-name -
standard
```

Using the cscutil command

Execute the cscutil command in the operating environment. Specify request_service in the -target option and stop in the -operation option.

For details about the cscutil command, see *cscutil (Various operations)* in the manual *Cosminexus Service Platform Reference*.

The execution format of the cscutil command depends on whether or not a property definition file is used.

When a property definition file is not used

In the -props option, specify the HCSC server name, J2EE server name, and termination flag.

```
cscutil -user login-user-ID -pass login-password -mng manager-name -target
request_service -operation stop -props "CSCSrvName=HCSC-server-name,
J2EESrvName=J2EE-server-name, ForceFlag=termination-flag"
```

You can use the cscrepls command to check the Manager name, HCSC server name, and J2EE server name that are specified in the cscutil command. For details about the cscrepls command, see *cscrepls (Displaying the repository information)* in the manual *Cosminexus Service Platform Reference*.

The termination flag specifies whether normal termination, planned termination, or forced termination is to be executed. In this flag, specify one of the following values:

- Normal termination: NORMAL_OPTION
- Planned termination: WAIT_OPTION
- Forced termination: FORCE_OPTION

When a property definition file is used

Specify the name of the property definition file name in the -propfile option. The property definition file must be created beforehand in the J2SE property file format.

```
cscutil -user login-user-ID -pass login-password -mng manager-name -target
request_service -operation stop -propfile property-definition-file-name
```

5.3.29 Stopping the user -defined reception

This subsection describes prerequisites and methods for stopping user-defined receptions.

(1) Prerequisites

To stop user-defined receptions, the following conditions must be fulfilled:

- The HCSC server is in running status
  For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".
- User-defined reception is in running status
  For details on how to check the user-defined reception status, see "5.3.19 Checking the information of user-defined receptions".

(2) Stopping method

To stop user-defined receptions, execute the cscrcptnstop command or the csccompostop command in the operating environment.

Use the cscrcptnstop and csccompostop commands in the following cases:

- cscrcptnstop command
  - Use this command to stop user-defined receptions and standard receptions in a batch.
  - Use this command to stop the user-defined reception deployed on the HCSC server in a batch.
  - You can also stop user-defined receptions in a batch for each cluster. Note that you cannot stop only a specific user-defined reception.
  - Use this command to stop user-defined receptions in the operating environment in which the corresponding repository exists.
- csccompostop command
  - Use this command to stop the service adapter, business process, and user-defined reception in a batch.
  - You cannot stop only user-defined receptions in a batch.
  - Use this command to stop specific user-defined receptions deployed on the HCSC server.
  - You can also stop specific user-defined receptions for each cluster.
  - Use this command to stop user-defined receptions in the operating environment in which the corresponding repository exists.

The description of how to execute each command is as follows:

●Using the cscrcptnstop command

Execute the cscrcptnstop command in the operating environment.

For details on the cscrcptnstop command, see "cscrcptnstop (stopping standard receptions and user-defined receptions) " in "Service Platform Reference Guide".

Execution format of the cscrcptnstop command is as follows:

To stop user-defined receptions deployed on all HCSC servers within the cluster in a batch (for each cluster)

Execute the command by specifying the cluster name.

The user-defined receptions deployed on all HCSC servers within the cluster specified in the -cluster option are stopped in a batch (all standard receptions that are not stopped are also not stopped at the same time).

```
cscrcptnstop -user <login user ID> -pass <login password> -cluster <cluster name>
```

To stop only the user-defined reception without stopping the standard reception, specify the -userdef option.

```
cscrcptnstop -user <login user ID> -pass <login password> -cluster <cluster name> -userdef
```

To stop user-defined receptions deployed on the HCSC server in a batch (for each HCSC server)

Execute the command by specifying the HCSC server name.

The user-defined receptions deployed on the HCSC server specified in the -csc option are stopped (all the unstopped standard receptions also stop concurrently).

```
cscrcptnstop -user <login user ID> -pass <login password> -csc <HCSC server name>
```

If you want to stop only the user-defined reception without stopping the standard reception, specify the-userdef option.

```
cscrcptnstop -user <login user ID> -pass <login password> -csc <HCSC server name> -userdef
```

●When using the csccompostop command

Execute the csccompostop command in the operating environment.

For details on the csccompostop command, see "csccompostop (stopping HCSC components)" in "Service Platform Reference Guide".

Execution format of the csccompostop command is as follows:

To stop user-defined receptions deployed on all HCSC servers within the cluster in a batch (for each cluster)

Execute the command by specifying the cluster-name and the -all option.

The user-defined receptions deployed on all HCSC servers within the cluster specified with the -cluster option are stopped in a batch (all the unstopped service adapters and business processes are also stopped concurrently).

```
csccompostop -user <login user ID> -pass <login password> -cluster <cluster name> -all
```

To stop user-defined receptions deployed on the HCSC server in a batch (for each HCSC server)

Execute the command by specifying the HCSC server name and the -all option.

The user-defined receptions deployed on the HCSC server specified in the -csc option are stopped (all the unstopped service adapters and business processes are also stopped concurrently).

```
csccompostop -user <login user ID> -pass <login password> -csc <HCSC server name> -all
```

To stop specific user-defined receptions deployed on all HCSC servers within the cluster

Execute the command by specifying the cluster-name and the reception ID of the user-defined reception.

```
csccompostop -user <login user ID> -pass <login password> -cluster <cluster name> -name
<reception ID of user-defined reception>
```

To stop specific user-defined receptions deployed on the HCSC server

Execute the command by specifying the HCSC server name and the reception ID of user-defined reception.

```
csccompostop -user <login user ID> -pass <login password> -csc <HCSC server name> -name
<reception ID of user-defined reception >
```

5.3.30 Terminating the Service Adapter

This subsection describes the prerequisites for terminating the service adapter and how to terminate it.

(1) Prerequisites

To terminate the service adapter, the following conditions must be met:

- The HCSC server is running.
  For details about how to check HCSC server status, see *5.3.15 Checking the HCSC server information*.
- The service adapter is in active status.
  For details about how to check service adapter status, see *5.3.17 Checking the service adapter information*.

(2) Termination method

This subsection describes how to terminate the service adapter.

(a) Using windows

To terminate the service adapter using windows in the operating environment:

1. In the tree view, double-click the service adapter to be terminated.
   Information about the double-clicked service adapter is displayed on the Operations page in the editor area.
   For details about the Operations page for service adapters, see *4.4 Operations page* in the manual *Cosminexus Service Platform Reference*.
2. Check the information displayed in the Operations page, and then click the Stop button.
   A dialog box confirming termination of the service adapter is displayed.
3. Check the information displayed in the dialog box and then click the OK button.
   Service adapter termination processing begins. Log information during termination processing is displayed in the console view.
   If the **Cancel** button is clicked, the system returns to the Operations page without executing termination processing.
   When service adapter termination processing is completed, a dialog box indicating the execution result is displayed.
4. Check the dialog box indicating the execution result.
   If termination processing was successful:
   Click the **OK** button to return to the Operations page.
   On the Operations page, the service adapter status is set to inactive. Also, the **Stop** button is disabled and the **Start** button is enabled.
   If termination processing failed:
   The dialog box displays the nature of the error. Check the message ID provided in the detailed information, and then take appropriate action.

(b) Using commands

To terminate a service adapter, execute the `csccompostop` command or `cscutil` command in the operating environment.

Use the `csccompostop` and `cscutil` commands in the following cases:

- `csccompostop` command
  To terminate a service adapter in the operating environment where the corresponding repository exists.
- `cscutil` command
  To terminate a service adapter in an environment (for example, execution environment operating directly in JP1) where the `cscutil` command can be used and where the corresponding repository does not exist.

The following describes how to execute the above commands:

Using the `csccompostop` command

Execute the `csccompostop` command in the operating environment.

For details about the `csccompostop` command, see *csccompostop (Stopping the HCSC components)* in the manual *Cosminexus Service Platform Reference*.

The execution format of the `csccompostop` command is described below:

To terminate the service adapters deployed on all the HCSC servers in the cluster, in a batch (for each cluster)

Specify the cluster-name and the `-all` option and execute the command.

The service adapters deployed on all the HCSC servers in the cluster specified with the `-cluster` option terminate in a batch (all the business processes and user-defined receptions that are not terminated already are also terminated at the same time).

```
csccompostop -user login-user-ID -pass login-password -cluster Cluster-name -all
```

If you want to terminate only the service adaptor without terminating the business processes and user-defined receptions, specify the service ID of the service adapter.

```
csccompostop -user login-user-ID -pass login-password -cluster cluster-name -
name service-ID-of-the-service-adapter
```

To terminate the service adapters deployed on an HCSC server in a batch (for each HCSC server)

Specify the HCSC server name and the `-all` option and execute the command.

The service adapters deployed on the HCSC server specified with the `-csc` option are terminated (all the business processes and user-defined receptions that are not terminated already are also terminated at the same time).

```
csccompostop -user login-user-ID -pass login-password -csc HCSC-server-name -all
```

If you want to terminate only the service adapter without terminating the business processes and user-defined receptions, specify the service ID of the service adapter.

```
csccompostop -user login-user-ID -pass login-password -csc HCSC-server-name -
name service-ID-of-the-service-adapter
```

Using the `cscutil` command

Execute the `cscutil` command in the operating environment. Specify `compo` in the `-target` option and stop in the `-operation` option.

For details about the `cscutil` command, see *cscutil (Various operations)* in the manual *Cosminexus Service Platform Reference*.

The execution format of the `cscutil` command depends on whether or not a property definition file is used.

When a property definition file is not used

In the `-props` option, specify the service adapter's service ID, HCSC server name, and J2EE server name.

```
cscutil -user login-user-ID -pass login-password -mng manager-name -target
compo -operation stop -props "AdapterName=service-ID-of-the-service-adapter,
CSCSrvName=HCSC-server-name, J2EESrvName=J2EE-server-name"
```

You can use the `cscrepls` command to check the Manager name, service adapter's service ID, HCSC server name, and J2EE server name that are specified in the `cscutil` command. For details about the `cscrepls` command, see *cscrepls (Displaying the repository information)* in the manual *Cosminexus Service Platform Reference*.

When a property definition file is used

Specify the name of the property definition file name in the `-propfile` option. The property definition file must be created beforehand in the J2SE property file format.

```
cscutil -user login-user-ID -pass login-password -mng manager-name -target
compo -operation stop -propfile property-definition-file-name
```

5.3.31 Terminating the Business Process

This subsection describes the prerequisites for terminating the business process and how to terminate it.

(1) Prerequisites

To terminate the business process, the following conditions must be met:

- The HCSC server is in active status.
  For details about how to check HCSC server status, see *5.3.15 Checking the HCSC server information*.
- The business process is in active status.
  For details about how to check business process status, see *5.3.18 Checking the business process information*.

(2) Termination method

This subsection describes how to terminate the business process.

(a) Using windows

To terminate the business process using windows in the operating environment:

1. In the tree view, double-click the business process to be terminated.
   Information about the double-clicked business process is displayed in the editor area.
2. In the editor area, choose the Operations page.
   Information about operations of the business process you chose in step 1 is displayed.
   For details about the Operations page for business processes, see *4.4 Operations page* in the manual *Cosminexus Service Platform Reference*.
3. Check the information displayed in the Operations page, and then click the Stop button.
   A dialog box confirming termination of the business process is displayed.
4. Check the information displayed in the dialog box and then click the OK button.
   Business process termination processing begins. Log information during termination processing is displayed in the console view.
   If the **Cancel** button is clicked, the system returns to the Operations page without executing termination processing.
   When business process termination processing is completed, a dialog box indicating the execution result is displayed.
5. Check the dialog box indicating the execution result.
   If termination processing was successful:
   Click the **OK** button to return to the Operations page.
   On the Operations page, the business process status is set to inactive. Also, the **Stop** button is disabled and the **Start** button is enabled.
   If termination processing failed:
   The dialog box displays the nature of the error. Check the message ID provided in the detailed information, and then take appropriate action.

(b) Using commands

To terminate a business process, execute the `csccompostop` command or `cscutil` command in the operating environment.

Use the `csccompostop` and `cscutil` commands in the following cases:

- `csccompostop` command
  To terminate a business process in an operating environment where the corresponding repository exists.
- `cscutil` command
  To terminate a business process in an environment (for example, execution environment operating directly in JP1) where the `cscutil` command can be used and where the corresponding repository does not exist.

The following describes how to execute the above commands:

Using the `csccompostop` command

Execute the `csccompostop` command in the operating environment.

For details about the `csccompostop` command, see *csccompostop (Stopping the HCSC components)* in the manual *Cosminexus Service Platform Reference*.

The execution format of the `csccompostop` command is described below:

To terminate the business processes deployed on all the HCSC servers in the cluster in a batch (for each cluster)

Specify the cluster-name and the `-all` option and execute the command.

The business processes deployed on all the HCSC servers in the cluster specified with the `-cluster` option terminate in a batch (all the service adapters and user-defined receptions that are not terminated are also terminated at the same time).

```
csccompostop -user login-user-ID -pass login-password -cluster cluster-name -all
```

If you want to terminate only the business process without terminating the service adapters and user-defined receptions, specify the service ID of the business process.

```
csccompostop -user login-user-ID -pass login-password -cluster cluster-name -
name service-ID-of-the-business-process
```

To terminate the business processes deployed on an HCSC server in a batch (for each HCSC server)

Specify the HCSC server name and the `-all` option and execute the command.

The business processes deployed on the HCSC server specified with the `-csc` option are terminated (all the service adapters and user-defined receptions that are not terminated are also terminated at the same time).

```
csccompostop -user login-user-ID -pass login-password -csc HCSC-server-name -all
```

If you want to terminate only the business process without terminating the service adapters and user-defined receptions, specify the service ID of the business process.

```
csccompostop -user login-user-ID -pass login-password -csc HCSC-server-name -
name service-ID-of-the-business-process
```

Using the `cscutil` command

Execute the `cscutil` command in the operating environment. Specify `compo` in the `-target` option and `stop` in the `-operation` option.

For details about the `cscutil` command, see *cscutil (Various operations)* in the manual *Cosminexus Service Platform Reference*.

The execution format of the `cscutil` command depends on whether or not a property definition file is used.

When a property definition file is not used

In the `-props` option, specify the business process's service ID, HCSC server name, and J2EE server name.

```
cscutil -user login-user-ID -pass login-password -mng manager-name -target
compo -operation stop -props "AdapterName=service-ID-of-the-business-process,
CSCSrvName=HCSC-server-name, J2EESrvName=J2EE-server-name"
```

You can use the `cscrepls` command to check the Manager name, business process's service ID, HCSC server name, and J2EE server name that are specified in the `cscutil` command. For details about the `cscrepls` command, see *cscrepls (Displaying the repository information)* in the manual *Cosminexus Service Platform Reference*.

When a property definition file is used

Specify the name of the property definition file name in the `-propfile` option. The property definition file must be created beforehand in the J2SE property file format.

```
cscutil -user login-user-ID -pass login-password -mng manager-name -target
compo -operation stop -propfile property-definition-file-name
```

5.3.32 Terminating the HTTP Server

The methods to stop HTTP Server are normal stop and planned stop.

Normal stop

If a currently executing request processing is stopped, HTTP Server stops without waiting for the request processing to end. As the HTTP server stops without waiting for the request processing to end, the processing of the in-process requests is not guaranteed.

Planned termination

If a currently executing request processing is stopped, HTTP Server stops after the request processing ends. As the HTTP server stops after waiting for the request processing to end, the processing of the in-process requests is guaranteed.

The planned stop has already been setup, by default. To change the setup, perform settings in the cscmng.server.<HCSC server name>.hws.svstop parameter of the HCSC-Manager definition file. Also, in case of planned stop, you can also set the timeout value for the planned stop of HTTP server. Set the timeout value in the cscmng.server.<HCSC server name>.hws.svstop.timeout parameter of the HCSC-Manager definition file.

For details on the HCSC-Manager definition file, see "HCSC-Manager definition file" in "Service Platform Reference Guide".

(1) Stopping method

To stop HTTP Server, execute the cscsvstop command in the operating environment. Execute the command by specifying the logical server name of HTTP Server in the -logical option.

For details on the cscsvstop command, see "cscsvstop (stopping HCSC servers) " in "Service Platform Reference Guide".

Execution format of the cscsvstop command is as follows:

```
cscsvstop -user <login user ID> -pass <login password> -csc <HCSC server name> -logical
<logical server name of HTTP Server>
```

5.3.33 Terminating the HCSC Server

This subsection describes the prerequisites for terminating the HCSC server and how to terminate it.

(1) Prerequisites

To terminate the HCSC server, the user-defined reception and the standard reception must be terminated.

For details about how to check the standard reception status, see *5.3.15 Checking the HCSC server information* and for details about how to check the user-defined reception status, see *5.3.19 Checking the information of user-defined reception*.

If you use commands to terminate the HCSC server, you can execute forced termination. Forced termination enables you to forcibly terminate the HCSC server even while another command is executing or when an internal error has occurred. Furthermore, you can also terminate the HCSC server even if the user-defined reception and standard reception are active.

(2) Termination method

This subsection describes how to terminate the HCSC server.

(a) Using windows

To terminate the HCSC server using windows in the operating environment:

1. In the tree view, double-click the HCSC server to be terminated.
   Information about the chosen HCSC server is displayed in the editor area.
2. In the editor area, choose the Operations tab.
   The Operations page displays information about operations of the HCSC server you chose in step 1.
   For details about the Operations page for an HCSC server, see *4.4 Operations page* in the manual *Cosminexus Service Platform Reference*.
3. Check the information displayed in the Operations page, and then, under HCSC-Server, click the Stop button.
   A dialog box confirming termination of the HCSC server is displayed.
4. Check the information displayed in the dialog box and then click the OK button.
   HCSC server termination processing begins. Log information during termination processing is displayed in the console view.
   If the **Cancel** button is clicked, the system returns to the Operations page without executing termination processing.
   When HCSC server termination processing is completed, a dialog box indicating the execution result is displayed.
5. Check the dialog box indicating the execution result.
   If termination processing was successful:
   Click the OK button to return to the Operations page.

On the Operations page, HCSC server status is set to inactive. Also, the **Stop** button is disabled and the **Start** button is enabled.

If termination processing failed:

The dialog box displays the nature of the error. Check the message ID provided in the detailed information, and then take appropriate action.

(b) Using commands

To terminate the HCSC server, execute the `cscsvstop` command or `cscutil` command in the operating environment. To terminate the HCSC servers in the cluster in a batch or to terminate the logical server, execute the `cscsvstop` command.

Use the `cscsvstop` and `cscutil` commands in the following cases:

- `cscsvstop` command

  To terminate the HCSC server in the operating environment where the corresponding repository exists.

- `cscutil` command

  To terminate the HCSC server in an environment (for example, execution environment directly operating in JP1) where the `cscutil` command can be used and where the corresponding repository does not exist.

The following describes how to execute the above commands:

Using the `cscsvstop` command

Execute the `cscsvstop` command in the operating environment.

For details about the `cscsvstop` command, see *cscsvstop (Stopping the HCSC server)* in the manual *Cosminexus Service Platform Reference*.

The execution format of the `cscsvstop` command is described below:

To terminate the HCSC servers in the cluster in a batch

Specify the cluster name and execute the command.

```
cscsvstop -user login-user-ID -pass login-password -cluster cluster-name
```

If you want to terminate the logical server when you terminate the HCSC servers in the cluster, specify the `-system` option. However, the logical server must be registered in the HCSC-Manager definition files. For details on registering the logical server, see *5.3.1 (1) Preparation before starting operations*.

```
cscsvstop -user login-user-ID -pass login-password -cluster cluster-name -system
```

Furthermore, if you want to terminate only the specified logical server without terminating the HCSC server, specify the `-logical` option.

```
cscsvstop -user login-user-ID -pass login-password -cluster cluster-name -
logical logical-server-name
```

Note that when terminating the HTTP Server within the logical server by specifying the `-system` or `-logical` option, there are two types of termination methods, standard termination and planned termination. For details about how to terminate the HTTP Server, see *5.3.32 Terminating the HTTP Server*.

To terminate each HCSC server individually:

Specify the HCSC server name and execute the command.

```
cscsvstop -user login-user-ID -pass login-password -csc HCSC-server-name
```

If you want to terminate the logical server when you terminate the HCSC server, specify the `-system` option.

```
cscsvstop -user login-user-ID -pass login-password -csc HCSC-server-name -system
```

Furthermore, if you want to terminate only the specified logical server without terminating the HCSC server, specify the `-logical` option.

```
cscsvstop -user login-user-ID -pass login-password -csc HCSC-server-name -
logical logical-server-name
```

Note that when terminating the HTTP Server within the logical server by specifying the `-system` or `-logical` option, there are two types of termination methods, standard termination and planned termination. For details about how to terminate the HTTP Server, see *5.3.32 Terminating the HTTP Server*.

Using the `cscutil` command

Execute the `cscutil` command in the operating environment. Specify `server` in the `-target` option and `stop` in the `-operation` option.

For details about the `cscutil` command, see *cscutil (Various operations)* in the manual *Cosminexus Service Platform Reference*.

The execution format of the `cscutil` command depends on whether or not a property definition file is used.

When a property definition file is not used

In the `-props` option, specify the HCSC server name, J2EE server name, and termination flag.

```
cscutil -user login-user-ID -pass login-password -mng manager-name -target
server -operation stop -props "CSCSrvName= HCSC-server-name, J2EESrvName=J2EE-
server-name, ForceFlag=termination-flag"
```

You can use the `cscrepls` command to check the Manager name, HCSC server name, and J2EE server name that are specified in the `cscutil` command. For details about the `cscrepls` command, see *cscrepls (Displaying the repository information)* in the manual *Cosminexus Service Platform Reference*.

The termination flag specifies whether normal termination or forced termination is to be executed. In this flag, specify one of the following values:

- Normal termination: false
- Forced termination: true

When a property definition file is used

Specify the name of the property definition file name in the `-propfile` option. The property definition file must be created beforehand in the J2SE property file format.

```
cscutil -user login-user-ID -pass login-password -mng manager-name -target
server -operation stop -propfile property-definition-file-name
```

5.3.34 Terminating PRF

To terminate PRF, execute the `cscsvstop` command in the operating environment. Specify the logical server name for PRF with the `-logical` option and execute the command.

For details about the `cscsvstop` command, see *cscsvstop (Stopping the HCSC server)* in the manual *Cosminexus Service Platform Reference*.

The execution format of the `cscsvstop` command is described below:

```
cscsvstop -user login-user-ID -pass login-password -csc HCSC-server-name -logical
logical-server-name-of-PRF
```

5.3.35 Terminating a Database

This subsection explains how to terminate the database.

(1) Termination method

The procedure for terminating the database is explained below:

(a) In the case of HiRDB

To terminate HiRDB, execute the `pdstop` command on the database server.

For details on the `pdstop` command, see the manual *HiRDB Command Reference*.

(b) In the case of Oracle

For details on how to terminate Oracle, see the documentation published by Oracle Corporation.

5.4 HCSC server operations (for FTP linkage)

This subsection describes the flow of operations of the FTP linkage system and the procedure required to perform operations.

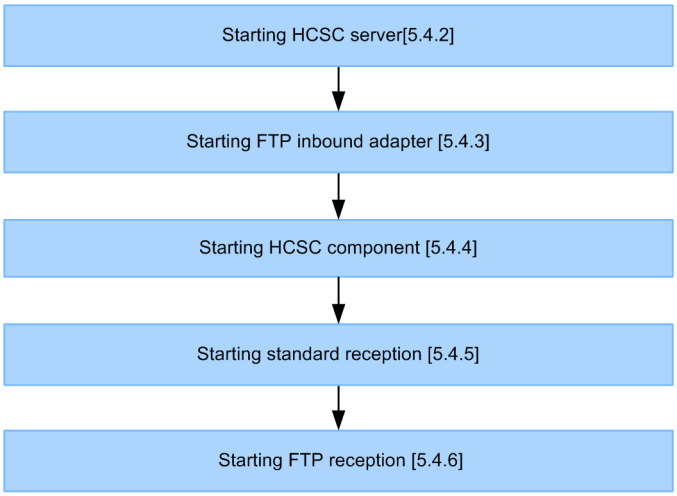
5.4.1 Flow of FTP linkage system operations

This subsection describes operations at the time of starting and stopping the FTP linkage system separately.

(1) When you start FTP linkage system operations

The following figure shows the flow of starting the operations of the FTP linkage system:

Figure 5–3: Flow of starting the operations of the FTP linkage system

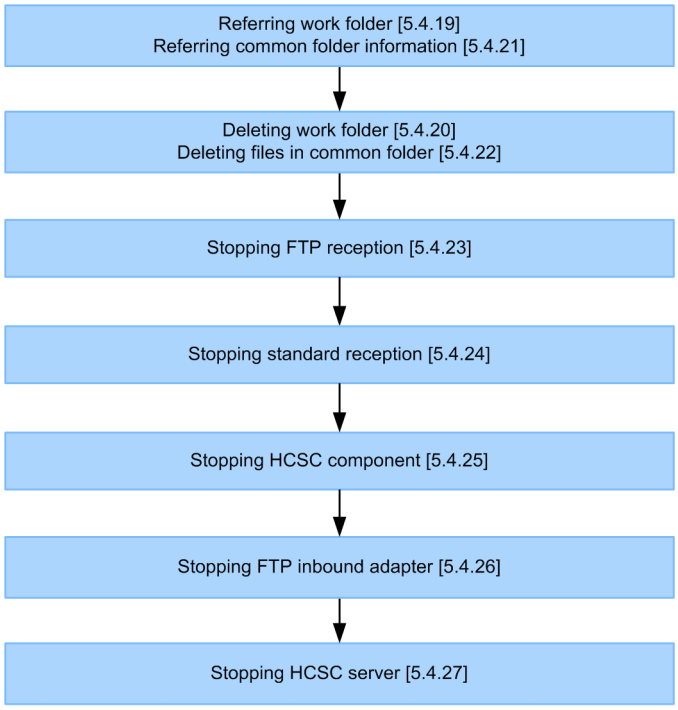


Legend:
[]:Reference section

(2) When you stop FTP linkage system operations

The following figure shows the flow of stopping the operations of the FTP linkage system:

Figure 5–4: Flow of stopping the operations of the FTP linkage system



Legend:
[]: Reference section

5.4.2 Starting the HCSC server

For details on how to start the HCSC server, see "5.3.4 Starting HCSC server".

5.4.3 Starting FTP inbound adapters

This subsection describes prerequisites and method of starting the FTP inbound adapter.

(1) Prerequisites

To start the FTP inbound adapter, the HCSC server must be in a running state.

For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".

(2) Starting method

To start FTP inbound adapter, execute the cjstartrar command in the operating environment.

Execution format for starting FTP inbound adapter is as follows:

```
<Installation directory of Service platform>\CC\admin\bin\cjstartrar <J2EEserver name> -
resname <display name of the resource adapter>
```

For details on the cjstartrarcommand, see "2.4 Resource operation commands used in the J2EE server" in "Application Server Command Reference Guide".

5.4.4 Starting HCSC components

This subsection describes the prerequisites and method for starting HCSC components subsequent to the already deployed HCSC components in the execution environment.

- FTP adapter
- File operations adapter
- Business process

(1) Prerequisites

To start HCSC components, the HCSC server must be in a running state.

For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".

(2) Starting method

To start HCSC components, execute the csccompostart command in the operating environment.

- Starting the FTP adapter
  Execution format for starting the FTP adapter is as follows:

```
csccompostart -user <login user ID> -pass <login password> -cluster <cluster name> -name
<service ID of the FTP adapter>
```

- Starting the File operations adapter
  Execution format for starting the File operations adapter is as follows:

```
csccompostart -user <login user ID> -pass <login password> -cluster <cluster name> -name
<service ID of the file operations adapter>
```

- Starting the business process
- Execution format for starting the business process is as follows:

```
csccompostart -user <login user ID> -pass <login password> -cluster <cluster name> -name
<service ID of the business process>
```

For details, see "csccompostart (starting HCSC components) " in " Service Platform Reference Guide".

5.4.5 Starting the standard reception

For details on how to start the standard reception, see "*5.3.9 Starting standard receptions*".

5.4.6 Starting the FTP reception

This subsection describes the prerequisites and the method for starting the FTP reception.

(1) Prerequisites

To start FTP reception, the following conditions must be fulfilled:

- HCSC server is running
- Business processes defined by FTPreception is running

For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".

(2) Starting method

To start FTP reception, execute the csccompostart command in the operating environment.

Execution format the time of starting FTP reception is as follows:

```
csccompostart -user <login user ID> -pass <login password> -cluster <cluster name> -name
<reception ID of the FTP reception>
```

For details, see "csccompostart (starting HCSC components) " in "Service Platform Reference Guide

5.4.7 Checking the information of the HCSC server

For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".

5.4.8 Checking the information of FTP inbound adapter

This subsection describes the prerequisites and method for checking the information of FTP inbound adapter.

(1) Prerequisites

To check the information of the FTP inbound adapter, the HCSC server must be running.

For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information* ".

(2) Starting method

To check the information of the FTP inbound adapter, execute the cjlistrar command.

The execution format for checking FTP inbound adapter is as follows:

```
<Installation directory of Service platform>\CC\admin\bin\cjlistrar <J2EEserver name>
```

For details on the cjstartrar command, see "2.4 Resource operation commands used in the J2EE server" in "Application Server Command Reference Guide".

An example of execution results is as follows:

```
KDJE37400-I Connecting to <J2EEserver name>...
running  FTP_Inbound_Resource_Adapter
KDJE37508-I All rars have been listed successfully. (number = [1])
```

"Running" indicates that the FTP inbound adapter is running. "Stopped" is output when the FTP inbound adapter is stopped.

5.4.9 Checking the information of HCSC components

This subsection describes method for checking the information of the following HCSC components that are already deployed in the execution environment.

- FTP adapter
- File operations adapter
- Business process
- FTP reception

To check the information of HCSC components, execute the cscstatus (status display) command or the cscutil (various operations) command.

You can execute the cscstatus command and the cscutil command in the operating environment.

Command-wise methods for checking the information of the HCSC components are as follows:

(1) Using the cscstatuscommand to check the information

To check the information of HCSC components with the cscstatus command, execute the cscstatus command by specifying the -system option and the -type option and then specifying "compo" in the -type option.

Execution format for checking the information of HCSC component is as follows:

```
cscstatus -user <login user ID> -pass <login password> -csc <HCSC server name> -type compo
```

For details, see "cscstatus (status display) " in "Service Platform Reference Guide".

(2) Using the cscutil command to check the information

To check the information of HCSC components with the cscutil command, execute the cscutil command by specifying compo in the -target option and get_bp_info in the -operation option and then specifying "compo" in the -type option.

The execution format of the cscutil command depends on whether you use the property definition file.

(a) When you do not use the property definition file

Specify the HCSC server name and the service ID of the business process in the -props option.

```
cscutil -user <login user ID> -pass <login password> -mng <Manager name> -target compo -
operation get_bp_info -props "CSCSrvName=<HCSC sever name>, AdapterName=<Service ID of the
business process>"
```

For details, see "cscutil (various operations) " in "Service Platform Reference Guide".

Reference note

You can use the cscrepls command to check the Manager name, HCSC server name, and the service ID of the business process that are specified in the cscutil command. For details, see "cscrepls (displaying the repository information)" in "Service Platform Reference Guide".

(b) When you use the property definition file

Specify the property definition file name in the -propfile option The property definition file must be created beforehand in the J2SE property file format.

```
cscutil -user <login user ID> -pass <login password> -mng <Manager name> -target compo -
operation get_bp_info -propfile <property definition file name>
```

For details, see "cscutil (various operations) " in "Service Platform Reference Guide".

Important note

- If you acquire information of the undeployed business process, the character string "null" is displayed.
- If you execute the cscutil command without the specifying the service ID of the business process, information on all business processes managed by the HCSC server is output.

5.4.10 Changing the definition information of the HCSC server

To change the definition information of the HCSC server, use the same method when you set the definition information of the HCSC server.For details on how to set the definition information of the HCSC server, see "*3.1.4 Setting up the HCSC server definition information*".

5.4.11 Changing the definition information of the FTP inbound adapter

This subsection describes the prerequisites and method for changing the property definition of the FTP inbound adapter during operations.

(1) Prerequisites

To change the property definition of the FTP inbound adapter, the following conditions must be fulfilled:

- HCSC server is running
- FTP reception and FTP inbound adapter are in a stopped state

For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".

(2) Changing method

To change the definition information of the FTP inbound adapter, acquire the attribute from the RAR file of the FTP inbound adapter, create a property file, and edit that property file to reflect the definitions.

The procedure for changing the definition information of the FTP inbound adapter is as follows:

1. Acquiring attributes from the RAR file of the FTPinbound adapter, and create the property file.
   Execution format for creating the property file from the RAR file of the FTP inbound adapter:

```
<Installation directory of Service platform>\CC\admin\bin\cjgetrarprop <J2EE server name> -
resname FTP_Inbound_Resource_Adapter -c <file path of the property file>
```

   For details on the cjgetrarprop command, see "2.4 Resource operation commands used in the J2EE server" in "Service Platform Reference Guide".

2. Editing the property file.
   For definition items of the property file, see "*3.2.3(3)(b) Contents of the property file*".

3. Executing the following command to reflect the property definition of the FTP inbound adapter:

```
<Installation directory of Service platform >\CC\admin\bin\cjsetrarprop <J2EE server name> -
resname <display name of the resource adapter> -c <property file path>
```

   For details on the cjsetrarprop command, see "2.4 Resource operation commands used in the J2EE server" in "Service Platform Reference Guide".

5.4.12 Changing and confirming the user information of the FTP inbound adapter

This subsection describes how to check and change the user information of the FTP inbound adapter during operations.

(1) Checking the user information of the FTP inbound adapter

The prerequisites and method for checking the user information of the FTP inbound adapter are as follows:

(a) Prerequisites

To check the user information of the FTP inbound adapter, the following conditions must be fulfilled:

- HCSC server is running
- FTP reception and FTP inbound adapter are in stopped state

For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".

(b) Checking method

Execution format for checking the user information of the FTP inbound adapter is as follows:

```
csmftplsusr
```

For details, see "csmftplsusr (displays the user of the FTP inbound adapter) " in "Service Platform Reference Guide".

(2) Changing the user information of the FTP inbound adapter

The prerequisites for checking the user information of the FTP inbound adapter and method for checking are as follows:

(a) Prerequisites

To check the user information of the FTP inbound adapter, the following conditions must be fulfilled:

- HCSC server is running
- FTP reception and FTP adapter are in stopped state

For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".

(b) Changing method

Execution format for changing the user information of the FTP inbound adapter is as follows:

- Adding the user

```
csmftpaddusr -usr <username> -pass <userpassword>
```

- Deleting the user

```
csmftpdelusr -usr <username>
```

For details, see "csmftpaddusr (registering and updating users of the FTP inbound adapter) " and "csmftpdelusr (deleting users of the FTP inbound adapter) " in "Service Platform Reference Guide".

! Important note

- When you add or delete multiple users, execute command for the number of times equal to the number of users.
- When you change the user password of the FTP inbound adapter, once delete the user for whom the password is to be changed and then add the user for whom the password has been changed.

5.4.13 Changing the definition information of the FTP adapter

This subsection describes how to change the definition information of the following FTP adapters during operations:

- FTP-adapter runtime-environment property file
- FTP execution permission list file

(1) Prerequisites

To check the definition information of the FTP adapter, the following conditions must be fulfilled:

- HCSC server is running
- FTP reception and FTP adapter are in a stopped state

For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".

(2) Changing method

(a) Changing the FTP-adapter runtime-environment property file

Edit the file directly to change the FTP-adapter runtime- environment property file.

The storage destination of the FTP-adapter runtime- environment property file is as follows:

```
<Service Platform installation directory>\CSC\custom-adapter\FTP\config
\<Service ID>.properties
```

(b) Changing the FTP execution permission list file

Edit the file directly to change the FTP execution permission list file.

5.4.14 Checking and changing the user information of the FTP adapter

This subsection describes how to check and change the user information of the FTP adapter during operations.

(1) Checking the user information of the FTP adapter

The prerequisites for confirming the user information of the FTP adapter, and method for starting are as follows:

(a) Prerequisites

To check the user information of the FTP adapter, the following conditions must be fulfilled:

- HCSC server is running
- FTP reception and FTP adapter are in stopped state

For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".

(b) Checking method

To check the user information of the FTP adapter, execute the csaftpuserls command in the operating environment.

Execution format for checking the user information of the FTP adapter is as follows:

```
csaftpuserls -f <FTP adapter account definition file path>
```

For details, see "csaftpuserls (displaying users of the FTP adapter) " in "Service Platform Reference Guide".

(2) Changing the user information of the FTP adapter

The prerequisites for confirming the user information of the FTP adapter, and method for starting are as follows:

(a) Prerequisites

To check the user information of the FTP adapter, the following conditions must be fulfilled:

- HCSC server is running
- FTP reception and FTP adapter are in stopped state

For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".

(b) Changing method

To change the user information of the FTP adapter, execute the csaftpuserls command in the operating environment.Furthermore, ifaccounting information is set even in the request message of the FTP adapter, the accounting information changed with the csaftpuserls command is ignored, and the request message settings of the FTP adapter are enabled.

Execution format for adding, deleting users of the FTP adapter, and changing the user password is as follows:

- **Adding the user**

```
csaftpuseradd -user <user name> -pass <user password> -f <FTP adapter account definition
file path>
```

When you add multiple users, execute command for the number of times equal to the number of users.

Execution format for registering the user set in the accounting information is as follows:

```
csaftpuseradd -user <user name> -pass <user password> -account <accounting information> -f
<FTP adapter account definition file path>
```

- **Deleting the user**

```
csaftpuserdel -user <user name> -f <FTP adapter account definition file path>
```

When you delete multiple users, execute command for the number of times equal to the number of users.

- **Changing the user password**

```
csaftpuseradd -user <user name> -pass <user password> -r -f <FTP adapter account definition
file path>
```

The execution format for adding the accounting information to the user and deleting the accounting information set in the user is as follows:

- **Adding the accounting information to the user**

```
csaftpuseradd -user <user name> -pass <user password> -account <accounting information> -r -
f <FTP adapter account definition file path>
```

- **Deleting the accounting information set for the user**

```
csaftpuseradd -user <user name> -pass <user password> -r -f <FTP adapter account definition
file path>
```

For details, see "csaftpuseradd (registering and updating users of the FTP adapter) " or "csaftpuserdel (deleting users of the FTP adapter)" in "Service Platform Reference Guide".

5.4.15 Changing the definition information of the file operations adapter

This subsection describes the prerequisites for changing the definition information of the following file operations adapters, during operations and starting method.

- When you change the file operations adapter definition file
- When you change the FTP-adapter runtime-environment property file

(1) Prerequisites

To change the definition information of the file operations adapter, the following conditions must be fulfilled:

- HCSC server is running
- FTP reception and file operations adapter is in the stopped status

For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".

(2) Changing method

The method to change the definition information of the file operation adapter is as follows:

(a) Changing the definition file of the file operations adapter

Use the following procedure for changing the file operations adapter definition file:

1. Undeploy the file operations adapter for which the definition is to be changed
   Execution format for undeploying the file operations adapter is as follows:

```
csccompoundeploy -cluster <cluster name> -user <login user ID> -pass <login password> -name
<service ID>
```

   For details, see "csccompoundeploy (deleting deployed HCSC components) " in "Service Platform Reference Guide".
2. Change the file operations adapter definition file.
   Execution format for changing the file operations adapter definition file is as follows:

```
csccmctl -cluster <cluster name> -user <login user ID> -pass <login password> -cluster
<cluster name> -name <service ID> -operation get -targetfilename
cscFileOperation.properties -basedir <file path of the directory in which
cscFileOperation.properties are stored>
```

For details, see "csccmctl (managing definition files) " in "Service Platform Reference Guide".

3. Deploy the file operation adapter for which definition is changed.

   Execution format for deploying the file operations adapter definition file is as follows:

```
csccompodeploy -cluster <cluster name> -user <login user ID> -pass <login password> -name
<service ID>
```

For details, see "csccompodeploy (deploying HCSC components) " in "Service Platform Reference Guide".

(b) Changing the file operations adapter runtime environment property file

Edit the file directly to change the file operations adapter runtime environment property file.

The storage destination of the file operations adapter runtime environment property file is as follows:

```
<Service Platform installation directory>\CSC\config\adpfop
\<ServiceID>.properties
```

5.4.16 Changing the definition information of FTP reception

This subsection describes the prerequisites for change the definition information of the following FTP receptions, during operation and the starting method.

- FTP reception definition file
- FTP reception configuration file
- FTP execution permission list file, FTP command permission list definition file (for FTP reception), and list command option definition file.

(1) Prerequisites

To change the definition information of FTP reception, the following conditions must be fulfilled:

- HCSC server is running
- FTP reception is stopped

For details on how to check the status of the HCSC server, "*5.3.15 Checking the HCSC server information*".

(2) Changing method

The method to change the definition information of FTP is as follows:

(a) Changing the FTP reception definition file

Use the following procedure for changing FTP reception definition file:

1. Undeploy FTP reception for which the definition file is to be changed.

   Execution format for undeploying FTP reception is as follows:

```
csccompoundeploy -user <login user ID> -pass <login password> -cluster <cluster name> -name
<service ID>
```

For details, see "csccompoundeploy (deleting deployed HCSC components) " in "Service Platform Reference Guide".

2. Change the FTP reception definition file

   Execution format for changing the FTP reception definition file is as follows:

```
csccmctl -user <login user ID> -pass <login password> -cluster <cluster name> -name
<service ID> -operation set -targetfilename cscurecpftp.properties -basedir <file path of
the directory in which cscurecpftp.properties are stored>
```

For details, see "csccmctl (managing definition files) " in "Service Platform Reference Guide".

3. Deploy FTP reception for which the definition file is changed.

   The execution format for deploying FTP reception is as follows:

```
csccompodeploy -user <login user ID> -pass <login password> -cluster <cluster name> -name
<service ID>
```

For details, see "csccompodeploy (deleting deployed HCSC components) " in "Service Platform Reference Guide".

(b) Changing the FTP reception configuration file

Edit the file directly to change the FTP reception configuration file.

The storage destination of the FTP reception configuration file is as follows:

```
<Service Platform installation directory>\CSC\config\ftprecp
\<ServiceID>.properties
```

(c) Changing the FTP execution permission list file, FTP command permission list definition file (for FTP reception), or list command option definition file

Edit the file directly to change the FTP execution permission list file, FTP command permission list definition file (for FTP reception), and list command option definition file.

The FTP execution permission list file, FTP command permission list definition file (for FTP reception), and list command option definition file are stored in the path specified in the FTP reception configuration file.

5.4.17 Modifying repositories

Use the following procedure for modifying repositories, when you have changed the definitions of HCSC components in the execution environment, after importing repositories in the operating environment:

1. Export the repository.

   Export the repository in which the edited definition is saved.

   Export the repository in the development environment.

   For details on exporting repositories, see "*4.2 Exporting Repository Information*".

2. Stop the FTP inbound adapter.

   For details on how to stop the FTP inbound adapter, see "*5.4.26 Stopping FTP inbound adapters*".

3. Execute the csccompostop command to stop HCSC components.

   For details, see "csccompostop (stopping HCSC components) " in "Service Platform Reference Guide".

4. Execute the csccompoundeploy command to delete the deployed HCSC components.

   For details, see "csccompoundeploy (deleting deployed HCSC components) " in "Service Platform Reference Guide".

5. Enter the following command to delete the definition file of the file operations adapter and FTP reception from the operating environment.

   Execution format of the command is as follows:

   - To delete the definition file of the file operations adapter

```
csccmctl -user <login user ID> -pass <login password> -cluster <cluster name> -name
<service ID of the file operations adapter> -operation reset  -targetfilename
cscFileOperation.properties
```

   - To delete the definition file of FTP reception

```
csccmctl -user <login user ID> -pass <login password> -cluster <cluster name> -name
<reception ID of the FTP reception> -operation reset  -targetfilename cscurecpftp.properties
```

For details, see "csccmctl (managing definition files) " in "Service Platform Reference Guide".

6. Import the repository.
   Import the repository exported in the development environment to the operating environment.
   For details on importing repositories, see "*4.3 Importing a repository*".

5.4.18 Acquiring the transfer history

To acquire the transfer history, execute the csmftplshistory command in the operating environment.

The csmftplshistory command can be executed only by users having administrative privileges.

Execution format for acquiring the transfer history is as follows:

```
csmftplshistory <J2EE server name>
```

For details, see "csmftplshistory (displaying transfer history) " in "Service Platform Reference Guide".

Note that, the transfer history is output in the file as a transfer history log. For the storage destination and log file names of the transfer history log file, see "*7.7.11(1)(d) Transfer history log (FTP inbound adapter)*".

5.4.19 Referencing the work folder

To reference the list of folders in the work folder, execute the cscfswls command in the operating environment.

The execution formats for acquiring the status before and after deleting the work folder are as follows:

- For acquiring the status before deleting the work folder

```
cscfswls -user <login user ID> -pass <login password> -all -csc <HCSC server name> <file
path of the list result before deleting the work folder >
```

- For acquiring the status after deleting the work folder

```
cscfswls -user <login user ID> -pass <login password> -all -csc <HCSC server name> <file
path of the list result after deleting the work folder>
```

For details, see "cscfswls (referencing the work folder) " in "Service Platform Reference Guide".

5.4.20 Deleting the work folder

This subsection describes the prerequisites and method for deleting the work folder.

(1) Prerequisites

To delete the work folder, the reception managing the work folder, and business processes invoked from that reception, must be in the stopped status.

(2) Deletion method

To delete the work folder, execute the cscfswrm command in the operating environment.

Execution format for deleting the work folder is as follows:

```
cscfswrm -user <login user ID> -pass <login password> -d 0 -all -csc <HCSC server name>
```

For details, see "cscfswrm (deleting the work folder) " in "Service Platform Reference Guide".

5.4.21 Referencing the information of the common folder

To reference the list of files in the common folder, execute the cscfscls command in the operating environment.

The execution formats for acquiring the status before and after deleting the common folder are as follows:

(1) For acquiring the status before deleting the common folder

```
cscfscls -user <login user ID> -pass <login password> -cluster <cluster name> -folder
<common folder definition name > -csc <HCSC server name> < file path of the list result
before deleting files within the common folder>
```

(2) For acquiring the status after deleting the common folder

```
cscfscls -user <login user ID> -pass <login password> -cluster <cluster name> -folder
<common folder definition name> -csc <HCSC server name> <file path of the list result after
deleting files within the common folder>
```

For details, see "cscfscls (referencing the common folder) " in "Service Platform Reference Guide".

5.4.22 Deleting files in the common folder

To delete files in the common folder, execute the cscfscrm command in the operating environment.

Execution format for deleting the files in the common folder is as follows:

```
cscfscrm -user <login user ID> -pass <login password> -cluster <cluster name> -folder
<common folder definition name> -d 0 -csc <HCSC server name>
```

For details, see "cscfscrm (deleting the common folder" in "Service Platform Reference Guide".

5.4.23 Stopping the FTP reception

To stop the FTP reception, execute the csccompostop command in the operating environment. Execution format for stopping FTP reception is as follows:

```
csccompostop -user <login user ID> -pass <login password> -cluster <cluster name> -name
<reception ID of the FTP reception>
```

For details on the csccompostop command, see "csccompostop (stopping HCSC components) " in "Service Platform Reference Guide".

5.4.24 Stopping the standard reception

For details on how to stop the standard reception, see "*5.3.28 Terminating the Standard Reception*".

5.4.25 Stopping HCSC components

This subsection describes the prerequisites for stopping the following HCSC components that are already deployed in the execution environment and the starting method.

- FTP adapter
- File operation adapter
- Business process

(1) Prerequisites

To stop components, the HCSC server must be running.

For checking the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".

(2) Stopping method

To stop HCSC components, execute the csccompostop commands in the operating environment.

Execution format for stopping HCSC components is as follows:

```
csccompostop -user <login user ID> -pass <login password> -cluster <cluster name> -all
```

For details, see "csccompostop (stopping HCSC components)" in "Service Platform Reference Guide".

5.4.26 Stopping FTP inbound adapters

This subsection describes the prerequisites and method for stopping FTP inbound adapters.

(1) Prerequisites

To stop FTP inbound adapters, the following conditions must be fulfilled:

- HCSC server is running
  For details on how to check the status of the HCSC server, see "*5.3.15 Checking the HCSC server information*".
- FTP inbound adapter must be started
  For checking the status of FTP inbound adapters, see "4.6 Referencing the list of resource adapters" in "Application Server Application Setup Guide".

(2) Stopping method

The execution format for stopping FTP inbound adapters is as follows:

```
<Service Platform installation directory>\CC\admin\bin\cjstoprar <J2EE server name> -
resname <display name of the resource adapter>
```

For details on the cjstoprar command, see "2.4 Resource operation commands used in the J2EE server" in "Application Server Command Reference Guide".

5.4.27 Stopping HCSC servers

For details on how to stop HCSC servers, see "*5.3.33 Terminating the HCSC Server*".

5.5 Additional operationsin the case of mail interaction

Describes how to operate a Mail adapter.

5.5.1 Managing the user information

This subsection describes how to manage the user information (user name and password) that is required for authentication when you connect to the mail server from the mail adapter.

User information management can be classified as follows:

- Adding and updating the user information
- Deleting users
- Displaying users

(1) Adding and updating the user information

You can register the user information in the mail adapter account definition file by executing the csmmailaddusr command in the operating environment. Also, you can change the passwords of already registered users with the csmmailaddusr command.

Execution example of the command for adding and updating the user information is as follows:

- **Adding the user information**

```
csmmailaddusr -user <login user name> -pass <login password of the user> -f <mail adapter
account definition file path>
```

When you add multiple users, execute command for the number of times equal to the number of users.

- **Changing the user password**

```
csmmailaddusr -user <login user name> -pass <login password of the user after changing> -r -
f <mail adapter account definition file path>
```

For details on the csmmailaddusr command, see "csmmailaddusr (registering and updating the mail adapter user information) " in "Application Server Command Reference Guide".

(2) Deleting the user information

You can delete the user information of the mail adapter from the mail adapter account definition file by executing the csmmaildelusr command in the operating environment.

The execution example of the command for deleting the user information is as follows:

```
csmmaildelusr -user <login user name> -f <mail adapter account definition file path>
```

When you delete multiple users, execute the command for the number of times equal to the number of users.

For details on the csmmaildelusr command, see "csmmaildelusr (deleting the mail adapter user information) " in "Application Server Command Reference Guide".

(3) Displaying the user information

You can reference the user information of the mail adapter registered in the mail adapter account definition file by executing the csmmaillsusr command in the operating environment.

The execution example of the command for displaying the user information is as follows:

```
csmmaillsusr -f <mail adapter account definition file path>
```

For details on the csmmaillsusrcommand, see "csmmaillsusr (displaying the mail adapter user information) " in "Application Server Command Reference Guide".

5.5.2 Startingand stoppingthe mail adapter

The following are the two methods for starting and stopping the mail adapter:

- Starting and stopping by using screens of the operating environment of the Service Platform
- Starting and stopping by using commands of the Service Platform

For details on how to start, see "*5.3.6 Starting Service Adapters*". For details on how to stop, see "*5.3.30 Terminating the Service Adapter*".

5.5.3 Performance tuning ofthe mail adapter

You can change various settings in the mail adapter runtime environment property file when it is necessary to perform settings for performance tuning during mail adapter operations.

For the mail adapter runtime environment property file, see "Mail adapter runtime environment property file" in "Service Platform Reference Guide". The following table lists the items that you can set for Performance tuning:

Table 5–6: Settings for Performance tuning

Item	Key name	Range of setting values	Unit
Mail body size	mailadp.mail.body.size	1~2,048,000	Byte
Size of attachments	mailadp.attach.file.size	0~5,242,880	Byte
Number of attachments	mailadp.max.attach.count.per.mail	0~100	Nos.

The procedure for changing the settings of the mail adapter runtime environment property file during mail adapter operations is as follows:

1. Stop the standard reception.
   For details, see "*5.3.28 Terminating the Standard Reception*".
2. Stop user-defined receptions (receptions other than standard receptions such as SOAP reception and FTP reception).
   For details, see "*5.3.29 Stopping the user -defined reception*".
3. Stop the mail adapter.
   For details on how to stop the mail adapter, see "*5.5.2 Starting and stopping the mail adapter*".
4. To change the setting value, open the mail adapter runtime environment property file with the text editor.
   The storage location of the mail adapter runtime environment property file is "<Service Platform installation directory>\CSC\config\mail".
5. Start the mail adapter.
   For details on how to start the mail adapter, see "*5.5.2 Starting and stopping the mail adapter*".
6. Start user-defined receptions (receptions other than standard receptions such as SOAP reception and FTP reception).
   For details, see"*5.3.8 Starting user-defined receptions*".
7. Start the standard reception.
   For details, see "*5.3.9 Starting standard receptions*".

5.6 Operations with a Cluster Configuration

This section describes operations with a cluster configuration, specifically a load-balancing cluster configuration and a high availability cluster configuration.

5.6.1 Operations in the load-balancing cluster configuration

This subsection describes how to start and end operations using a load-balancing cluster configuration. It also describes how to add, change, and delete HCSC server that configures the load-balancing cluster during operations.

(1) Starting operations

You can start system operations of the load-balancing cluster configuration after you finish configuring and setting up the environment. Procedure to start operations is as follows:

1. Check the status of the execution environment components.

   To start system operations of the load-balancing cluster configuration, the following components of the execution environment listed must be already started and active in all load-balancing clusters:

   - Administration Agent
   - Management Server
   - PRF
   - Smart Agent
   - CTM (applicable if a CTM is used)[#1]
   - J2EE server[#2]
   - HCSC server[#3]
   - HTTP Server (applicable if HTTP Server is used)

   #1

   The CTM domain manager and CTM daemon must also be active.

   #2

   The status of applications such as Reliable Messaging must match. The system name of Reliable Messaging must be unique in each HCSC server in the load-balancing cluster.

   #3

   The deployed service adapter, business process, and standard reception must have the same status.

2. Service requester transmission control

   Set the service requester to a status in which it can accept service component execution requests by connecting the network for the service requester that cannot accept service component execution requests because its network was disconnected during setup.

(2) Ending operations

To end the operations of the system having load-balancing cluster configuration:

1. Service requester transmission control

   Ddisconnect the service requester network so that HCSC servers can no longer accept service module execution requests. In this case, confirm that no execution request is currently being processed.

2. Stop execution environment components.

   Stop the components of the execution environment in all load-balancing clusters in the following order:

   - HTTP Server (applicable if HTTP Server is used)
   - HCSC server
   - J2EE server

- CTM (applicable when a CTM is used)
- Smart Agent
- PRF
- Management Server
- Administration Agent

(3) Adding and deleting HCSC servers in the load-balancing cluster

You can add or delete HCSC servers that configure the load-balancing cluster without stopping operations. For a load balancer, you can add or delete the HCSC server without stopping the operations only when the function for dynamically adding and deleting IP addresses is available. The method to add and delete HCSC servers that configure the load-balancing cluster is as follows:

(a) Adding the HCSC server

1. Set up the execution environment for the HCSC server to be added.

   For details on how to set up the execution environment, see "*2.5.2(2) Execution environment setup*".

   If you set up the HCSC server configuration definition file and the HCSC server setup definition file, confirm that the following values are the same in all HCSC servers in the load-balancing cluster:

   HCSC server configuration definition file

   - Cluster display name
   - Cluster type
   - Call type

   HCSC server setup definition file

   - All properties other than the rm-systemname and naming-service-hostname properties

     For the rm-systemname property, specify a Reliable Messaging system name that is unique in each HCSC server within the load-balancing cluster. For the naming-service-hostname property, specify the host name of the Naming Service that is set in the J2EE server on which each HCSC server has been set up.

2. Start the HCSC-Server.

   For details on how to start the HCSC server, see "*5.3.4 Starting HCSC server*".

3. Deploy the service adapter.

   For details on how to deploy service adapters, see "*3.1.8 Deploying a service adapter*".

4. Deploy the business process.

   For details on how to deploy business processes, see "*3.1.13 Deploying a business process*".

5. Start the service adapter.

   For details on how to start service adapters, see "*5.3.6 Starting Service Adapters*".

6. Start the business process.

   For details on how to start business processes, see "*5.3.7 Starting Business Processes*".

7. Start the standard reception.

   For details on how to start the standard reception, see "*5.3.9 Starting standard receptions*".

8. Set up the load balancer.

   Set up the load balancer so that service component execution requests are dynamically sent to the HCSC server you have added.

   If you are using CTM, all HCSC servers must have the same CTM domain manager name and Smart Agent port number.

   For details on how to set up a load balancer, see the documentation for the load balancer in use.

   ! Important note

   If you are using CTM, service component execution requests are assigned to HCSC servers when the standard reception for the added HCSC server starts.

(b) Deleting HCSC servers

1. Set up the load balancer.

   Set up the load balancer so that that no service component execution request is sent to the HCSC server to be deleted. At this time, confirm that all execution requests that are currently being processed are completed. If you are using CTM, lock the queue for sending service component execution requests to the target J2EE server.For details on locking of the queue when you are using CTM, see "3.7.4 Lock control of the schedule queue" in "Application Server Expansion Guide".

   For details on how to set up a load balancer, see the documentation for the load balancer you are using.

2. Stop the standard reception.

   For details on how to stop the standard reception, see"*5.3.28 Terminating the Standard Reception*".

3. Stop the business process.

   For details on how to stop business processes, see "*5.3.31 Terminating the Business Process*".

4. Stop the service adapter.

   For details on how to stop service adapters, see "*5.3.30 Terminating the Service Adapter*".

5. Delete the business process.

   For details on how to delete business processes, see "*3.3.2 Deleting a business process*".

6. Delete the service adapter.

   For details on how to delete service adapters, see "*3.3.1 Deleting a service adapter*".

7. Stop the HCSC server to be deleted.

   For details on how to stop the HCSC server, "*5.3.33 Terminating the HCSC Server*".

8. Delete the HCSC server.

   For details on how to delete HCSC servers, see "*3.3.5 Unsetting up an HCSC server*".

(4) Adding and deleting service adapters to and from the load-balancing cluster

You can add or delete new service adapters without stopping service adapters that are already deployed in HCSC servers. The procedure for adding and deleting service adapters is as follows:

(a) Adding service adapters

1. Deploy the service adapter to be added to all HCSC servers that configure the load-balancing cluster.

   For details on how to deploy service adapters, see "*3.1.8 Deploying a service adapter*".

2. Start the added service adapter.

   For details on how to start service adapters, see "*5.3.6 Starting Service Adapters*".

3. Perform settings to invoke the added service adapter.

   ! Important note

   Set such that the added service adapter is invoked after deploying and starting the service adapter to all the HCSC servers that configure the load-balancing cluster.

(b) Deleting service adapters

1. Perform settings such that the service adapter to be deleted is not invoked.

2. Stop the service adapter to be deleted.

   For details on how to delete service adapters, see "*5.3.30 Terminating the Service Adapter*".

3. Delete the service adapter from all HCSC servers that configure the load-balancing cluster.

   For details on how to delete service adapters, see"*3.3.1 Deleting a service adapter*".

   ! Important note

   Set so that the service adapter to be deleted is not invoked, and then delete the service adapter.

(5) Adding and deleting business processes to and from the load-balancing cluster

You can add or delete a new business process without stopping business processes that are already deployed to HCSC servers. The procedure for adding and deleting the business process is as follows:

(a) Adding the business process

1. Deploy the business process to be added to all HCSC servers that configure the load-balancing cluster.
   For details on how to deploy business processes, see "*3.1.13 Deploying a business process*".
2. Start the added business process.
   For details on how to start business processes, see "*5.3.7 Starting Business Processes*".
3. Perform settings to invoke the added business process.

! Important note

Set so that the added business process is invoked after deploy and starting the business processes in all HCSC servers that configure the load-balancing cluster.

(b) Deleting business process

1. Perform settings such that the business process to be deleted is not invoked.
2. Stop the business process to be deleted.
   For details on how to delete business processes, see "*5.3.31 Terminating the Business Process*".
3. Delete the business process from all HCSC servers that configure the load-balancing cluster.
   For details on how to delete business processes, see "*3.3.2 Deleting a business process*".

! Important note

Set such that the business process to be deleted is not invoked, and then delete the business process.

(6) Changing service adapters in the load-balancing cluster configuration

You can change service adapters without stopping service adapters that are already deployed to HCSC servers. The procedure for changing the service adapter is as follows:

1. Perform settings such that the service adapter to be changed is not invoked.
2. Stop the service adapter to be changed.
   For details on how to stop service adapters, see "*5.3.30 Terminating the Service Adapter*".
3. Delete the service adapter to be changed from all HCSC servers that configure the load-balancing cluster.
   For details on how to delete service adapters, see "*3.3.1 Deleting a service adapter*".
4. Import the repository in which the changed information of the service adapter is saved.
   For details on how to import, see "*4.3 Importing a repository*".
5. Deploy the changed service adapter to all HCSC servers that configure the load-balancing cluster.
   For details on how to deploy service adapters, see "*3.1.8 Deploying a service adapter*".
6. Start the changed service adapter.
   For details on how to start service adapters, see "*5.3.6 Starting Service Adapters*".
7. Perform settings to invoke the changed service adapter.

! Important note

Set such that the service adapter to be changed is not invoked, and then change the service adapter.

(7) Changing business processes in the load-balancing cluster configuration

You can change business processes without stopping business processes that are already deployed in HCSC servers. The method to change the business process is as follows:

1. Perform settings such that the business process to be changed is not invoked.

2. Stop the business process to be changed.
   For details on how to stop business processes, see "*5.3.31 Terminating the Business Process*".
3. Delete the business process to be changed from all HCSC servers that configure the load-balancing cluster.
   For details on how to delete business processes, see "*3.3.2 Deleting a business process*".
4. Import the repository in which the changed information of the business process is saved.
   For details on how to import repositories, see "*4.3 Importing a repository*".
5. Deploy the business process to all HCSC servers that configure the load-balancing cluster.
   For details on how to deploy business processes, see "*3.1.13 Deploying a business process*".
6. Start the changed business process.
   For details on how to start business processes, see "*5.3.7 Starting Business Processes*".
7. Perform settings to invoke the changed business process.

! Important note

Set the business process such that it is not invoked, and then change the business process.

(8) Preventing HCSC server failure

To prevent failure of HCSC servers that configure the load-balancing cluster, it is recommended that that you prepare for sufficient number of HCSC servers for the load-balancing cluster.For details, see "*7.9.2(1) Failure and recovery in load-balancing cluster configuration*".

5.6.2 Operations Using a High Availability Cluster Configuration

This subsection describes how to start operations using a high availability cluster configuration, perform system switchover in the event of a failure at the executing node during operations, and recover the system.

(1) Starting operations

After you finish configuring and setting up the environment, you can start system operations using a high availability cluster configuration. To start operations:

1. Check the status of the components of the executing and standby nodes.
   To start operating the system with a high availability cluster configuration, the components of the executing and standby nodes must be in the status shown in the table below.

Table 5–7: Component status during operations with a high availability cluster configuration

Component	Status	
	Executing node	Standby node
Administration Agent	Y	-
Management Server	Y	-
PRF	Y	-
J2EE server	Y	-
HCSC server	Y	-
HTTP Server	Y	-

Legend:
Y: Running
- : Stop

2. Connect the service requester network.
   Connect the service requester network that was disconnected during setup.

When the service requester network is connected, service module execution requests can be accepted by the HCSC server at the executing node.

3. Service requester transmission control

Place the service requester in a status in which it can accept service module execution requests, such as by connecting the network for the service requester whose function for accepting service module execution requests was disabled during the setup.

5.6.3 Operations in N-to-1cluster configuration

This subsection describes the start and end of operations in the N-to-1 cluster configuration. Furthermore, it describes the method to add, change, and delete HCSC servers that configure N-to-1 cluster during operations.

(1) Starting operations

You can start the operations of the N-to-1 cluster configuration system after the creation and setup of the environment ends. To start operations:

1. Check the status of components of the executing node and the standby node

The components of the executing node and standby node that are equivalent to the High availability cluster cpmfogiratopmmust be in the status listed in the following table in all load-balancing clusters of N-to-1 cluster configuration.

Table 5–8: Status of components equivalent to the High availability cluster configuration

Components	Status	
	Executing node	Standby node
Administration Agent	Y	-
Management Server	Y	-
PRF	Y	-
Smart Agent	Y	-
CTM (applicable if CTM is used)#1	Y#1	-
J2EE server	Y#2	-
HCSC server	Y#3	-
HTTP Server	Y	-

Legend:

Y: Started.

--: Stopped

#1

The CTM domain manager and CTM daemon must also be active.

#2

The status of applications such as Reliable Messaging must match. The system name for Reliable Messaging must be unique in each HCSC server in the load-balancing cluster.

#3

The deployed service adapter and business process, and standard reception must have the same status.

2. Service requester transmission control

Set the service requester to a status in which it can accept service component execution requests by connecting the network for the service requester that cannot accept service component execution requests because its network was disconnected during setup.

(2) Ending operations

The method to end operations of the system of the N-to-1 cluster configuration is the same as the load-balancing cluster configuration. For details on how to end the operations of the load-balancing cluster configuration, see "*5.6.1(2) Ending operations*".

(3) Adding and deleting HCSC servers to the N-to-1 cluster

You can add or delete HCSC servers that configure the N-to-1 cluster without stopping operations. In the case of a load balancer, you can add or delete the HCSC server without stopping operations only when the function for dynamically adding and deleting IP addresses is available.

The method to add and delete HCSC servers that configure the N-to-1 cluster is as follows:

(a) Adding HCSC servers

1. Set up the execution environment for the HCSC server to be added to the N-to-1 environment.

   For details on how to setup the execution environment equivalent to the load-balancing cluster, see "*2.5.2(2) Execution environment setup*".

   For details on how to setup the execution environment equivalent to the High availability cluster, see "*2.6.2(2) Execution environment (standby node) setup*" and "*2.6.2(3) Execution environment (executing node) setup*".

2. Start up the HCSC server

   For details on how to start up HCSC servers, see "*5.3.4 Starting HCSC server*".

3. Deploy the service adapter.

   For details on how to deploy service adapters, see "*3.1.8 Deploying a service adapter*".

4. Deploy the business process.

   For details on how to deploy business processes, see "*3.1.13 Deploying a business process*".

5. Start the service adapter.

   For details on how to start service adapters, see "*5.3.6 Starting Service Adapters*".

6. Start the business process.

   For details on how to start business processes, see "*5.3.7 Starting Business Processes*".

7. Start the standard reception.

   For details on how to start the standard reception, see "*5.3.9 Starting standard receptions*".

8. Set up the load balancer.

   Set up the load balancer such that service component execution requests are dynamically sent to the HCSC server you have added.

   If you are using CTM, all HCSC servers must have the same CTM domain manager name and Smart Agent port number.

   For details on how to set up a load balancer, see the documentation for the load balancer you are using.

   ! Important note

   If you are using CTM, service component execution requests are assigned to HCSC servers when the standard reception for the added HCSC server starts.

(b) Deleting HCSC servers

1. Set up the load balancer.

   Set up the load balancer such that that no service component execution request is sent to the HCSC server to be deleted. At this time, confirm that all execution requests that are currently being processed are completed. If you are using CTM, the queue for sending service component execution requests to the target J2EE server is locked. For locking of the queue when you use CTM, see "3.7.4 Lock control of the schedule queue" in "Application Server Expansion Guide".

   For details on how to set up a load balancer, see the documentation for the load balancer you are using.

2. Stop the standard reception.

   For details on how to stop the standard reception, see "*5.3.28 Terminating the Standard Reception*".

3. Stop the business process.
   For details on how to stop business processes, see "*5.3.31 Terminating the Business Process*".
4. Stop the service adapter.
   For details on how to stop service adapters, see "*5.3.30 Terminating the Service Adapter*".
5. Delete the business process.
   For details on how to delete business processes, see "*3.3.2 Deleting a business process*".
6. Delete the service adapter.
   For details on how to delete service adapters, see "*3.3.1 Deleting a service adapter*".
7. Stop the HCSC server to be deleted.
   For details on how to stop the HCSC server, "*5.3.33 Terminating the HCSC Server*".
8. Delete the HCSC server.
   For details on how to delete HCSC servers, see "*3.3.5 Unsetting up an HCSC server*".

(4) Adding, deleting,and changing service adapters and business processes to the HCSC server

This subsection describes how to add, delete, and change service adapters and business processes to HCSC servers that configure the N-to-1 cluster.

You add, delete, or change service adapters and business processes to HCSC servers that configure the N-to-1 cluster for each set of the High availability cluster configuration in a sequence.

(a) Adding and deleting service adapters

For details on how to add and delete new service adapters without stopping service adapters already deployed to the HCSC server, see "*5.6.1(4) Adding and deleting service adapters to and from the load-balancing cluster*".

(b) Adding and deleting business processes

For details on how to add and delete new business processes without stopping business processes already deployed to the HCSC server, see "*5.6.1(5) Adding and deleting business processes to and from the load-balancing cluster*".

(c) Changing service adapters

For details on how to change service adapters without stopping service adapters already deployed to the HCSC server, see "*5.6.1(6) Changing service adapters in the load-balancing cluster configuration*".

(d) Changing business processes

For details on how to change business processes without stopping business processes already deployed to the HCSC server, see "*5.6.1(7) Changing business processes in the load-balancing cluster configuration*".

(5) Preventing HCSC server failure

To prevent failure of HCSC servers that configure the load-balancing cluster, it is recommended that that you prepare for sufficient number of HCSC servers for the load-balancing cluster. For details, see "*7.9.2(1) Failure and recovery in load-balancing cluster configuration*".

5.6.4 Notes at the time of cluster configuration

Note the following points when you start up or stop service adapters and business processes, start the standard reception during operations in the High availability cluster configuration and N-to-1 cluster configuration.

- **When you start up and stop service adapters and business process**
  Use the following procedure for starting up and stopping service adapters and business processes:
  1. Disconnect the service requester network to prevent service component execution requests from being accepted in the executing and standby nodes.
  2. You start or stop the same service adapter and business process at both the executing and standby nodes.

When node switching occurs in the high availability cluster configuration, the status of service adapters and business processes is not inherited. Therefore, if a service adapter is terminated in the running executing node and node switching occurs in this status, consistency is lost in the status of service adapters and business processes in the executing and standby nodes.

- **When you stop the standard reception**

  To stop the standard reception, you first prevent execution requests from being accepted regardless of the standard reception status, by disconnecting the service requester network. After that, you stop the standard reception. If node switching occurs in the high availability cluster configuration, the standard reception is started in the standby node. To temporarily prevent execution requests from being accepted at the running executing node, the standard reception is terminated at the executing node. If node switching occurs in this status, execution requests may be accepted at the standby node.

If the system switches over to the High availability cluster configuration while the operating screen of the Screen Platform is still running during the operations in the High availability cluster configuration or the N-to-1 cluster configuration, various statuses displayed in the window correctly cannot be reflected.

When you re-execute the business process from another HCSC server during operations in the load-balancing cluster configuration and the N-to-1 cluster configuration, if you want to re-execute the business process after the node switching processing to the standby node in the High availability cluster configuration, store each type of information in the following location:

Type of information	Storage location of information
Work folder	Common disk device
Common folder	
Input output permission file used in the file adapter	
Text file and attachment of the mail body used in the mail adapter	Local disk device #
Definition file used in HCSC server operations	
Definition file used in HCSC components	

#

Set the same value in each HCSC server in the case of load-balancing cluster configuration and N-to-1 class configuration, and in the executing node and the standby node in the case of High availability cluster configuration.

5.7 Operations when you change the IP addressorthe host name after building the environment

This subsection describes the operating procedure when you change the IP address or the host name of the database, the operating environment, and components after building the environment.

5.7.1 When you change the IP address and the host nameof the database operating machine

To change the IP address or the host name of the database operating machine, depending on the type of the database, you perform the following activities mentioned in (1) or (2):

(1) When you change the IP address or the host name of the machine on which the database used by the HCSC server is running, when HCSC server is setup

Confirm the definition items of the following definition files when you change the IP address or host name of the machine on which the database used by the HCSC server is running. For details on how to define the properties of the HCSC server setup definition file, see "HCSC server setup definition file" in "Service Platform Reference Guide".

Table 5–9: Definition items to be confirmed at the time of changing IP address or host name

Definition file name	Definition items
HCSC server setup definition file	• For Oracle jdbc-url • Other than Oracle jdbc-dbhostname
DB Connector definition file	• For HiRDB DBHostName • Other than HiRDB serverName

The methods to change the IP address and the host name differ depending on the contents defined in the definition items.

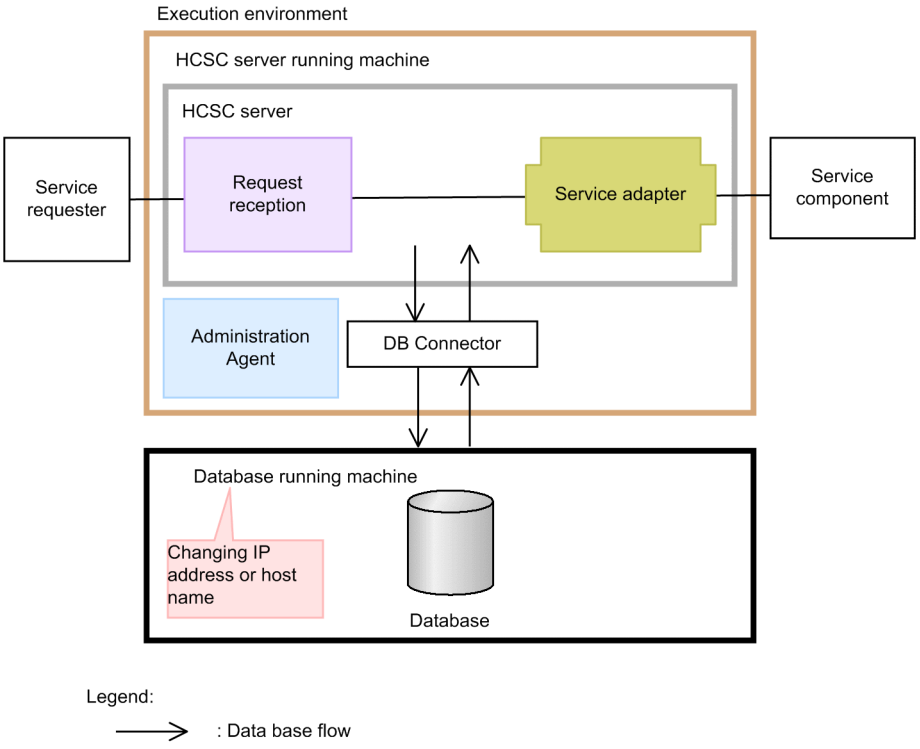
Table 5–10: Methods to change the IP address or the host name

Definition content of definition items	Methods for changing	
	Changing IP address	Changing host name
localhost	Even if you want to change either the IP address or the host name of the machine, you need not change the settings of the definition file.	
Host name	If you change the IP address of the machine without changing the host name, you need not change the settings of the definition file. You can change simply by restarting Administration Agent, Management Server, and the HCSC server.	You cannot change the host name of the machine. To change the host name, you must re-set up the HCSC server.
IP address	You cannot change the IP address of the machine. To change the IP address, you must re-set up the HCSC server.	--

Legend:
--: Not applicable.

The following figure shows an example of changing the IP address or the host name:

Figure 5–5: Changing the IP address or the host name of the machine on which a database used by HCSC server is running (when the HCSC server is setup)



(2) When you change the IP address or the host name of the database to which the database adapter is connected

Confirm the definition items of the following definition files when you change the IP address or host name of the database to which the database adapter is connected:

Table 5–11: Definition items to be confirmed at the time of changing IP address or host name

Definition file name	Definition name
DB Connector definition file	• For HiRDB DBHostName • Other than HiRDB serverName

The methods to change the IP address and the host name differ depending on the contents defined in the definition items.

Table 5–12: Methods to change the IP address or the host name

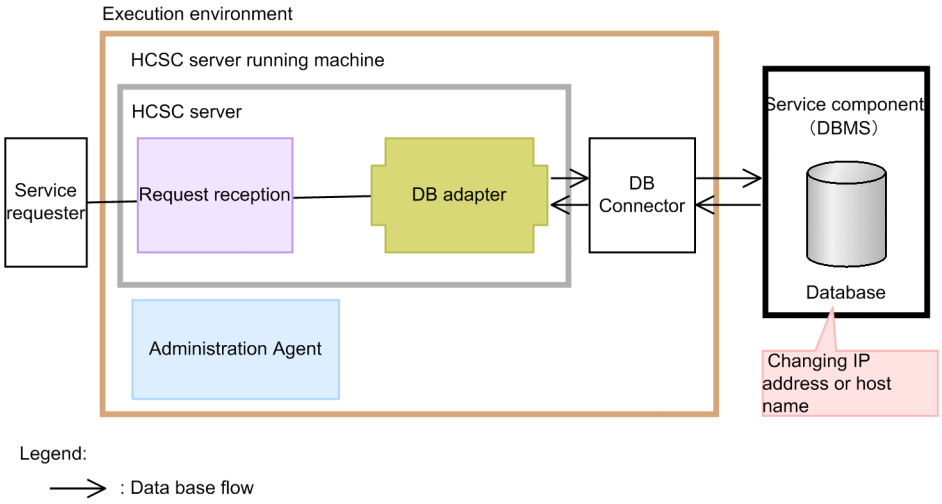
Definition content of definition items	Methods for changing	
	Changing IP address	Changing host name
Localhost	Even if you want to change either the IP address or the host name of the machine, you need not change the settings of the definition file.	
Host name	You can change either the IP address or the host name of the machine with the following procedure: 1. Change the definition content (IP address or host name) of the definition file 2. Reflect the definition file with the cjsetrarprop command to the DB Connector 3. Restart the HCSC server	

Definition content of definition items	Methods for changing	
	Changing IP address	Changing host name
IP address	You must implement the following procedure to change the IP address of the machine: 1. Change the definition content (IP address) of the definition file 2. Reflect the definition file with the cjsetrarprop command to the DB Connector 3. Restart the HCSC server	--

Legend:
--: Not applicable.

The following figure shows an example of changing the IP address or the host name:

Figure 5–6: FigureChanging the IP address or the host name of the database to which the database adapter is connected



5.7.2 When you change the IP address or the host name of Web server of the standard reception (synchronous reception (Web service)) and the standard reception (asynchronous reception (MDB(WS-R))

Confirm the definition items of the definition file mentioned hereafter when you change the IP address or the host name of Web server of the standard reception (synchronous reception (web service)) and the standard reception (asynchronous reception (MDB(WS-R)) For details on how to define the property definition of the HCSC server configuration definition file, "HCSC server configuration definition file" in "Service Platform Reference Guide".

Table 5–13: Definition items to be confirmed at the time of changing IP address and host name

Definition file name	Definition name
HCSC server configuration definition file	IP address or host name of Web Server

The methods to change the IP address and the host name differ depending on the contents defined in the definition items.

Table 5–14: How to change IP address or host name

Definition contents of definition items	Changing method	
	Changing IP address	Changing host name
localhost	Even if you want to change either the IP address or the host name of the machine, you need not change the settings of the definition file.	
Host name	To change the IP address of the machine, you can change by restarting the entire process after changing the hosts file or DNS.	To change the host name of the machine, change the definition contents of the HCSC server configuration definition file, and execute the cscsvsetup command (HCSC server setup) one more time.#
IP address	To change the IP address of the machine, change the definition contents of the HCSC server configuration definition file, and execute the cscsvsetup command (HCSC server setup) one more time.#	--

Legend:

--:Not applicable.

#

You execute the cscsvsetup command (HCSC server setup) when the HCSC server, service adapters, business processes, and user-defined reception are stopped.

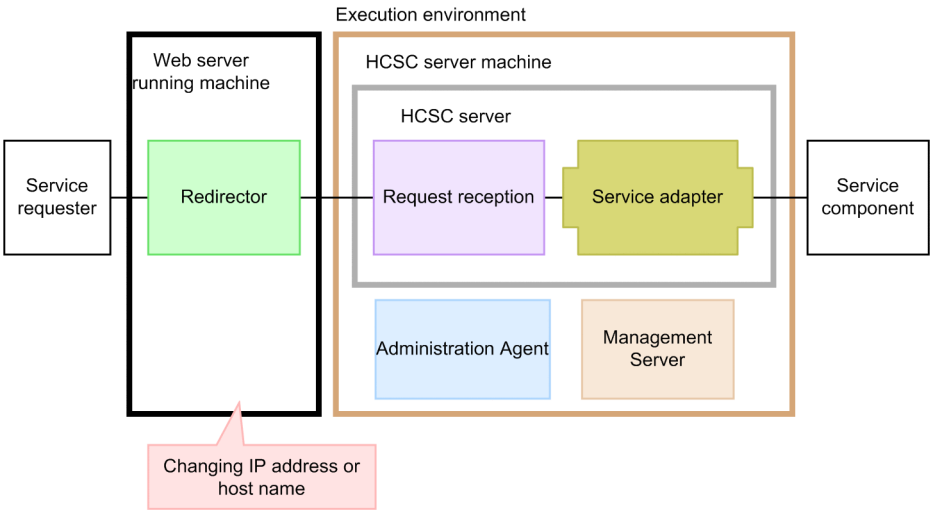
Important note

If you export repositories from the operating environment and import these repositories to the development environment after changing IP addresses or host names, the display contents in the screens in the development environment are changed as follows:

- Service Adapter Settings screen
  IP addresses or host names displayed in the address of the service component control information.
- HCSC component information display screen
  Host name or IP address and, the host name or IP address of the end point URL of WSDL that is output when the [Acquire WSDL] button is clicked.

The following figure shows an example of changing the IP address or the host name of Web server of the standard reception (synchronous reception (web service)) and the standard reception (asynchronous reception (MDB(WS-R)):

Figure 5–7: Changing the IP address or the host name of Web server of the standard reception (synchronous reception (web service)) and the standard reception (asynchronous reception (MDB(WS-R))



5.8 Operations to suppress FullGC at the time of executing the operation command

You can suppress FullGC executing internally by specifying the -nogc option in the following commands of the operating environment:

- csccompoundeploy command
- csccompostart command
- csccompostop command
- cscrcptnstart command
- cscrcptnstop command

The following subsections describe the methods to suppress FullGC while stopping online and while being online.

5.8.1 When you replace HCSC components by stopping online

It is recommended that you suppress FullGC occurrence when you execute various stop commands and the start command of the business process and the service adapter.

When you replace HCSC components by stopping online, you can suppress the frequency of FullGC occurrence by specifying the -nogc option in each operating command as shown in the following procedure example:

1. Stop reception
   ```
   cscrcptnstop -csc <HCSC server name> -nogc
   ```
2. Stopping business processes and service adapters
   ```
   csccompostop -csc <HCSC server name> -name <serviceID> -nogc
   ```
3. Deleting business processes and service adapters
   ```
   csccompoundeploy -csc <HCSC server name> -name <serviceID> -nogc
   ```
4. Importing repositories
   ```
   cscrepctl -import <repositoryZIP>
   ```
5. Deploying business processes and service adapters
   ```
   csccompodeploy -csc <HCSC server name> -all
   ```
6. Starting business processes and service adapters
   ```
   csccompostart -csc <HCSC server name> -all -nogc
   ```
7. Start reception
   ```
   cscrcptnstart -csc <HCSC server name> -nogc
   ```
   If you do not specify the -nogc option with this command, FullGC occurs once at each of the point in time mentioned below.FullGC does not occur at any other time.
   - At the time of starting the standard reception immediately after the HCSC server set up
   - At the time of starting the user-defined reception immediately after executing the csccompodeploy command
8. Explicit issue of FullGC (optional)
   ```
   javagc -p <process ID of J2EE server>
   ```
   The FullGC issue before the online start shown in this operation is not mandatory, but if you want to explicitly issue FullGC, use the javagc command
   For details on the javagc command, see "10. Commands Used in JavaVM" in "Application Server Command Reference Guide".

Because FullGC occurrence is suppressed in steps 1.~3., steps 6.~7., FullGC occurs only once in step 8. within the entire procedure in this example.

5.8.2 When you replace HCSC components online

Because the business stops during FullGC occurrence, it is recommended that you suppress FullGC occurrence.

When you replace HCSC components online, you can suppress the frequency of FullGC occurrence by specifying the -nogc option in each operating command as shown in the following procedure example:

1. Stopping business processes and service adapters

   ```
   csccompostop -csc <HCSC server name> -name <serviceID> -nogc
   ```

2. Deleting business processes and service adapters

   ```
   csccompoundeploy -csc <HCSC server name> -name <serviceID> -nogc
   ```

3. Importing repositories

   ```
   cscrepctl -import <repositoryZIP> -compo
   ```

4. Deploying business processes and service adapters

   ```
   csccompodeploy -csc <HCSC server name> -name <serviceID>
   ```

5. Starting business processes and service adapters

   ```
   csccompostart -csc <HCSC server name> -name <serviceID> -nogc
   ```

Because FullGC occurrence is suppressed in steps 1~2, step 5, FullGC does not occur even once in the entire procedure in this example.

6 Management of Execution Log

This chapter describes the method for managing the execution log of process instances at the time of system operation.

6.1 Management of execution log of process instances

You can monitor the execution status of process instances of a business process as a log in database. This is called as **persistence**. You can manage the execution log of process instances only when you are using database.

If you persist, specify the target process instance from the execution log of process instances, and you can check the status, delete the execution log, re-execute and use it in following cases:

- **Query handling when an error occurs**
  On requests from service requester, you can check the status of the specified process instance, delete the execution log of process instance or re-execute the process instance when required.
- **Test support of business process**
  At the time of business process development, you can improve the business process by confirming the status of process instance that is executed as a test. Also, you can delete the execution log of process instance or re-execute the process instance when required.

In order to confirm which activity is appropriate for which part of business process, you need to get Transition Diagram (screen at the time of business process development) of the business process activity prepared from the developer of business process in advance.

6.1.1 Using the Process Instance Execution Log

The following describes how to use the execution log:

(1) Using the execution log to handle an inquiry about an error that has occurred

To handle an inquiry about an error that has occurred, use the execution log for process instances as follows:

1. Use the business process execution log's error messages to identify the cause of the error and correct it.
2. Check the status of the process instances.

   When there is a correlation set that can be identified

   Search the process instances, using as the search condition the correlation set in the request message that was sent by the service requester. You can uniquely identify the target by using a correlation set as the search condition.

   When the correlation set is unknown

   Search the process instances based on the process instance start date and time acquired from the request message, or based on the status of the target process instance (such as Executing).
3. From the search result, acquire detailed information about the process instance's correlation set, variable, or activity in order to identify the target process instance.

   If you used a correlation set for the search, you can also identify the process instance based on the displayed start date and time.
4. Perform one of the following operations according to the status of the process instance:

   When the status is "Executing" or `Error occurred`

   Re-execute the process instance or delete the process instance execution log. Then, issue a request to the service requester to re-transmit the request message.

   When there is no information about the process instance (no hit in the search result)

   Issue a request to the service requester to re-transmit the request message.

(2) Using the execution log to facilitate testing of a business process

After a test run of a process instance finishes during development of a process instance, you can also check the status to improve the process instance. The following procedure shows how you can use the execution log of process instances to facilitate testing of a business process:

1. Search the process instance execution logs for a business process that has been made persistent, using a correlation set, date/time, or status as the search condition in order to narrow the target.
2. From the search result, acquire detailed information about the process instance's correlation set, variable, or activity in order to identify the target process instance.
3. Perform one of the following operations according to the status of the process instance:
   - Acquire the status of the process instance that was executed.
   - Re-execute the process instance whose status is Executing or `Error occurred`.
   - Delete any unneeded process instances.

The following subsections describe how to search process instances, view their information and statuses, delete execution log information, and re-execute process instances.

(3) Displaying the Tracking page from the GUI

You can use either windows or commands to manage the process instance execution log.

If you use windows to manage the process instance execution log, you can display information on the Tracking page. To display the **Tracking** page, do the following:

1. In the tree view, select the business process whose process instance execution log you wish to check.
2. In the editor area, choose the Tracking tab.
   The Tracking page is displayed in the editor area.

6.1.2 Searching the execution log of a process instance

You can use screen, command or SQL to search the execution log of a process instance. For SQL, search with the RD area name.

Regarding the execution log of a process instance, the following table describes Search Criteria that can be specified with screen and command:

Search Criteria	Search with screen (execution management page)	Search with command (cscpiselect command)	Reference location
Start date of process instance	Y	Y	"*(2) Search with start time as a criteria*" "*(6) Search by combining start date and state*"
State of process instance (search by specifying "Executing", "Completed", "Occurrence of an error", or "End fault")	Y	Y	"*(3) Search with status as a criteria*" "*(6) Search with a combination of start time and status as a criteria*"
State of activity instance	N	Y	--
Correlation set information (search by specifying the correlation set that uniquely specifies process instance)	Y	Y	"*(4) Search with correlation set as a criteria*"
Identifier of process instance	Y	Y	"*(5) Search with the process instance identifier as a criteria*"

Search Criteria	Search with screen (execution management page)	Search with command (cscpiselect command)	Reference location
Process overview information (search performed by using correlation set, search performed without using correlation set)	N	Y	--
Activity information	N	Y	--
Link information	N	Y	--
Variable information (string variable information, numeric variable information, boolean variable information, message variable information)	N	Y	--
Message associated information	N	Y	--
Information of all the execution logs in the execution log information table	N	Y	--
Number of lines for search result	N	Y	--
Business process Definition Name	N	Y	"*(1) Search with business process Definition Name as a criteria*"
Name of the executed HCSC server	N	Y	"*(7) Search with name of executed HCSC server as a criteria*"

Legend:

Y: Search can be performed.

N: Search cannot be performed.

For details on log management page, see "4.6 Log management page" in "Service Platform Reference Guide".

Also, you can output the search result of command to CSV file. For details, see "cscpiselect (search of process instance) " in "Service Platform Reference Guide".

Hereafter, search of the execution log of process instance is explained with search examples.

(1) Search with business process Definition Name as a criteria

(a) Using screen to search execution log

On the screen, as there is no item with which you can search the execution log of process instance with business process definition name, all the execution logs are displayed, from this search the appropriate business process definition name. The procedure is as follows:

1. Click the [Search by Date/ State] tab.
2. Select the [Without specification] radio button of the start date of process instance.
3. Check all the check boxes for the state of process instance (Executing, Completed, Occurrence of an error, or End fault).
4. Select the sort method of search result in Search Criteria.
5. Click the [Search] button.

   From all the execution logs displayed on the search result field, search the appropriate business process Definition Name in [Business process Definition Name].

(b) Using command to search execution log

The procedure to search the execution log of process instance by business process Definition Name is as follows:

1. Determine the HCSC server to be accessed.
2. Execute the following command to perform the search.
   - When directly specifying the where clause

```
cscpiselect -user <Login user ID> -pass <Login password> -csc <HCSC server name> -where <where clause># -table process -orderby <Sort condition>
```

Note#

Specify the SQL condition for the column name ProcessDefinitionName.

- When using a file in which the where clause is specified

```
cscpiselect -user <Login user ID> -pass <Login password> -csc <HCSC server name> -wherefile < file name in which the where clause is specified># -table process -orderby <Sort condition> -encoding <Encoding name>
```

Note #

Specify the SQL condition for the column name ProcessDefinitionName.

- When directly specifying the business process Definition Name

```
cscpiselect -user <Login user ID> -pass <Login password> -csc <HCSC server name> -processname <Business process Definition Name> -table process -orderby <Sort condition>
```

Example: Enter the command with the following conditions to search the process instance execution log:

- Business process Definition Name: Hello business process
- HCSC server to be accessed: HCSC
- Sort condition: Ascending order of start time

Command

- **When the -wherefile option is specified**

```
cscpiselect -user <Login user ID> -pass <Login password> -csc HCSC -wherefile sql_where.txt
-table process -orderby "StartTime ASC"
```

For sql_where.txt

```
ProcessDefinitionName = 'Hello business process'
```

- **When the -processname option is specified**

```
cscpiselect -user <Login user ID> -pass <Login password> -csc HCSC -processname Hello
business process -table process -orderby "StartTime ASC"
```

Output result

```
KEOS52019-I cscpiselect will now start.
KEOS52049-I Communication with the HCSC-Server, to search for process instances, will now start.
KEOS52050-I Communication with the HCSC-Server, to search for process instances, is complete.
ProcessID,ProcessDefinitionName,ProcessDefinitionVersion,State,StartTime,EndTime,CSCServerName
J2EEServer_192168116131_HelloBusinessProcess_1325067837024_5828360283_138,HelloBusinessProcess,1,Completed,2011/12/28 10:23:57,2011/12/28 10:23:59,HCSC
J2EEServer_192168116131_HelloBusinessProcess_1325068542983_9702993874_139,HelloBusinessProcess,1,Completed,2011/12/28 10:35:42,2011/12/28 10:35:43,HCSC
J2EEServer_192168116131_HelloBusinessProcess_1325068544587_4728548730_137,HelloBusinessProcess,1,Completed,2011/12/28 10:35:44,2011/12/28 10:35:44,HCSC
J2EEServer_192168116131_HelloBusinessProcess_1325069450165_5398959934_136,HelloBusinessProcess,1,Error,2011/12/28 10:50:50,,HCSC
J2EEServer_192168116131_HelloBusinessProcess_1325069470181_2734343598_138,HelloBusinessProcess,1,Error,2011/12/28 10:51:10,,HCSC
J2EEServer_192168116131_HelloBusinessProcess_1325125374434_3398636230_136,HelloBusinessProcess,1,Completed,2011/12/29 02:22:54,2011/12/29 02:22:54,HCSC
J2EEServer_192168116131_HelloBusinessProcess_1325125384512_4896451771_139,HelloBusinessProcess,1,Completed,2011/12/29 02:23:04,2011/12/29 02:23:04,HCSC
KEOS52020-I cscpiselect ended normally.
```

For details on the cscpiselect command, see "cscpiselect (searching process instance)" of "Service Platform Reference Guide".

(2) Search with start time as a criteria

(a) Using screen to search execution log

The procedure to search the execution log of process instance by using start date is as follows:

1. Click the [Search by Date/ State] tab.
2. Select the [With specification] radio button of the start date of process instance.

3. For the start time search range, enter the year and select the month, date, hour, minute, and second from the drop-down lists.
4. For the search result sort condition, select the appropriate radio button.
5. Click the [Search] button.
   The search result is displayed in the search result field.

(b) Using command to search execution log

The process to search execution log of process instance using start date is as follows:

! Important note

The start date and time to be specified for search differs as per the hour system used in the option specified in the command.

- When specified in the file in which the -where option or the where clause of the -wherefile option is specified: Greenwich mean time (GMT)
- When specified in the -date option: Default time zone

---

1. Determine the HCSC server to be accessed.
2. Execute the following command to perform the search.
   - When directly specifying the where clause

```
cscpiselect -user <Login user ID> -pass <Login password> -csc <HCSC server name> -where <where clause># -table process -orderby <Sort-condition>
```

Note #
Specify the SQL condition for the column name StartTime.

- When using a file in which the where clause is specified

```
cscpiselect -user <Login user ID> -pass <Login password> -csc <HCSC server name> -wherefile < file-name in which the where clause is specified># -table process -orderby <Sort-condition> -encoding <Encoding name>
```

Note #
Specify the SQL condition for the column name StartTime.

- When directly specifying a start time range:

```
cscpiselect -user <Login user ID> -pass <Login password> -csc <HCSC server name> -date <inquiry-start-date-and-time >#,<inquiry-end-date-and-time> -table process -orderby <Sort-condition>
```

Note #
Inquiry start date/time can be omitted.

(Example) Enter the command using the following conditions to search the process instance execution logs:

- Business process definition name: Hello business-process
- Start date and time range: Before 2011/12/28 14:59:59 (Greenwich mean time)
- HCSC server to be accessed: HCSC
- Sort condition: Ascending order by start time

Command

- **When the -wherefile option is specified:**

```
cscpiselect -user <Login user ID> -pass <Login password> -csc HCSC -wherefile sql_where.txt -table process -orderby "StartTime ASC"
```

For contents of sql_where.txt

```
ProcessDefinitionName = 'Hello business process' AND StartTime <= '2011-12-28 14:59:59'
```

- **When the -date option is specified:**

```
cscpiselect -user <Login user ID> -pass <Login password> -csc HCSC -processname Hello
business process-date ,20111228235959# -table process -orderby "StartTime ASC"
```

Note #

By default, Japan time is used for time zone in -date option.

Output result

```
KEOS52019-I cscpiselect will now start.
KEOS52049-I Communication with the HCSC-Server, to search for process instances, will now start.
KEOS52050-I Communication with the HCSC-Server, to search for process instances, is complete.
ProcessID,ProcessDefinitionName,ProcessDefinitionVersion,State,StartTime,EndTime,CSCServerName
J2EEServer_192168116131_HelloBusinessProcess_1325067837024_5828360283_138,HelloBusinessProcess,1,Completed,2011/12/28 10:23:57,2011/12/28 10:23:59,HCSC
J2EEServer_192168116131_HelloBusinessProcess_1325068542993_9702993874_139,HelloBusinessProcess,1,Completed,2011/12/28 10:35:42,2011/12/28 10:35:43,HCSC
J2EEServer_192168116131_HelloBusinessProcess_1325068544587_4728548730_137,HelloBusinessProcess,1,Completed,2011/12/28 10:35:44,2011/12/28 10:35:44,HCSC
J2EEServer_192168116131_HelloBusinessProcess_1325069450165_5398959934_136,HelloBusinessProcess,1,Error,2011/12/28 10:50:50,,HCSC
J2EEServer_192168116131_HelloBusinessProcess_1325069470181_2734343598_138,HelloBusinessProcess,1,Error,2011/12/28 10:51:10,,HCSC
KEOS52020-I cscpiselect ended normally.
```

Example: Enter the command using the following conditions to search the process instance execution logs:

- Business process Definition Name: Hello business process
- Start date and time range: 2011/12/28 10:00:00 - 2011/12/29 14:59:59 ((Greenwich Mean Time)
- HCSC server to be accessed: HCSC
- Sort condition: Ascending order by start time

Command

- **When the -wherefile option is specified:**

```
cscpiselect -user <Login user ID> -pass <Login password> -csc HCSC -wherefile sql_where.txt
-table process -orderby "StartTime ASC"
```

For contents of sql_where.txt

```
ProcessDefinitionName = 'Hello business process' AND StartTime BETWEEN '2011-12-28
10:00:00' AND '2011-12-29 14:59:59'
```

- **When the -date option is specified:**

```
cscpiselect -user <Login user ID> -pass <Login password> -csc HCSC -processname Hello
business process-date 20111228190000# ,20111228235959# -table process -orderby "StartTime
ASC"
```

Note #

By default, Japan time is used for time zone in -date option.

Output result

```
KEOS52019-I cscpiselect will now start.
KEOS52049-I Communication with the HCSC-Server, to search for process instances, will now start.
KEOS52050-I Communication with the HCSC-Server, to search for process instances, is complete.
ProcessID,ProcessDefinitionName,ProcessDefinitionVersion,State,StartTime,EndTime,CSCServerName
J2EEServer_192168116131_HelloBusinessProcess_1325067837024_5828360283_138,HelloBusinessProcess,1,Completed,2011/12/28 10:23:57,2011/12/28 10:23:59,HCSC
J2EEServer_192168116131_HelloBusinessProcess_1325068542993_9702993874_139,HelloBusinessProcess,1,Completed,2011/12/28 10:35:42,2011/12/28 10:35:43,HCSC
J2EEServer_192168116131_HelloBusinessProcess_1325068544587_4728548730_137,HelloBusinessProcess,1,Completed,2011/12/28 10:35:44,2011/12/28 10:35:44,HCSC
J2EEServer_192168116131_HelloBusinessProcess_1325069450165_5398959934_136,HelloBusinessProcess,1,Error,2011/12/28 10:50:50,,HCSC
J2EEServer_192168116131_HelloBusinessProcess_1325069470181_2734343598_138,HelloBusinessProcess,1,Error,2011/12/28 10:51:10,,HCSC
KEOS52020-I cscpiselect ended normally.
```

For details on cscpiselect command, See "cscpiselect (Searching process instance) " in "Service Platform Reference Guide".

(3) Search with status as a criteria

(a) Using screen to search execution log

The process to search execution log of process instance by status is as follows:

1. Click the Search by [Date/Time or Status] tab.
2. Select the check box for the status of the process instance that is to be searched (Executing, Completed, occurrence of error, or Faulted).

   If you select multiple check boxes, the status that satisfies one of the conditions is searched.
3. For the search result sort condition, select the appropriate radio button.

4. Click the [Search] button.
5. The search result is displayed in the Search Results field.

(b) Using command to search execution log

The procedure to search execution logs of process instance by status is as follows:

1. Determine the HCSC server to be accessed.
2. Execute the following command to perform the search.
   - When directly specifying the where clause

```
cscpiselect -user <Login user ID> -pass <Login password> -csc <HCSC server name> -where
<where clause># -table process -orderby <Sort-condition>
```

Note #

Specify the SQL condition for the column name State.

- When using a file in which the where clause is specified

```
cscpiselect -user <Login user ID> -pass <Login password> -csc <HCSC server name> -wherefile
< file name in which the where clause is specified># -table process -orderby <Sort
condition> -encoding <Encoding name>
```

Note #

Specify the SQL condition for the column name State.

- When directly specifying the status:

```
cscpiselect -user <Login user ID> -pass <Login password> -csc <HCSC server name> -status
{executing|completed|faulted|error|executingwait|completedwait|all}# -table process -orderby
<Sort-condition>
```

Note #

Specify one of these items.

Example: Enter the command using the following conditions to search the process instance execution logs:

- Business process definition name: Hello business process
- Status of process instance: Occurrence of error
- HCSC server to be accessed: HCSC
- Sort condition: Ascending order by start time

Command

- **When the -wherefile option is specified**

```
cscpiselect -user <Login user ID> -pass <Login password> -csc HCSC -wherefile sql_where.txt
-table process -orderby "StartTime ASC"
```

For contents of sql_where.txt

```
ProcessDefinitionName = 'Hello business process' AND State = 'Error'
```

- **When the -status option is specified**

```
cscpiselect -user <Login user ID> -pass <Login password> -csc HCSC -processname Hello
business process -status error -table process -orderby "StartTime ASC"
```

Output result

```
KEOS52019-I cscpiselect will now start.
KEOS52049-I Communication with the HCSC-Server, to search for process instances, will now start.
KEOS52050-I Communication with the HCSC-Server, to search for process instances, is complete.
ProcessID,ProcessDefinitionName,ProcessDefinitionVersion,State,StartTime,EndTime,CSCServerName
J2EEServer_192168116131_HelloBusinessProcess_1325069450165_5398959934_136,HelloBusinessProcess,1,Error,2011/12/28 10:50:50,,HCSC
J2EEServer_192168116131_HelloBusinessProcess_1325069470181_2734343598_138,HelloBusinessProcess,1,Error,2011/12/28 10:51:10,,HCSC
KEOS52020-I cscpiselect ended normally.
```

For details on cscpiselect command, see "cscpiselect (Searching process instance) " in "Service Platform Reference Guide".

(4) Search with correlation set as a criteria

(a) Using screen to search execution log

The process to search execution log of process instance by correlation set is as follows:

1. Click the [Search by Correlation Set] tab
2. Enter the correlation set definition name and correlation set value. Make sure that you enter values in both fields.
3. Click the [Search] button.
   The search result is displayed in the Search Results field.

How to specify the correlation set value

You can configure the correlation set by connecting one or multiple components included in message. If the correlation set is made persistent, treat one or more specified components as a correlation set value. The correlation set value is configured according to the following rules:

- **When there is only one component**
  The component value is used as it is.
- **When there are multiple components**
  Each component value is linked by ">".

(Example)

If the correlation set definition name "ABC" consists of two components X and Y, and their values are "100" and "300" respectively, then the correlation set value would be "100>300".

- **When a component value contains @**
  Specify two consecutive "@" marks.

(Example)

If the correlation set definition name "ABC" contains the component X and its value is "@200", then the correlation set value would be "@@200".

- **When a component value contains ">"**
  Replace it with "@G".

(Example)

If the correlation set definition name "ABC" contains the component X and its value is "30>", then the correlation set value would be "30@G".

(b) Using command to search execution log

The procedure to search execution log of process instance by correlation set is as follows:

1. Determine the HCSC server to be accessed.
2. Execute the following command to perform the search.
   - When directly specifying the where clause

```
cscpiselect -user <Login user ID> -pass <Login password> -csc <HCSC server name> -where
<where clause>[#] -table process_set
```

Note#

If you conduct the search by correlation set definition name, specify the SQL condition for the column name CorrelationSetName. If you conduct the search by correlation set value, specify the SQL condition for the column name CorrelationSetValue.

   - When using a file in which the where clause is specified

```
cscpiselect -user <Login user ID> -pass <Login password> -csc <HCSC > -wherefile < file
name in which the where clause is specified>[#] -table process_set -encoding <Encoding name>
```

Note#

If you conduct the search by correlation set definition name, specify the SQL condition for the column name CorrelationSetName. If you conduct the search by correlation set value, specify the SQL condition for the column name CorrelationSetValue.

Example: Enter the command using the following conditions to search the process instance execution logs:

- Business process definition name: commodity arrangement
- Correlation set definition name: set
- Correlation set value: HDD compatible 60 inch Plasma TV
- HCSC server to be accessed: HCSC
- Sort condition: Ascending-order-of-start-time

Command

```
cscpiselect -user <Login user ID> -pass <Login password> -csc HCSC -wherefile sql_where.txt
-table process_set -orderby "StartTime ASC"
```

For the contents of sql_where.txt

```
C.ProcessDefinitionName = 'Commodity arrangement' AND C.CorrelationSetName = 'set' AND
C.CorrelationSetValue = 'HDD compatible 60 inch Plasma TV'
```

Output result

```
KEOS52019-I cscpiselect will now start.
KEOS52049-I Communication with the HCSC-Server, to search for process instances, will now start.
KEOS52050-I Communication with the HCSC-Server, to search for process instances, is complete.
ProcessID,ProcessDefinitionName,ProcessDefinitionVersion,State,StartTime,EndTime,CSCServerName
J2EEServer_192168116131_ProductStock_1325124051606_5646637389_137,ProductStock,1,Completed,2011/12/29 02:00:51,2011/12/29 02:00:51,HCSC
KEOS52020-I cscpiselect ended normally.
```

Example: Enter the command using the following conditions to search the process instance execution logs:

- Business process definition name: Commodity arrangement
- Correlation set definition name: set2
- Correlation set value: HDD compatible 60-inch Plasma TV > 1(HDD compatible 60 inch Plasma TV)
- HCSC server to be accessed: HCSC
- Sort condition: Ascending-order-of-start-time

Command

```
cscpiselect -user <Login user ID> -pass <Login password> -csc HCSC -wherefile sql_where.txt
-table process_set -orderby "StartTime ASC"
```

For the contents of sql_where.txt

```
C.ProcessDefinitionName = 'Commodity arrangement' AND C.CorrelationSetName = 'set2' AND
C.CorrelationSetValue = ' HDD-compatible-60-inch-Plasma-TV>1'
```

Output result

```
KEOS52019-I cscpiselect will now start.
KEOS52049-I Communication with the HCSC-Server, to search for process instances, will now start.
KEOS52050-I Communication with the HCSC-Server, to search for process instances, is complete.
ProcessID,ProcessDefinitionName,ProcessDefinitionVersion,State,StartTime,EndTime,CSCServerName
J2EEServer_192168116131_ProductStock_1325124051606_5646637389_137,ProductStock,1,Completed,2011/12/29 02:00:51,2011/12/29 02:00:51,HCSC
KEOS52020-I cscpiselect ended normally.
```

For details on cscpiselect command, see "cscpiselect (Searching process instance) " in "Service Platform Reference Guide".

(5) Search with the process instance identifier as a criteria

(a) Using screen to search execution log

The process to search execution log of process instance by process instance identifier is as follows:

1. Click the [Search by Identifier] tab.

2. Enter the process instance identifier.
   Enter the process instance identifier acquired from a command or a log.
3. Click the [Search] button.
   The search result is displayed in the **Search Results** field.

(b) Using command to search execution log

The process to search execution logs of process instance by process instance identifier.

1. Determine the HCSC server to be accessed.
2. Execute the following command to search:
   - When directly specifying the where clause

```
cscpiselect -user <Login user ID> -pass <Login password> -csc <HCSC server name> -where
<where clause># -table process -orderby <Sort condition>
```

Note#
Specify the SQL condition for the column name ProcessID.

   - When using a file in which the where clause is specified

```
cscpiselect -user <Login user ID> -pass <Login password> -csc <HCSC server name> -wherefile
< file name in which the where clause is specified># -table process -orderby <Sort
condition> -encoding <Encoding name>
```

Note#
Specify the SQL condition for the column name ProcessID.

Example: Enter the command using the following conditions to search the process instance execution logs:

- Business process definition name: Hello business process
- Process instance identifier: J2EEServer_010210084218_Hello business process _1237946140968_3843192274_138
- HCSC server to be accessed: HCSC
- Sort condition: Ascending order of start time

Command

```
cscpiselect -user <Login user ID> -pass <Login password> -csc HCSC -wherefile sql_where.txt
-table process -orderby "StartTime ASC"
```

For the contents of sql_where.txt

```
ProcessDefinitionName = 'Hello business process ' AND ProcessID =
'J2EEServer_192168116131_Hello business process_1325125384512_4896451771_139'
```

Output result

```
KEOS52019-I cscpiselect will now start.
KEOS52049-I Communication with the HCSC-Server, to search for process instances, will now start.
KEOS52050-I Communication with the HCSC-Server, to search for process instances, is complete.
ProcessID,ProcessDefinitionName,ProcessDefinitionVersion,State,StartTime,EndTime,CSCServerName
J2EEServer_192168116131_HelloBusinessProcess_1325125384512_4896451771_139,HelloBusinessProcess,1,Completed,2011/12/29 02:23:04,2011/12/29 02:23:04,HCSC
KEOS52020-I cscpiselect ended normally.
```

For details on cscpiselect command, see "cscpiselect (Searching process instance) " in "Service Platform Reference Guide".

(6) Search with a combination of start time and status as a criteria

(a) Using screen to search execution log

You can specify a combination of start time and status as the search condition.

The process to search execution log of process instance by using combination of start time and status is as follows:

1. Click the [Search by Date/Time or Status] tab.

2. Select [With specification] radio button of start time of process instance.
3. For the start time search range, enter the year and select the month, date, hour, minute, and second from the drop-down lists.
4. Select the check box for the status of the process instance that is to be searched (Executing, Completed, Error occurred, or Faulted).
   If you select multiple check boxes, the status that satisfies one of the conditions is searched.
5. For the search result sort condition, select the appropriate radio button.
6. Click the [Search] button.
   The search result is displayed in the Search Results field.

(b) Using command to search execution log

The process to search execution log of process instance by using combination of start time and status is as follows:

! Important note

For Start time and date when you are searching, hours method used differs due to option specified in command.

- When specified in the file in which the-where option or the where clause of the -wherefile option is specified: Greenwich Mean Time (GMT)
- When specified in the -date option: Default time zone

---

1. Determine the HCSC server to be accessed.
2. Execute the following command to perform the search.
   - When directly specifying the where clause

```
cscpiselect -user <Login user ID> -pass <Login password> -csc <HCSC server name> -where
<where clause>[#] -table process -orderby <Sort-condition>
```

Note#
Specify the SQL condition for the column names StartTime and State.

   - When using a file in which the where clause is specified

```
cscpiselect -user <Login user ID> -pass <Login password> -csc <HCSC server name> -wherefile
< file name in which the where clause is specified>[#] -table process -orderby <Sort-
condition> -encoding <Encoding name>
```

Note#
Specify the SQL condition for the column names StartTime and State

   - When directly specifying the start time range and status:

```
cscpiselect -user <Login user ID> -pass <Login password> -csc <HCSC server name> -date <
inquiry-start-date-and-time >[#1],< inquiry end date and time> -status {executing|completed|
faulted|error|executingwait|completedwait|all}[#2] -table process -orderby <sort-condition>
```

Note #1
Inquiry start date/time can be omitted.

Note #2
Specify one of these items.

(Example) Enter the command using the following conditions to search the process instance execution logs:

- Business process definition name: Hello Business Process
- Start date and time range: 2011/12/27 15:00:00 - 2011/12/28 10:51:00 (Greenwich mean time)
- Status: Occurrence of error
- HCSC server to be accessed: HCSC
- Sort condition: Ascending order by start time

Command

- **When the -wherefile option is specified**

```
cscpiselect -user <Login user ID> -pass <Login password> -csc HCSC -wherefile sql_where.txt
-table process -orderby "StartTime ASC"
```

For the contents of sql_where.txt

```
ProcessDefinitionName = 'Hello business process' AND StartTime BETWEEN '2011-12-27
15:00:00' AND '2011-12-28 10:51:00' AND State = 'Error'
```

- **When the -date option and -status option are specified**

```
cscpiselect -user <Login user ID> -pass <Login password> -csc HCSC -processname Hello
business process -date 20111228000000#,20111228195100# -status error -table process -orderby
"StartTime ASC"
```

Note #

By default, Japan time is used for time zone in -date option.

Output result

```
KEOS52019-I cscpiselect will now start.
KEOS52049-I Communication with the HCSC-Server, to search for process instances, will now start.
KEOS52050-I Communication with the HCSC-Server, to search for process instances, is complete.
ProcessID,ProcessDefinitionName,ProcessDefinitionVersion,State,StartTime,EndTime,CSCServerName
J2EEServer_192168116131_HelloBusinessProcess_1325069450165_5398959934_136,HelloBusinessProcess,1,Error,2011/12/28 10:50:50,,HCSC
KEOS52020-I cscpiselect ended normally.
```

For details on cscpiselect command, see "cscpiselect (Searching process instance) " in " Service Platform Reference Guide".

(7) Search with name of executed HCSC server as a criteria

The procedure to search execution logs of process instance using name of executed HCSC server as condition is as follows:

1. Determine the HCSC server to be accessed.
2. Execute the following command to perform the search.

```
cscpiselect -user <Login user ID> -pass <Login password> -csc <HCSC server name> -table
process -targetcsc <HCSC server name targeted to search>
```

(Example) Enter the command using the following conditions to search the process instance execution logs:

- HCSC server to be accessed: CSCSrv1
- Executed HCSC server: CSCSrv2

Command

```
cscpiselect -csc CSCSrv1 -table process -targetcsc CSCSrv2
```

For details on cscpiselect command, see "cscpiselect (Searching process instance) " in " Service Platform Reference Guide".

(8) Searching all execution logs of process instance

The procedure to search all execution logs of process instance is as follows: Further, you can search all execution logs of process instance only using command.

1. Determine the HCSC server to be accessed.
2. Execute the following command to perform the search.

```
cscpiselect -user <Login user ID> -pass <Login password> -csc <HCSC server name> -table
process
```

(Example) Enter the command using the following conditions to search the process instance execution logs:

- HCSC server to be accessed: HCSC

Command

```
cscpiselect -user <Login user ID> -pass <Login password> -csc HCSC -table process
```

Output result

```
KEOS52019-I cscpiselect will now start.
KEOS52049-I Communication with the HCSC-Server, to search for process instances, will now start.
KEOS52050-I Communication with the HCSC-Server, to search for process instances, is complete.
ProcessID,ProcessDefinitionName,ProcessDefinitionVersion,State,StartTime,EndTime,CSCServerName
J2EEServer_192168116131_HelloBusinessProcess_1325067837024_5828360283_138,HelloBusinessProcess,1,Completed,2011/12/28 10:23:57,2011/12/28 10:23:59,HCSC
J2EEServer_192168116131_HelloBusinessProcess_1325068542993_9702993874_139,HelloBusinessProcess,1,Completed,2011/12/28 10:35:42,2011/12/28 10:35:43,HCSC
J2EEServer_192168116131_HelloBusinessProcess_1325068544587_4728548730_137,HelloBusinessProcess,1,Completed,2011/12/28 10:35:44,2011/12/28 10:35:44,HCSC
J2EEServer_192168116131_HelloBusinessProcess_1325069450165_5398959934_136,HelloBusinessProcess,1,Error,2011/12/28 10:50:50,,HCSC
J2EEServer_192168116131_HelloBusinessProcess_1325069470181_2734343598_138,HelloBusinessProcess,1,Error,2011/12/28 10:51:10,,HCSC
J2EEServer_192168116131_ProductStock_1325118816684_8764247803_137,ProductStock,1,Completed,2011/12/29 00:33:36,2011/12/29 00:33:37,HCSC
J2EEServer_192168116131_ProductStock_1325118847700_4348494840_139,ProductStock,1,Completed,2011/12/29 00:34:07,2011/12/29 00:34:07,HCSC
J2EEServer_192168116131_ProductStock_1325118853387_5995008787_138,ProductStock,1,Completed,2011/12/29 00:34:13,2011/12/29 00:34:13,HCSC
J2EEServer_192168116131_ProductStock_1325118855044_9852277080_139,ProductStock,1,Completed,2011/12/29 00:34:15,2011/12/29 00:34:15,HCSC
KEOS52020-I cscpiselect ended normally.
```

For details on cscpiselect command, see "cscpiselect (Searching process instance) " in "Service Platform Reference Guide".

(9) Search with RD area name as a criteria

If you specify "IN ('<RD area name>')" in SELECT statement of SQL, you can search in RD area unit. When you want to confirm data in RD area unit, check whether deletion of RD area unit is executed correctly or not.

(Example) CSCBP_<Cluster name>_in RD area of PROCESS table (RDA11, RDA21 and RDA31) , search how much data is stored.

```
SELECT count(*) FROM CSCBP_<Cluster name>_PROCESS IN ('RDA11,RDA21,RDA31') WITHOUT LOCK
NOWAIT;
```

(10) Output of all execution logs to a CSV file

You can use the process instance execution logs as maintenance information by searching them periodically and saving all information as historical data in one CSV file HCSC server unit. The procedure to output execution logs of process instance to CSV file is as follows:

1. Determine the HCSC server to be accessed.
2. Execute the following command to perform the search.

```
cscpiselect -user < Login user ID> -pass <Login password> -csc <HCSC server name> -detail -
table {process|activity|link|set|string|numeric|boolean|message|relation}#
```

Note #

Specify one of these items.

(Example) Enter the command using the following conditions to output the process instance execution logs to CSV files in batch mode:

- Store all information in HCSC server unit in CSV file.
- HCSC server to be accessed: HCSC

Command

```
cscpiselect -user <Login user ID> -pass <Login password> -csc HCSC -detail -table process >
yyyymmdd_process.csv
cscpiselect -user <Login user ID > -pass <Login password > -csc HCSC -detail -table
activity > yyyymmdd_activity.csv
cscpiselect -user <Login user ID > -pass < Login password > -csc HCSC -detail -table link >
yyyymmdd_link.csv
cscpiselect -user <Login user ID > -pass <Login password > -csc HCSC -detail -table set >
yyyymmdd_set.csv
cscpiselect -user < Login user ID > -pass <Login password > -csc HCSC -detail -table string
> yyyymmdd_string.csv
cscpiselect -user <Login user ID > -pass <Login password > -csc HCSC -detail -table numeric
> yyyymmdd_numeric.csv
cscpiselect -user <Login user ID > -pass <Login password > -csc HCSC -detail -table boolean
```

```
> yyyymmdd_boolean.csv
cscpiselect -user <Login user ID > -pass <Login password > -csc HCSC -detail -table message
> yyyymmdd_message.csv
cscpiselect -user <Login user ID > -pass <Login password > -csc HCSC -detail -table
relation > yyyymmdd_relation.csv
```

For details on cscpiselect command, see "cscpiselect (Searching process instance) " in "Service Platform Reference Guide".

(11) See search result by screen

Search result is displayed as total cases and list in search result field. List displays up to 20 cases at one time.

Also, as per time difference at the time of search, the search result, total number of cases and number of cases to be displayed may differ. For example, the total number of searched items might be 13, whereas the number of items displayed might be 60. In this case you must search again, because even if the number of items displayed exceeds 20, the **Next** button is disabled, making it impossible to display more than 20 items.

Also, after clicking [Back], [Next] button of search result list, number of cases of process instance may change. For example, if you click [Next] button when total number of cases are 45 and number of cases to be displayed are 21-40, total number of cases may become 10. In this case, 1-10 cases are displayed.

6.1.3 Acquiring detailed information from the process instance execution logs

You can acquire detailed information of the process instance execution logs depending on what you want to accomplish.

- If you are using the correlation set value to identify a process instance:
  Acquire a list of correlation set definition names and correlation set values, which are the correlation set information items that uniquely identifies each process instance.
- If you are using the variable value to identify a process instance:
  Acquire a list of variable definition names and variable values, which is global variable information that belongs to each process instance.
- If you are checking a process instance's execution status:
  Acquire the information of each activity that is defined in the business process for process instance.

(1) Acquiring detailed information about correlation sets

(a) Using screen to acquire detailed information from the execution log

The procedure to acquire detailed information of the process instance execution log (correlation set information) is as follows:

1. Search the process instances.
2. Select the execution log of the process instance that acquires information from search result list.
3. Click the [Correlation Set Information] button.
   Detailed information is displayed in the Detailed Information field.

(b) Using commands to acquire detailed information of the execution log

The procedure to acquire detailed information of the process instance execution log (correlation set information) is as follows:

1. Determine the HCSC server to be accessed.
2. Execute the following command to perform the search.
   - When directly specifying the where clause

```
cscpiselect -user <Login user ID> -pass <Login password> -csc <HCSC server name> -where
<where clause>[#] -table set
```

Note #

Specify the condition for the process instance whose information you are acquiring.

- When using a file in which the where clause is specified

```
cscpiselect -user <Login user ID> -pass <Login password> -csc <HCSC server name> -wherefile
< file name in which the where clause is specified>[#] -table set -encoding <Encoding name>
```

Note #

Specify the condition for the process instance whose information you are acquiring.

- When searching with executed HCSC server name as criteria

```
cscpiselect -user <Login user ID> -pass <Login password> -csc <HCSC server name> -table set
-targetcsc <HCSC server name targeted to search>
```

(Example) Enter the command using the following conditions to acquire correlation set information:

- J2EEServer_010209010042_XXXPurchaseRegisterService_1142479241203_760331597_2115
- HCSC server to be accessed: HCSC

Command

```
cscpiselect -user <Login user ID> -pass <Login password> -csc HCSC -wherefile sql_where.txt
-table set
```

For contents of sql_where.txt

```
ProcessID =
'J2EEServer_010209010042_XXXPurchaseRegisterService_1142479241203_760331597_2115'
```

Output result

```
KEOS52019-I cscpiselect will now start.
KEOS52049-I Communication with the HCSC-Server to search for process instances will now start.
KEOS52050-I Communication with the HCSC-Server to search for process instances is complete.
ProcessID,CorrelationSetName,CorrelationSetValue
J2EEServer_010209010042_XXXPurchaseRegisterService_1142479241203_760331597_2115,correlation1,XXX
KEOS52020-I cscpiselect ended successfully.
```

For details on cscpiselect command, see "cscpiselect (Searching process instance) " in "Service Platform Reference Guide".

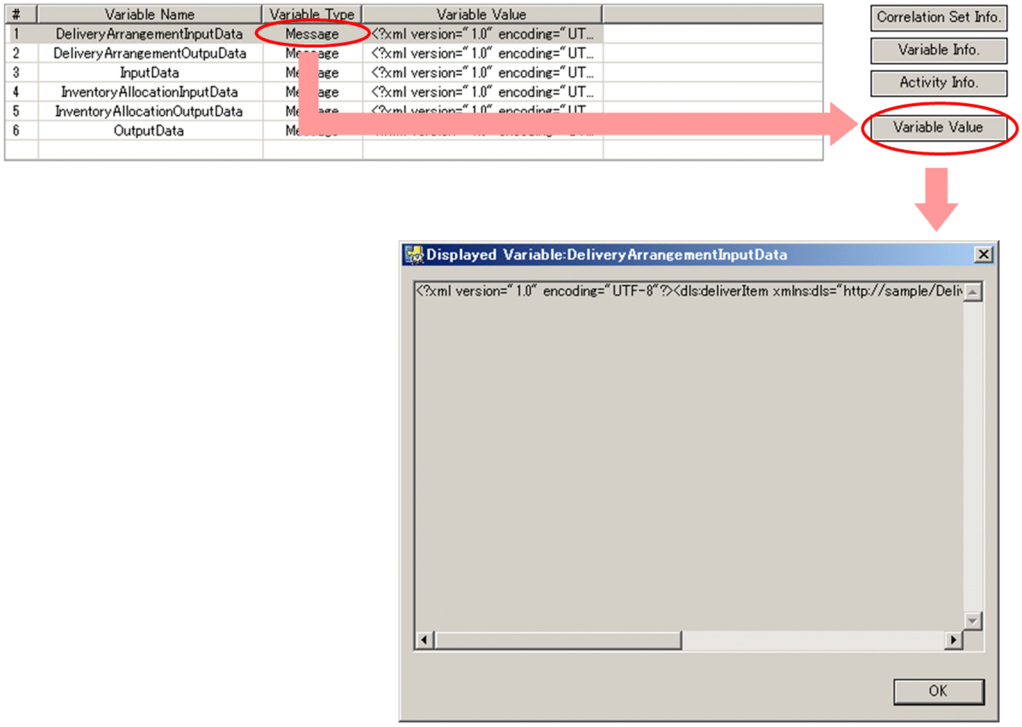
(2) Acquiring detailed information of variable

(a) Acquire detailed information of execution log using screen

The procedure to acquire detailed information (variable information) of process instance execution log is as follows:

1. Search process instance.
2. Select process instance execution log that acquires information from search result list.
3. Click the [Variable information] button.
   Detailed information is displayed in detailed information field.
4. When variable type is String or Message, select appropriate variable and click the [Display variable value] button.
   As shown in following figure, detailed information of variable value is displayed in other window:

Figure 6–1: Figure Display screen of variable information details



(b) Acquiring detailed information of execution log using command

The procedure to acquire detailed information (Variable information) of process instance execution log is as follows:

1. Determine the HCSC server to be accessed.
2. Execute the following command to perform the search.

- When directly specifying the where clause

```
cscpiselect -user <Login user ID> -pass <Login password> -csc <HCSC server name> -where
<where clause>#1 -table {string |numeric | boolean | message}#2
```

Note #1

Specify the condition for the process instance whose information you are acquiring.

Note #2

Specify one of these items.

- When using a file in which the where clause is specified

```
cscpiselect -user < Login user ID > -pass < Login password > -csc <HCSC server name > -
wherefile < file name in which the where clause is specified>#1 -table {string|numeric|
boolean|message}#2 -encoding <Encoding name>
```

Note #1

Specify the condition for the process instance whose information you are acquiring.

Note #2

Specify one of these items.

- When using the name of executed HCSC server as criteria

```
cscpiselect -user <Login user ID> -pass <Login password> -csc <HCSC server name> -table
{string|numeric|boolean|message} -targetcsc <HCSC server name to be searched>
```

Since the variable information is provided in a separate table for each variable. If the variable type is not clear, search all tables.

(Example) Enter the following condition to acquire variable information.

- Process ID to be acquired: J2EEServer_010210084218_Commodity arrangement_1237948143515_3919056788_140
- HCSC server to be accessed: HCSC

Command

- When displaying string variable information

```
cscpiselect -user <Login user ID> -pass <Login password> -csc HCSC -wherefile sql_where.txt
-table string
```

- When displaying numeric variable information

```
cscpiselect -user < Login user ID > -pass < Login password > -csc HCSC -wherefile
sql_where.txt -table numeric
```

- When displaying boolean variable information

```
cscpiselect -user < Login user ID> -pass < Login password > -csc HCSC -wherefile
sql_where.txt -table boolean
```

- When displaying message variable information

```
cscpiselect -user < Login user ID > -pass < Login password > -csc HCSC -wherefile
sql_where.txt -table message
```

Contents of sql_where.txt

```
ProcessID = 'J2EEServer_010210084218_commodity arrangement_1237948143515_3919056788_140'
```

Output result

- For string variable information

```
KEOS52019-I cscpiselect will now start.
KEOS52049-I Communication with the HCSC-Server, to search for process instances, will now start.
KEOS52050-I Communication with the HCSC-Server, to search for process instances, is complete.
ProcessID,VariableName,VariableValue
J2EEServer_010210084218_ProductStock_1237948143515_3919056788_140,orderID,MyOrder0001
KEOS52020-I cscpiselect ended normally.
```

- For numeric variable information

```
KEOS52019-I cscpiselect will now start.
KEOS52049-I Communication with the HCSC-Server, to search for process instances, will now start.
KEOS52050-I Communication with the HCSC-Server, to search for process instances, is complete.
ProcessID,VariableName,VariableValue
J2EEServer_010210084218_ProductStock_1237948143515_3919056788_140,repeatCount,5.0
KEOS52020-I cscpiselect ended normally.
```

- For boolean variable information

```
KEOS52019-I cscpiselect will now start.
KEOS52049-I Communication with the HCSC-Server, to search for process instances, will now start.
KEOS52050-I Communication with the HCSC-Server, to search for process instances, is complete.
ProcessID,VariableName,VariableValue
J2EEServer_010210084218_ProductStock_1237948143515_3919056788_140,isResult,1
KEOS52020-I cscpiselect ended normally.
```

- For message variable information

```
KEOS52019-I cscpiselect will now start.
KEOS52049-I Communication with the HCSC-Server, to search for process instances, will now start.
KEOS52050-I Communication with the HCSC-Server, to search for process instances, is complete.
ProcessID,VariableName,
VariableValue
J2EEServer_0102100842l8_ProductStock_1237948143515_3919056788_140,InventoryAllocationInputData,
<?xml version="1.0" encoding="UTF-8"?><ims:reserveItem xmlns:ims="http://sample/InventoryManagementService"><ims:ItemName>26 LCD television w
ith other digital measures</ims:ItemName><ims:Quantity>1</ims:Quantity></ims:reserveItem>
J2EEServer_0102100842l8_ProductStock_1237948143515_3919056788_140,InputData,
<?xml version="1.0" encoding="UTF-8"?><arrangeItem xmlns="http://sample/ArrangementService" xmlns:soapenv="http://schemas.xmlsoap.org/soap/en
velope/" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><ItemName>26 LCD television with
other digital measures</ItemName><Quantity>1</Quantity></arrangeItem>
J2EEServer_0102100842l8_ProductStock_1237948143515_3919056788_140,DeliveryArrangementInputData,
<?xml version="1.0" encoding="UTF-8"?><dls:deliverItem xmlns:dls="http://sample/DeliveryService"><dls:ReservationNumber>R00000010</dls:Reserv
ationNumber></dls:deliverItem>
J2EEServer_0102100842l8_ProductStock_1237948143515_3919056788_140,InventoryAllocationOutputData,
<?xml version="1.0" encoding="UTF-8"?><reserveItemResponse xmlns="http://sample/InventoryManagementService" xmlns:soapenv="http://schemas.xml
soap.org/soap/envelope/" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><ReservationNumbe
r>R00000010</ReservationNumber></reserveItemResponse>
J2EEServer_0102100842l8_ProductStock_1237948143515_3919056788_140,DeliveryArrangementOutpuData,
<?xml version="1.0" encoding="UTF-8"?><deliverItemResponse xmlns="http://sample/DeliveryService" xmlns:soapenv="http://schemas.xmlsoap.org/so
ap/envelope/" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><DeliveryNumber>D00000010</D
eliveryNumber></deliverItemResponse>
J2EEServer_0102100842l8_ProductStock_1237948143515_3919056788_140,OutputData,
<?xml version="1.0" encoding="UTF-8"?><ars:arrangeItemResponse xmlns:ars="http://sample/ArrangementService"><ars:DeliveryNumber>D00000010</ar
s:DeliveryNumber></ars:arrangeItemResponse>
KEOS52020-I cscpiselect ended normally.
```

For details on cscpiselect command, see "cscpiselect (Searching process instance) " in "Service Platform Reference Guide".

(3) Acquiring detailed information about activities

! Important note

When you define data transformation activity in the definition of business process, output activity type of execution log as assign activity.

(a) Using screen to acquire detailed information of the execution log

The procedure to acquire detailed information from the process instance execution log (activity information) is as follows:

1. Search the process instances.
2. From the search results list, select the execution log of the process instance for which you require detailed information.
3. Click the [Activity Information button.
   Detailed information is displayed in the Detailed Information field.

(b) Using commands to acquire detailed information of the execution log

The procedure to specify process ID and acquiring detailed information of process instance execution log is as follows:

1. Determine the HCSC server to be accessed.
2. Execute the following command to perform the search.
   - When directly specifying the where clause

```
cscpiselect -user <Login user ID> -pass <Login password> -csc <HCSC server name> -where
<where clause>[#] -table activity
```

Note #

Specify the condition for the process instance whose information you are acquiring.

   - When using a file in which the where clause is specified

```
cscpiselect -user < Login user ID > -pass < Login password > -csc <HCSC server name > -
wherefile < file name in which the where clause is specified>[#] -table activity -encoding
<Encoding name>
```

Note #

Specify the condition for the process instance whose information you are acquiring.

   - When searching with the of executed HCSC server as criteria

```
cscpiselect -user < Login user ID > -pass < Login password > -csc <HCSC server name > -
table activity -targetcsc <name of HCSC server to be searched >
```

(Example) Enter command in following condition to acquire activity information.

- Process ID to be acquired: J2EEServer_010210084218_commodity arrangement_1237856438531_3676477500_139
- HCSC server to be accessed: HCSC

Command

```
cscpiselect -user < Login user ID > -pass < Login password > -csc HCSC -wherefile
sql_where.txt -table activity
```

contents of sql_where.txt

```
ProcessID = 'J2EEServer_010210084218_commodity arrangement_1237856438531_3676477500_139'
```

Output result

```
KEOS52019-I cscpiselect will now start.
KEOS52049-I Communication with the HCSC-Server, to search for process instances, will now start.
KEOS52050-I Communication with the HCSC-Server, to search for process instances, is complete.
ProcessID,ActivityNumber,ActivityDefinitionName,ActivityKind,State,StartTime,EndTime,WaitTime
J2EEServer_010210084218_ProductStock_1237948143515_3919056788_140,0,@GLOBAL,SCOPE,Completed,2009/03/24 01:00:38,2009/03/24 01:00:38,
J2EEServer_010210084218_ProductStock_1237948143515_3919056788_140,1,seq1,SEQUENCE,Completed,2009/03/24 01:00:38,2009/03/24 01:00:38,
J2EEServer_010210084218_ProductStock_1237948143515_3919056788_140,2,StockAllocationResultCheck,SWITCH,Completed,2009/03/24 01:00:38,2009/03/24 01:00:38,
J2EEServer_010210084218_ProductStock_1237948143515_3919056788_140,3,StockAllocation,INVOKE,Completed,2009/03/24 01:00:38,2009/03/24 01:00:38,
J2EEServer_010210084218_ProductStock_1237948143515_3919056788_140,4,StockAllocationPre-processing,ASSIGN,Completed,2009/03/24 01:00:38,2009/03/24 01:00:38,
J2EEServer_010210084218_ProductStock_1237948143515_3919056788_140,5,Receive,RECEIVE,Completed,2009/03/24 01:00:38,2009/03/24 01:00:38,
J2EEServer_010210084218_ProductStock_1237948143515_3919056788_140,6,seq3,SEQUENCE,Omitted,,2009/03/24 01:00:38,
J2EEServer_010210084218_ProductStock_1237948143515_3919056788_140,7,seq2,SEQUENCE,Completed,2009/03/24 01:00:38,2009/03/24 01:00:38,
J2EEServer_010210084218_ProductStock_1237948143515_3919056788_140,8,Reply_ArrangementSuccess,REPLY,Completed,2009/03/24 01:00:38,2009/03/24 01:00:38,
J2EEServer_010210084218_ProductStock_1237948143515_3919056788_140,9,DeliveryNumberArrangement,ASSIGN,Completed,2009/03/24 01:00:38,2009/03/24 01:00:38,
J2EEServer_010210084218_ProductStock_1237948143515_3919056788_140,10,DeliveryArrangement,INVOKE,Completed,2009/03/24 01:00:38,2009/03/24 01:00:38,
J2EEServer_010210084218_ProductStock_1237948143515_3919056788_140,11,DeliveryArrangementPre-processing,ASSIGN,Completed,2009/03/24 01:00:38,2009/03/24 01:00:38,
J2EEServer_010210084218_ProductStock_1237948143515_3919056788_140,12,Reply_NostockError,REPLY,Omitted,,2009/03/24 01:00:38,
J2EEServer_010210084218_ProductStock_1237948143515_3919056788_140,13,NoStockArrangement,ASSIGN,Omitted,,2009/03/24 01:00:38,
KEOS52020-I cscpiselect ended normally.
```

For details on cscpiselect command, see "cscpiselect (Searching process instance) " in "Service Platform Reference Guide".

6.1.4 Deleting process instance execution logs

When you resend requests or delete process instances whose execution has been tested, you can one by one delete the process instances execution log that is no longer needed.

Also, since the process instance execution log is added daily, unless the information is deleted periodically, a database capacity shortage may occur. Therefore, the administrator must periodically delete process instance execution log information from the execution log information table in the database. During daily operations, you can normally delete execution log information in batch mode.

You can use screen method, commands method or database creation utility (pdload) to delete process instance execution logs.

(1) Using screen to delete execution logs

(a) Deleting execution logs individually

The procedure to delete a process instance execution log one by one using screen is as follows:

1. Search the process instances.
2. From the search results list, select the process instance execution log you want to delete.
3. Click the [Delete] button.

   A dialog box confirming deletion of the process instance execution log is displayed.

   If the deletion target includes a process instance in Executing status, a dialog box confirming deletion of the execution log for the process instance that is executing is displayed.
4. Click the [OK] button.

   The process instance execution log is deleted, and a dialog box showing the result of deleting the process instance execution log is displayed.
5. Click the [OK] button.

6. The list of search results is updated.

(b) Deleting in batch mode

The procedure to delete process instance execution log in batch mode using screen is as follows:

1. Search the process instances.
2. From the search results list, select the process instance execution log you want to delete.
   Use the [**Ctrl**] or [**Shift**] key to select multiple process instances.
3. Click the [Delete] button.
   A dialog box confirming deletion of the process instance execution log is displayed.
   If the deletion target includes a process instance in Executing status, a dialog box confirming deletion of the execution log for the process instance that is executing is displayed.
4. Click the [OK] button.
   The process instance execution log is deleted, and a dialog box showing the result of deleting the process instance execution log is displayed.
5. Click the [OK] button.
   The list of search results is updated.

! Important note

If batch deletion fails, none of the selected process instances is deleted.

(2) Using commands to delete execution logs

Here it is explained about deleting execution log using cscpidelete command. For details on cscpidelete command, see "cscpidelete (Deleting process instance execution logs) " in "Service Platform Reference Guide".

(a) Deleting execution logs individually

The procedure to delete process instance execution log individually using command is as follows:

1. Determine the HCSC server to be accessed.
2. Use the cscpiselect command to search the process instance to be deleted.
3. From the search results, identify the process ID of the process instance whose execution log you wish to delete.
4. Execute the following command to delete the execution log:
   - When directly specifying the where clause

```
cscpidelete -user <Login user ID> -pass <Login password> -csc <HCSC server name> -where
<where clause>#
```

Note #
Specify the deletion condition for the process instance whose execution log you are deleting.

- When using a file in which the where clause is specified

```
cscpidelete -user <Login user ID> -pass <Login password> -csc <HCSC server name > -
wherefile < file name in which the where clause is specified>#
```

Note #
Specify the deletion condition for the process instance whose execution log you are deleting.

- When specifying a file containing a list of IDs

```
cscpidelete -user < Login user ID > -pass < Login password > -csc <HCSC server name > -
idlist < file name in which a list of ID is specified>
```

(Example) Enter command using following condition to delete process instance execution log.

- Process ID to be deleted:
  J2EEServer_010209010042_XXXPurchaseRegisterService_1142479241203_760331597_2115

- HCSC server to be accessed: HCSC

Command

- **When the -wherefile option is specified**

```
cscpidelete -user < Login user ID > -pass < Login password > -csc HCSC -wherefile
delete_where.txt
```

Contents of delete_where.txt

```
ProcessID =
'J2EEServer_010209010042_XXXPurchaseRegisterService_1142479241203_760331597_2115'
```

- **When -idlist option is specified**

```
cscpidelete -user < Login user ID > -pass < Login password > -csc HCSC -idlist
delete_id_list.txt
```

Contents of delete_id_list.txt

```
J2EEServer_010209010042_XXXPurchaseRegisterService_1142479241203_760331597_2115
```

(b) To delete execution logs in a batch by specifying the business process definition name of the process instances

The procedure to specify business process definition name of process instance using command and deleting execution log in batch mode is as follows:

1. Determine the HCSC server to be accessed.
2. Execute the following command to delete the execution log:

- When directly specifying the where clause

```
cscpidelete -user < Login user ID > -pass < Login password > -csc <HCSC server name > -
where <where clause>#
```

Note #

Specify the SQL condition for the column name ProcessDefinitionName.

- When using a file in which the where clause is specified

```
cscpidelete -user < Login user ID > -pass < Login password > -csc <HCSC server name > -
wherefile < file name in which the where clause is specified>#
```

Note #

Specify the SQL condition for the column name ProcessDefinitionName.

- When directly specifying a business process definition name

```
cscpidelete -user < Login user ID > -pass < Login password > -csc <HCSC server name > -
processname < Business process definition name >
```

(Example) Enter command using following condition to delete process instance execution log in batch mode.

- *Business process definition name:* Hello business process
- HCSC server to be accessed: HCSC

Command

- **When the -wherefile option is specified:**

```
cscpidelete -user < Login user ID > -pass < Login password > -csc HCSC -wherefile
delete_where.txt
```

Contents of delete_where.txt

```
ProcessDefinitionName=' Hello business process '
```

- **When the -processname option is specified:**

```
cscpidelete -user < Login user ID > -pass < Login password > -csc HCSC -processname Hello
business process
```

(c) To delete execution logs in a batch by specifying start date and time of process instances

The procedure to specify start date and time of process instance using command and deleting execution log in batch mode is as follows:

! Important note

The start date and time to be specified for deleting execution logs differs as per the hour system used in the option specified in the command.

- When specified in the file in which the-where option or the where clause of the -wherefile option is specified: Greenwich Mean Time (GMT)
- When specified in the -date option: Default time zone

---

1. Determine the HCSC server to be accessed.
2. Execute the following command to delete the execution log:
   - When directly specifying the where clause

```
cscpidelete -user < Login user ID > -pass <Login password > -csc <HCSC server name> -where
<where clause>#
```

Note #

Specify the SQL condition for the column name StartTime.

- When using a file in which the where clause is specified

```
cscpidelete -user < Login user ID > -pass <Login password > -csc <HCSC server name > -
wherefile < file name in which the where clause is specified >#
```

Note #

Specify the SQL condition for the column name StartTime.

- When directly specifying a start time range

```
cscpidelete -user <Login user ID> -pass <Login password > -csc <HCSC server name > -date <
inquiry start date and time>#,< inquiry end date and time >
```

Note #

Inquiry start date/time can be omitted.

(Example) Enter the command using the following conditions to delete process instance execution logs in batch mode:

- Start date and time range: Before 2008/10/09 14:59:59 (Greenwich Mean Time)
- HCSC server to be accessed: HCSC

Command

- **When the -wherefile option is specified:**

```
cscpidelete -user <Login user ID > -pass <Login password > -csc HCSC -wherefile
delete_where.txt
```

For contents of delete_where.txt

```
StartTime <= '2008-10-09 14:59:59'
```

- **When the -date option is specified**

```
cscpidelete -user < Login user ID > -pass < Login password > -csc HCSC -date ,
20081009235959#
```

Note #

By default, Japan time is used for time zone in -date option.

(Example) Enter the command using the following conditions to delete process instance execution logs in batch mode:

- Start date and time range: 2008/10/08 15:00:00 - 2008/10/09 14:59:59(Greenwich Mean Time)
- HCSC server to be accessed: HCSC

Command

- **When the -wherefile option is specified**

```
cscpidelete -user < Login user ID > -pass <Login password> -csc HCSC -wherefile
delete_where.txt
```

Contents of delete_where.txt

```
StartTime BETWEEN '2008-10-08 15:00:00' AND '2008-10-09 14:59:59'
```

- **When the -date option is specified**

```
cscpidelete -user < Login user ID > -pass < Login password > -csc HCSC -date
20081009000000#,20081009235959#
```

Note #

By default, Japan time is used for time zone in -date option.

(d) To delete execution logs in a batch by specifying the status of the process instances

The procedure to use commands to specify the status of the process instances and delete execution logs in batch mode is as follows:

1. Determine the HCSC server to be accessed.
2. Execute the following command to delete the execution log:
   - When directly specifying the where clause

```
cscpidelete -user < Login user ID > -pass < Login password > -csc <HCSCserver name> -where
<where clause>#
```

Note #

Specify the SQL condition for the column name State.

- When using a file in which the where clause is specified

```
cscpidelete -user < Login user ID > -pass <Login password > -csc <HCSC server name> -
wherefile < file name in which the where clause is specified>#
```

Note #

Specify the SQL condition for the column name State.

- When directly specify the status

```
cscpidelete -user < Login user ID > -pass <Login password > -csc <HCSC server name> -status
{executing | completed | faulted | error | all}#
```

Note #

Specify one of these items.

(Example) Enter the command using the following conditions to delete process instance execution logs in batch mode:

- Status of process instance: Executing
- HCSC server to be accessed: HCSC

Command

- **When the -wherefile option is specified**

```
cscpidelete -user < Login user ID > -pass <Login password > -csc HCSC -wherefile
delete_where.txt
```

Contents of delete_where.txt

```
State='Executing'
```

Note #

Note that, if you specify a condition other than State='Completed', be careful as process instances except for completed process instances get deleted.

- **When the -status option is specified**

```
cscpidelete -user < Login user ID > -pass <Login password > -csc HCSC -status executing
```

(e) To delete execution logs in a batch by combining the business process definition name, start date and time, and status of the process instances

The procedure to specify the after combining business process definition name of process instances, start date and time, and status using command, and deleting execution logs in a batch mode is as follows:

! Important note

The start date and time to be specified for deleting execution logs differs as per the hour system used in the option specified in the command.

- When specified in the file in which the-where option or the where clause of the -wherefile option is specified: Greenwich Mean Time (GMT)
- When specified in the `-date` option: Default time zone

---

1. Determine the HCSC server to be accessed.
2. Execute the following command to delete the execution log:
   - When directly specifying the where clause

```
cscpidelete -user <Login user ID> -pass < Login password> -csc <HCSC server name> -where
<where clause>#
```

Note #

Specify the SQL condition for the column names ProcessDefinitionName, StartTime, and State.

- When using a file in which the where clause is specified

```
cscpidelete -user < Login user ID> -pass <Login password > -csc <HCSC server name > -
wherefile < file name in which the where clause is specified>#
```

Note #

Specify the SQL condition for the column names ProcessDefinitionName, StartTime, and State.

- When directly specifying the business process definition name, start time range and status:

```
cscpidelete -user <Login user ID> -pass <Login password> -csc <HCSC server name> -
processname < Business process definition name > -date < inquiry start date and time>#1,<
inquiry end date and time > -status {executing | completed | faulted | error | all}#2
```

Note #

Inquiry start date/time can be omitted.

Note #

Specify one of these items.

(Example) Enter the command using the following conditions to delete process instance execution logs in batch mode:

- Business process definition name: Hello business process
- Start date and time range: before 2008/10/09 14:59:59(Greenwich Mean Time)
- Status of process instance: Executing
- HCSC server to be accessed: HCSC

Command

- **When the -wherefile option is specified**

```
cscpidelete -user <Login user ID> -pass <Login password> -csc HCSC -wherefile
delete_where.txt
```

Contents of delete_where.txt

```
ProcessDefinitionName='Hello business process' AND StartTime <= '2008-10-09 14:59:59' AND
State='Executing'
```

- **When the -processname option, -date option, and -status option are specified**

```
cscpidelete -user <Login user ID> -pass <Login password> -csc HCSC -processname Hello
business process -date ,20081009235959# -status executing
```

Note #

By default, Japan time is used for time zone in -date option.

(f) To delete the execution logs for all process instances in a batch

The procedure to use commands to delete all process instance execution logs in batch mode is as follows:

1. Determine the HCSC server to be accessed.
2. Execute the following command to delete the execution log:

```
cscpidelete -user <Login user ID> -pass <Login password> -csc <HCSC server name> -force
```

(Example) Enter the command using the following conditions to delete all process instance execution logs in batch mode:

- HCSC server to be accessed: HCSC

Command

```
cscpidelete -user < Login user ID> -pass < Login password > -csc HCSC -force
```

(g) To delete execution logs in a batch by specifying the deletion process time

If the quantity of process instance execution logs that you want to delete is large, long period will be required for completing all the deletion processes. You can limit time required for batch deletion process so that deletion process will not affect request process.

You can specify the elapsed time till the deletion process is stopped in seconds in-canceltimer option of cscpidelete command. With this you can stop the deletion process if the time after commit is exceeds the specified time and the deletion process after this point will not be executed.

(Example)

In the following example, data saved till 31/3/2005 is deleted in 600 seconds

```
cscpidelete -csc CSCSrv1 -date ,20050331235959 -canceltimer 600
```

For details on cscpidelete command, see "cscpidelete (Deleting process instance execution logs) " in " Service Platform Reference Guide".

(3) Using database creation utility (pdload) to delete execution logs

In the environment that uses table split function, you can delete execution log of business process RD area (Month) wise using HiRDB function. When you use table split function, in order to execute cyclic allocation of RD area, you must periodically delete execution logs which are added daily.

However, when you are using RD area wise deletion of execution log, data with status "Executing (Executing)" or "Error (Error)"is also deleted. Check in advance if the data that you do not want to delete is included using following method:

Example of confirmation method

```
SELECT count(*) FROM CSCBP_<Cluster name>_PROCESS IN ('<RD area name 1 which you want to
delete>,< RD area name 2 which you want to delete >,･) WHERE State IN ('Executing','Error')
WITHOUT LOCK NOWAIT
```

Store the data that you do not want to delete in advance. The storage process and deletion process of execution log is as follows:

(a) Steps to save execution log

Prerequisites when storing data are as follows:

- Confirm that reception of all the HCSC servers is stopped.
- Confirm that there is no request is in progress.
- Do not perform command of Service Coordinator.
- Execute storage process using memory (Java program).

Storage process of data is as follows:

1. Connect to database (HiRDB) using JDBC driver.

   Be careful about following points when connecting

   - It is recommended to set LONGVARBINARY_ACCESS of user property when connecting as LOCATOR.

     When you set REAL in LONGVARBINARY_ACCESS, set maximum value appropriate for HiRDB_for_Java_MAXBINARYSIZE.

     When HiRDB_for_Java_MAXBINARYSIZE is not set, since 147,483,639 byte memory is allocated in data acquisition of Variable value of CSCBP_<Cluster name>_MSG_VARIABLE table, there is a possibility that java.lang.OutOfMemoryError may occur.

     Also, when setting value of HiRDB_for_Java_MAXBINARYSIZE is less than maximum length of data stored in VariableValue of CSCBP_<Cluster name>_MSG_VARIABLE table, exceeded data is omitted and there is possibility that system may not operate normally.

   - Disabling automatic commit is recommended.

     If it is not disabled, in case of an error in storage process, the system may not operate normally.

2. Identify the process instances to be stored.

   For storing the process instances which are stored in RD area to be deleted or when status of process instance is "Executing" or "Error", issue the following SQL and acquire a list of Process instance identifier to be stored.

```
SELECT ProcessID FROM CSCBP_<Cluster name>_PROCESS
        IN ('<RD area name 1 which you want to delete>,<RD area name 2 which you want to
delete>,･)
        WHERE State IN ('Executing', 'Error')
       WITHOUT LOCK NOWAIT;
```

3. Change the storage location of the process instances to be stored.

   Consider Process instance identifier acquired in procedure 2.as key and change storage location of the entire following table.

   - CSCBP_<Cluster name>_PROCESS
   - CSCBP_<Cluster name>_ACTIVITY
   - CSCBP_<Cluster name>_LINK
   - CSCBP_<Cluster name>_CORRELATIONSET
   - CSCBP_<Cluster name>_STR_VARIABLE
   - CSCBP_<Cluster name>_NUM_VARIABLE
   - CSCBP_<Cluster name>_BOOL_VARIABLE
   - CSCBP_<Cluster name>_MSG_VARIABLE
   - CSCBP_<Cluster name>_MSG_RELATION

   The procedure to change storage location is as follows. When you have acquired multiple Process instance identifiers, perform process (i)-(iii) multiple times.

(i)Acquire entire data of target Process instance identifier

Issue following SQL and acquire entire data to be stored.

```
SELECT * FROM CSCBP_<Cluster name>_PROCESS
    IN ('<RD area name 1 which you want to delete>,<RD area name 2 which you want to
delete>,・)
WHERE ProcessID = <Process instance identifier> WITHOUT LOCK NOWAIT;

SELECT * FROM CSCBP_<Cluster name>_ACTIVITY
    IN ('<RD area name 1 which you want to delete>,<RD area name 2 which you want to
delete>,・)
WHERE ProcessID = <Process instance identifier> WITHOUT LOCK NOWAIT;

SELECT * FROM CSCBP_<Cluster name>_LINK
    IN ('<RD area name 1 which you want to delete>,<RD area name 2 which you want to
delete>,・)
WHERE ProcessID = <Process instance identifier> WITHOUT LOCK NOWAIT;

SELECT * FROM CSCBP_<Cluster name>_CORRELATIONSET
    IN ('<RD area name 1 which you want to delete>,<RD area name 2 which you want to
delete>,・)
WHERE ProcessID = <Process instance identifier> WITHOUT LOCK NOWAIT;

SELECT * FROM CSCBP_<Cluster name>_STR_VARIABLE
    IN ('<RD area name 1 which you want to delete>,<RD area name 2 which you want to
delete>,・)
WHERE ProcessID = <Process instance identifier> WITHOUT LOCK NOWAIT;

SELECT * FROM CSCBP_<Cluster name>_NUM_VARIABLE
    IN ('<RD area name 1 which you want to delete>,<RD area name 2 which you want to
delete>,・)
WHERE ProcessID = <Process instance identifier> WITHOUT LOCK NOWAIT;

SELECT * FROM CSCBP_<Cluster name>_BOOL_VARIABLE
    IN ('<RD area name 1 which you want to delete>,<RD area name 2 which you want to
delete>,・)
WHERE ProcessID = <Process instance identifier> WITHOUT LOCK NOWAIT;

SELECT * FROM CSCBP_<Cluster name>_MSG_VARIABLE
    IN ('<RD area name 1 which you want to delete>,<RD area name 2 which you want to
delete>,・)
WHERE ProcessID = <Process instance identifier> WITHOUT LOCK NOWAIT;

SELECT * FROM CSCBP_<Cluster name>_MSG_RELATION
    IN ('<RD area name 1 which you want to delete>,<RD area name 2 which you want to
delete>,・)
WHERE ProcessID = <Process instance identifier> WITHOUT LOCK NOWAIT;
```

(ii)Update value of SplitKey column and re-enter in the table.

Change value of SplitKey column in such a way that next it is allocated to next RD area to be deleted (For example: when breakup of RD area is per 1 month and current target deletion is 12 months ('12'), change it to 1 ('01'), issue INSERT statement.

For this, issue following SQL for all acquired data, you need to re-register in such a way that data to be stored is allocated to other RD area. Issue INSERT statement only with number records acquired in SELECT statement of procedure (i)

```
INSERT INTO CSCBP_<Cluster name>_PROCESS
(ProcessID,ProcessDefinitionName,ProcessDefinitionVersion,State,ChangeCount,
StartTime,EndTime,CSCServerName,SplitKey)
VALUES (<Data except for data in SplitKey example acquired in (i)>, '01');

INSERT INTO CSCBP_<Cluster name>_ACTIVITY
(ProcessID,ActivityNumber,ActivityDefinitionName,ActivityKind,ParentNumber,
ScopeNumber,RepeatNumber,State,FirstChildNumber,LastChildNumber,StartTime,EndTime,
WaitTime,SplitKey)
VALUES (<Data except for data in SplitKey example acquired in (i)>, '01');

INSERT INTO CSCBP_<Cluster name>_LINK
(ProcessID,LinkDefinitionName,RepeatNumber,State,SplitKey)
VALUES (<Data except for data in SplitKey example acquired in (i)>, '01');

INSERT INTO CSCBP_<Cluster name>_CORRELATIONSET
(ProcessID,ProcessDefinitionName,ProcessDefinitionVersion,ScopeDefinitionName,
ScopeNumber,CorrelationSetName,CorrelationSetValue,State,SplitKey)
VALUES (<Data except for data in SplitKey example acquired in (i)>, '01');

INSERT INTO CSCBP_<Cluster name>_STR_VARIABLE
(ProcessID,ScopeNumber,VariableName,VariableValue,SplitKey)
VALUES (<Data except for data in SplitKey example acquired in (i)>, '01');
```

```
INSERT INTO CSCBP_<Cluster name>_NUM_VARIABLE
(ProcessID,ScopeNumber,VariableName,VariableValue,SplitKey)
VALUES (<Data except for data in SplitKey example acquired in (i)>, '01');

INSERT INTO CSCBP_<Cluster name>_BOOL_VARIABLE
(ProcessID,ScopeNumber,VariableName,VariableValue,SplitKey)
VALUES (<Data except for data in SplitKey example acquired in (i)>, '01');

INSERT INTO CSCBP_<Cluster name>_MSG_VARIABLE
(ProcessID,ScopeNumber,VariableName,VariableValue,SplitKey)
VALUES (<Data except for data in SplitKey example acquired in (i)>, '01');

INSERT INTO CSCBP_<Cluster name>_MSG_RELATION
(MessageID,ProcessID,ActivityNumber,SendOrReceive,
AsynchronousMessagingID,SplitKey)
VALUES (<Data except for data in SplitKey example acquired in (i)>, '01');
```

Note #

- When you are updating 1-9 months, put 0 before the number as shown in "01".
- Do not change value other than value in SplitKey column.
- Match the value of SplitKey column of similar Process instance identifier.

Note that, when you invoke subsequent process after re-executing stored process instance and specifying correlation set, the value of SplitKey column in data newly stored in database is the value similar to value of SplitKey which is INSERT in this procedure and not the value in "month (GMT) when process instance was started"

(iii) Commit transaction

If you execute large number of processes when automatic commit is disabled, there is possibility that shortage of resources may occur. Issue commit of transaction periodically (Example: per 100 Process instance identifier), release resources.

4. Abort connection.

(b) Procedure to delete execution log

The deletion procedure per RD area is as follows:

1. Block RD area wherein the data to be deleted is stored.
   Execute following command for RD area for index and RD area for data both.

```
pdhold -r <RD area name>
```

2. Unloading the data stored in RD area which is to be deleted.
   This process is optional. It is performed only when you want to take back up of the data stored in RD area.
   Perform unload per table as shown in following format.

```
pdrorg -k unld -t <Table name>#1 -r <RD area name for data> <Control information file name>#2
```

Note #1

Specify following names in table name.

CSCBP_<Cluster name>_PROCESS
CSCBP_<Cluster name>_ACTIVITY
CSCBP_<Cluster name>_LINK
CSCBP_<Cluster name>_CORRELATIONSET
CSCBP_<Cluster name>_STR_VARIABLE
CSCBP_<Cluster name>_NUM_VARIABLE
CSCBP_<Cluster name>_BOOL_VARIABLE
CSCBP_<Cluster name>_MSG_VARIABLE
CSCBP_<Cluster name>_MSG_RELATION

Note #2

Describe following contents in specified control information file.

In HiRDB/Single Server

```
unload < path of file that unloads data of each table>
```

In HiRDB/Parallel Server

```
unload <Backend server name>:< path of file that unloads data of each table>
```

For details on storing the data unloaded in pdrorg to table and method of fixing, see description of pdrorg output binary format file in "HiRDB Version 9 Command reference (For Windows(R))" or "HiRDB Version 9 Command reference (For UNIX(R)".

3. By deleting the data stored in RD area, load data with 0 cases. Loading method is as follows. The index information matching with data contents is also loaded. See contents of error information file which is output and confirm that error has not occurred.

```
pdload -d CSCBP_<Cluster name>_PROCESS <Control information file name>
pdload -d CSCBP_<Cluster name>_ACTIVITY <Control information file name>
pdload -d CSCBP_<Cluster name>_LINK <Control information file name>
pdload -d CSCBP_<Cluster name>_CORRELATIONSET <Control information file name>
pdload -d CSCBP_<Cluster name>_STR_VARIABLE <Control information file name>
pdload -d CSCBP_<Cluster name>_NUM_VARIABLE <Control information file name>
pdload -d CSCBP_<Cluster name>_BOOL_VARIABLE <Control information file name>
pdload -d CSCBP_<Cluster name>_MSG_VARIABLE <Control information file name>
pdload -d CSCBP_<Cluster name>_MSG_RELATION <Control information file name>
```

In specified control information file, describe following contents. Arrange for the file with data in which there are 0 cases (Contents are empty), to be specified in <Data file path>.

For HiRDB/Single Server

```
source <RD area name for data> <Data file path>
```

For HiRDB/Parallel Server

```
source < RD area name for data > <Backend server name>:< Data file path >
```

4. Release the lock in RD area

Execute following command and release the lock of RD area which was implemented in step 1.

```
pdrels -r <RD area name>
```

Issue following SQL and confirm if RD area units are deleted correctly with this procedure:

```
SELECT count(*) FROM CSCBP_<Cluster name>_PROCESS IN ('<RD area name 1 which you want to
delete>,<RD area name 2 which you want to delete>,･) WITHOUT LOCK NOWAIT;
```

6.1.5 Re-executing process instances

You can re-execute each process instance whose execution was cancelled due to failure, such as the shutdown of a machine on which the Cosminexus system is running, or a service module call error.

Also, you can re-execute multiple process instances in batch mode. To perform batch re-execution of the process instance execution logs, you can use commands only.

Furthermore, you can request a re-execution of the business process from the service requester to re-execute the business process.

for details on conditions in which you can re-execute process instance and re-executing business process using service requester, see "3.5 Re-executing a business process" in "BPM/ESB Service Platform Overview".

! Important note

As per the time lag that occurs between the time for searching execution log using screen or command till its re-execution, status of process instance execution log displayed in search result differs from status of status of real process instance execution log. In this case, even if you perform re-execution for process instances with status "Completed" or "Completed with fault", actually the re-execution fails and does not get implemented. For this, acquire latest information and perform re-execution.

(1) Using screens to re-execute process instances

(a) Re-executing process instances individually

The procedure to re-execute process instances one by one using screens is as follows:

1. Search the process instances.
   The result is displayed on the search results list.
2. From the search results list, select a process instance whose status is [Executing] or [Error occurred], and then click the [Activity Information]. button.
   The list of detailed information displays the activity information.
3. Confirm that activity appropriate for condition required for re-execution of process instance is included from detailed information list.
   The following table describes the condition wherein you can re-execute the process instance.

   Table 6–1: Table condition wherein re-execution of process can be performed

Activity type	Status of activity instance
Invoke service	Executing
	Error occurred
Standby	Executing
Scope	Executing (Standby)
	Error occurred
	Completed (Standby)
Response	Completed (Standby)

4. Click the [Reexec] button.
   A dialog box confirming re-execution of the process instance is displayed.
5. 5. Click the [OK] button.
   The process instance is re-executed and a dialog box appears showing the result of process instance re-execution.
6. 6. Click the [OK] button
   The list of search results is updated. This list is updated even if re-execution fails.

(b) Precautions

Do not re-execute process instances running on the HCSC server. For re-executing the process instances, first check the error contents in the response and the message logs from the HCSC server, eliminate the cause of the errors, and then re-execute process instances.

(2) Using commands to re-execute process instances

(a) Re-executing process instances individually

The procedure to re-execute process instances one by one using commands is as follows:

1. Determine the HCSC server to be accessed.
2. Use the cscpiselect command to search for those process instances that include the following activities:
   - Invoke service activity with the status [Executing] or [Error occurred]
   - Standby activity with the status Executing
   - Scope activity with status "Executing (Standby)", "Error occurred", "Completed (Standby)"
   - Response activity with status "Completed (Standby)"
3. Identify the process ID and business process definition name for the process instance you wish to re-execute.
4. Execute the following command to re-execute the process instance:

```
cscpireexec -user <Login user ID> -pass <Login password> -csc <HCSC server name> {-
processid <Process ID>|-processidfile < Process ID file name>}# {-processnamefile <Business
process definition file name> | -processname < Business process definition name >#
```

Note #

Specify one of them.

(Example): Enter the command using the following conditions to re-execute the process instance:

- Process ID to be re-executed: J2EEServer_010210084218_Hello business process_1237946140968_3843192274_138
- Business process definition name: Hello business process
- HCSC server to be accessed: HCSC

Command

```
cscpireexec -user <Login user ID> -pass <Login password> -csc HCSC -processidfile
process_id.txt -processname Hello business process
```

Contents of process_id.txt

```
J2EEServer_010210084218_Hello business process_1237946140968_3843192274_138
```

Output result

```
KEOS52076-I cscpireexec will now start.
KEOS52040-I Communication with the HCSC-Server, to re-execute a process instance, will now start.
KEOS52041-I Communication with the HCSC-Server, to re-execute a process instance, is complete.
ProcessID,ProcessDefinitionName,Result,ErrorMessage
J2EEServer_010210084218_HelloBusinessProcess_1237946140968_3843192274_138,HelloBusinessProcess,Success,
KEOS52077-I cscpireexec ended normally.
```

For details on cscpireexec command "cscpireexec (Re-executing process instance) " in "Service Platform Reference Guide".

(b) Re-executing process instances in batch mode by specifying the business process definition name

The procedure to re-execute process instances in a batch mode by specifying the business process definition name as follows:

1. Determine the HCSC server to be accessed.
2. Identify the business process definition name for the process instances you intend to re-execute.
3. Execute the following command to re-execute the process instance:

```
cscpireexec -user < Login user ID > -pass < Login password > -csc <HCSC server name> {-
processname <Business process definition name>|-processnamefile < Business process
definition file name >}#
```

Note #

Specify one of them.

(Example): Enter the command using the following conditions to re-execute the process instance in batch mode:

- Business process definition name: Hello-business-process
- HCSC server to be accessed: HCSC

Command

```
cscpireexec -user <Login user ID> -pass <Login password> -csc HCSC -processname Hello
business process
```

For details on cscpireexec command, see "cscpireexec (re-executing business process) " in "Service Platform Reference Guide".

(c) Re-executing all the targeted process instances in the batch mode

The procedure to re-execute all the target process instances in the batch mode is as follows:

1. Determine which HCSC server is to be accessed.
2. Execute the following command to re-execute the process instance:

```
cscpireexec -user <Login user ID> -pass <Login password> -csc <HCSC server name> -all
```

(Example): Enter the command using the following conditions to re-execute all the target process instances in the batch mode:

- HCSC server to be accessed: HCSC

Command

```
cscpireexec -user < Login user ID > -pass < Login password > -csc HCSC -all
```

For details on cscpireexec command, see "cscpireexec (re-executing business process) " in "Service Platform Reference Guide".

(d) Re-executing process instances in batch mode specifying HCSC server

The procedure to specify HCSC server targeted to re-execute, and re-executing targeted process instances in batch mode is as follows:

1. Determine which HCSC server is to be accessed.
2. Execute the following command to re-execute the process instance:

```
cscpireexec -user <Login user ID> -pass <Login password> -csc <HCSC server name> -all -
targetcsc <Name of the HCSC server targeted for re-execution> [-status <status of activity
which is condition for re-execution>]
```

(Example 1): Enter command using following condition to re-execute targeted process instances in batch mode

- HCSC server to be accessed: HCSC1
- HCSC server targeted for re-execution: HCSC2

Command

```
cscpireexec -user <Login user ID> -pass <Login password> -csc HCSC1 -all -targetcsc HCSC2
```

For details on cscpireexec command, see "cscpireexec (re-executing business process) " in "Service Platform Reference Guide"

(Example 2): Enter command using following condition to re-execute targeted process instances in batch mode

- HCSC server to be accessed: HCSC1
- HCSC server targeted for re-execution: HCSC2
- Status targeted for re-execution: "Executing", "Executing (Standby)", "Completed (Standby)"

Command

```
cscpireexec -user < Login user ID > -pass < Login password > -csc HCSC1 -all -targetcsc
HCSC2 -status executing,executingwait,completedwait
```

(e) Precautions

Do not re-execute process instances running on the HCSC server. For re-executing the process instances, first check the error contents in the response and the message logs from the HCSC server, eliminate the cause of the errors, and then re-execute process instances.

If the process instance for re-execution is not present, command ends abnormally.

(3) Output of response message when re-executing process instance

Result of re-execution of process instance receives response message from process instance even if result is successful or failure due to SOAP fault. In this case, set contents shown below in HCSC-Manager definition file, you can output response message to file.

```
cscmng.pireexec.response.dir= response message storage directory
cscmng.pireexec.response.encoding= response message storage character code
```

For details on creating HCSC-Manager definition file, see "*2.4.1(1) Storage directory of HCSC-Manager definition file*", for details on HCSC-Manager definition file, see "HCSC-Manager definition file" in "Service Platform Reference Guide".

Furthermore, process ID can have long character string (maximum 240 characters). If you set thorough directory in response message output directory, be careful as there is possibility that file cannot be generated. If response message file does not generate even if you perform re-execution, message is output.

(4) Information about SOAP fault

When re-execution of process instance fails due to SOAP fault, type and handling of SOAP fault information received from process instance is as follows:

- Fault code: displayed in error message
- Fault character string: displayed in error message.
- Fault generator: displayed in error message.
- Details of fault: same as response message at the time of successful re-execution, file is output to directory used for storing response message. However, output encode code is only UTF-8

6.2 Managing execution log information table

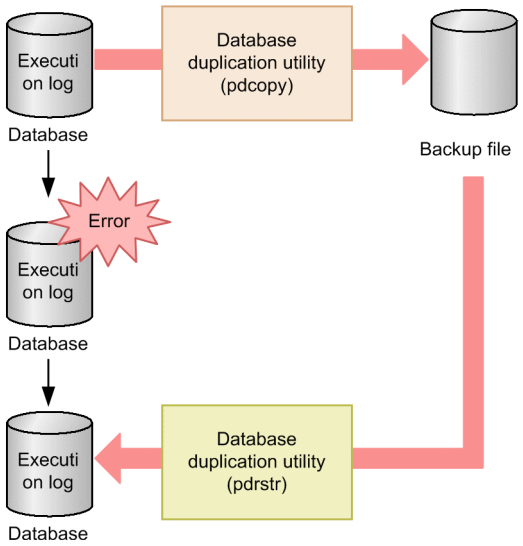
Since execution log of process instance continues to increase every day, administrator should acquire backup, delete records of execution log information table and manage.

6.2.1 Acquiring a Backup of the Execution Log Information Table

(1) Using HiRDB to acquire a backup

You can use HiRDB's database copy utility (pdcopy) to periodically acquire a backup of the execution log information table. You can also use the database recovery utility (pdrstr) to restore the database. The following figure shows database backup and recovery using HiRDB's database copy utility (pdcopy).

Figure 6–2: Database backup and recovery using HiRDB



If you use HiRDB to acquire a backup, select a backup acquisition mode using the -M option of HiRDB's database copy utility (pdcopy). The mode you select depends on whether the HCSC server is active or inactive.

- When the HCSC server is active

  Select the updatable mode (s).

  If you select the updatable mode, you can reference and update the target RDAREA during backup processing.

  You can restore the RDAREA to any synchronization point that falls after backup acquisition. To restore the database, you need the backup copy and the system log that was obtained after the synchronization point immediately before backup acquisition.

- When the HCSC server is inactive (such as during maintenance)

  Select the reference-possible mode (r) or reference/update-impossible mode (x).

  If you select the reference-possible mode (r), you can reference the RDAREA subject to backup during backup acquisition, but you cannot update it.

  If you select the reference/update-impossible mode, you can neither reference nor update the RDAREA subject to backup during the backup acquisition. Before acquiring the backup, you must use the HiRDB command pdhold -c to place the target RDAREA in shutdown and closed status.

  By using the backup acquired with these modes, you can restore the database to the point at which the backup was acquired. If you use the system log, you can restore the database to any desired synchronization point that falls after backup acquisition.

For details about HiRDB's database copy utility (pdcopy), database recovery utility (pdrstr), and backup acquisition modes, see the manual *HiRDB Description*.

(2) Acquiring a backup using Oracle

You can use Oracle's Recovery Manager (RMAN) function to periodically back up the execution log information table. This function enables you to obtain a differential backup from the previous backup. For details, see the documentation provided with the product.

6.2.2 Operations involving a backup of the execution log information table

Execution log increases every time process instance is executed, capacity of database is pressed. When you acquire backup of execution log information while HCSC server is operating, the records in execution log information table remain even after acquiring the backup.

Therefore, you can deal with depletion of disc capacity and increase in database by acquiring backup of table, by deleting execution log, and reorganizing table of database periodically. The procedure is as follows:

1. Acquire difference backup of execution table using database copy utility (pdcopy) of HiRDB.
2. Delete execution log of process instance using cscpidelete command.
3. Reorganize the table of database using database reorganization utility (pdrorg) of HiRDB.

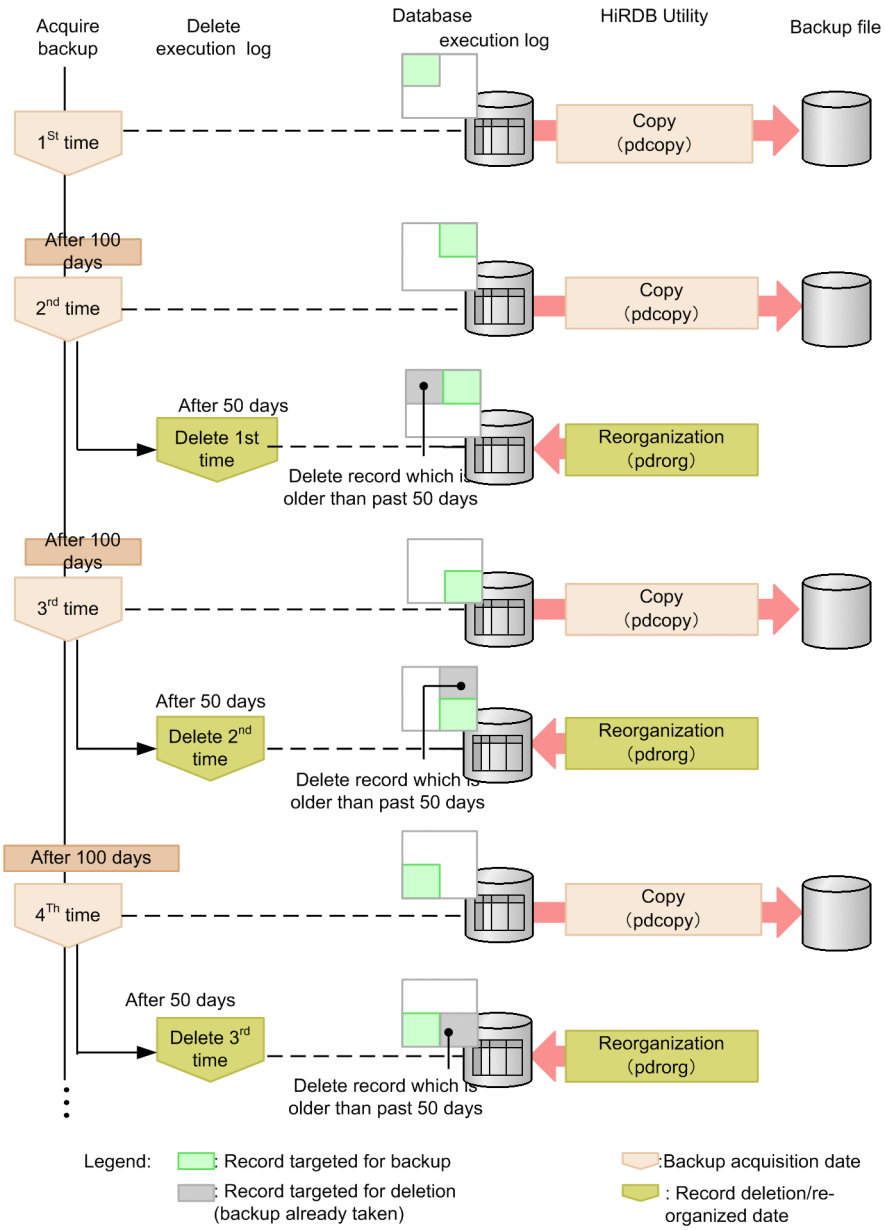
   If you repeat addition and deletion of execution log, storage efficiency of data becomes poor and performance degrades. In order to prevent this, reorganize the table periodically using pdrorg command (Database reorganization utility). Note that, you need to re-create the index as well since index is defined in execution log information table.

   For details on reorganization of HiRDB table, see manual "HiRDB System Operation Guide" and for details on pdrorg command, see manual "HiRDB Command Reference".

Because backup and deletion intervals depend on the nature of the user application, the administrator must handle these periodic operations.

The following figure shows an example of operations involving a backup of the execution log information table and deletion of records:

Figure 6–3: Examples of operations involving a backup of the execution log information table and deletion of records



Description

1. Acquire a backup of the execution log information table (first backup).
2. At the second backup, acquire a differential backup from the first backup.
3. Use the execution log search command to log whose date and time fall before a specified date and time, and the process instances that are in a specified status that you intend to delete (in this example, the command searches for records that are more than 50 days old).
4. After acquiring a backup, use the execution log deletion command to delete the old records (in this example, the command deletes records that are more than 50 days old).
5. Reorganize the table.
6. At the third backup, acquire a differential backup from the second backup.
7. Use the execution log search command to find log whose date and time fall before a specified date and time, and execution log of process instances that are in a specified status that you intend to delete (in this example, the command searches for records that are more than 50 days old).

8. After acquiring a backup, use the execution log deletion command to delete the old records (in this example, the command deletes records that are more than 50 days old).
9. Reorganize the table.
10. At the fourth backup, acquire a differential backup from the third backup.
11. Use the execution log search command to find the log whose date and time fall before a specified date and time, and the process instances that are in a specified status that you intend to delete (in this example, the command searches for records that are more than 50 days old)
12. After acquiring a backup, use the execution log deletion command to delete the old records (in this example, the command deletes records that are more than 50 days old).

7 Troubleshooting

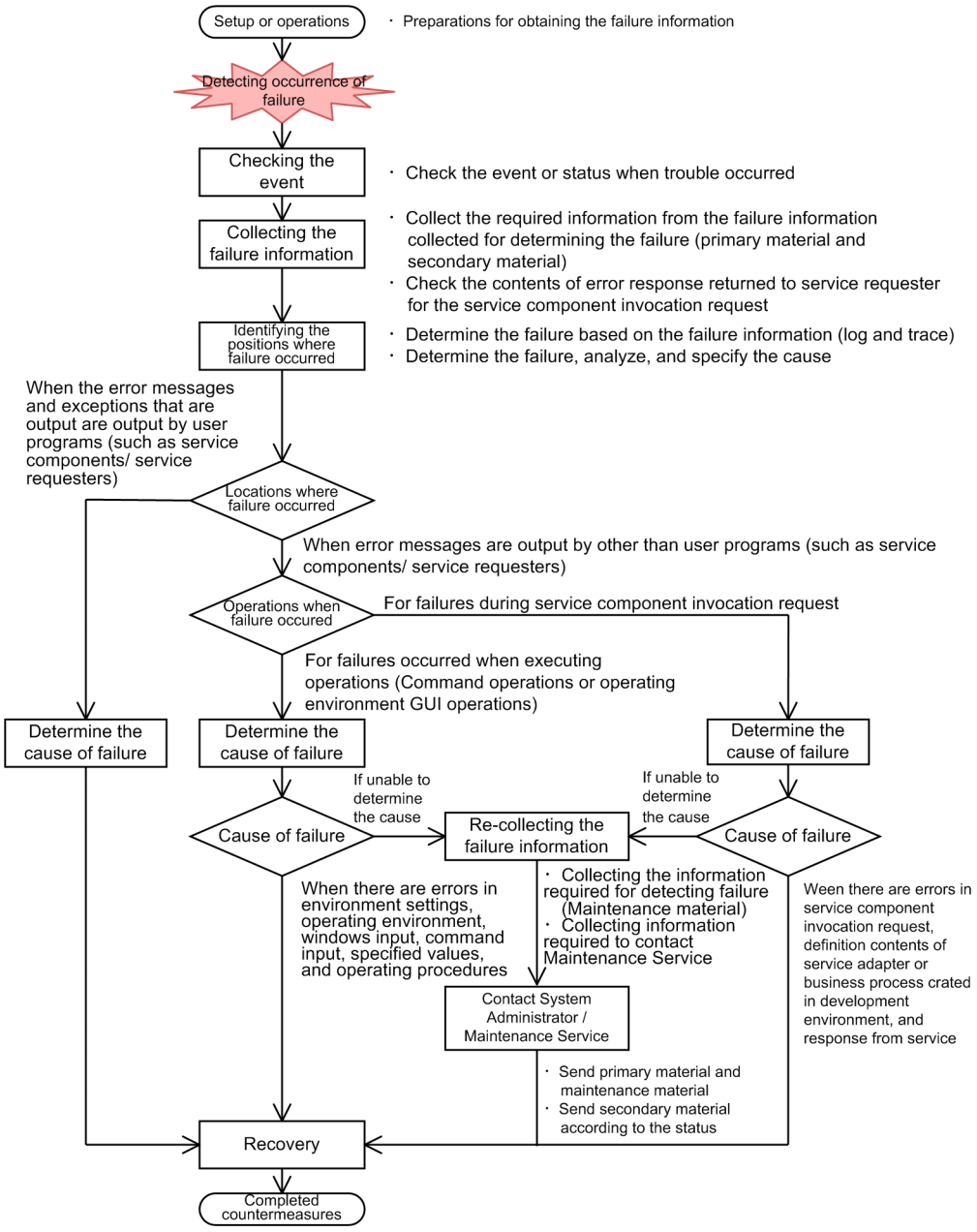
This chapter discusses troubleshooting, including what kinds of information can be acquired in the event of failures that may occur during system configuration and operations, and how to handle failures.

In UNIX environment, substitute "\" in the directory to "/".

7.1 Troubleshooting Procedures

Specify the reasons for failure in the procedure of the following figure, when there is an error in setting up the environment due to failure in setting up or operating the system:

Figure 7–1: Troubleshooting



The description of each procedure is as follows:

1. Confirming the phenomenon

   Confirms as to what phenomenon occurred in which type of environment for error analysis.

   For details about the items to be checked, see *7.2 Information required for investigating errors*.

2. Collecting the error information

   Collects the necessary error information (primary data and secondary data) from the error information (such as log to trace) acquired for error investigations. The primary data is used for primary detection and investigation of

errors. The secondary data is the error information used depending on the error contents determined in the primary detection.

For details about the necessary data, see *7.2 Information required for investigating errors*. For details about how to acquire the error information, see *7.3 Acquiring failure information*. Please note that there are items that must be acquired always and items that require acquisition settings depending on the type of error information.

3. Specifying the places where error occurred

   Checks the contents of collected error information and performs error investigations and specifies the places where error occurred. As a result of error investigations, when an error message or exception is output by user programs such as service requester or service components, you must consult the system developer, and the system developer must specify the reasons for error and restore the user programs.

   Alternatively, you must detect the reasons as to whether error occurred in service components invoking requester while executing the operations (command operations or operations from screens of operating environment).

   For details about the viewpoints (Output format) on log and trace output by HCSC server and HCSC-Manager, see *7.4 Types of error information*. For details about the error information output by other prerequisite products, see the manual of each product.

4. Specifying the reason for error

   Specifies the reason for error from the places where error occurred or operations when error occurred.

5. Recollecting the error information

   Collects the maintenance data required to contact the system administrator or Maintenance Service when the reason for error cannot be specified. For details, see *7.2 Information required for investigating errors*.

6. Contact the system administrator or Maintenance Service

   Contact the system administrator or Maintenance Service and send the primary data or maintenance data. Send the secondary data depending on the status of the error occurred.

7. Restoration

   Eliminate the reason (cause) for error and perform restoration so that normal operations are performed and then start the operations again.

7.2 Information required for investigating errors

This section describes the types of data required for checking the status when error occurred:

- Information required for investigating errors

  The data that must be acquired differs depending on the type of the error. This point describes the types of errors assumed on Service Platform and the list of data that must be acquired according to the type of error.
- Information required when you contact the system administrator or Maintenance Service

  Depending on the error contents, you must contact the system administrator or Maintenance Service. Maintenance Service is the inquiry contact as per the purchasing contract.

  When you contact the Maintenance Service, you might be required to acquire the data in addition to the information required for error investigation.

7.2.1 Information required for investigating errors

(1) Checking the phenomenon

In case of failure, check and consolidate the status as to in which environment what phenomenon occurred. The following table describes the items to be checked in case of failure:

Table 7–1: Items to be checked in case of failure

No.	Item to be checked		Machine on which error is detected				
			Machine on which HCSC server is running	Machine on which operating environment is running	Machine on which service requester is running	Machine on which service component is running	Machine on which database is running
1	Basic points	Time when failure occurred	Confirm as to when (from when) the error occurred.				
2		Operation executed just before failure occurrence	Confirm as to which operations were performed when the error occurred.				
3		Machine on which error was detected	Confirm as to on which machine the error was detected. 1. Machine on which HCSC server is running 2. Machine on which operating environment is running 3. Machine on which service requester is running 4. Machine on which service component is running 5. Machine on which database is running				
4		Error contents	Specifically mention the type of phenomenon that occurred.				
5	Operating environment	Version of Service Platform	Y	--	--	--	--
6		J2EE server product name and version	--	--	Y	Y	--
7		Database product name and version	--	--	--	--	Y
8		OS type and version	Y	Y	Y	Y	Y
9		Number of processors	Y	Y	Y	Y	Y
10		Memory	Y	Y	Y	Y	Y
11		Virtual memory	Y	Y	Y	Y	Y
12		Java version	Y	Y	Y	Y	Y

No.	Item to be checked		Machine on which error is detected				
			Machine on which HCSC server is running	Machine on which operating environment is running	Machine on which service requester is running	Machine on which service component is running	Machine on which database is running
13	Operating environment	Patch applicable status	Y	Y	Y	Y	Y
14	Reproducibility	Reproducibility	Confirm whether it can be reproduced.				
15		Occurrence frequency	In the case of reproducibility, confirm the frequency of error occurrence.				
16	Configuration changes	Whether changed when occurred	Confirm whether the coding or environment was changed before occurrence of corresponding error.				
17		Contents of changed places	If there are any changes, then specifically mention the changed contents.				

Legend:

Y: Must be confirmed.

--: Confirmation not required.

(2) Collecting the error information

The information described in Table 7-2 for each error type is required as data for investigations in Service Platform system.

Note that there are items that require settings for acquiring error information. For details about error information acquisition, see *7.3 Acquiring failure information*. For details about the place where acquired error information is output, see *7.3 Acquiring failure information* and *7.4 Types of error information*.

The information for which the acquisition of error information is not set is the information that is not required for error investigations or inquiry. However, the acquisition of this information might be required depending on the status of error investigations. The information required for error investigations differ depending on the places of error occurrence.

Table 7–2: Information acquired for error investigation

No.	Information that can be acquired		Error type		
			When error message or exception is output by user program	When error occurs in service component invoking request	When error occurs in operations (command operations or operations from screens of operating environment)
1	Material for the Service Platform	*Message log*	P	P	P
2		*Request trace*	P	P	--
3		*Performance analysis trace*	--	S	--
4		*User message trace*	S	S	--

No.	Information that can be acquired			Error type		
				When error message or exception is output by user program	When error occurs in service component invoking request	When error occurs in operations (command operations or operations from screens of operating environment)
5	Material for the Service Platform	*Definition information*	HCSC server configuration definition file	--	P	P
6			HCSC server setup definition file	--	P	P
7			HCSC server runtime definition file:	--	P	P
8			HCSC-Manager definition file	--	P	P
9			The HCSC-Manager command definition file	--	P	P
10			HCSC-Messaging command definition file	--	P	P
11			Service-information change definition file	--	S	S
12			User-defined reception runtime definition file	--	S	S
13			SOAP fault operation definition file	--	S	S
14			Client definition file	--	S	S
15	*Material for J2EE server*	Logs of J2EE server#, redirector, and server management commands		P	P	S
16		Logs of Administration Agent, Management Agent, and Management Server (Integrated log)		P	S	P
17		DABroker Library log		S	S	S
18		DB Connector (Activity log of resource adapter)		P	P	P
19		EJB client application log		P	P	--
20		User log		P	S	--
21		Definition information	Setup file of Component Container	S	P	P
22			Setup file of Manager	S	P	P
23			DB Connector property information setup in `dbcon-xadisplayname`	S	P	S
24			DB Connector property information setup in `dbcon-nodisplayname`	S	S	P
25	*Material for Reliable Messaging*	Start stop message log		--	S	P
26		Message log for J2EE server#		S	P	P

No.	Information that can be acquired			Error type		
				When error message or exception is output by user program	When error occurs in service component invoking request	When error occurs in operations (command operations or operations from screens of operating environment)
27	*Material for Reliable Messaging*	Method trace		S	P	P
28		Line trace		S	P	P
29		Definition information	Setup information of Reliable Messaging configuration property	S	P	P
30	*Data of SOAP Communication Infrastructure*	Trace		S	P	--
31		Application log		S	P	--
32		Definition information	Definition file (SOAP Communication Infrastructure)	S	P	--
33			Server definition files (SOAP Communication Infrastructure)	S	P	--
34	*Data of JAX-WS engine*	Trace		S	P	--
35		Application log		S	P	--
36		Definition information	Common definition file (JAX-WS engine)	S	P	--
37	*Log and trace of HTTP Server*			P	S	--
38	*Error information of database*	When HiRDB is used	HiRDB log (Including HiRDB definition information)	--	S	S
39			HiRDB client log and trace	--	S	S
40			Exception log and trace of HiRDB Type4 JDBC driver	--	S	S
41		When Oracle is used	Oracle log	--	S	S
42			Oracle JDBC Thin Driver log	--	S	S
43	*Error information of JavaVM*	JavaVM output message log		--	S	S
44		JavaVM thread dump		--	S	S
45		Log of garbage collection of JavaVM		--	S	S

Legend:

P: Primary material

S: Secondary material

--: Not required

#

The default directory to which the J2EE server outputs log data is *Service-Platform-installation-directory*`\CC\server\public\ejb\`*J2EE-server-name*`\logs`. Hereafter, this directory is called the *J2EE server's log output directory*.

You can change this directory by using the `ejb.server.log.directory` key in the `usrconf.cfg` file (option definition file for the J2EE server).

7.2.2 Information required to contact the system administrator or the maintenance service

Contact the system administrator or Maintenance Service when error occurs and in case of following conditions:

- When the "Contact Maintenance Service" option is available in the actions to deal with the output error message
- When the cause of failure is not understood even after investigations
- When actions are taken as per the contents or the actions written in the error message, and still the problem cannot be resolved

Regarding the information required to contact the system administrator or Maintenance Service, the information described in Table 7-3for each type of error is also required in addition to the information described in " *7.2.1 Information required for investigating errors*". The information for which the acquisition of error information is not set is the information that is not required for error investigations or inquiry. However, you may be required to acquire this information depending on the status of error investigations. The information required to contact the system administrator or Maintenance Service differ depending on the locations of error occurrence.

The default directory where the log is output by the J2EE server is<Installation directory of Service Platform>\CC \server\public\ejb\<J2EE server name>\logs. Hereafter, this directory is mentioned as "Log output directory of J2EE server"

You can change the directory of log output by J2EE server with the ejb.server.log.directory key of usrconf.cfg (Option definition file of J2EE server).

Table 7–3: Information required to contact the system administrator or Maintenance Service

No	Information to be acquired			Failure type		
				When error message or exception is output by the user program	For failures during service component invocation request	For failures during the execution of operation (like command operations or operations from screens of the operating environment)
1	Service platform documents	*Exception log*		Y	Y	Y
2		*Maintenance log*		-	-	Y
3		*Installation log*		-	-	Y
4		*Method trace*		Y	Y	Y
5		*Maintenance information*	HCSC server repository information	-	Y	Y
6			HCSC-Manager maintenance information	Y	Y	Y
7			HCSC server maintenance information	Y	Y	Y
8	J2EE server documents	Maintenance log[#1]		Y	Y	Y

No	Information to be acquired		Failure type		
			When error message or exception is output by the user program	For failures during service component invocation request	For failures during the execution of operation (like command operations or operations from screens of the operating environment)
9	SOAP communication infrastructure documents	Maintenance log[#2]	Y	Y	Y
10	JAX-WS engine documents	Maintenance log[#3]	Y	Y	Y
11	JavaVM failure information	Memory dump	Y	Y	Y

Legend:

Y: Required.hosyujoho

-: Not required.

Note#1

For details on the maintenance log of the J2EE server, see "Application Server Maintenance and Migration Guide ".

Note#2

The maintenance log of SOAP Communication Infrastructure is output to <Log output directory of J2EE server>\WS \maintenance. For details on how to acquire the information when a failure other than log occurs,

see "14.2 Documents to be acquired when a failure occurrs" in "Application Server SOAP Application Development Guide".

Note#3

The maintenance log for the JAX-WS engine is output to <Product working directory>\ejb\<server name>\log\CJW \maintenance. For details on how to acquire the information when a failure other than log occurs, see "39.2 Documents to be acquired when a failure occurrs" in "Application Server Web Service Development Guide".

7.3 Acquiring failure information

Select any of the following methods to rotate the log file or the trace file:

Rotation method	Description
Wraparound mode(default)	Numbers of files are added to the file name. **(example) When the log file name is "hntrN.log" and the number of files is"2"** Log file name: "hntr1.log", "hntr2.log"
Shift mode	The file name is fixed, and the numbers of files are added to the name of backup files. **(example) When the log file name is "hntr.log", and the number of files is"2"** Log file name: "hntr.log" (fixed) Backup file name of the log file:"hntr1.log","hntr2.log"

There are two timings for switching the output destination file:

- Switching with the file size
- When the file size reaches the specified value, you can switch the output destination file.
- Switching with the file size or at a timing
  If either of the following conditions is met, you can switch the output destination file.
  - The specified time has been reached.
  - The specified file size has been reached.

The method that can be used differs depending on the log type as follows:

Log type	Rotation method		Method to switch the output destination file	
	Wraparound mode	Shift mode	Switching with file size	Switching with the file size or at a timing
HCSC-Manager log	A	N	A	N
Integrated message log	A	Y	A	Y
Activity log of J2EE server	A	Y	A	Y
Request trace	A	Y	A	Y
Performance analysis trace	-	-	-	-
User message trace	A	Y	A	Y
Maintenance log	A	Y	A	Y

Legend:
A: Can use (default).
Y: Can use.
N: Cannot use.
-: Not applicable.

For the method to rotate the log file or the trace file, and the timings to switch the output destination file, see"3.2.1 Contents which you can set " in "Application Server Maintenance and Migration Guide".

7.3.1 How to acquire log or trace output by Cosminexus Service Platform

This subsection describes about how to acquire the message logs, trace, and various information output by Cosminexus Service Platform. For details about the types of error information output by Cosminexus Service Platform, see *7.4 Types of error information*.

(1) Collecting the message log

The message log is output always.

The file size and number of files that are output by message log can be changed as and when required. For details about commands, see *7.4.1 Message log*.

(a) HCSC-Manager log

Specify the following parameters in the HCSC-Manager definition file:

- `cscmng.log.message.filesize=`*message-log-file-size*
- `cscmng.log.message.filenum=`*message-log-number-of-files*

For details about the HCSC-Manager definition file, see *HCSC-Manager definition file* in the manual *Cosminexus Service Platform Reference*.

(b) Cosminexus integrated message log

Specify the file size and number of files for integrated message log in `manager.cfg` (Manager log setup file). For details about `manager.cfg`, see *10.10 manager.cfg (Manager setup file)* in the manual *Cosminexus Application Server Server Definitions*.

(c) Cosminexus J2EE server activity log

Specify the file size and number of files for J2EE server activity logs in `usrconf.properties` (User property file for J2EE server). For details about `usrconf.properties`, see *2.4 usrconf.properties (User property file for J2EE servers)* in the manual *Cosminexus Application Server Server Definitions*.

(2) Request trace

Specify whether the request trace can be collected in the following properties of HCSC server runtime definition file while acquiring request trace.

Furthermore, you can change the output destination path, file size, and number of files.

- `requesttrace=`*whether-or-not-request-trace-is-to-be-collected* (specify `ON`)
- `requesttrace-filepath=`*path-of-request-trace-output-destination*
- `requesttrace-filesize=`*size-of-request-trace*
- `requesttrace-filenum=`*request-traces-count*

For details about request trace see *7.4.2 Request trace*.

(3) Performance analysis trace

The collection method and output destination of the performance analysis trace file are common to the entire Cosminexus system. For details about the performance analysis trace, see *7.4.3 Performance Analysis Trace*. For details about how to acquire the performance analysis trace file and output destination, see *7.3 Performance analysis trace file* in the manual *Cosminexus Application Server Function Guide - Maintenance, Migration, and Compatibility*.

(4) User message trace

Specify whether the user message trace can be collected in the following properties of HCSC server runtime definition file while acquiring user message trace:

- `telegramtrace=` Whether user message trace is collected or not (Set as ON)

The output destination path, file size and number of files can be changed in the following properties:

- `telegramtrace-filepath=` User message trace output destination path
- `telegramtrace-filesize=` User message trace file size

- `telegramtrace-filenum=` Number of user message trace files
- `telegramtrace-trigger=` Timing of user message trace output

For details about the user message trace, see *7.4.4 User message trace*.

(5) Definition information

A definition set in Cosminexus Service Platform is required for error investigations. The following table describes about the definition file of Cosminexus Service Platform. For details about the definition, see *6. Definition Files* in the manual *Cosminexus Service Platform Reference*.

(6) How to acquire maintenance information

This section describes how to acquire the maintenance information required to contact the system administrator or Maintenance Service. For details about the maintenance log and trace, see *7.4.5 Maintenance log and trace*.

(a) Exception log

The exception log is output always. You can change the file size and number of files that are output.

For details about the exception log, see *7.4.5(1) Exception log*.

(b) Maintenance log

The maintenance log is output always. You can change the file size and number of files that are output for maintenance log.

Specify the following parameters in the HCSC-Manager definition file:

- `cscmng.log.maintenance.filesize=`*maintenance-log-file-size*
- `cscmng.log.maintenance.filenum=`*maintenance-log-number-of-files*

For details about the HCSC-Manager definition file, see *HCSC-Manager definition file* in the manual *Cosminexus Service Platform Reference*.

(c) Installation log

Output always.

(d) Method trace

A method trace is output always. To perform method trace, you must determine its output destination, file size, number of files, and output level. Specify the following properties in the HCSC server runtime definition file:

Specify the following properties in the HCSC server runtime definition file:

- `methodtrace-filepath=`*path-of-method-trace-output-destination*
- `methodtrace-filesize=`*size-of-method-trace-file*
- `methodtrace-filenum=`*number-of-method-trace-files*
- `methodtrace-level=`*method-trace-output-level*

For details about the HCSC server runtime definition file, see *HCSC server runtime definition file* in the manual *Cosminexus Service Platform Reference*.

(e) Maintenance information

The following table describes the maintenance information required for error investigation:

Table 7–4: Maintenance information

Maintenance information	Output destination of data
HCSC server repository information	All the files and directories under *Service Platform installation directory*\CSC\repository[#1]
HCSC-Manager maintenance information	All the files and directories under *Service Platform installation directory*\CSC\config\manager
HCSC server maintenance information	All the files and directories under *Service Platform installation directory*\CSC\spool
	All the files and directories under *Service Platform installation directory*\CSC\system
	All the files and directories under the folder specified in hcscserver-data-filepath property of HCSC server setup definition file (When the hcscserver-data-filepath property is not specified, all the files and directories under the <*Service Platform installation directory*>\CSC\spool\msg\)[#2]

#1

When many operating and execution environments (Environment variable CSCMNG_HOME is set) are build on one machine, consider all the files and directories under %CSCMNG_HOME%\repository.

#2

This directory is required when HCSC server is setup in a configuration that does not use a database.

7.3.2 How to acquire the failure informationoutput by pre-requisite products other than Service Platform

This subsection gives an overview of how to acquire the main pre-requisite products. For details on the failure information output by the pre-requisite products other than the Service Platform, see the manual of the respective product.

From among the failure information output by pre-requisite products other than the Service Platform, the default directory for the logs output by the J2EE server is <Installation directory of Service Platform>\CC\server\public\ejb\<J2EE server name>\logs. This directory is mentioned as "Log output directory of J2EE server" hereafter. You can change the directory of the log output by the J2EE server with the ejb.server.log.directory key of usrconf.cfg (option definition file for J2EE server).

(1) How to acquire the failure information output by the J2EE server

(a) Log

When a failure occurs and it is difficult to specify the cause of failure from the log or the trace output by the Service Platform, the following failure information output by the J2EE server is required:

- Maintenance log
- Log of J2EE servers, redirectors, and server management commands
- Log of Administration Agent, Management Agent, and Management Server
- Log of DABroker Library
- DB Connector log
- Log of EJB client application
- User log
- Maintenance log

Use the following commands to acquire the failure information output by the J2EE server in a batch (can be acquired manually). When failure information is acquired in a batch, there may be information that partially overlaps with the log and the trace output by the Service Platform.

- snapshotlog command
- mngsvrutil command (specify collect snapshot in the sub command)

For details on the snapshot log command, see "snapshotlog (collecting snapshot logs) " in "Application Server Command Reference Guide". For details on the mngsvrutil command, see "mngsvrutil (management command of Management Server) " in "Application Server Command Reference Guide". For details on how to acquire the failure information output by the J2EEserver, see "Application Server Maintenance and Migration Guide".

By executing the above commands, you acquire the information in the following directories:

- <Installation directory of Service Platform>\CC\server\public\ejb*\logs\csc
- <Installation directory of Service Platform>\CC\server\public\ejb*\logs\csc\maintenance
- <Installation directory of Service Platform>\CSC\config\manager
- <Installation directory of Service Platform>\CSC\config\msg
- <Installation directory of Service Platform>\CSC\log\manager
- <Installation directory of Service Platform>\CSC\repository
- <Installation directory of Service Platform>\CSC\spool
- <Installation directory of Service Platform>\CSC\system\msg

Specify the information to be acquired in the definition file for collecting a snapshot log. If required, change the definition file used for collecting a snapshot log, and then change the information to be acquired. For details on the definition file for collecting a snapshot log, see "12.2 Definition file for collecting snapshot logs" in "Application Server Definition Reference Guide".

(b) Failure information of the J2EE server that requires preparation before starting operations

Define the type (Path) of the failure information to be acquired beforehand when you perform batch acquisition by using commands. Specify the primary delivery material that is sent immediately by mails and the secondary delivery material that is sent separately. For details, see "2.4 Types of documents that must be acquired" in "Application Server Maintenance and Migration Guide".

(c) Preference information required for failure investigation

The definitions set up in the J2EE server are required for investigating failure. The following table describes definition files other than the Service Platform:

Table 7–5: Table Definition file other than the Service Platform

Definition file	Description
Setup file of Component Container[#1]	All the files and directories under <Installation directory of Service Platform>\CC\server\usrconf\ejb\<J2EE server name>\directory
Setup file of Manager[#1]	All the files and directories under <Installation directory of Service Platform>\manager\config\directory
Property information of DB Connector set in dbcon-xadisplayname [#2]	Definition file set in "*3.1.2(8) Setting up DB Connector(When Reliable Messaging is used)*".
Property information of DB Connector set in dbcon-nodisplayname[#2]	

Note#1

For details on definitions, see "Application Server Definition Reference Guide ".

Note#2

For details on definitions, see "4.1 Connector property file" in "Application Server Application and Resource Definition Reference Guide".

(2) How to acquire the failure information output by Reliable Messaging

You can identify the cause of failure by acquiring the failure information output by Reliable Messaging when using the following reception or service adapter:

- Standard reception of asynchronous (MDB (WS-R))
- Standard reception of asynchronous (MDB (database queue))
- MDB (WS-R) adapter
- MDB (Database queue) adapter

For details on how to acquire failure information output by Reliable Messaging, see "9.1 Overview of the information output at the time of failure" in "Reliable Messaging".

(a) Messages output by Reliable Messaging

The messages output by Reliable Messaging are output to the following log. There are 2 types of logs; start and stop messages log and message log for the J2EE server. The following table lists and describes the messages output by Reliable Messaging:

Table 7–6: TableLog that becomes the output destination of messages output by Reliable Messaging

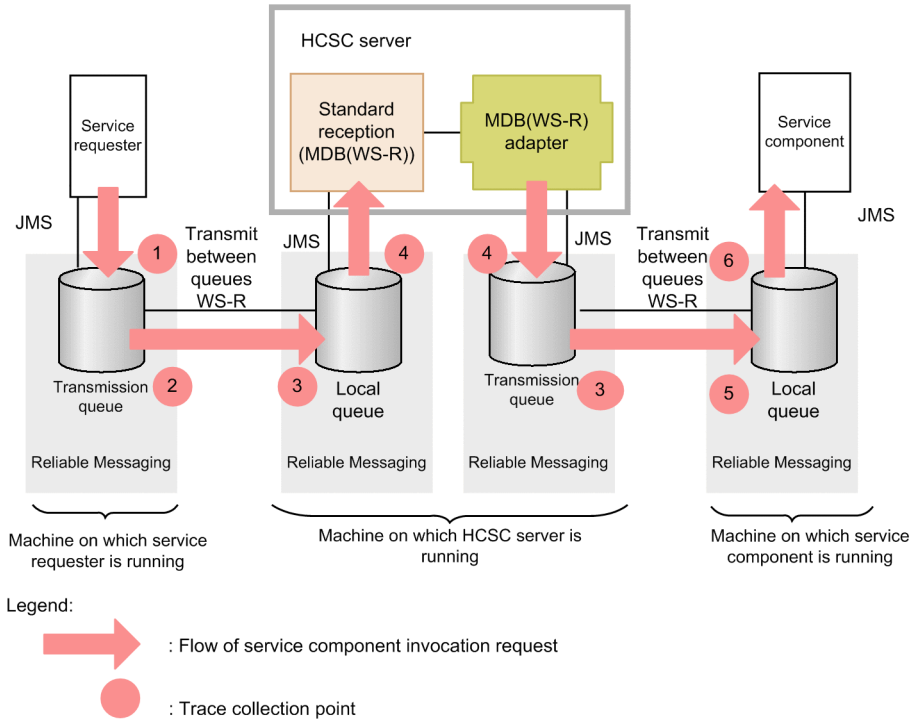
Log type	Output contents	Directory and file name
Start and stop messages log	Information on start and stop, and value of the property specified by the user.	• Directory <Log output directory of J2EE server>\connectors\ • File name <Display name of Reliable Messaging><File number>.log
Message log for the J2EE server	Information of Reliable Messaging for starting, stopping, and during operations.	• Directory <Log output directory of J2EE server > • File name Output to the same file in which the Service Platform outputs the message log.

(b) Relationship between the HCSC server and the trace of Reliable Messaging

The relationship between the HCSC server and the trace of Reliable Messaging differs when you use the local queue and the transfer queue, and when you use the shared queue.

- **When you use the local queue or the transfer queue**
  There are two types of Reliable Messaging trace namely; method trace and line trace. The method trace outputs error information (cause of exception occurrence) and the entry information, exit information, and debug information of method. The line trace outputs the information of messages transmitted between queues. The following figure shows the trace collection point when using local queue or transfer queue:

Figure 7–2: Figure Trace collection point when using local queue or transfer queue



The following table lists and describes the relationship between trace collection point and file names. "Number in figure" in this table corresponds to the numbers in "*Figure7-2 Trace collection point when using local queue or transfer queue*".

Table 7–7: TableRelationship between the trace collection point and file names

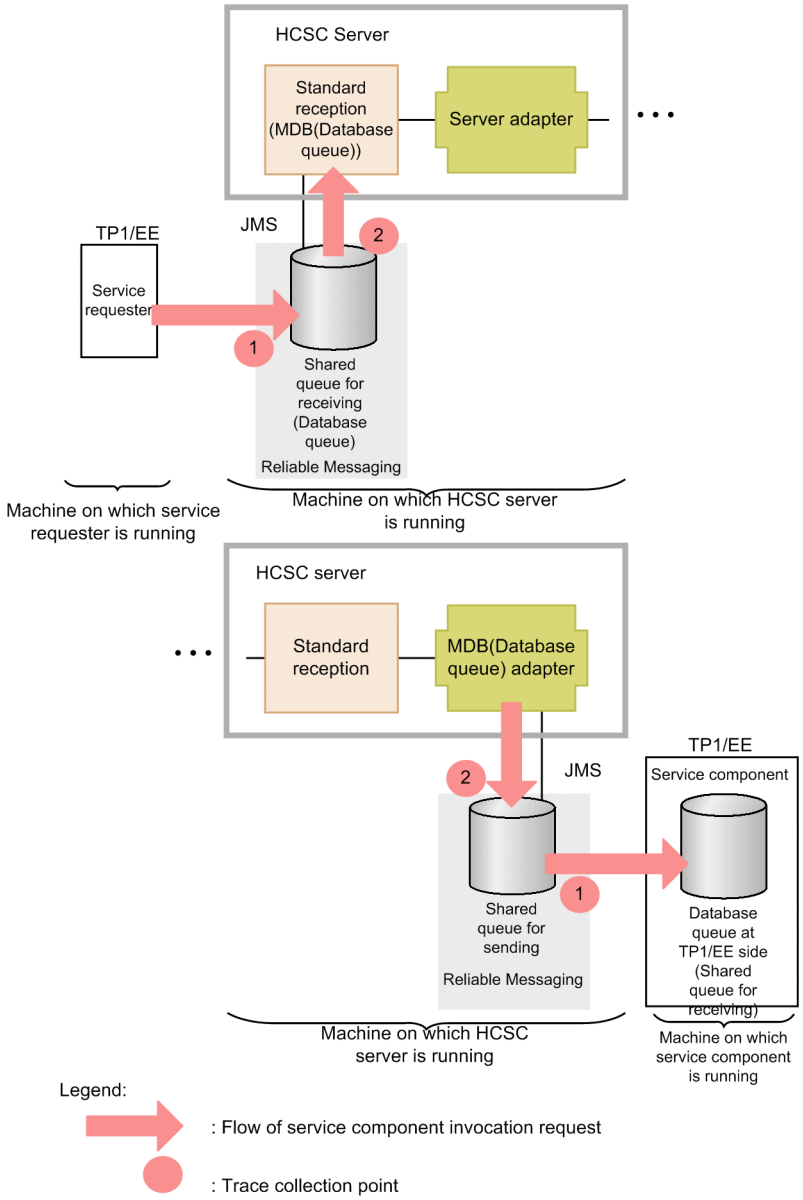
Number in figure	Collection point	Trace			
		Type	Output machine	Output destination	File name
1	When sending a request from the service requester to transfer queue	Method trace	Service requester machine	<Log output directory of the J2EE server>\RM \maintenance	mtd_<Display name of Reliable Messaging of the service requester>_<numbers>.log
2	When transferring from the transfer queue of the service requester to the local queue of HCSC server	Line trace			lin_<Display name of Reliable Messaging of the service requester>_<numbers>.log
3	When accepting transfer from the transfer queue of the service requester to the local queue of the HCSC server, and when transferring from the transfer queue of the HCSC server to the local queue of the service component.	Line trace	Machine on which the HCSC server is running	<Log output directory of the J2EE server >\RM \maintenance	lin_<Display name of Reliable Messaging of the HCSC server>_<numbers>.log
4	When HCSC server fetches messages from the local queue, and when sending requests from the service adapter to the transfer queue	Method trace			mtd_<Display name of Reliable Messaging of the HCSC server>_<numbers>.log
5	When accepting transfer from the transfer queue at the HCSC server	Line trace	Machine on which the service	<Log output directory of the	lin_<Display name of Reliable Messaging of the service component >_<numbers>.log

Number in figure	Collection point	Trace			
		Type	Output machine	Output destination	File name
5	to the local queue of the service component	Line trace	component is running	J2EE server >\RM \maintenance	lin_<Display name of Reliable Messaging of the service component >_<numbers>.log
6	When the service component fetches messages from the local queue	Method trace			mtd_<Display name of Reliable Messaging of the service component >_<numbers>.log

- **When you use the shared queue**

  There are two types of Reliable Messaging trace namely, method trace and shared queue event trace. The method trace outputs the error information (cause for occurrence of exception) and entry information, exit information, and debug information of the method. The share queue event trace outputs the information of an event indicating that the messages are stored in share queue. The following figure shows the trace collection point when using the shared queue:

Figure 7–3: Figure Trace collection point when using the shared queue



The following table lists and describes the relationship between the trace collection point and the file name. "Number in figure" in this table corresponds to the numbers in "*Figure7-3 Trace collection point when using the shared queue*".

Table 7–8: Table Relationship between the trace collection point and the file name

Number in figure	Collection point	Trace			
		Type	Output machine	Output destination	File name
1	When messages are saved from the service requester to the shared queue for reception in HCSC server, and when messages are saved from the service adapter of HCSC server to the shared queue for sending	Shared queue event trace	Machine on which the HCSC server is running	<Log output directory of the J2EE server >\RM \maintenance	shq_<Display name of Reliable Messaging of the HCSC server>_<numbers>.log

Number in figure	Collection point	Trace			
		Type	Output machine	Output destination	File name
2	When HCSC server fetches messages from the local queue, and when sending requests from service adapters to transfer queue	Method trace	Machine on which the HCSC server is running	<Log output directory of the J2EE server >\RM \maintenance	mtd_<Display name of Reliable Messaging of the HCSC server >_<numbers>.log

RM trace that requires preparations before starting operations

To change the type of information that is output by changing the output level of method trace or line trace, you must change Reliable Messaging settings before starting the HCSC server. Perform these changes by using the RMMethodTraceLevel and RMLineTraceLevel configuration properties of Reliable Messaging.

(c) Setup information required for investigating failures

The information set up for Reliable Messaging configuration properties is required for investigating failures. The following table describes the definition files of Reliable Messaging required for investigating failures. For details on definition files, see " 6. Configuration Property" in "Reliable Messaging".

Table 7–9: Table Definition files of Reliable Messaging required for investigating failures

Definition file	Description
Setup information of Reliable Messaging properties	Definition files setup in "*3.1.2(9) Setting up Reliable Messaging*".

(3) How to acquire the failure information output by SOAP Communication Infrastructure or JAX-WS engine

When using synchronous standard reception(Web Service) or SOAP adapter, you can identify the cause of failure by acquiring the failure information output by SOAP Communication Infrastructure or the JAX-WS engine. You can identify the cause of failure when there is an error in the sent and received user messages, by checking the message format of SOAP Messages when invoking the HCSC server from service requester, and the SOAP Messages when invoking service component from the service adapter of the HCSC server.

For details on how to acquire the failure information output by SOAP Communication Infrastructure ,see "14.Troubleshooting" in "Application Server SOAP Application Development Guide".

For details on how to acquire the failure information output by JAX-WS engine, see "39.Troubleshooting" in "Application Server Web Service Development Guide".

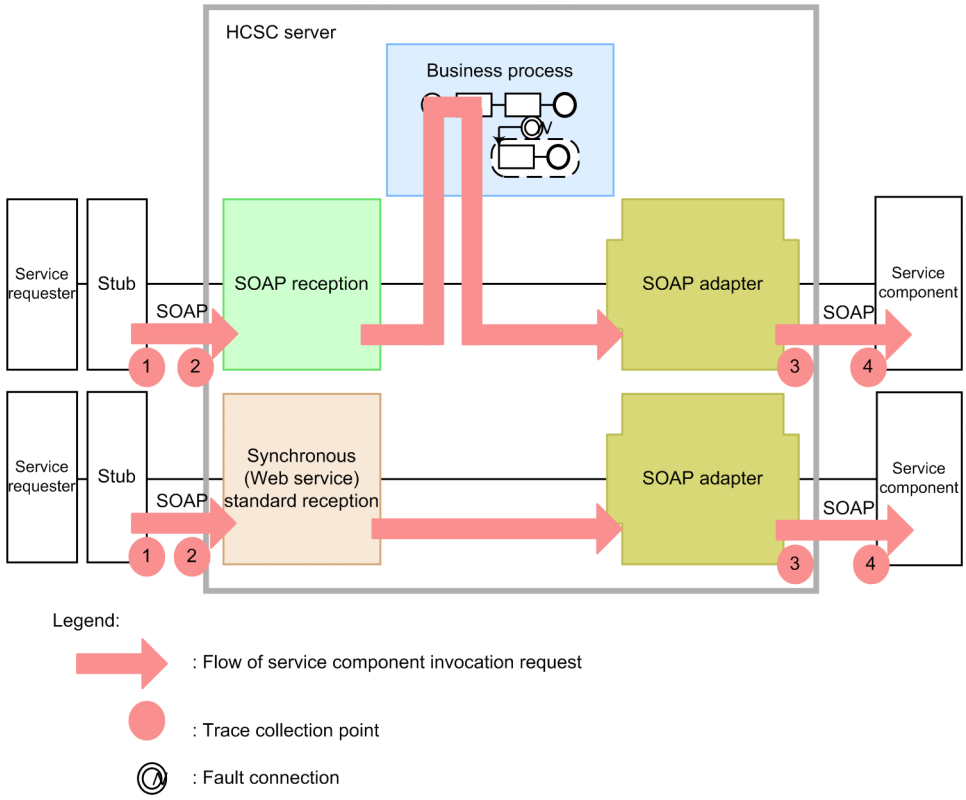
(a) Relationship between the HCSC server and SOAP trace or Application log

This sub-section describes the relationship between the collection point and SOAP trace or file names of application logs in the HCSC server configuration. This relationship differs when invoking SOAP adapter from the reception of Web Services and when invoking SOAP adapter from a reception other than Web Services.

- **When invoking SOAP adapter from synchronous standard reception (Web Services) or SOAP reception**

  The SOAP trace or application log is output with the following names when you invoke the SOAP adapter from synchronous standard reception (Web Services) or from the SOAP reception. The same names are output when it passes through the business process on the way. The following figure shows the collection point of SOAP trace and application log:

Figure 7–4: Figure Collection point of SOAP trace or application logs (when you invoke the SOAP adapter from the reception of Web Services)



The following table lists and describes the relationship between the trace collection point and file names. The numbers in the *Number in figure* column of the table correspond to the numbers in the above figure.

Table 7–10: Table Relationship between trace collection points and file names (when you invoke the SOAP adapter from the reception of Web Services)

Number in figure	Collection point	File name	
		Trace[#1]	Application log[#1]
1[#2]	SOAP communication trace when requests (sending) are sent from the service requester, and when there is a response (receiving) from the service requester	**When using SOAP Communication Infrastructure** "<prefix>-j2ee-<J2EE server name>-<numbers>.log" <prefix>[#3] is set in the client definition file of service requester side. **When using JAX-WS engine** "cjwmessage<numbers>.log"	**When using SOAP Communication Infrastructure** "<prefix>-j2ee-<J2EE server name>-aplog-<numbers>.log" <prefix>[#3] is set in the client definition file of service requester side. **When using JAX-WS engine** "cjwtransport<numbers>.log"
2	SOAP Communication trace when requests are received (receiving) from the service requester with the request reception of the HCSC server, and when there is a response (sending) from the HCSC server	**For synchronous standard reception (Web Services)** "<cluster name>-j2ee-<J2EE server name>-<numbers>.log" **For SOAP reception** "<Reception ID>-j2ee-<J2EE server name>-<numbers>.log"	**For synchronous standard reception (Web Services)** "<cluster name>-j2ee-<J2EE server name>-aplog-<numbers>.log" **For SOAP reception** "<Reception ID>-j2ee-<J2EE server name>-aplog-<numbers>.log"
3	SOAP Communication trace when requests are sent (sending) from the service adapter of the HCSC server, and when there is a response	Output to a trace file same as number 2 in the figure.	Output to the application log file same as number 2 in the figure.

Number in figure	Collection point	File name	
		Trace#1	Application log#1
3	(receiving) from the service adapter	Output to a trace file same as number 2 in the figure.	Output to the application log file same as number 2 in the figure.
4#2	Communication trace when requests from the service adapter of the HCSC server are received (receiving) in the service component , and when there is a response (sending) from the service component	**When using SOAP Communication Infrastructure** "<prefix>-j2ee-<J2EE server name>-<numbers>.log" <prefix>#3 is set in the server definition file of the service component. **When using JAX-WS engine** "cjwmessage<numbers>.log"	**When using SOAP Communication Infrastructure** "<prefix>-j2ee-<J2EE server name>-aplog-<numbers>.log" <prefix>#3 is set in the server definition file of the service component. **When using JAX-WS engine** "cjwmessage<numbers>.log"

Note#1

The output destinations of trace and application logs differ as follows according to the Communication Infrastructure in use:

When using SOAP Communication Infrastructure

The <Log output directory of J2EE server>\WS on each running machine.

When using JAX-WS engine

The < Log output directory of J2EE server>\CJW on each running machine.

Note#2

Traces can be collected when the SOAP Communication Infrastructure or JAX-WS engine provided by Service Platform is used on the machine on which the service requester or service component is running.

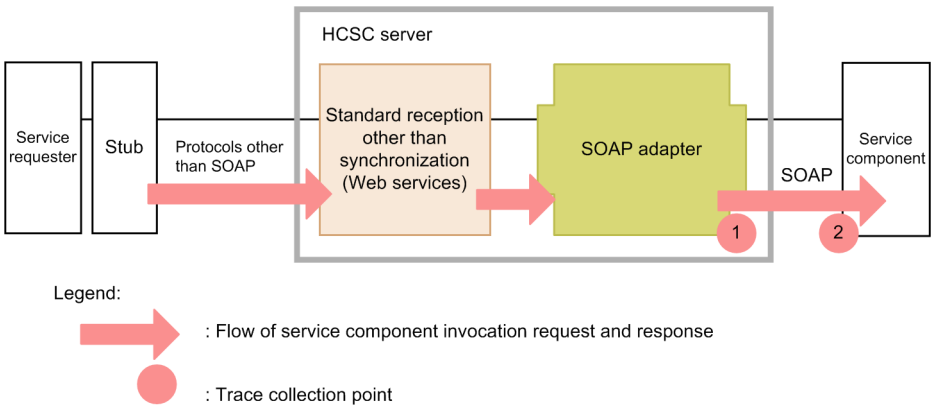
Note#3

The name setup in prefix (c4web.logger.<identifier>.log_file_prefix) of trace files or application logs in the service definition file (c4websv.cfg) or the client definition file (c4webcl.properties).

- **When invoking SOAP adapters from a reception other than Web Services**

The SOAP trace or application log is output with the following names when you invoke SOAP adapters from a request reception other than the synchronous standard reception or the SOAP reception . The following figure shows the collection point of SOAP trace and application log:

Figure 7–5: Figure Collection points of SOAP trace or application log (when you invoke a service adapter from a reception other than Web Services)



The following table lists and describes the relationship between the trace collection point and file names. The numbers in the *Number in figure* column of the table correspond to the numbers in the above figure.

Table 7–11: Table Relationship of trace collection point and file names (when you invoke a SOAP adapter from a reception other than Web Services)

Number in figure	Collection point	File name	
		Trace#1	Application log#1
1	SOAP Communication trace when requests are sent (sending) from the service adapters of the HCSC server, and when there is a response (receiving) from service adapters	"<service ID>-j2ee-<J2EE server name>-<numbers>.log"#3	"<service ID>-j2ee-<J2EE server name>-aplog-<numbers>.log"#3
2#2	SOAP Communication trace when requests from the service adapter of the HCSC server are received (receiving) by service components, and when there is a response (sending) from service components	**When using SOAP Communication Infrastructure** "<prefix>-j2ee-<J2EE server name>-<numbers>.log" <prefix>#4 is set in the server definition file of the service component. **When using JAX-WS engine** "cjwmessage<numbers>.log"	**When using SOAP Communication Infrastructure** "<prefix>-j2ee-<J2EE server name>-aplog-<numbers>.log" <prefix>#4 is set in the server definition file of the service component. **When using JAX-WS engine** "cjwtransport<numbers>.log"

Note#1

The output destination of trace and application logs differs as follows according to the Communication Infrastructure in use:

When using SOAP Communication Infrastructure

The <Log output directory of J2EE server>\WS on each running machine.

When using JAX-WS engine

The <Log output directory of J2EE server>\CJW on each running machine.

Note#2

Can be acquired when a machine on which the service component is running uses SOAP Communication Infrastructure or the JAX-WS engine provided by the Service Platform.

Note#3

Even if you specify prefix of trace files and application logs in the client definition file setup in the Service adapter settings screen, the specified value is not enabled. The service ID is assigned as a unique prefix.

Note#4

The name where the prefix (c4web.logger.<identifier>.log_file_prefix) is setup for trace files or application logs in the server definition file (c4websv.cfg).

(b) Preparations required for SOAP trace and application logs before starting the operations

If you acquire the log of SOAP messages, you can identify the cause of failure when there is an error in the sent and received user messages by checking the message format of SOAP Messages when invoking the HCSC server from the service requester and the SOAP messages when invoking the service component from the service adapter of the HCSC server.

The log output is set in the following common definition files on which HCSC server is running:

- For SOAP Communication Infrastructure: c4webcom.cfg
- For JAX-WS engine:cjwconf.properties

The following table describes the settings to the common definition file of the machine on which HCSC server is running:

Table 7–12: Table Settings of a machine on which the HCSC server is running to the common definition file

Item	Key name	Setting (Default)	Description
Importance of application log output	c4web.logger.aplog_level	WARN	Specify INFO while capturing (check the message format of SOAP Messages) the log of SOAP Messages. Must be set in advance before starting the HCSC server.

For details on creating common definition files used by SOAP Communication Infrastructure, see"10.4 Setting up the common definition file" in "Application Server SOAP Application Development Guide".

For details on creating common definition files used by the JAX-WS engine, see"10.1.2 Settings of the common definition file" in "Application Server Web Service Development Guide".

(c) Setup information required for investigating failure

The setup information of SOAP Communication Infrastructure and the JAX-WS engine is required for investigating failures. The following table describes definition files of SOAP Communication Infrastructure:

Table 7–13: Table Definition file of SOAP Communication Infrastructure

Definition file	Description	File save location	File name
Server definition file	Controls the operations of SOAP Communication in the request reception of a machine on which the HCSC server is running	Following folders of machine on which the HCSC server is running: For Windows <Installation directory of Service Platform>\c4web\conf For other OS /opt/Cosminexus/c4web/conf	c4websv.cfg
Common definition file	Controls the common operations of SOAP Communication the in request reception and the service adapter of a machine on which HCSC server is running	Following folders of machine on which the HCSC server is running: For Windows <Installation directory of Service Platform>\c4web\conf For other OS /opt/Cosminexus/c4web/conf	c4webcom.cfg

For details on definition files when using SOAP Communication Infrastructure, see "10.2 Setting up the server definition file" in "Application Server SOAP Application Development Guide". For details on common definition files when using SOAP Communication Infrastructure, see "10.4 Setting the common definition file" in "Application Server SOAP Application Development Guide ".

The following table describes the definition file for the JAX-WS engine:

Table 7–14: Table Definition file for the JAX-WS engine

Definition file	Explanation	File storage location	File name
Common definition file	Controls the SOAP communication operations common to the request reception and the service adapter of a machine on which the HCSC server is running.	Following folders of machine on which the HCSC server is running: For Windows <Installation directory of Service Platform>\jaxws\conf For other OS /opt/Cosminexus/jaxws/conf	cjwconf.properties

For details on definition files when using JAX-WS engine, see "10.1 Action definition file" in "Application Server Web Service Development Guide".

(4) How to acquire the failure information output by the HTTP Server

The failure information output by the HTTP Server is required when operations are performed using the HTTP Server. For details on how to acquire the failure information output by HTTP Server, see "HTTP Server".

(5) How to acquire failure information output by database

When the cause of failure exists in the database, you can identify the cause by checking the failure information of the database. There is server side and client side information in the failure information of database. The following figure

shows the relationship between the database (client side) and of a machine on which HCSC server is running and the database (server side):

Figure 7–6: Figure Relationship between the database (client side) of machine on which HCSC server is running and the database (server side)

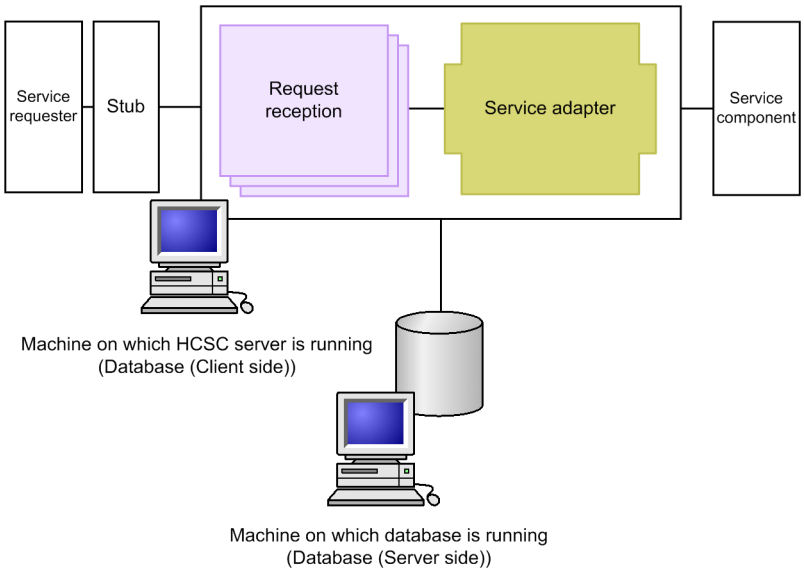


Table 7–15: Table Failure information of database at server side and client side

Database used	Server/Client	Failure information
When HiRDB is used	Server side failure information	• HiRDB log All files under %PDDIR%\SPOOL
	Server side failure information (definition information)	• Definition information of HiRDB All files under %PDCONFPATH%
	Client side failure information	• SQL trace file and error log file of HiRDB client Directory specified in environment variable PDCLTPATH (Output to the following directory when environment variable PDCLTPATH is omitted. %PDDIR%\spool\hubspool\external-server-name\) • File size specified in SQL trace environment variable PDSQLTRACE of HiRDB client (SQL trace is not output when environment variable PDCLTPATH is omitted) • Exception trace log# of HiRDB Type4 JDBC driver Directory specified in environment variable PDJDBFILEDIR (Output to the following directory when environment variable PDJDBFILEDIR is omitted. <Installation directory of Service Platform>\CC\server\public\ejb\<J2EE server name>\<J2EE server name>excX.trc)
When Oracle is used	Server side failure information	Oracle log
	Client side failure information	Oracle JDBC Thin Driver log

Note#

For HiRDB Type4 JDBC Driver, the exception trace log is disabled even if it is described in the environment variable of OS or HiRDB.ini OS. Specify by connecting with semicolons in the property definition "EnvironmentVariables" of the used DB Connector as follows:

(Example) PDSQLTRACE=0;PDCLTPATH=c:\tmp

The Exception trace log is not acquired if you use DABroker.

If you use HiRDB, see " HiRDB System Operation Guide". If you use Oracle, see the documentation published by Oracle Corporation.

(6) How to acquire JavaVM information

(a) JavaVM output message log

When the JavaVM crashes, the debug information is output to standard output and error report file by JavaVM. For details, see "4.11 JavaVM output message log (standard output or error report file) " in "Application Server Maintenance and Migration Guide". The output destination and output file name of the error report file is as follows:

- **For Windows**

```
<Installation directory of Service Platform>\CC\server\usrconf\ejb\<J2EEserver name>
\hs_err_pid<Process ID of server process>.log
```

- **For UNIX**

```
<Installation directory of Service Platform>/CC/server/usrconf/ejb/<J2EE server name>/
hs_err_pid<Process ID of server process>.log
```

(b) Thread dump of JavaVM

JavaVM statistics and stack status of threads is output. For details, see "4.7 Thread dump of JavaVM" in "Application Server Maintenance and Migration Guide". The output destination is as follows:

- **In Windows**

```
<Installation directory of Service Platform>\CC\server\usrconf\ejb\<J2EE server name>
\javacore*.txt
```

- **In UNIX**

```
<Installation directory of Service Platform>/CC/server/usrconf/ejb/<J2EEserver name>/
javacore*.txt
```

(c) Garbage collection log of JavaVM

Garbage collection of JavaVM is output in active state. For details, see "4.8 Garbage collection log of JavaVM" in "Application Server Maintenance and Migration Guide".

(d) Memory dump

When there is a failure in the system, the system administrator or Maintenance Service use the memory dump to analyze the error. For details, see "4.9 Memory dump" in "Application Server Maintenance and Migration Guide".

7.3.3 Estimating Trace Files

Based on the number of messages and number of days for which trace is to be saved, calculate the total file size for the trace files, as shown below:

- Messages received per day (Unit: Number)
- Period for saving the trace information (Unit: Days)

From the calculated total file size, estimate the trace file size and number of trace files. Specify the trace file size and number of trace files in the HCSC server runtime definition file. For details about the HCSC server runtime definition

file, see *HCSC server runtime definition file* in the manual *Cosminexus Service Platform Reference*. Calculate the estimates by referencing each manual of the related prerequisite products.

7.3.4 Notes while acquiring log and trace

The following limitations and notes apply to all logs and traces other than the performance analysis trace.

(1) General notes

The following notes apply to all logs and traces other than the performance analysis traces:

- Files cannot be edited.
- A text viewer or editor with a lock option is not supported. If files are locked, no trace can be output.
- File access permissions cannot be changed.

  If you need to set access permissions manually, set appropriate access permissions. If the access permissions you set are not appropriate, trace output is disabled.
- The file update time cannot be changed.

  If you change the file update time, the output target file may be altered.
- Do not rename or delete a file during trace output processing.

  The target file can be determined from information in the management file. If the management file is not available or is damaged, the output target file is determined based on the file update time. If you need to rename or delete a file, first terminate all trace output processes.

(2) Notes about HCSC-Manager log

- The linefeed code at the end of a message is always **CR**+**LF** regardless of the platform you are using.
- The following notes also apply to exception and maintenance logs:
  - To enable the function for changing a file size, the number of files, or the mode option, you may need to delete files. Before you delete a file, terminate the trace output process.
  - In an output trace file, data up to the first EOF character (0x1A) is valid. Data following the EOF character is not guaranteed. Note that the first EOF character may be followed by another EOF character.
  - Even when a trace is output, updating of the file update time is not guaranteed. Whether or not the trace has been output cannot be determined based on the file update time. The file update time is updated when trace output processing is terminated.

7.4 Types of error information

In the event of a failure during operations, information needed for troubleshooting is output as log information to a log file and as trace information to a trace file. This section describes the types of log and trace output by Cosminexus Service Platforms such as HCSC server or HCSC-Manager.

7.4.1 Message log

Acquires The information when operating the HCSC server or error information when a failure occurs, and the information of a running HCSC server or error information if a failure occurs is acquired as message log. With this you can detect the occurrence of a failure and analyze the cause of failure.

The types of message logs of Service Platform are as follows:

- HCSC-Manager log
- Integrated message log
- J2EE server activity log

(1) Contents output in the message log

The following messages are output. For details on the content of the message log, see "Service Platform Messages".

(a) HCSC-Manager log

Acquires messages output by HCSC-Manager.

(b) Integrated message log

Acquires messages output by Administration Agent, Management Agent, and Management Server.

(c) Activity log of J2EE server

Acquires the messages output by a running J2EE server. Also outputs messages that are output by the HCSC server running on the J2EE server to the activity log.

(2) How to acquire the message log

The message log is always output. For details on how to acquire, see "*7.3.1(1) Collecting the message log*".

(3) Output destinations of the Message log

The following table lists and describes the output destinations of the message log and log file names:

Table 7–16: Table Output destinations of the Message log and file names

Log type	Path of the output destination of the message log	Log file name
HCSC-Manager log	Path specified in the cscmng.log.dir parameter of the HCSC-Manager definition file[#1]	message<number of files>.log
Integrated message log	Path specified in the output destination of the integrated message log[#2]	mngmessage<number of files>.log
Activity log of the J2EE server	Path specified in the output destination of the J2EE server activity log[#3]	• For Wraparound mode cjmessage<number of files>.log[#4] • For Shift mode cjmessage.log

Note#1

For details on the specification of the output destination and number of files of the HCSC-Manager definition file, see "HCSC-Manager definition file" in "Service Platform Reference Guide".

Note#2

Specify the output destination of the integrated message log in manager.cfg (Manager log settings file). The default output destination is as follows:

```
<Installation directory of Service Platform>\manager\log
```

For details on the specification of the output destination and number of files, see "10.10 manager.cfg (Manager configuration file) " in "Application Server Definition Reference Guide".

Note#3

Specify the output destination of the activity log of the J2EE server with the ejb.server.log.directory key of usrconf.cfg (option definition file of J2EE server).The default output destination is as follows:

```
<Installation directory of Service Platform>\CC\server\public\ejb\<J2EE server name>\logs
```

For details on usrconf.cfg, see "2.3 usrconf.cfg (option definition file for J2EE server) in "Application Server Definition Reference Guide".

Note#4

Specify the file count of the output files in the ejbserver.logger.channels.define.<channel name>.filenum key of the user property file (usrconf.properties) for the J2EE server on which the HCSC server is running. Specify the output file size in the ejbserver.logger.channels.define.<channel name>.filesize key.

For details on usrconf.properties, see"2.4 usrconf.properties (user property file for J2EE server) " in "Application Server Definition Reference Guide".

7.4.2 Request trace

In the messaging infrastructure of HCSC server, you can acquire the following contents as request trace:

- Request for invoking service component received in request reception or response results
- Requests when business process is invoked or response results
- Requests when service components are invoked from the service adapter or response results

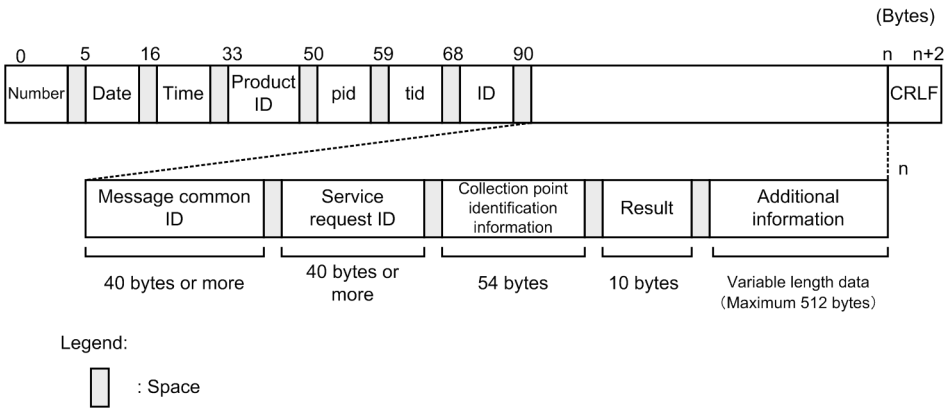
The request trace is used to analyze the cause of failure of requests.

(1) Output format and contents of the request trace

(a) Output format

The following figure shows the output format of the request trace:

Figure 7–7: Figure Output format of request trace



(b) Output contents

The following table lists and describes the contents output to the request trace:

Table 7–17: Table Contents output to the request trace

Item		Content
Number		The request identification information (parent ID) is displayed.
Date		The trace record collection date (yyyy/mm/dd format) is output.
Time		The trace record collection time (hh:mm:ss.sss format) in milliseconds in local time is output.
Product ID		The "CSCMSG" that indicates the identifier messaging infrastructure to identify product is output.
pid		The ID to identify the process is output.
Tid		The ID to identify the thread is output.
ID		Not displayed.
Message common ID		The request identification information (parent ID) is output.
Service request ID		The request identification information (child ID) is output.
Collection point identification information	Collection location	The trace collection point (collection location) is output: • RCP:Standard reception • URCP:User-defined reception • SVSND: Server-to-server transfer (sending) • SVRCV: Server-to-server transfer (receiving) • BPRCP:Business process request reception • BPREQ:Invoking a business process • SVC: Invoking Service components (within the service adapter) • SVCGP: Invoking service group
	Protocol type	The trace collection point information (protocol type) is output. However, the information is not displayed if the collection location is BPRCP, BPREQ, or SVCGP. • SOAP:Web Services • EJB:SessionBean • WSR:MDB (WS-R) • DBQ:MDB (DB queue) • CUSTM:Protocols other than those mentioned above
	Detailed location	The trace collection point information (detailed location) is output: • IN:Reception • OUT:Response • CAL:Invoke (other components) • RET:Receive response (other components) • WRN:Exception
	Name	The trace collection point information (name) is output. However, the information is not displayed if the collection location is RCP, URCP, BPREQ, or SVRCV. • Server name • Service ID of service adapter • Service ID of business process • Service group name
	Adapter type	The trace collection point information (adapter type) is output. However, the information is not displayed if the collection location is RCP, URCP, BPRCP, SVCGP, SVSND, or SVRCV. • SVA:Service adapter • BP:Business process

Item	Content
Result	The response result type is output. However, if the detailed location is IN or CAL, this information is not displayed. • Normal end: NORMAL • Abnormal end: ERROR
Additional information	The additional information for the response result is output.
CRLF	Record end code is output.

(2) Request trace collection point

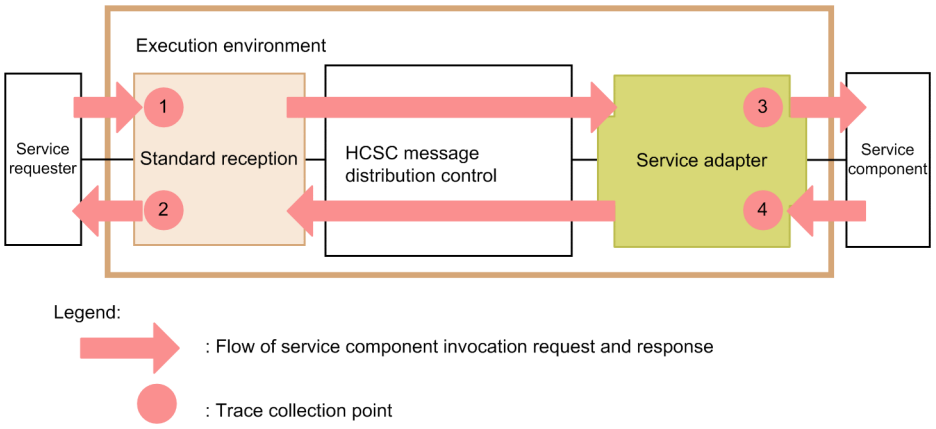
Timing of request trace output is of following types and the collection point differs for each type:

- When executing individual services
- When executing business process services
- When checking the operating status

(a) When executing an individual service

The following figure shows the trace collection point of request when executing an individual service:

Figure 7–8: Figure Trace collection point of request (when executing individual services)



The following table lists trace collection points. The "Numbers in figure" in this table corresponds to the numbers in "*Figure7-8 Trace collection point of request(when executing individual services)*".

Table 7–18: Table Trace collection point of request (when executing individual services)

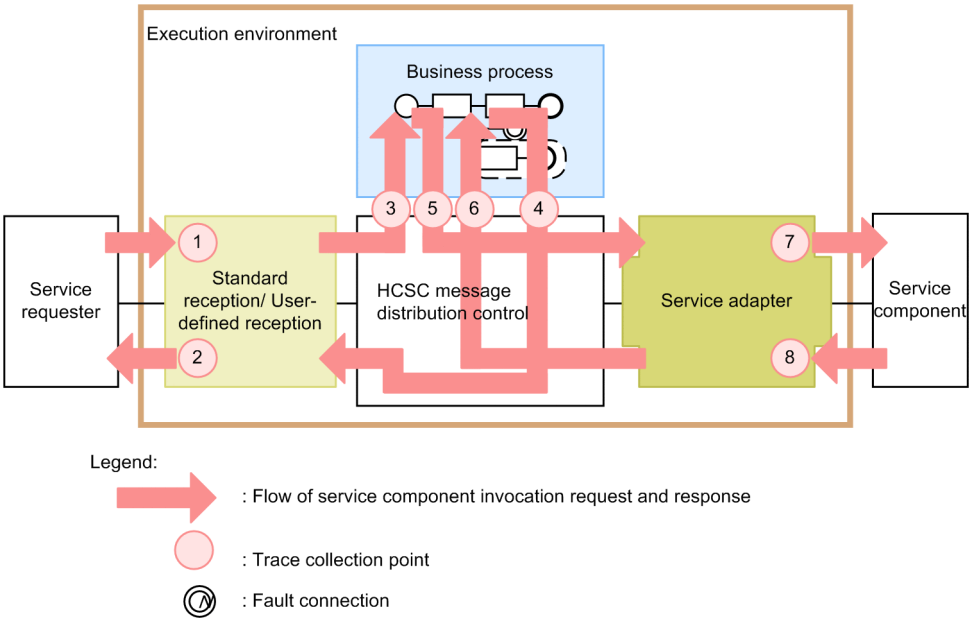
Number in figure	Trace collection point
1	Entry to standard reception (Web Services)
2	Exit from standard reception (Web Services)
1	Entry to standard reception (SessionBean)
2	Exit from standard reception (SessionBean)
1	Entry to standard reception (MDB(WS-R))
2	Exit from standard reception (MDB(WS-R))
1	Entry to standard reception (MDB(DB queue))
2	Exit from standard reception (MDB(DB queue))

Number in figure	Trace collection point
3	Invocation of service components of SOAP adapter
4	Point for receiving response from service components of SOAP adapter
3	Invocation of service components of SessionBean adapter
4	Point for receiving response from service components of SessionBean adapter
3	Invocation of service components of MDB (WS-R) adapter
4	Point for receiving response from service components of MDB (WS-R) adapter
3	Invocation of service components of MDB(DB queue) adapter
4	Point for receiving response from service components of MDB(DB queue) adapter
3	Invocation of service components of service adapters(CUSTOM) other than those mentioned above
4	Point for receiving response from service components of service adapters(CUSTOM) other than those mentioned above

(b) When executing business process services

The following figure shows the trace collection point of the request trace when executing business process services:

Figure 7–9: Figure Trace collection point of request (when executing business process services)



The following table lists trace collection points. The "Numbers in figure" in this table corresponds to the numbers in "*Figure 7-9 Trace collection point of request (when executing business process services)*".

Table 7–19: Table Trace collection point of request (when executing business process services)

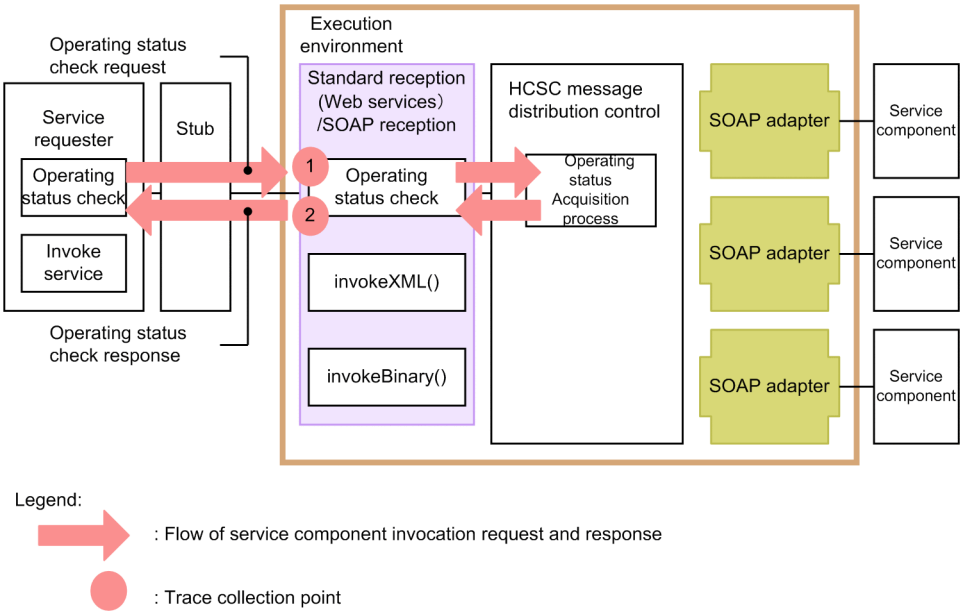
Number in figure	Trace collection point
1	Entry to standard reception (Web Services)
2	Exit from standard reception (Web Services)
1	Entry to standard reception (SessionBean)

Number in figure	Trace collection point
2	Exit from standard reception (SessionBean)
1	Entry to standard reception (MDB(WS-R))
2	Exit from standard reception (MDB(WS-R))
1	Entry to standard reception (MDB(DB queue))
2	Exit from standard reception (MDB(DB queue))
1	Entry to user-defined reception
2	Exit from user-defined reception
7	Invocation of service components of SOAP adapter
8	Point for receiving response from service components of SOAP adapter
7	Invocation of service components of SessionBean adapter
8	Point for receiving response from service components of SessionBean adapter
7	Invocation of service components of MDB (WS-R) adapter
8	Point for receiving response from service components of MDB (WS-R) adapter
7	Invocation of service components of MDB(DB queue) adapter
8	Point for receiving response from service components of MDB(DB queue) adapter
7	Invocation of service components of service adapters(CUSTOM) other than those mentioned above
8	Point for receiving response from service components of service adapters(CUSTOM) other than those mentioned above
3	Invocation of business process services
4	Point for receiving response from business process services
5	Entry to business process reception
6	Exit from business process reception

(c) When checking the operating status

The following figure shows the trace collection point of the request trace when checking the operating status:

Figure 7–10: FigureTrace collection point of request (when checking the operating status)



The following table lists trace collection points. The "Number in figure" in this table corresponds to the numbers in "*Figure 7-10 Trace collection point of request (when checking the operating status)*".

Table 7–20: Table Trace collection point of request (when checking the operating status)

Number in figure	Trace collection point
1	Entry to standard reception (Web Services)
2	Exit from standard reception (Web Services)
1	Entry to SOAP reception
2	Exit from SOAP reception

(3) How to acquire the request trace

Settings are required to acquire the request trace. For details, see "*7.3.1(2) Request trace*".

(4) Output destination of request trace

Following is the output destination of request trace:

```
Path specified in the request trace-filepath property of the HCSC server
runtime definition file.
```

If the specified path does not exist, or in case of an incorrect path, trace is output in the output destination of the omitted value.

The following table shows the trace file name of request trace:

Table 7–21: Table Trace file name of request trace

Output mode of trace file	Trace file name
For Wraparound mode	cscmsgreq_<HCSC server name>_<number of files>.log
For Shift mode	cscmsgreq_<HCSC server name>_.log

7.4.3 Performance Analysis Trace

The performance analysis trace (**PRF trace**) is trace information used to analyze the performance of the Service platform system. The performance analysis trace file is a text file in which the performance analysis trace is edited and output in the CSV format. The information that is output as the performance analysis trace is used to analyze performance bottlenecks throughout the system, including J2EE applications. It is used to troubleshoot and prevent such bottlenecks. For details on performance analysis trace functionality, see "7. Performance analysis using performance analysis trace" in "Application Server Maintenance and Migration Guide".

(1) Output format and output contents of the performance analysis trace file

(a) Output format

The format that is output in the performance analysis trace file is same as that of the performance analysis trace of the J2EE server. For details about the performance analysis trace file, see "7.3 Collecting performance analysis trace file using Management Server" in "Application Server Maintenance and Migration Guide".

(b) Output contents

For HCSC server (Messaging infrastructure)

The following table lists and describes the content that is output to the performance analysis trace file:

Table 7–22: Table Contents output to the performance analysis trace file (messaging infrastructure)

Item		Content
Event ID		The Event ID of the collection point is output. For details, see the following points: • "*Table 7-28 Performance analysis trace collection point(when executing individual services)*" • "*Table 7-29 Performance analysis trace collection point(when executing business process services)*" • "*Table 7-30 Performance analysis trace collection point(Executing database access)*" • "*Table 7-31 Performance analysis trace collection point(when accessing files)*"
Return code		The type of collection point is output. • 0:Normal end • 1:Abnormal end
Interface name		Class name is output.
Operation name		Method name is output.
Option information	Message common ID	The request identification information (parent ID) is output.
	Service request ID	The request identification information (child ID) is output.
	Additional information	The additional information specific to the output destination is output.

For HCSC server (business process infrastructure)

The following table lists and describes the content that is output to the performance analysis trace file:

Table 7–23: Table Content output to the performance analysis trace file (business process infrastructure)

Item	Content
Event ID	The Event ID of the collection point is output. For details, see "*Table7-32 Performance analysis trace collection point (business process infrastructure)*".

Item	Content
Return code	The type of the collection point is output. • 0:Normal end • 1:Abnormal end
Interface name	Any of the following names is displayed: • Business process definition name • Java class name • Data Transform • Service name For details, see"*Table 7-32 Performance analysis trace collection point (business process infrastructure)*".
Operation name	Is not output.
Option information	Option information is output. For details, see"*Table 7-32 Performance analysis trace collection point (business process infrastructure)*".

For HCSC server (Database adapter)

The following table lists and describes contents output to the performance analysis trace file:

Table 7–24: Table Contents output to the performance analysis trace file (Database adapter)

Item		Content
Event ID		The Event ID of the collection point is output. For details, see the following points: • "*Table 7-33 Performance analysis trace collection point (When starting DB adapter)*" • "*Table 7-33 Performance analysis trace collection point (When starting DB adapter)*"
Return code		The type of the collection point is output. • 0:Normal end • 1:Abnormal end
Interface name		Class name is output. Package name is not displayed.
Operation name		Method name is output.
Option information	Message common ID	The request identification information (parent ID) is output. Value becomes null when the information is not set.
	Service request ID	The request identification information (child ID) is output. Value becomes null when the information is not set.
	Additional information	Individual information is output.

For HCSC server (data transformation infrastructure)

The following table lists and describes contents output to the performance analysis trace file:

Table 7–25: Table Content output to the performance analysis trace file (Data transformation infrastructure)

Item	Content
Event ID	The Event ID of the collection point is output. For details, see the following points:

Item		Content
Event ID		• "*Table 7-35 Performance analysis trace collection point(data transformation infrastructure)*"
Return code		The type of the collection point is output. • 0:Normal end • 1:Abnormal end
Interface name		Class name is output.
Operation name		Method name is output.
Option information	Message common ID	The request identification information (parent ID) is output.
	Service request ID	The request identification information (child ID) is output.
	Additional information	The additional information specific to the output destination is output.

For HCSC server (component-common UOC)

The following table lists and describes contents output to the performance analysis trace file.

Table 7–26: Table Content output to the performance analysis trace file (component-common UOC)

Item		Content
Event ID		The Event ID of the collection point is output. For details, see the following points: • "*Table7-36 Performance analysis trace collection point (when using component-common UOC)*"
Return code		The type of the collection point is output. • 0:Normal end • 1:Abnormal end
Interface name		Class name of UOC class is output.
Operation name		Method name of UOC class is output.
Option information	Message common ID	The request identification information (parent ID) is output.
	Service request ID	The request identification information (child ID) is output.
	Additional information	Option information is output. For details, see "*7.4.3(2)(e) For HCSC server (component-common UOC)*".

(2) Collection point of the performance analysis trace

(a) For HCSC server (Messaging infrastructure)

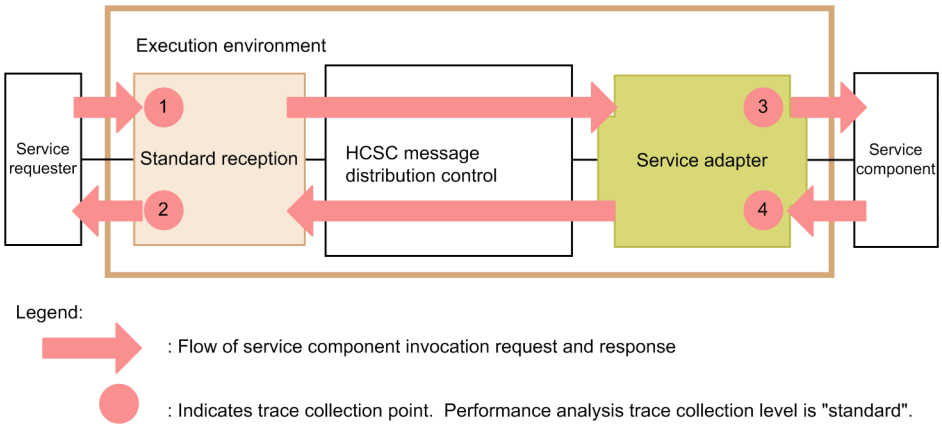
Performance analysis trace files are output at the following times, and the trace collection point for each time is different:

- When executing individual services
- When executing business process services
- When executing database access
- When executing file access

When executing individual services

The following figure shows the trace collection point of the performance analysis trace when executing individual services:

Figure 7–11: Figure Trace collection point of the performance analysis trace (when executing individual services)



The following table lists the event ID, trace collection point, and performance analysis trace collection point. The "Number in figure" in this table corresponds to the numbers in "*Figure7-11 Trace collection point of the performance analysis trace (when executing individual services)*".

Table 7–27: Table Performance analysis trace collection point (when executing individual services)

Event ID	Number in figure	Trace collection point	Level
0x9800	1	Entry to standard reception (Web Services)	A
0x9801	2	Exit from standard reception (Web Services)	A
0x9802	1	Entry to standard reception (SessionBean)	A
0x9803	2	Exit from standard reception (SessionBean)	A
0x9804	1	Entry to standard reception (MDB(WS-R))	A
0x9805	2	Exit from standard reception (MDB(WS-R))	A
0x9806	1	Entry to standard reception (MDB(DB queue))	A
0x9807	2	Exit from standard reception (MDB(DB queue))	A
0x9810	3	Invocation of service components of SOAP adapter	A
0x9811	4	Point for receiving response from service components of SOAP adapter	A
0x9812	3	Invocation of service components of SessionBean adapter	A
0x9813	4	Point for receiving response from service components of SessionBean adapter	A
0x9814	3	Invocation of service components of MDB (WS-R) adapter	A
0x9815	4	Point for receiving response from service components of MDB (WS-R) adapter	A
0x9816	3	Invocation of service components of MDB (DB queue) adapter	A
0x9817	4	Point for receiving response from service components of MDB (DB queue) adapter	A
0x9818	3	Invocation of service components of service adapters(CUSTOM) other than those mentioned above	A
0x9819	4	Point for receiving response from service components of service adapters(CUSTOM) other than those mentioned above	A

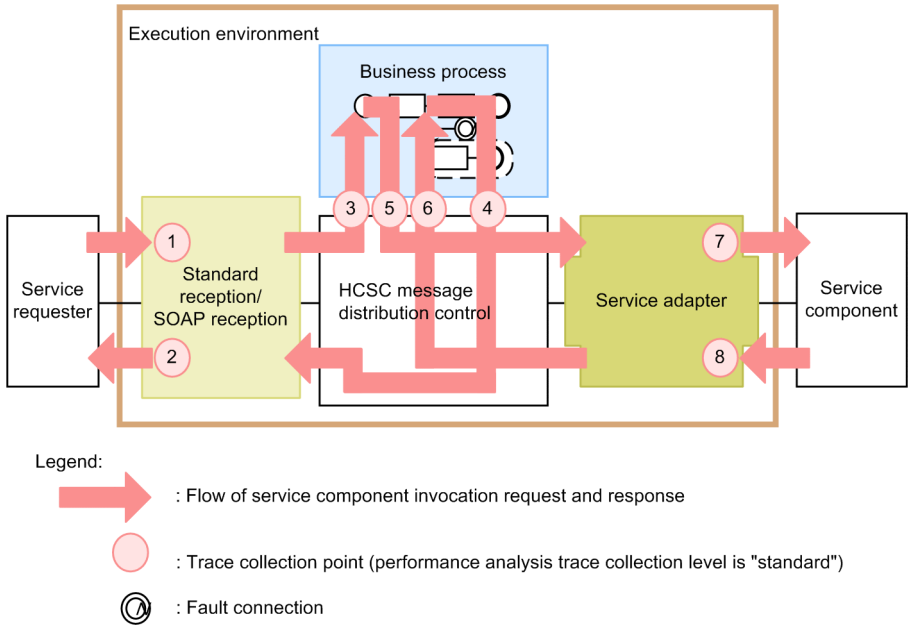
Legend:

A: Indicates the "Standard" level.

When executing business process services

The following figure shows the trace collection point of the performance analysis trace when executing business process services:

Figure 7–12: FigureTrace collection point of the performance analysis trace (when executing business process services)



The following table lists the event ID, trace collection point, and the performance analysis trace collection level. The "Number in figure" in this table corresponds to the numbers in "*Figure7-12 Trace collection point of the performance analysis trace (when executing business process services)*".

Table 7–28: Table Performance analysis trace collection point(when executing business process services)

Event ID	Number in figure	Trace collection point	Level
0x9800	1	Entry to standard reception (Web Services)	A
0x9801	2	Exit from standard reception (Web Services)	A
0x9802	1	Entry to standard reception (SessionBean)	A
0x9803	2	Exit from standard reception (SessionBean)	A
0x9804	1	Entry to standard reception (MDB(WS-R))	A
0x9805	2	Exit from standard reception (MDB(WS-R))	A
0x9806	1	Entry to standard reception (MDB(DB queue))	A
0x9807	2	Exit from standard reception (MDB(DB queue))	A
0x9808	1	Entry to SOAP reception	A
0x9809	2	Exit from SOAP reception	A
0x9810	7	Invocation of service components of SOAP adapter	A
0x9811	8	Point for receiving response from service components of SOAP adapter	A
0x9812	7	Invocation of service components of SessionBean adapter	A

Event ID	Number in figure	Trace collection point	Level
0x9813	8	Point for receiving response from service components of SessionBean adapter	A
0x9814	7	Invocation of service components of MDB (WS-R) adapter	A
0x9815	8	Point for receiving response from service components of MDB (WS-R) adapter	A
0x9816	7	Invocation of service components of MDB (DB queue) adapter	A
0x9817	8	Point for receiving response from service components of MDB (DB queue) adapter	A
0x9818	7	Invocation of service components of service adapters(CUSTOM) other than those mentioned above	A
0x9819	8	Point for receiving response from service components of service adapters(CUSTOM) other than those mentioned above	A
0x9840	3	Invocation of business process services	A
0x9841	4	Point for receiving response from business process services	A
0x9842	5	Entry to business process reception	A
0x9843	6	Exit from business process reception	A

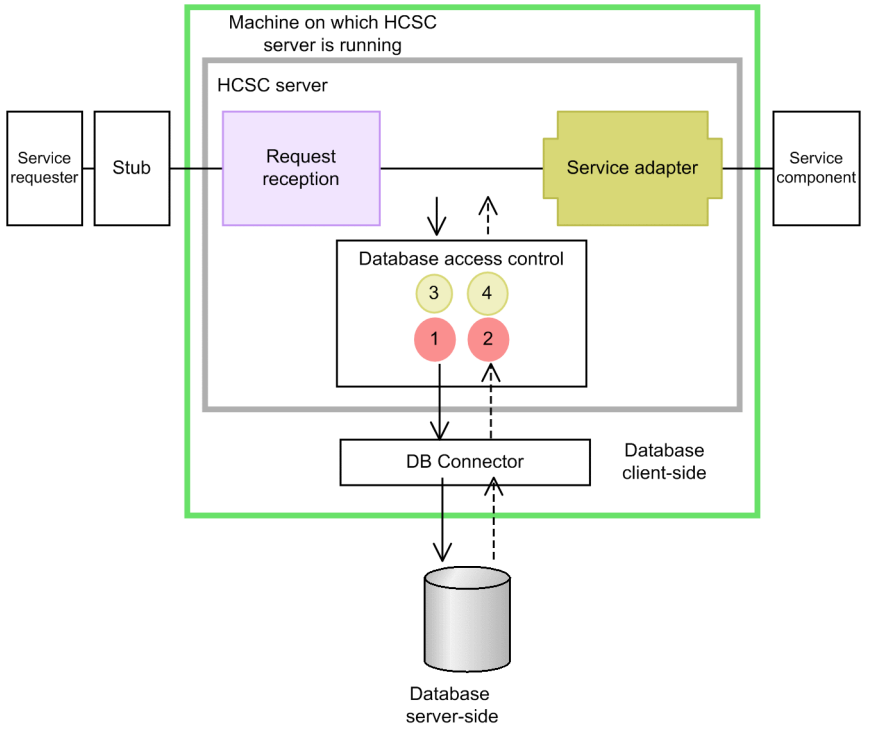
Legend:

A:Indicates the "Standard" level.

When executing database access

The following figure shows the collection point of performance analysis trace at the time of accessing the database when the HCSC server fetches commands.

Figure 7–13: Figure Performance analysis trace collection point (when executing database access)



Legend:

: Indicates trace collection point (performance analysis trace collection level is "standard")

: Indicates trace collection point (performance analysis trace collection level is "detailed")

The following table lists the event ID, trace collection point, and the performance analysis trace collection level. The "Number in figure" in this table corresponds to the numbers in "*Figure7-13 Performance analysis trace collection point (when executing database access)*".

Table 7–29: Table Performance analysis trace collection point(when executing database access)

Event ID	Number in figure	Trace collection point	Level
0x9850	1	Invocation of DB connector	A
0x9851	2	Point for receiving response from DB connector	A
0x9852	3	Invocation of execution log of DB connector	B
0x9853	4	Point for receiving response from execution log of DB connector	B

Legend:

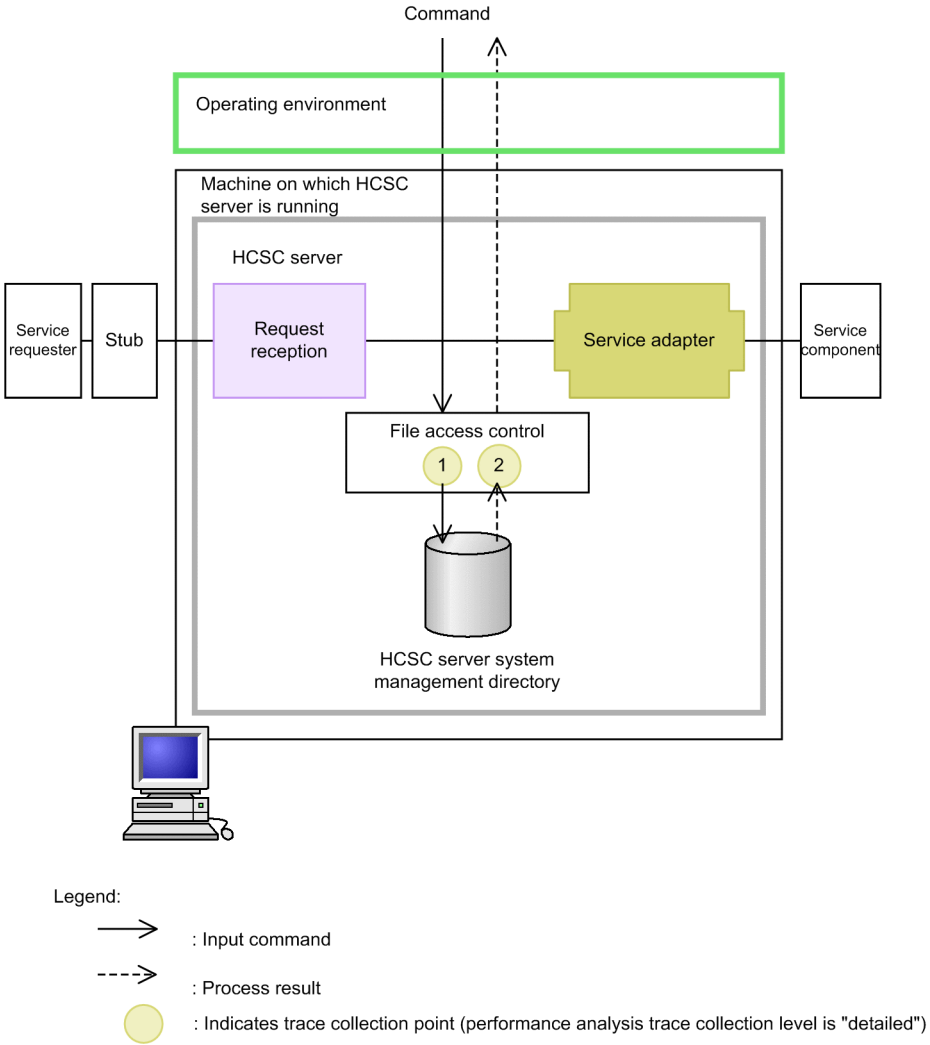
A:Indicates the "Standard" level.

B:Indicates the "Detail" level.

When executing the file access

When you setup the HCSC server in a configuration in which the database is not used, files are accessed instead of the database when the command is processed. Acquire the performance analysis trace while accessing these files. The following figure shows the collection point when accessing files:

Figure 7–14: Figure Performance analysis trace collection point (when accessing files)



The following table lists the event ID, trace collection point, and the performance analysis trace collection level. The "Number in figure" in this table corresponds to the numbers in "*Figure7-14 Performance analysis trace collection point (when accessing files)*".

Table 7–30: Table Performance analysis trace collection point (when accessing files)

Event ID	Number in figure	Trace collection point	Level
0x9854	1	Invocation of file access (before opening the file)	B
0x9855	2	Point for receiving response from file access (after closing the file)	B

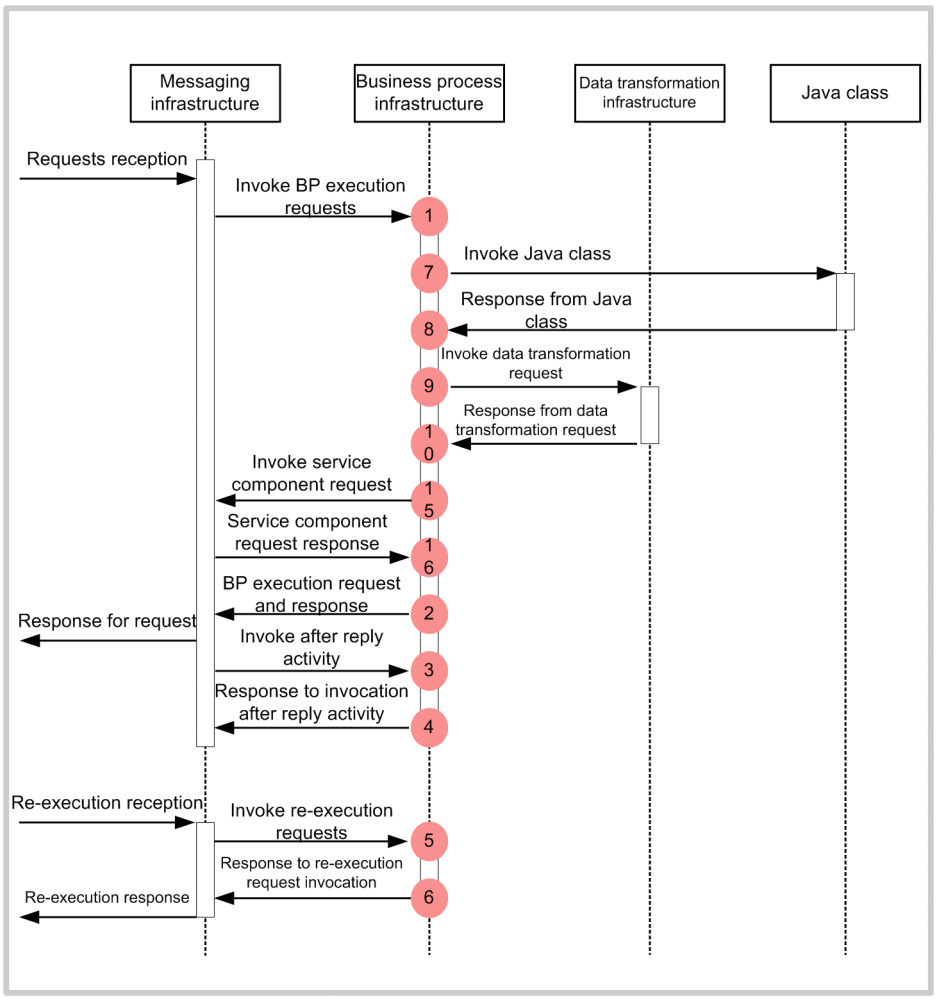
Legend:
B:Indicates the "Detail" level.

(b) For HCSC server (Business process infrastructure)

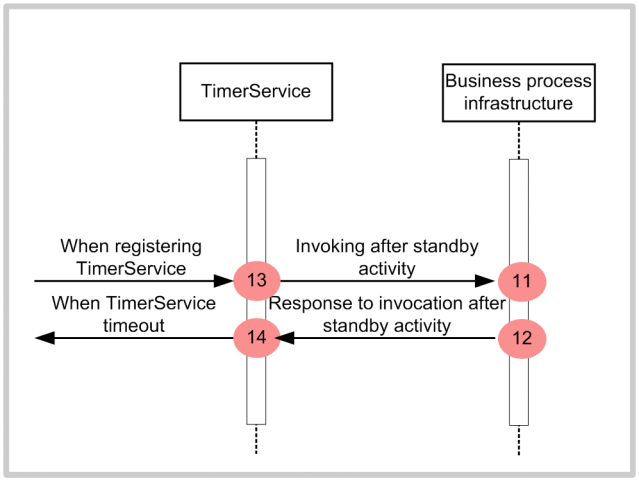
The following figure shows the performance analysis trace collection point:

Figure 7–15: Figure Trace collection point of performance analysis trace (business process infrastructure)

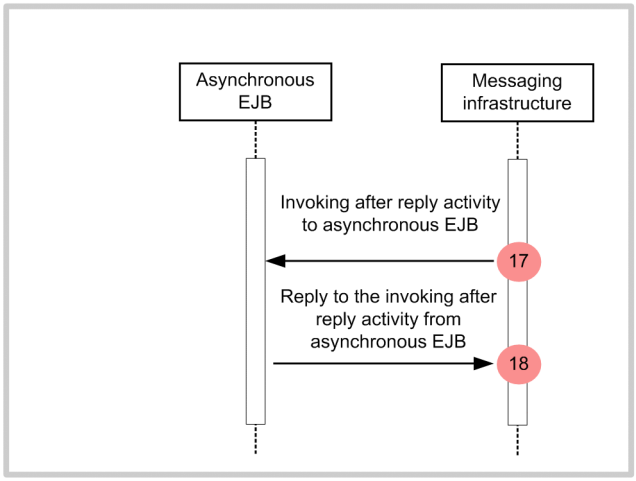
- When invoking from messaging infrastructure



- When invoking from TimerService



● When invoking asynchronous EJB



Legend:

: Indicates trace collection point (PRF trace collection level is "standard")

The following tables lists the event ID, trace collection point, and the performance analysis trace collection level, and indicates the output content of Interface name and Option information for each event ID. The numbers in the *Number in figure* column of the table correspond to the numbers in the above figure.

Table 7–31: Table Performance analysis trace collection point(business process infrastructure)

Event ID	Number in figure	Trace collection point	Level	Interface name	Option information
0x9900	1	Invoking a request for business process execution from messaging infrastructure	A	Business process definition name	• Message common ID
0x9901	2	Response to messaging infrastructure for the request to execute business process	A	Business process definition name	• Message common ID • Fault name(when abnormal)
0x9902	3	Invoking after reply activity from messaging infrastructure	A	Business process definition name	• Message common ID
0x9903	4	Response to invocation after reply activity from messaging infrastructure	A	Business process definition name	• Message common ID • Fault name(when abnormal)
0x9904	5	Invoking the request to re-execute from messaging infrastructure	A	Business process definition name	• Message common ID
0x9905	6	Response to invocation of the request to re-execute from messaging infrastructure	A	Business process definition name	• Message common ID • Fault name(when abnormal)
0x9906	7	Invoking the user-created Java class	A	Java class name	None
0x9907	8	Response from the user-created Java class	A	Java class name	• Fault name(when abnormal)
0x9908	9	Invoking data transformation request	A	"Data Transform"	None
0x9909	10	Response from data transformation request	A	"Data Transform"	• Fault name(when abnormal)

Event ID	Number in figure	Trace collection point	Level	Interface name	Option information
0x990A	11	Invoking from TimerService after the standby activity	A	Business process definition name	• Message common ID
0x990B	12	Response to invocation from TimerService after the standby activity	A	Business process definition name	• Message common ID • Fault name(when abnormal)
0x990C	13	When registering of TimerService	A	Business process definition name	• Message common ID • Standby cancellation time
0x990D	14	In the case of TimerService timeout	A	Business process definition name	• Message common ID
0x9910	15	Invoking a service component request to messaging infrastructure	A	Service name	• Message common ID • Hash code for parent thread (at the time of parallel execution)
0x9911	16	Response to the service component request from messaging infrastructure	A	Service name	• Message common ID • Hash code for parent thread (at the time of parallel execution) • Fault name(when abnormal)
0x9912	17	Invoking after reply activity from messaging infrastructure to asynchronous EJB	A	Business process definition name	• Message common ID • Process instance identifier
0x9913	18	Response to the Invoking after reply activity from asynchronous EJB to messaging infrastructure	A	Business process definition name	• Message common ID • Process instance identifier

Legend:

A:Indicates the "Standard" level.

Note

The event IDs that are not listed in the table (0x9A00 to 0x9AFF) are issued from the data transformation infrastructure.

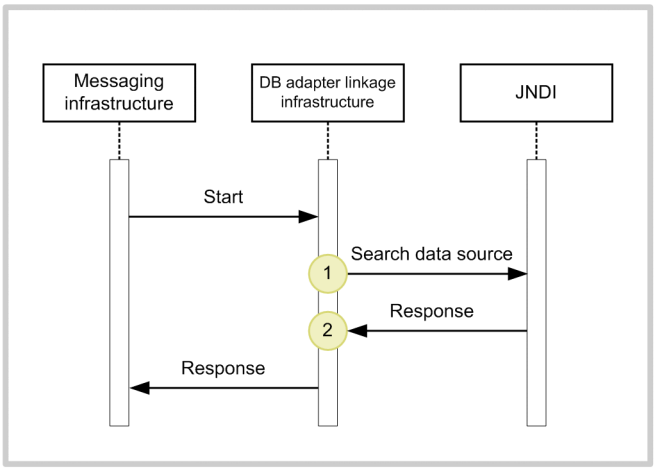
(c) For HCSC server (Database adapter)

The trace collection point of performance analysis trace differs depending on whether you execute startup operations or service components.

At the time of starting

The following figure shows the performance analysis trace collection point at the time of starting:

Figure 7–16: Figure Trace collection point of performance analysis trace (when starting the DB adapter)



Legend:

: Indicates trace collection point (PRF trace collection level is "detailed")

The following table lists the event ID, trace collection point, and the performance analysis trace collection level. The "Number in figure" in this table corresponds to the numbers in "*Figure7-16 Trace collection point of performance analysis trace (when executing DB adapter service)*".

Table 7–32: Table Performance analysis trace collection point (when starting DB adapter)

Event ID	Number in figure	Trace collection point	Level
0x9B60	1	Immediately before data source search	B
0x9B61	2	Immediately after data source search	B
0x9B62			B

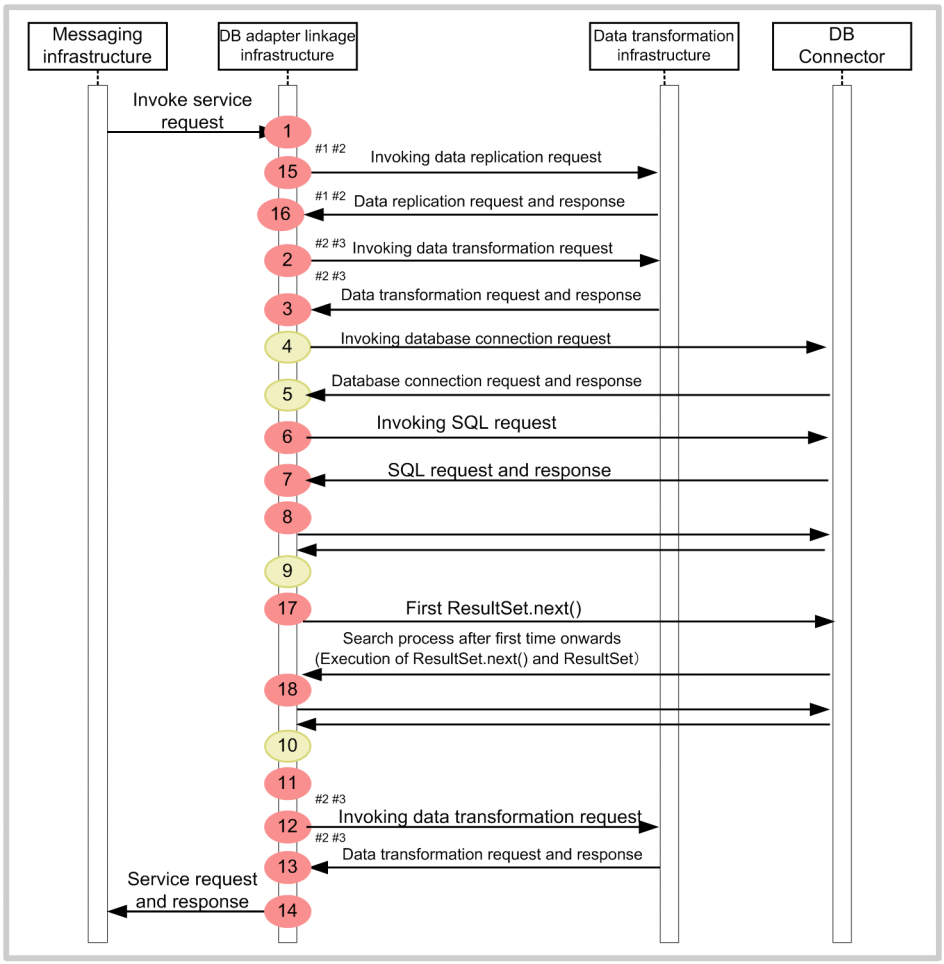
Legend:

B:Indicates the "Detail" level.

When executing service components

The following figure shows the trace collection point of performance analysis trace when executing service components:

Figure 7–17: Figure Trace collection point of performance analysis trace (when executing DB adapter service)



Legend:

: Indicates trace collection point (PRF trace collection level is "standard")

: Indicates trace collection point (PRF trace collection level is "detailed")

#1
Indicates trace collection point when there is no data transformation definition.
#2
Indicates trace collection point when data transformation definition has a binary message as the standard message type.
#3
Indicates trace collection point when data transformation definition has an XML message as a standard message type.

The following table lists the event ID, trace collection point, and the performance analysis trace collection level. The "Number in figure" in this table corresponds to the numbers in "*Figure7-17 Trace collection point of performance analysis trace(when executing DB adapter service)*".

Table 7–33: Table Performance analysis trace collection point(when executing DB adapter service)

Event ID	Number in figure	Trace collection point	Level
0x9B00	1	Immediately after invoking a service component request from messaging infrastructure	A
0x9B01	14	Immediately before the response to the service component request from messaging infrastructure	A
0x9B02			A
0x9B20	$2^{\#1\#2}$, $12^{\#1\#2}$	Immediately before invoking a data transformation request	A
0x9B21	$3^{\#1\#2}$, $13^{\#1\#2}$	Immediately after invoking a data transformation request	A

Event ID	Number in figure	Trace collection point	Level
0x9B22	3[#1#2], 13[#1#2]	Immediately after invoking a data transformation request	A
0x9B23	15[#2#3]	Immediately before invoking a data replication request	A
0x9B24	16[#2#3]	Immediately after the response to the data replication request	A
0x9B25			A
0x9B63	4	Immediately before invoking a request to connect to database	B
0x9B64	5	Immediately after invoking a request to connect to database	B
0x9B65			B
0x9B66	6	Immediately before invoking an SQL request	A
0x9B67	7	Immediately after the response to the SQL request	A
0x9B68			A
0x9B69	6	Immediately before invoking an SQL request	A
0x9B6A	7	Immediately after the response to the SQL request	A
0x9B6B			A
0x9B6C	6	Immediately before invoking an SQL request	A
0x9B6D	7	Immediately after the response to the SQL request	A
0x9B6E			A
0x9B6F	17	When executing SELECT statement from DB adapter (only when ResultSet.next() is output for the first time)	A
0x9B70	18		A
0x9B71			A
0x9B40	8	Immediately before storing SQL (SELECT) execution results	A
0x9B41	11	Immediately after storing SQL (SELECT) execution results	A
0x9B42			A
0x9B43	9	Immediately before collecting SQL (SELECT) execution results	B
0x9B44	10	Immediately after collecting SQL (SELECT) execution results	B
0x9B45			B

Legend:

A:Indicates the "Standard" level.

B:Indicates the "Detail" level.

Note

The event IDs that are not listed in the table (0x9A00 to 0x9AFF) are issued from the data transformation infrastructure.

Note#1

Indicates the trace collection point when the data transformation definition has an XML message as the standard message type.

Note#2

Indicates the trace collection point when the data transformation definition has a binary message as the standard message type.

Note#3

Indicates the trace collection point when there is no data transformation definition.

(d) In HCSC server (data transformation infrastructure)

The following table lists the event ID, trace collection point, and the performance analysis trace collection level.

Table 7–34: Table Performance analysis trace collection point (data transformation infrastructure)

Event ID	Trace collection point	Level
0x9A07	Immediately before acquiring the value from XML	A
0x9A08	Immediately after acquiring the value from XML	A
0x9A0C	Immediately before setting up the value in XML	A
0x9A0D	Immediately after setting up the value in XML	A
0x9A11	Immediately before acquiring the node from XML	A
0x9A12	Immediately after acquiring the node from XML	A
0x9A16	Immediately before setting up the node in XML	A
0x9A17	Immediately after setting up the node in XML	A
0x9A43	Immediately before data transformation	A#
0x9A44	Immediately after data transformation	A#
0x9A52	Immediately before generating the data transformation template	A
0x9A53	Immediately after generating the data transformation template	A
0x9A65	Immediately before generating the XML schema instance	A
0x9A66	Immediately after generating the XML schema instance	A
0x9A6A	Immediately before generating the XML schema instance	A
0x9A6B	Immediately after generating the XML schema instance	A
0x9A77	Immediately before XML data analysis	A
0x9A78	Immediately after XML data analysis	A
0x9A7A	Immediately before XML schema validation	A
0x9A7B	Immediately after XML schema validation	A
0x9A7C	Immediately before XML schema validation	A
0x9A7D	Immediately after XML schema validation	A
0x9A80	Immediately before XML data analysis	A
0x9A81	Immediately after XML data analysis	A
0x9A82	Immediately before data transformation	A
0x9A83	Immediately after data transformation	A
0x9A84	Immediately before XML data analysis	A
0x9A85	Immediately after XML data analysis	A
0x9A88	Immediately before generating the XML schema instance	A
0x9A89	Immediately after generating the XML schema instance	A
0x9A8D	Immediately before generating the XML schema instance	A
0x9A8E	Immediately after generating the XML schema instance	A
0x9A8F	Before invoking transformation function jar	A

Event ID	Trace collection point	Level
0x9A90	After invoking transformation function jar	A

Legend:

A:Indicatesthe "Standard" level.

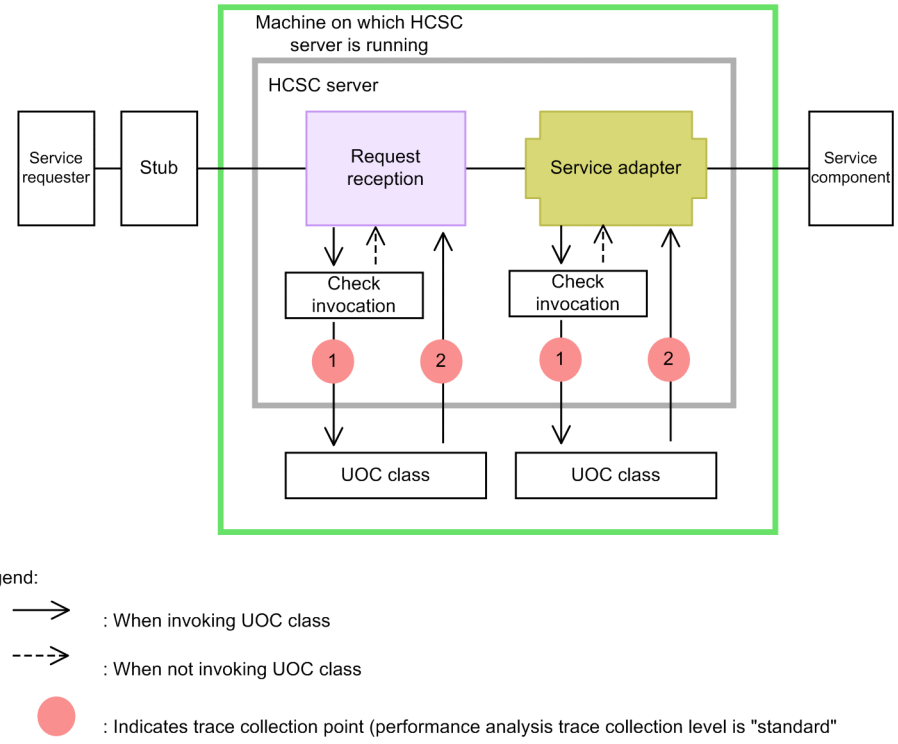
Note#

When invoking from the file operations adapter, the performance analysis trace collection level is "Detail".

(e) For HCSC server (component-common UOC)

The performance analysis trace when you use the Component-common UOC functionalityis output immediately before and after invoking the UOC class. The following figure shows the trace collection point of performance analysis trace when using component-common:

Figure 7–18: Figure Performance analysis trace collection point (when using component-common UOC)



The following table lists the event ID, trace collection point, and the performance analysis trace collection level. The "Number in figure" in this table corresponds to the numbers in "*Figure7-18 Performance analysis trace collection point (when using component-common UOC)*".

Table 7–35: Table Performance analysis trace collection point (when using component-common UOC)

Event ID	Number in figure	Trace collection point	Level
0x986C	1	Invocation of component-common UOC	A
0x986D	2	Point for receiving response from component-common UOC	A

Legend:

A:Indicates the "Standard" level.

The output format of the option information is as follows:

```
<Request identification information (parent ID)> <Request identification information (child ID)> Component type=<Component type (service adapter or reception)>, Component kind=<type>, Component ID=<Service ID of service adapter or reception ID#>, OP=<service operation name>
```

In case of abnormal end, the option information is output in the following format:

```
<Request identification information (parent ID)> <Request identification information (child
ID)> Component type=< Component type (adapter type or reception type)>, Component ID=<
Service ID of service adapter or reception ID #>, OP=< service operation name >,
Exception=<exception class name>
```

Note#

If you use the standard reception, the following fixed values are set:

Component	Reception ID
Standard reception (Web services) (SOAP1.1,SOAP 1.1/1.2 combined mode is common)	StandardReception_SOAP
Standard reception (SessionBean)	StandardReception_EJB
Standard reception (MDB(WS-R))	StandardReception_WSR
Standard reception (MDB(DB queue))	StandardReception_DBQ

(3) How to acquire the performance analysis trace and output destination

Settings are required to acquire performance analysis trace. For details, see "*7.3.1(3) Performance analysis trace*" and "7.3 Collecting performance analysis trace files using Management Server" in "Application Server Maintenance and Migration Guide".

7.4.4 "INDEXITEM="user message trace (troubleshooting)">User message trace

You can acquire the following contents as user message trace in messaging infrastructure of HCSC server:

- Request for invoking service component received in request reception or response messages
- Requests when business process is invoked or response messages
- Requests when service components are invoked from service adapter or response results
- Messages before and after transformation when data transformation is executed

The contents output in user message trace are configured from following three parts:

- User message trace start
- User message trace data
- User message trace end

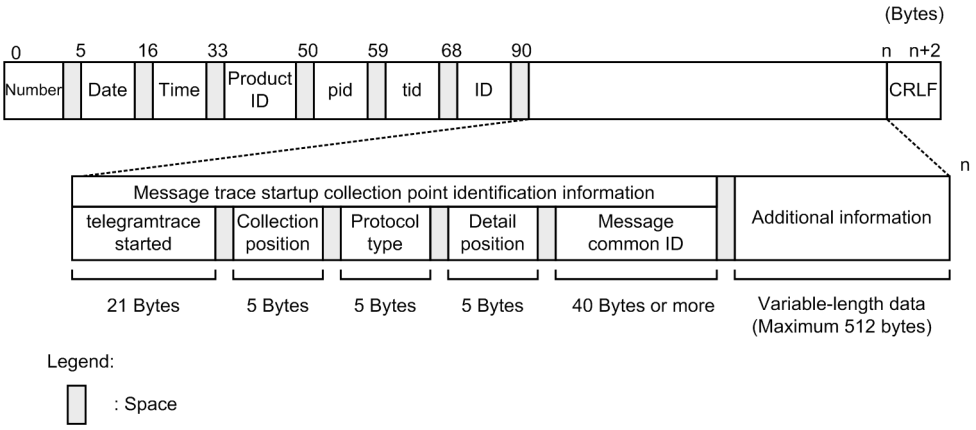
The description of each part is as follows:

(1) Output format and output content of user message trace start

(a) Output format

The following figure shows the output format of user message trace start:

Figure 7–19: Figure Output format of user message trace start



(b) Output content

The following table lists and describes contents output to user message trace start.

Table 7–36: Table Contents output to user message trace start

Item		Content
Number		The request identification information (parent ID) is displayed.
Date		The trace record collection date (yyyy/mm/dd format) is output.
Time		The trace record collection time (hh:mm:ss.sss format) in milliseconds in local time is output.
Product ID		An identifier to identify the product is output. • CSCMSG: Messaging infrastructure • CSCBP: Business process
pid		The ID to identify the process is output.
tid		The ID to identify the thread is output.
ID		Not displayed.
Message trace start collection point identification information	Message trace start	The character string "telegramtrace started" indicating the user message trace start is output.
	Collection location	The trace collection point (collection location) is output: • RCP:Standard reception • URCP:User-defined reception • BPRCP:Business process request reception • BPREQ:Invoking a business process • SVC: Invoking Service components (within the service adapter) • CNVST:Data transformation of service adapter • BPCNV:Data transformation activity of business process • BPASG:Assign activity of business process • BPJAV:Invoke Java activity of business process • BPSVC:Invoke service activity of business process • BPVLD:Validation activity of business process • BPFLT:Throw activity of business process • BPRPL:Reply activity of business process • BPSWT:Switch activity of business process

Item		Content
Message trace start collection point identification information	Protocol type	The trace collection point information (protocol type) is output. • SOAP: Web Services • EJB: SessionBean • WSR:MDB (WS-R) • DBQ:MDB (DB queue) • CUSTM:Protocols other than those mentioned above • Blank: If the collection location is: ・BPRCP or BPREQ ・Business process
	Detailed location	Outputs the trace collection point information (detailed location): • IN:Reception • OUT: Response • ERR: After error detection • CAL: Invocation (Invoking business process or service) • RET: Receiving response (Response for business process or invoking service) • RQB:Before data transformation when the request is from service adapter • RSA:After data transformation when the response is from service adapter • CVB:Before data transformation activity of business process • CVA:After data transformation activity of business process • ASB:Before assign activity of business process • ASA:After assign activity of business process • RQA:After the data transformation when the request is from User-defined reception • RSB: Before the data transformation when the response is from User-defined reception
	Message common ID	The request identification information (parent ID) is output.
Additional information		The following additional information is output: **(a) For request reception or service adapter** • Service request ID • Service name (service name) • Client correlation ID(Client ID) • PRF root application information (RootApInfo) **(b) For business process** • Process instance ID • Business process name (Process Definition Name) • Activity name (Activity Definition Name) • Variable definition name (Variable Name) • PRFroot application information (RootApInfo) **(c) For fault messages of request reception** • Service request ID • Service name (service name) • Client correlation ID(Client ID) • PRFroot application information (RootApInfo) • Fault name (fault name) **(d) For fault message of business process** • Process instance ID • Business process name (Process Definition Name)

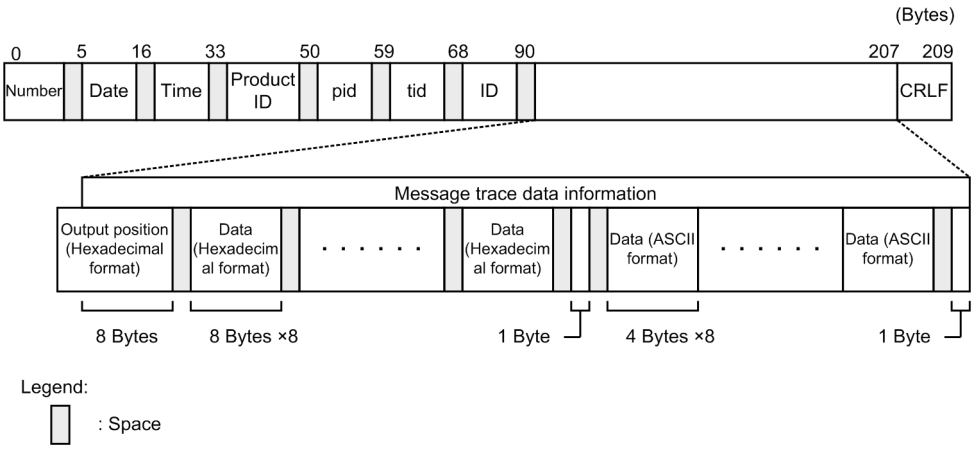
Item	Content
Additional information	• Activity name (Activity Definition Name) • PRFroot application information (RootApInfo) • Fault name (fault name)
CRLF	Record end code is output.

(2) Output format and output contents of user message trace data

(a) Output format

The following figure shows the output format of the user message trace data:

Figure 7–20: Figure Output format of user message trace data



(b) Output contents

The following table lists and describes the information that is output to the user message trace data.

Table 7–37: Table Contents output to user message trace data

Item		Content
Number		The request identification information (parent ID) is displayed.
Date		The trace record collection date (yyyy/mm/dd format) is output.
Time		The trace record collection time (hh:mm:ss.sss format) in milliseconds in local time is output.
Product ID		An identifier to specify the product is output. • CSCMSG: Messaging infrastructure • CSCBP: Business process
pid		The ID to identify the process is output.
tid		The ID to identify the thread is output.
ID		Not displayed.
Message trace data information	Output position (Hexadecimal format)	Offset value (Hexadecimal format) from the beginning of the user message is output.
	Data (Hexadecimal format)	Contents (Hexadecimal format) of user message are output.

Item		Content
Message trace data information	Data (ASCII format)	Contents (ASCII format) of user message are output. ASCII characters are output when the range is 0x20~0x7E. Period (.) is output if out of range.
CRLF		Record end code is output.

Note

For SOAP messages, the following information included in the user message is output in the user message trace data:

- Multiple child elements including soap:Header element
- One child element of soap:Body element

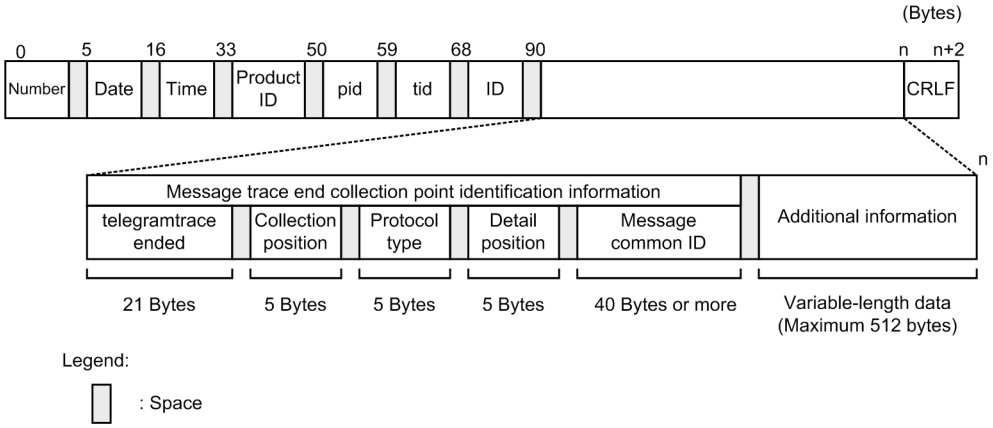
If the soap:Header element does not exist, only child element of soap: Body element is output as information.

(3) Output format and output contents of user message trace end

(a) Output format

The following figure shows the output format of user message trace end:

Figure 7–21: Figure Output format of user message trace end



(b) Output content

The following table lists and describes contents output to user message trace end:

Table 7–38: Table Contents output to user message trace end

Item	Output
Number	The request identification information (parent ID) is displayed.
Date	The trace record collection date (yyyy/mm/dd format) is output.
Time	The trace record collection time (hh:mm:ss.sss format) in milliseconds in local time is output.
Product ID	An identifier to specify the product is output. • CSCMSG:Messaging infrastructure • CSCBP:Business process
Pid	The ID to identify the process is output.
Tid	The ID to identify the thread is output.
ID	Not displayed.

Item		Output
Message trace end collection point identification information	Message trace end	The character string "telegramtrace ended" indicating user message trace end is output.
	Collection location	The trace collection point (collection location) is output: • RCP:Standard reception • URCP:User-defined reception • BPRCP:Business process request reception • BPREQ:Invoking a business process • SVC: Invoking Service components (within the service adapter) • CNVST:Data transformation of service adapter • BPCNV:Data transformation activity of business process • BPASG:Assign activity of business process • BPJAV:Invoke Java activity of business process • BPSVC:Invoke service activity of business process • BPVLD:Validation activity of business process • BPFLT:Throw activity of business process • BPRPL:Reply activity of business process • BPSWT:Switch activity of business process
	Protocol type	The trace collection point information (protocol type) is output. • SOAP: Web Services • EJB: SessionBean • WSR:MDB (WS-R) • DBQ:MDB (DB queue) • CUSTM:Protocols other than those mentioned above • Blank: If the collection location is: ・BPRCP or BPREQ ・Business process
	Detailed location	Outputs the trace collection point information (detailed location): • IN: Reception • OUT: Response • ERR: After error detection • CAL: Invocation (Invoking business process or service) • RET: Receiving response (Response for business process or invoking service) • RQB:Before data transformation when the request is from service adapter • RSA:After data transformation when the response is from service adapter • CVB:Before data transformation activity of business process • CVA:After data transformation activity of business process • ASB:Before assign activity of business process • ASA:After assign activity of business process
	Message common ID	The request identification information (parent ID) is output.
Additional information		The length (decimal format) of user message is output as additional information. When there is no user message, "0"or "null" is output.
CRLF		Record end code is output.

(4) Timing of user message trace output

Specify the timing of user message trace output in the telegramtrace-trigger property of the HCSC server runtime definition file. The following table lists and describes the output timings and combination with messages that can be specified with the telegramtrace-trigger property. Default timing in property is "NORMAL".

Table 7–39: Table Output timings and combination with messages that can be specified in the telegramtrace-trigger property

Output timing	Timing	Message type		
		Request message	Response message	Fault message
NORMAL	At the time of normal processing	Y	Y	N
	At the time of detecting system exceptions	N	N	N
	At the time of detecting faults (without catch)	N	N	N
	At the time of detecting faults (with catch)	N	N	N
SYSERR	At the time of normal processing	N	N	N
	At the time of detecting system exceptions	Y	N	N
	At the time of detecting faults (without catch)	Y	N	N
	At the time of detecting faults (with catch)	N	N	N
FAULT	At the time of normal processing	N	N	N
	At the time of detecting system exceptions	N	N	N
	At the time of detecting faults (without catch)	Y	N	Y
	At the time of detecting faults (with catch)	Y	N	Y

Legend:

Y: Output

N: Not output

(5) Collection point of user message trace

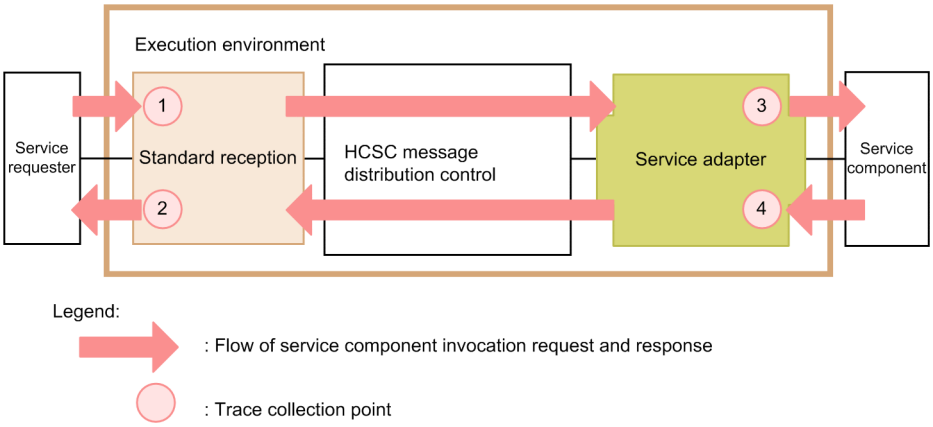
User message traces are output at the following times, and the trace collection point for each time is different:

- NORMAL (Executing individual services (when there is no data transformation))
- NORMAL (Executing individual services (when there is data transformation))
- NORMAL(when invoking a business process)
- NORMAL(when executing business process services)
- SYSERR (at the time of detecting system exceptions)
- FAULT(at the time of detecting faults)

(a) NORMAL (Executing individual services (when there is no data transformation))

The following figure shows the collection point of user message trace when executing individual services (when there is no data transformation):

Figure 7–22: Figure Collection point of user message trace (Executing individual services (when there is no data transformation))



The following table lists trace collection points. The "Number in figure" in this table corresponds to the numbers in "*Figure7-22 Collection point of user message trace (Executing individual services(when there is no data transformation))*".

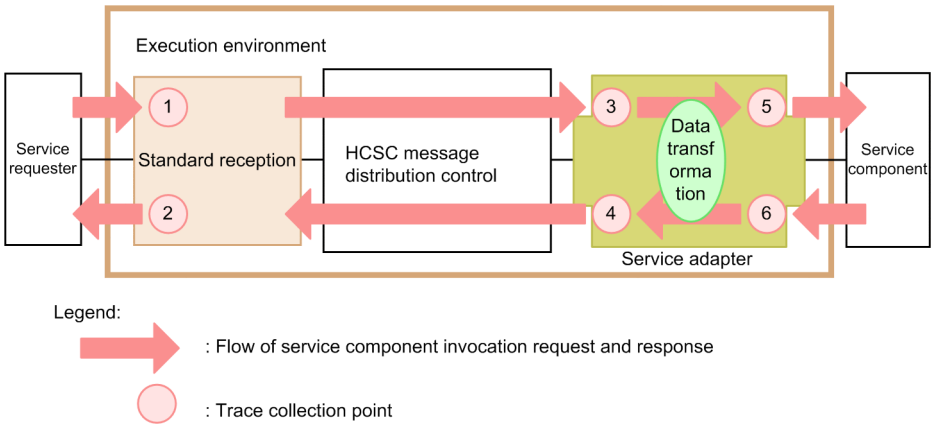
Table 7–40: Table User message trace collection point (Executing individual services (when there is no data transformation))

Number in figure	Trace collection point
1	Entry to standard reception (Web Services)
2	Exit from standard reception (Web Services)
1	Entry to standard reception (SessionBean)
2	Exit from standard reception (SessionBean)
1	Entry to standard reception (MDB(WS-R))
2	Exit from standard reception (MDB(WS-R))
1	Entry to standard reception (MDB(DB queue))
2	Exit from standard reception (MDB(DB queue))
3	Invocation of service components of SOAP adapter
4	Point for receiving response from service components of SOAP adapter
3	Invocation of service components of SessionBean adapter
4	Point for receiving response from service components of SessionBean adapter
3	Invocation of service components of MDB (WS-R) adapter
4	Point for receiving response from service components of MDB (WS-R) adapter
3	Invocation of service components of MDB (DB queue) adapter
4	Point for receiving response from service components of MDB (DB queue) adapter
3	Invocation of service components of service adapters(CUSTOM) other than those mentioned above
4	Point for receiving response from service components of service adapters(CUSTOM) other than those mentioned above

(b) NORMAL (Executing individual services(in case of data transformation))

The following figure shows the trace collection point of user message trace when executing individual services (in case of data transformation):

Figure 7–23: Figure Collection point of user message trace (Executing individual services(in case of data transformation))



The following table lists trace collection points. The "Number in figure" in this table corresponds to the numbers in "*Figure7-23 Collection point of user message trace (Executing individual services (in case of data transformation))*".

Table 7–41: Table User message trace collection point (executing individual services (in case of data transformation))

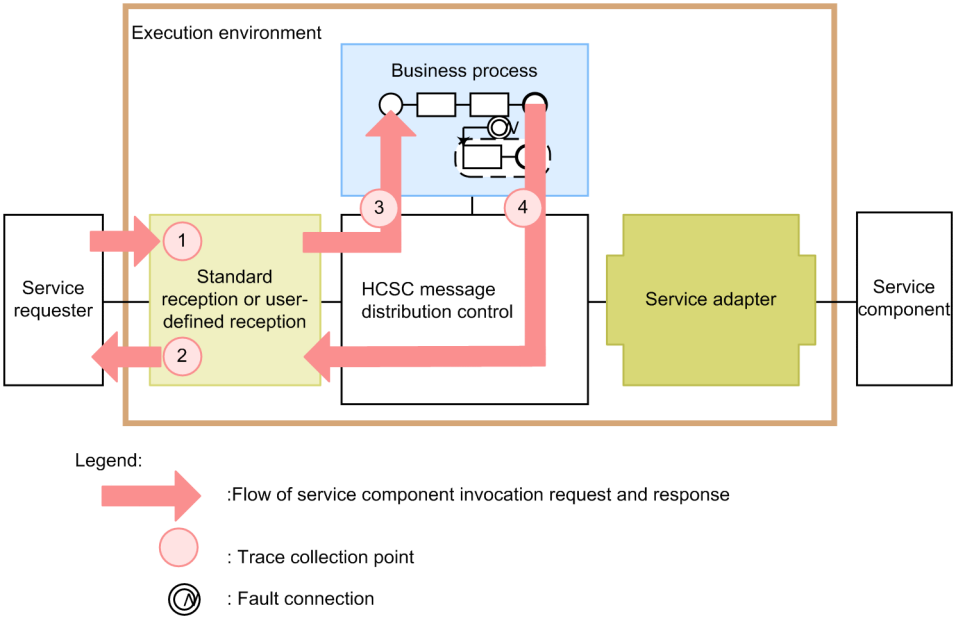
Number in figure	Trace collection point
1	Entry to standard reception (Web Services)
2	Exit from standard reception (Web Services)
1	Entry to standard reception (SessionBean)
2	Exit from standard reception (SessionBean)
1	Entry to standard reception (MDB(WS-R))
2	Exit from standard reception (MDB(WS-R))
1	Entry to standard reception (MDB(DB queue))
2	Exit from standard reception (MDB(DB queue))
3	Before data transformation when defining the standard message definition of SOAP adapter
4	After data transformation when defining the standard message definition of SOAP adapter
3	Before data transformation when defining the standard message definition of SessionBean adapter
4	After data transformation when defining the standard message definition of SessionBean adapter
3	Before data transformation when defining the standard message definition of MDB (WS-R) adapter
4	After data transformation when defining the standard message definition of MDB (WS-R) adapter
3	Before data transformation when defining the standard message definition of MDB (DB queue)
4	After data transformation when defining the standard message definition of MDB (DB queue)
3	Before data transformation when defining the standard message definition of service adapter (CUSTOM) other than those mentioned above
4	After data transformation when defining the standard message definition of service adapter (CUSTOM) other than those mentioned above

Number in figure	Trace collection point
5	Invocation of service components of SOAP adapter
6	Point for receiving response from service components of SOAP adapter
5	Invocation of service components of SessionBean adapter
6	Point for receiving response from service components of SessionBean adapter
5	Invocation of service components of MDB (WS-R) adapter
6	Point for receiving response from service components of MDB (WS-R) adapter
5	Invocation of service components of MDB (DB queue) adapter
6	Point for receiving response from service components of MDB (DB queue) adapter
5	Invocation of service components of service adapters(CUSTOM) other than those mentioned above
6	Point for receiving response from service components of service adapters(CUSTOM) other than those mentioned above

(c) NORMAL (when invoking a business process)

The following figure shows the trace collection point of the user message trace when invoking business process:

Figure 7–24: Figure Collection point of user message trace(when invoking a business process)



The following table lists trace collection points. The "Number in figure" in this table corresponds to the numbers in "*Figure7-24 Collection point of user message trace (when invoking a business process)*".

Table 7–42: Table User message trace collection point (when invoking a business process)

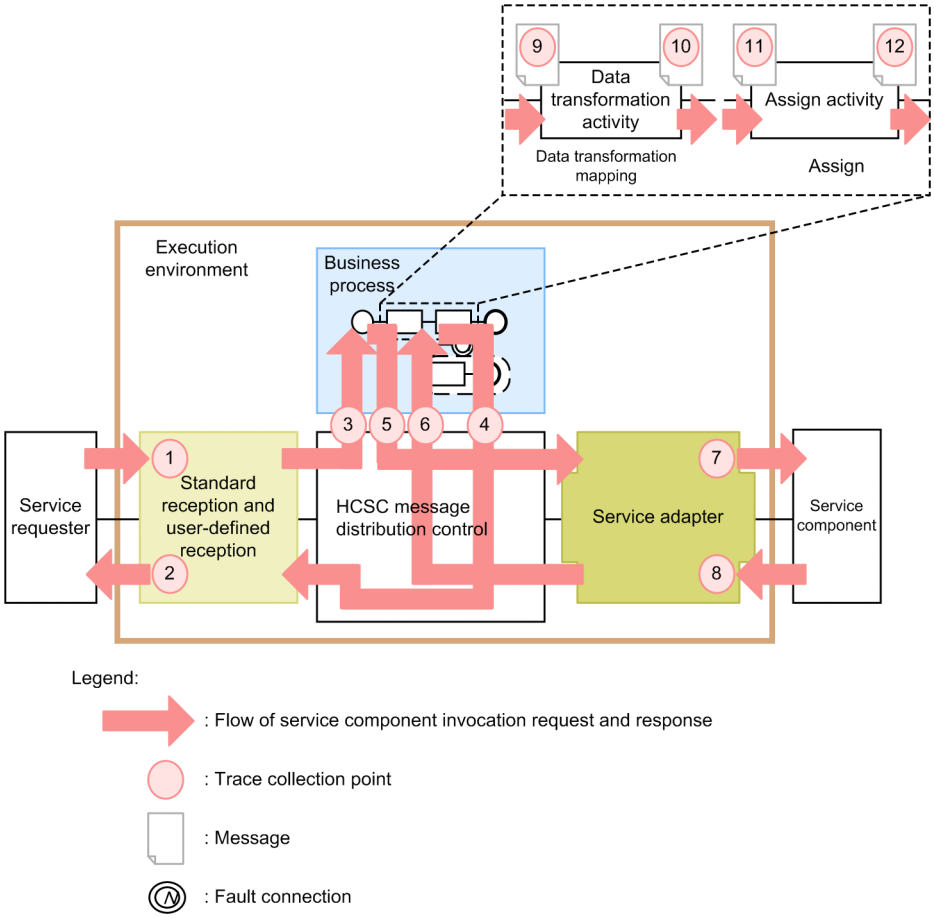
Number in figure	Trace collection point
1	Entry to standard reception (Web Services)
2	Exit from standard reception (Web Services)
1	Entry to standard reception (SessionBean)
2	Exit from standard reception (SessionBean)

Number in figure	Trace collection point
1	Entry to standard reception (MDB(WS-R))
2	Exit from standard reception (MDB(WS-R))
1	Entry to standard reception (MDB(DB queue))
2	Exit from standard reception (MDB(DB queue))
1	Entry to user-defined reception
2	Exit from user-defined reception
3	Invocation of business process services
4	Point for receiving response from business process services

(d) NORMAL(when executing business process services)

The following figure shows the trace collection point of the user message trace when executing business process services:

Figure 7–25: Figure Collection point of user message trace (when executing business process services)



The following table lists trace collection points. The "Number in figure" in this table corresponds to the numbers in "*Figure7-25 Collection point of user message trace (when executing business process services)*".

Table 7–43: Table User message trace collection point (when executing business process services)

Number in figure	Trace collection point
1	Entry to standard reception (Web Services)
2	Exit from standard reception (Web Services)
1	Entry to standard reception (SessionBean)
2	Exit from standard reception (SessionBean)
1	Entry to standard reception (MDB (WS-R))
2	Exit from standard reception (MDB (WS-R))
1	Entry to standard reception (MDB (DB queue))
2	Exit from standard reception (MDB (DB queue))
1	Entry to user-defined reception
2	Exit from user-defined reception
7	Invocation of service components of SOAP adapter
8	Point for receiving response from service components of SOAP adapter
7	Invocation of service components of SessionBean adapter
8	Point for receiving response from service components of SessionBean adapter
7	Invocation of service components of MDB (WS-R) adapter
8	Point for receiving response from service components of MDB (WS-R) adapter
7	Invocation of service components of MDB (DB queue) adapter
8	Point for receiving response from service components of MDB (DB queue) adapter
7	Invocation of service components of service adapters (CUSTOM) other than those mentioned above
8	Point for receiving response from service components of service adapters(CUSTOM) other than those mentioned above
3	Invocation of business process services
4	Point for receiving response from business process services
5	Entry to business process reception
6	Exit from business process reception
9	Transformation source of data transformation activity#1
10	Transformation destination of data transformation activity
11	Copy source of assign activity#2, #3
12	Copy destination of assign activity

Note#1

When multiple transformation source variables are defined, user message traces for the number of variables defined are output.

Note#2

When there are no messages (character strings, numeric values, or authentic value), the character string expression of variable is output as binary data encoded in UTF-8 as a user message.

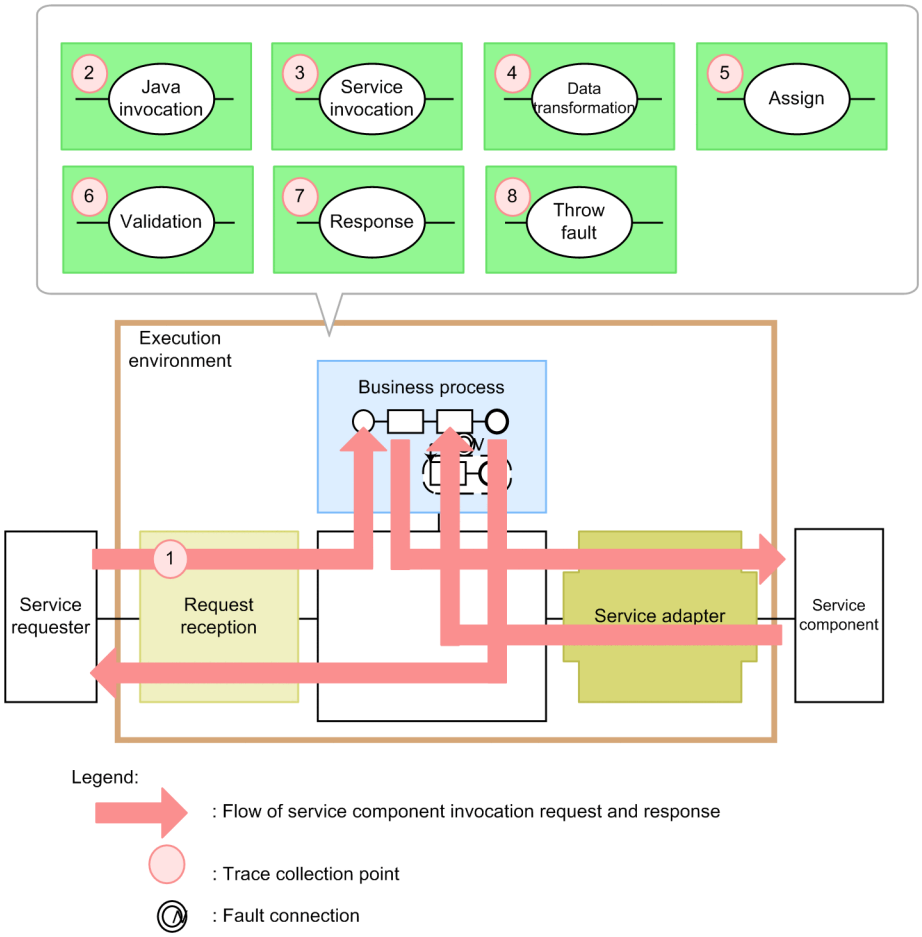
Note#3

The user message trace is not output when you specify format (Xpath) or a constant in copy source.

(e) SYSERR (At the time of detecting system exceptions)

The following figure shows the trace collection point of the user message trace when a system exception (does not include system error such as OutOfMemoryError) is detected:

Figure 7–26: Figure Collection point of user message trace (At the time of detecting system exceptions)



The following table describes the trace collection point. The "Number in figure" in this table corresponds to the numbers in Figure 7-26.Furthermore, standby activity, switch activity, while activity, and link connection is output.

Table 7–44: Table User message trace collection point (At the time of detecting system exceptions)

Number in figure	Output point	Output message	Details of user message trace start		
			Collection point	Protocol type	Detailed location
1	Request reception (when invoking a service)	Requester side message	RCP/URCP	SOAP/EJB/ WSR/DBQ/ CUSTM	ERR
2	Invoke Java activity	Argument when invoking Java program[#1]	BPJAV	-	
3	Invoke service activity	Request message when invoking services	BPSVC		
4	Data transformation activity	Transformation source variable[#2]	BPCNV		
5	Assign activity	Copy source variable[#3]	BPASG		

Number in figure	Output point	Output message	Details of user message trace start		
			Collection point	Protocol type	Detailed location
6	Validation activity	Variable to be validated[#2]	BPVLD	-	ERR
7	Reply activity	Response message to requester	BPRPL		
8	Throw activity	Variable that throws faults	BPFLT		

Legend:

-:Not applicable.

Note#1

When there are no messages (character strings, numeric values, or authentic value), the character string expression of variable is output as binary data encoded in UTF-8 as a user message.

Note#2

When multiple transformation source variables are defined, user message traces for the number of variables defined are output.

Note#3

The user message trace is not output in the following cases:

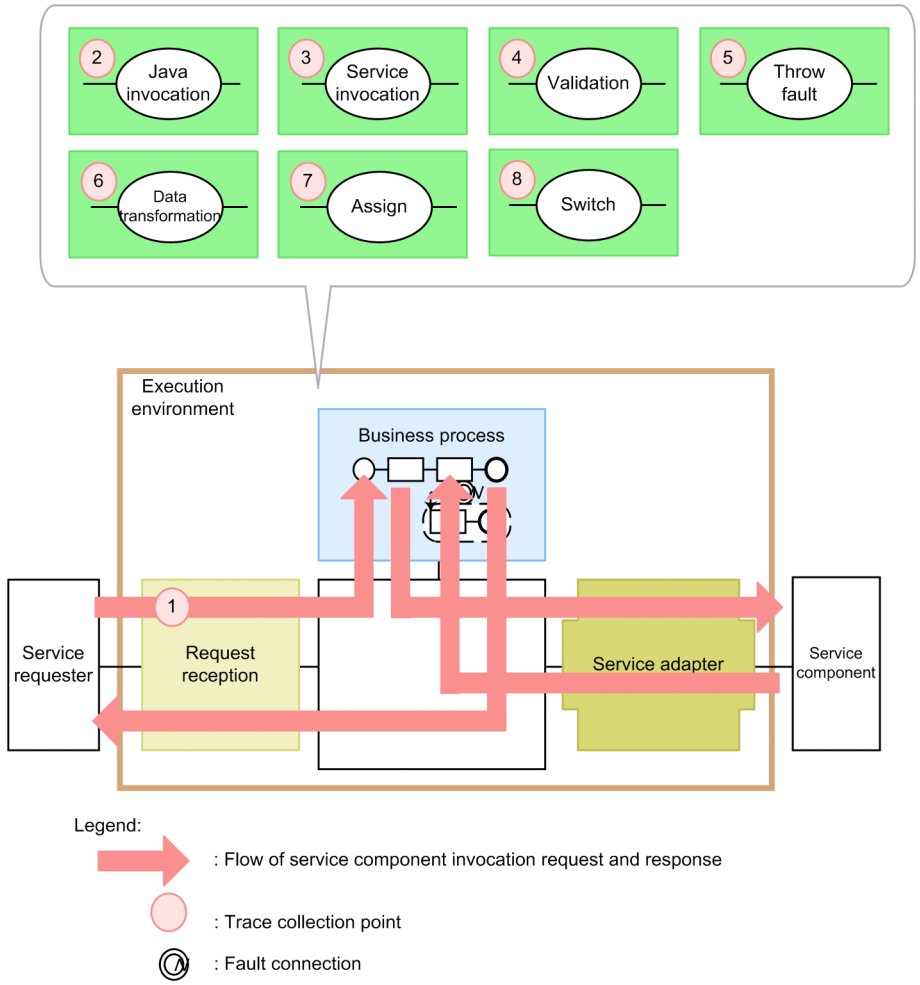
When you specify format (Xpath) in copy source

When you specify a constant in copy source

(f) FAULT (at the time of detecting faults)

The following figure shows the trace collection point of the user message trace when a fault is detected:

Figure 7–27: Figure Collection point of user message trace (at the time of detecting faults)



The following table describes the trace collection point. The "Number in figure" in this table corresponds to the numbers in Figure 7-27.

Table 7–45: Table User message trace collection point (at the time of detecting faults)

Number in figure	Output point	Output message	Details of user message trace start		
			Collection point	Protocol type	Detailed location
1	Request reception (when invoking a service)	Request message	RCP/URCP	SOAP/EJB/ WSR/DBQ	ERR
		Fault message		-	
2	Invoke Java activity	Argument when invoking Java program[#1]	BPJAV		
		Fault message			
3	Invoke service activity	Request message when invoking services	BPSVC		
		Fault message			
4	Validation activity	Variable to be validated[#2]	BPVLD		
		Fault message			

Number in figure	Output point	Output message	Details of user message trace start		
			Collection point	Protocol type	Detailed location
5	Throw activity	Variable that throws faults[#3]	BPFLT	-	ERR
6	Data transformation activity	Transformation source variable[#2]	BPCNV		
		Fault message			
7	Assign activity	Copy source variable[#4]	BPASG		
		Fault message			
8	Switch activity	Fault message	BPSWT		

Legend:

-:Not applicable.

Note#1

When there are no messages (character strings, numeric values, or authentic value), the character string expression of variable is output as binary data encoded in UTF-8 as a user message.

Note#2

When multiple transformation source variables are defined, user message traces for the number of variables defined are output.

Note#3

Since the variable information and fault message match, fault message is not output.

Note#4

When a fault exception occurs in a state when multiple copy source variables are defined, the copy source variable that caused to occur the fault is output in the log.

The user message trace is not output in the following cases:

When you specify format (Xpath) in copy source

When you specify constant in copy source

(6) How to acquire the user message trace

Settings are required to acquire the user message trace. For details, see "*7.3.1 How to acquire log or trace output by Cosminexus Service Platform*".

(7) Output destination of user message trace

The following is the output destination of the user message trace.

```
Path specified in telegramtrace-filepath property of the HCSC server runtime
definition file.
```

Furthermore, if the specified path does not exist, or if there is an error in the path, trace is output in the output destination of the omitted value.

The following table shows the trace file name of the user message trace:

Output mode of trace file	Trace file name
For Wrap around mode	csctelegram_<HCSC server name>_<number of files>.log
For Shift mode	csctelegram_<HCSC server name>_.log

7.4.5 Maintenance log and trace

Capture the log and trace for maintenance as information required for failure investigation.

(1) Exception log

The internal error information and the failure information of the business process when there is a failure while operating HCSC server is captured as exception log. Maintenance Service uses the exception log for analyzing the failure. The following table describes the contents output as exception log of Service Platform and the output destination:

Table 7–46: Table Output content and output destination of exception log

Type of exception log	Output contents	Output destination path of exception log file	Log file name
Exception log of HCSC-Manager	Acquires the internal exception information of HCSC-Manager.	Path specified in cscmng.log.dir parameter of HCSC-Manager definition file[#1]	exception<number of files>.log[#1]
Exception information when a J2EE server failure occurs	Acquires the internal exception information when a failure has occurred in the HCSC server.	Path specified in the output destination [#2] of exception log of J2EE server (exception information at the time of failure occurrence)	• For Wraparound mode cjexception<number of files>.log[#1] • For Shift mode cjexception.log
Exception log of HCSC server	Acquires the information of the exception (stack trace) that has occurred at the following locations: • EJB invocation part of Custom reception framework, Custom adapter development framework • Reception and service adapter using Custom reception framework, Custom adapter development framework • HCSC server (standard reception, SOAP reception, message delivery control, SOAP adapter, SessionBean adapter, MDB (WS-R) adapter, MDB (DB queue) adapter.	Path specified in the methodtrace-filepath property of the HCSC server runtime definition file[#3]	• For Wraparound mode cscmsgexp_<HCSC server name>_<number of files>.log[#3] • For Shift mode cscmsgexp_<HCSC server name>_.log
Exception log of DB adapter	Acquires the stack trace when a failure has occurred in DBadapter	Path specified in the methodtrace-filepath property of the HCSC server runtime definition file[#3]	• For Wraparound mode cscdbaexp_<HCSC server name>_<number of files>.log[#3] • For Shift mode cscdbaexp_<HCSC server name>_.log
Exception log of TP1 adapter	Acquires the stack trace when a failure has occurred in TP1 adapter	<Working directory of J2EE server>\ejb\<J2EE server name>\logs \CSCADP\TP1ADP \maintenance\<Service ID>	• For Wraparound mode exception< number of files>.log[#4] • For Shift mode exception.log
Exception log of Object Access adapter	Acquires the stack trace when a failure has occurred in Object Access adapter	<Working directory of J2EE server>\ejb\<J2EE server name>\logs \CSCADP\OAADP \maintenance\<Service ID>	• For Wraparound mode exception<number of files>.log[#5] • For Shift mode exception.log
Exception log of Message Queue adapter	Acquires the stack trace when a failure has occurred in Message Queue adapter	<Working directory of J2EE server>\ejb\<J2EE server name>\logs \CSCADP\MQADP \maintenance\<Service ID>	• For Wraparound mode exception<number of files>.log[#6] • For Shift mode exception.log

Type of exception log	Output contents	Output destination path of exception log file	Log file name
Exception log of FTP adapter	Acquires the stack trace when a failure has occurred in FTP adapter	Path specified in FTP adapter runtime-environment property file[#7]	• For Wraparound mode cscftpadpexp_<HCSC server name>_<number of files>.log[#7] • For Shift mode cscftpadpexp_<HCSC server name>_.log
Exception log of file operations adapter	Acquires the stack trace when a failure has occurred in file operations adapter	Path specified in file operations adapter runtime-environment property file[#8]	• For Wraparound mode cscadpfopexp_<HCSC server name>_<number of files>.log[#8] • For Shift mode cscadpfopexp_<HCSC server name>_.log
Exception log of mail adapter	Acquires the stack trace when a failure has occurred in mail adapter	Path specified in mail adapter runtime-environment property file[#9]	• For Wraparound mode cscmailadpexp_<HCSC server name>_<number of files>.log[#9] • For Shift mode cscmailadpexp_<HCSC server name>_.log
Exception log of business process	Acquires the stack trace when a failure has occurred in business process	Path specified in the methodtrace-filepath property of the HCSC server runtime definition file[#3]	• For Wraparound mode cscbpexp_<HCSC server name>_<number of files>.log[#3] • For Shift mode cscbpexp_<HCSC server name>_.log

Note#1

Specify the following parameters in the HCSC-Manager definition file:

cscmng.log.exception.filesize=Exception log file size

cscmng.log.exception.filenum= Exception log file numbers

cscmng.log.dir= Exception log output destination directory path

For details on the HCSC-Manager definition file, see"HCSC-Manager definition file" in "Service Platform Reference Guide".

Note#2

Specify the output destination of exception log (exception information when a failure occurs) of J2EE server to usrconf.cfg (option definition file for J2EE server). Default output destination is<Installation directory of Service Platform>\CC\server \public\ejb\<J2EE server name>\logs.

For details on usrconf.cfg,see "2.3 usrconf.cfg (option definition file for J2EE server) " in "Application Server Definition Reference Guide".

Specify the size and number of exception log files in usrconf.properties (user property file for J2EE server). For details on usrconf.properties, see "2.4 usrconf.properties (user property file for J2EE server) " in "Application Server Definition Reference". For the details on settings of the rotation method of log files, see "Application Server Definition Reference Guide".

Note#3

For details on the specification of output destination path and numbers of the HCSC server runtime definition file, see "HCSC server runtime definition file" in "Service Platform Reference Guide".

Note#4

For details on the specification of numbers of the TP1-adapter runtime-environment property fileTP1, see "TP1 adapter execution environment property file" in "Service Platform Reference Guide".

Note#5

For details on the specification of numbers of the Object Access adapter runtime-environment property file, see "Object Access adapter execution environment property file" in "Service Platform Reference Guide".

Note#6

For details on the specification of numbers of the Message Queue adapter runtime-environment property file, see "Message Queue adapter execution environment property file" in "Service Platform Reference Guide".

Note#7

For details on the output destination path and numbers of the FTP-adapter runtime-environment property file, see "FTP adapter execution environment property file" in "Service Platform Reference Guide".

Note#8

For details on the output destination path and numbers of File operations adapter runtime-environment property file, see "File operations adapter execution environment property file" in "Service Platform Reference Guide".

Note#9

For details on the output destination path and numbers of the Mail adapter runtime environment property file, see "Mail adapter execution environment property file" in "Service Platform Reference Guide".

(2) " INDEXITEM="maintenance log (failure information type)">Maintenance log

You can acquire the internal maintenance information of the HCSC-Manager internal as a maintenance log. The maintenance log is also used as a communication trace and message log between HCSC-Manager and external elements (such as Manager, HCSC management MBean, and the repository). The Maintenance Service uses the maintenance log for analyzing failures.

The following table lists and describes the content and the output destination that is output as the maintenance log:

Table 7–47: Table Content and the output destination of the maintenance log

Output content	Output destination path of the Maintenance log file	Log file name
Acquire the internal maintenance information of HCSC-Manager	Path specified in the cscmng.log.dir parameter of the HCSC-Manager definition file	maintenance<number of files>.log

(3) Method trace

If a failure occurs on a HCSC server and the cause is difficult to determine, you can acquire the required information as method trace. The Maintenance Service uses the method trace for analyzing failures.

The following table describes the output content and output destination of method traces.

Table 7–48: Table Output content and output destination of method trace

Method trace type	Output content	Output destination path of method trace	Trace file name
Method trace of HCSC server (messaging infrastructure)	Acquires the internal maintenance information of the HCSC server (messaging infrastructure).	Path specified in the methodtrace-filepath property of the HCSC server runtime-definition file. If the specified path does not exist, or if there is an error in the path, trace is output in the output destination of the omitted value.	• For Wraparound mode cscmsgmtd_<HCSC server name>_<number of files>.log • For Shift mode cscmsgmtd_<HCSC server name>_.log
Method trace of the HCSC server(business process infrastructure)	Acquires the internal maintenance information of the HCSC server(business process infrastructure). In the business process infrastructure, a trace is present when executing the trace and process instance related commands, when you execute the business process. This manual describes the trace when executing business processes. The trace at the time of executing process instance related commands is same as the trace output in Management Server. For details, see "Application Server Maintenance and Migration Guide".		• For Wraparound mode cscbpmtd_<HCSC server name>_<number of files>.log • For Shift mode cscbpmtd_<HCSC server name>_.log

Method trace type	Output content	Output destination path of method trace	Trace file name
Method trace of the HCSC server (DB adapter)	Acquires the internal maintenance information of the HCSC server (DB adapter). For details on the method trace of a service adapter other than DB adapter, see the description of each service adapter in "*7.7 Troubleshooting during service component invocation request*".	Path specified in the methodtrace-filepath property of the HCSC server runtime-definition file. If the specified path does not exist, or if there is an error in the path, trace is output in the output destination of the omitted value.	• For Wraparound mode cscdbamtd_<HCSC server name>_<number of files>.log • For Shift mode cscdbamtd_<HCSC server name>_.log

7.5 Troubleshooting During System Setup and Unsetup

7.5.1 Error investigations in software settings that are required in execution environment

This subsection describes about how to perform the investigations when there is an error while executing the system operations such as environment settings for setup. For details about the logs, see *7.3 Acquiring failure information*.

(1) When an error occurs while operating the database

Investigate the error messages output to HiRDB log (pdlog(n)) for HiRDB. For details about the Oracle, see the documents published by Oracle Corporation.

(2) When an error occurs while operating the Manager

If you encounter an error that prevents Management Server or Management Server - Administration Agent from starting, investigate the error messages that Service Platform outputs to the Administration Agent, Management Agent, and Management Server logs.

(3) When an error occurs while operating the Component Container (J2EE server or Component Container)

If you encounter an error while you are operating the J2EE server, investigate the error messages that the J2EE server outputs to the J2EE server, redirector, and server management command logs.

(4) When an error occurs while operating Reliable Messaging

Initially, investigate the error messages output to message log. Investigate the start stop message log, method trace of Reliable Messaging.

When error code such as `HRM-xxxxx` is output to message, see *7.9 Error code details* in the manual *Cosminexus Application Server Cosminexus Reliable Messaging* and take appropriate actions.

The information set up by Reliable Messaging for configuration property is required for investigating errors. Also the information set to DB Connector related to Reliable Messaging is required. These setup contents are checked again and investigations are done and respective actions are taken.

(5) When an error occurs while operating the DB Connector

Initially, investigate the error messages output to message log. Reference the operation log of the DB Connector (resource adapter) where error occurs.

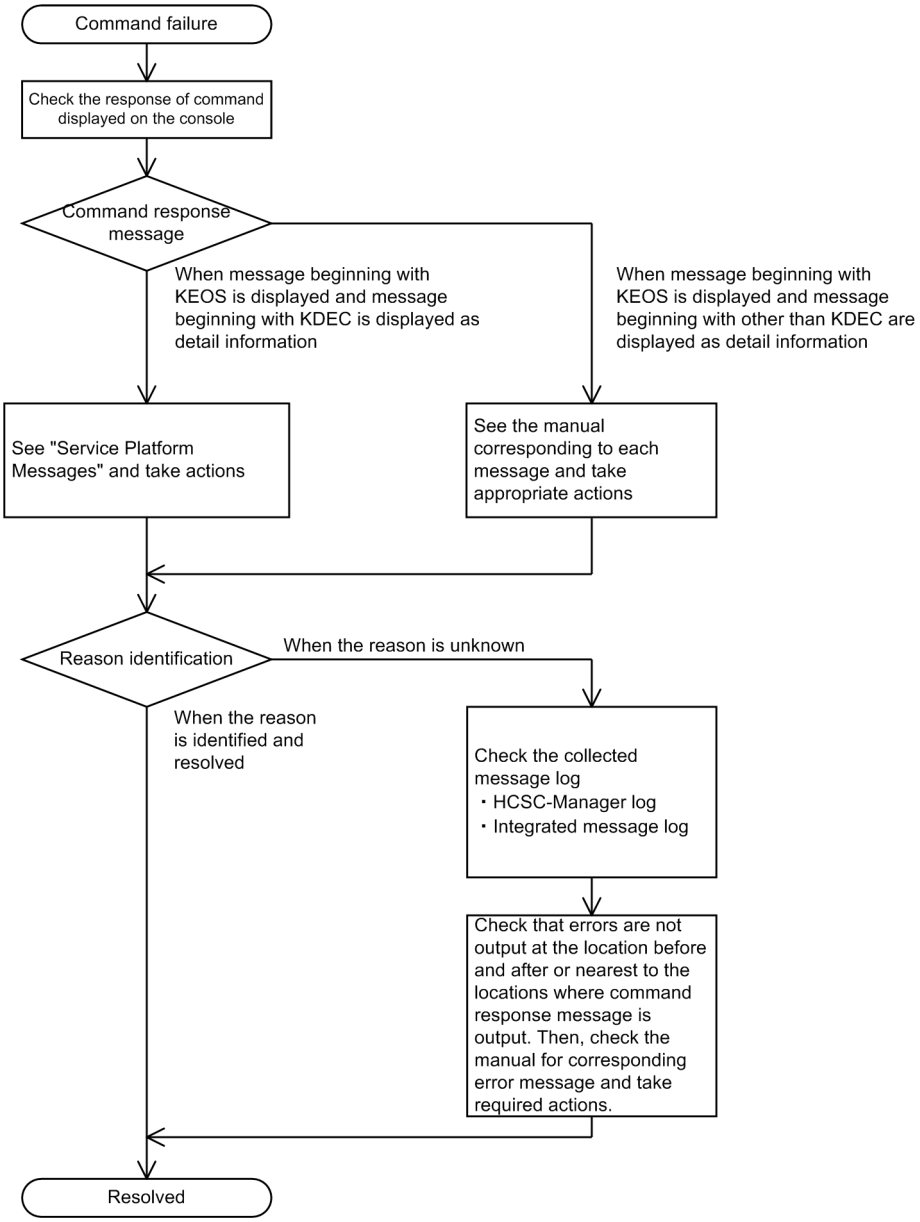
The information set up in DB Connector is required for investigating errors. Please investigate the setup contents and take respective actions while executing these setup contents.

7.5.2 Failure investigations when executing setup and unsetup

(1) Methods for log analysis and classification of failures

The following figure shows the investigation procedure when a failure occurs when executing setup or unsetup:

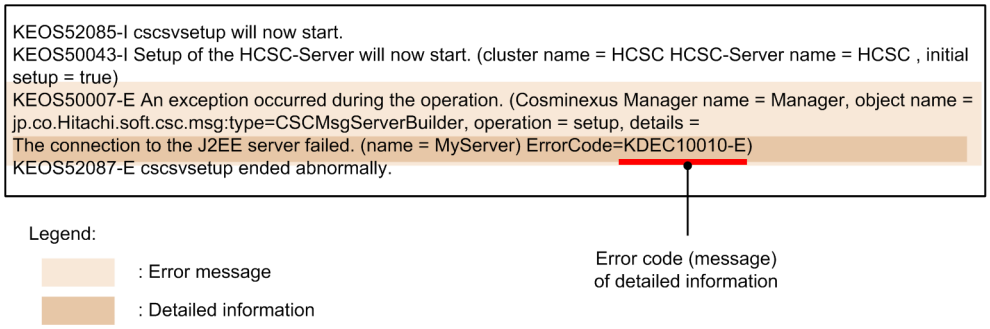
Figure 7–28: Figure Procedure to investigate failures (which occur during execution of setup or unsetup)



The flow of investigation shown in this figure is as follows:

1. When a failure occurs in setup or unsetup, first check the message that is output to console as a response to the command.

   Check if another message ID is output as detailed information of messages starting with KEOS (messages related to HCSC-Manager). The output example is as follows:



- For messages whose detailed information includes a message ID that begins with KDEC

  See the manual *uCosminexus Service Platform Messages*, and take countermeasures.

- For messages whose detailed information includes a message ID that does not begin with KDEC

  See the manual appropriate for the message. For example, if the detailed information includes a message ID that begins with KDJE, see the manual *uCosminexus Application Server Messages*.

2. Reference the acquired message log when the cause cannot be identified. The following message log is the failure information to be referenced when executing setup or unsetup. For details, see "*7.4.1 Message log*".

   - HCSC-Manager log
   - Integrated message log

   Failure occurrence might be caused due to environment settings or system status before command execution. Therefore, check the locations where command response messages are output, confirm that no other error messages appear, and take appropriate actions.

Furthermore, messages output to console are sometimes duplicated. Therefore, check for the appropriate execution time, when you check the contents of messages.

(2) Typical failures and countermeasures

This point describes the typical failures and countermeasures when executing setup and unsetup:

Table 7–49: Table Typical failures and countermeasures (failure investigation when executing setup and unsetup)

Procedure (Flow)		Representative error	Probable causes	Actions
At the time of setting the software required for execution environment	During setup of the database on the server	Cannot set up the permissions	Database definition utility, (pddef), path of SQL Executer is not set.	Set the database definition utility (pddef), path of SQL Executer.
	During setup of Manager	Management Server is not started	Error in mserver.properties format.	Review mserver.properties.For details, see "*3.1.2 Setting up the software required for the execution environment*".
			Error in mserver.cfg format.	Review mserver.cfg.
		Management Server and Administration Agent are not started automatically	Management Server and Administration Agent are not setup to be started automatically.	Setup the Management Server and Administration Agent so that they are started automatically.
		Administration Agent is not started	Error in adminagent.cfg format.	Review adminagent.cfg.
		KEOS27010-I message is not output while checking the startup of MBean	The definition file and jar does not exist under the <Installation directory of Service Platform>\manager\mbean-plugins.	Copy files under <Installation directory of Service Platform>\CSC\mbean-plugins to <Installation directory of Service Platform>\manager\mbean-plugins. For details, see "*3.1.2 Setting up the software required for the execution environment*".

Procedure (Flow)		Representative error	Probable causes	Actions
At the time of setting the software required for execution environment	During setup of PRF	-	-	-
	During setup of the J2EE server	J2EE server is not started	The system environment variables of J2EE server are not set correctly.	Review the system environment variables of J2EE server.
	During setup of HTTP Server	-	-	-
	During setup of the database on the client	-	-	-
	During setup of the JDBC driver	-	-	-
	During setup of DB Connector	Error occurs while executing cjstartrar and cjtestres of DB Connector	Database related problem: • HiRDB is not yet started • Insufficient HiRDB connections • Error in host name and IP address, or port number of HiRDB • Error in user name or password of HiRDB.	• Confirm whether HiRDB is started. • Execute any of the following when there are insufficient HiRDB connections: (1) Change the pd_max_users of %PDDIR%\CONF\pdsyspd_max_users to 50. (2) Reduce the MinPoolSize of DB Connector definition or Reliable Messaging configuration properties. • Reference the DB Connector definition, and check that there is no error in host name or IP address and port number. • Check if there is no error in user name or password of HiRDB.
		In UNIX/Linux environment, error occurs while executing cjstartrar or cjtestres in DB Connector KDJE37360-E KDJE48516-E (javax.resource.ResourceException: KDJE50018-E is output in the detailed message in exception name and exception)	The following paths are not set to LD_LIBRARY_PATH for Linux, and to LIBPATH forAIX: **(1)** DABroker path /opt/DABroker/lib **(2)** HiRDB client product path /opt/HiRDB/client/lib **(3)** HiRDB server product path $PDDIR/client/lib	Setup the paths mentioned in the left column in LD_LIBRARY_PATH for Linux and LIBPATH for AIX. Furthermore, (1) is required while connecting via DABroker. Either of (2) and (3) are set up as per the software installation status when connecting to HiRDB. For details, see "*3.1.2 Setting up the software required for the execution environment*".
	During setup of Reliable Messaging	Error occurs while executing cjstartrar or cjtestres of DB Connector	Database related problem: • HiRDB is not yet started • Insufficient HiRDB connections • Error in host name and IP address, or port number of HiRDB • Error in user name or password of HiRDB.	• Confirm whether HiRDB is started. • Execute any of the following when there are insufficient HiRDB connections: • Change the pd_max_users of %PDDIR%\CONF\pdsys to 50. (2) Reduce the MinPoolSize of DB Connector definition or Reliable Messaging configuration properties. • Reference the DB Connector definition, and check that there is no error in host name or IP address, port number, user name and password. • For details, see " *3.1.2 Setting up the software required for the execution environment*".

Procedure (Flow)		Representative error	Probable causes	Actions
At the time of setting the software required for execution environment	During setup of Reliable Messaging	KDJE48213-W is output when Reliable Messaging or J2EE server are running	There is an error in the description of the queue definition file specified in configuration properties of Reliable Messaging.	The specification of QueueConfigFileName of configuration properties of Reliable Messaging is not required when you use Service Platform version 07-50 or later.
	During setup of Service Coordinator - Manager	-	-	-
During setup of the HCSC server		The following error occurs when executing the setup of the HCSC server: KEOS27105-E	Management Server is not started.	Check if Management Server is running. Also confirm whether auto start is specified for Management Server.
		The following error occurs when executing the setup of the HCSC server: KEOS50007-E (KDEC10011-E is output in detailed code) KEOS27040-E	Administration Agent is not started.	Check if Administration Agent is running. Also check whether auto start is specified for Administration Agent. If started, confirm the contents of settings file of Management Server, and restart Management Server.
		The following error occurs when executing the setup of the HCSC server: KEOS50007-E (KDEC05001-E and KFPA11723-E is output in detailed code)	HiRDB is down.	Start the HiRDB server. When you cannot start the HiRDB server, see the manual "HiRDB Messages", and take respective actions.
		The following error occurs when executing the setup of the HCSC server: KEOS50007-E (KDEC05012-E is output in detailed code)	HiRDB Type4 JDBC Driver or Oracle JDBC Thin Driver settings are not performed.	Setup the class path of jar file of driver in the following three files: (1)Set up the web.add.class.path in the option definition file (mserver.cfg) for Management Server. (2) Set up the add.class.path in the option definition file (usrconf.cfg) of J2EE server. (3)Set up HCSC_ADDCLASSPATH in the HCSC-Messaging command definition file(cmdconf.bat or cmdconf).
		The following error occurs when executing the set up of the HCSC server: KEOS50007-E (KDEC10013-E is output in detailed code)	Reliable Messaging of resource adapter is not started.	Start Reliable Messaging.
		The following error occurs when executing	The J2EE server is not running.	Review the environment .[#1]

Procedure (Flow)	Representative error	Probable causes	Actions
During setup of the HCSC server	the set up of the HCSC server: KEOS50007-E (KDEC10010-E is output in detailed code)	The J2EE server is not running.	Review the environment .[#1]
	The following error occurs when executing the set up of the HCSC server: KEOS50004-E (KEOS27105-E is output in detailed code)	Administration Agent is not running normally. Or Manager does not manage the created J2EE server.	Review the environment .[#1] As per the review results, if there is no relevant cause, the created J2EE server might not be managed by Manager. In that case, specify the settings so that the server can be managed by Manager.[#2] Check whether the read J2EE server settings are set correctly, and at restore the settings to original at locations where the settings have been changed. After that, click the Apply button on the screen. After completing the entire review, click Deploy Preference Information on the top-right of the screen to apply the settings. Note that to manage a J2EE server with Manager logical performance tracer settings are required. Also, the following settings of "Basic Information" tab must be set to "Do not perform" (do not use) after reading. Therefore, change the settings as and when required: • Management Agent settings • Settings for the Management event issue functionality • Settings for the start option
During setup of the definition information of the HCSC server	-	-	-
During startup of the HCSC server	Fails to start the HCSC server The log includes "KDJE37356-E The communication timeout occurred."	Value of both maxBinarySize and LONGVARBINARY_AccessSize of DB Connector property are 0.	Change as mentioned in either (or both) of the following points: • Set up value other than 0 (Example: 64000) in maxBinarySize of DBConnector property. • Set up value other than 0 (Example: 64) in LONGVARBINARY_AccessSize.
	KEOS50007-E occurs and the command fails Either of the following messages are output to the machine log of the machine on which HCSC is running: • KDJE50012-E • KFDJ02005-E	The DB Connector specified in dbcon-nodisplayname of the HCSC server setup definition file is the DB Connector in which any item other than NoTransaction is specified in <transaction-support>	When two DB Connectors are not prepared, set up two DB Connectors. Acquire the property file of DB Connector, and specify NoTransaction in <transaction-support> and perform setup. Check that DB Connector is set up correctly in the HCSC Server setup definition file, and setup the HCSC server again. For details, see "*3.1.2 Setting up the software required for the execution environment*".
During deployment of service adapter, business process, or user-defined reception	KEOS50007-E occurs and command fails. and command fails Either of the following messages are output to the machine log of the	The DB Connector specified in dbcon-nodisplayname of the HCSC server setup definition file is the DB Connector in which anything other than	When two DB Connectors are not prepared, set up two DB Connectors. Acquire the property file of DB Connector, specify `NoTransaction` in <transaction-support> , and perform setup.

Procedure (Flow)	Representative error	Probable causes	Actions
During deployment of service adapter, business process, or user-defined reception	machine on which HCSC is running: • KDJE50012-E • KFDJ02005-E	NoTransaction is specified in <transaction-support>	Check that DB Connector is set up correctly in the HCSC Server setup definition file and setup the HCSC server again. For details, see "*3.1.2 Setting up the software required for the execution environment*".
During setup of the definition information for user-defined reception	-	-	-

Legend:

-: Not applicable.

Note#1

Review the following points:

- Whether Administration Agent is started on a host where the corresponding J2EE server is running.
- Whether the port number of the running Administration Agent and the port number of Administration Agent defined in the host of the configuration definition is the same.
- Whether you can communicate with the host defined in the configuration definition.
- Whether you are allowed to connect to the host running on the accessed Management Server with the property of Administration Agent.
- Whether the product version of Management Server and Administration Agent are the same.
- If the product edition of Management Server and Administration Agent differ, does this difference arise due to the editions that can be connected to by the user.
- Whether the remote management functionality of Manager is started by the specified "Host name (or IP address): Port number".

Note#2

Use the following procedure to perform settings so that the created J2EE sever can be managed with Manager:

1. In "Environment Configuration of Logical Server" on the management portal, select the J2EE server name existing under "Logical J2EE Server", and display the settings screen.
2. Select "Read settings from the connection destination host", and then click the "Read" button.
3. Click "Management Portal" on the top-right part of the screen. The control returns to the top page.
4. Click "Start/Stop Logical Server". Check whether you can start the desired J2EE server.

7.5.3 How to recover when executing HCSC server setup and unsetup

If the HCSC server setup fails, and the HCSC server cannot be set up again, or if HCSC server unsetup cannot be completed even after repeated attempts, take action by performing the following procedure:

Procedure

1. Execute the following command to delete the repository information:

```
cscsvunsetup -user <login user ID> -pass <login password> -csc <HCSC server name> -ignore
```

After deleting the repository information, if you need to delete the application, execute steps 2 to 5. If you do not need to delete the application, execute step 5.

2. Execute the following command to confirm the name of the HCSC application that you want to delete:

```
cscapputil -user <login user ID> -pass <login password> -host <IP address>:<port number> -
mnguser <management userID> -mngpass <management user password> -j2ee <J2EE server name> -
operation list
```

Following are the HCSC applications to be deleted. The resources of these applications are not shared in the cluster so delete all applications.

- CSCMessaging

- CSCMsgSyncServiceDelivery
- CSCMsgSyncServiceDeliveryWS
- CSCMsgAsyncServiceDelivery
- CSCMsgAsyncServiceDeliveryDBQ
- cscmsg_async

3. Execute the following command to stop the HCSC application to be deleted:

```
cscapputil -user <login user ID> -pass <login password> -host <IP address>:<port number> -
mnguser <management userID> -mngpass <management user password> -j2ee <J2EE server name> -
app <application name> -operation stop
```

4. Execute the following command to delete the HCSC application:

```
cscapputil -user <login user ID> -pass <login password> -host <IP address>:<port number> -
mnguser <management userID> -mngpass <management user password> -j2ee <J2EE server name> -
app <application name> -operation delete
```

5. Delete the resources (database tables, index, or view table) that cannot be deleted, in reference to the table given below.

   However, delete the resources that are shared in the cluster only when you are performing unsetup of the last HCSC server in the cluster.

   There might be cases when each resource is already deleted or a resource is not yet created. Resources need not be deleted if they do not exist.

Table 7–50: Table Resources used by HCSC server

No.	Item	Resource	Type	Shared
1	Database table, index, view table	CSCMSG_S<HCSC server name>_CSC_PERSIST	T	N
2		CSCMSG_C<class name>_CSC_CONNECT	T	Y
3		CSCMSG_S<HCSC server name>_LC_DIRECTORY	T	N
4		CSCMSG_S<HCSC server name>_LC_BPFORMAT	T	N
5		CSCMSG_S<HCSC server name>_RT_RULE	T	N
6		CSCMSG_S<HCSC server name>_CV_MAPPING	T	N
7		CSCMSG_S<HCSC server name>_CV_FORMAT	T	N
8		CSCMSG_C<class name>_EXECHISTORY	T	Y
9		CSCMSG_C<class name>_EXECHISTORY_I	I	Y
10		CSCMSG_C<class name>_CLUSTER[#1]	T	Y
11		CSCMSG_C<class name>_HA_ASYNC_ADP[#1]	T	Y
12		CSCBP_<class name>_PROCESS	T	Y
13		CSCBP_<class name>_PROCESS_IDX1	I	Y
14		CSCBP_<class name>_PROCESS_IDX2	I	Y
15		CSCBP_<class name>_PROCESS_IDX3	I	Y
16		CSCBP_<class name>_PROCESS_IDX4	I	Y
17		CSCBP_<class name>_ACTIVITY	T	Y
18		CSCBP_<class name>_ACTIVITY_IDX	I	Y
19		CSCBP_<class name>_LINK	T	Y
20		CSCBP_<class name>_LINK_IDX	I	Y

No.	Item	Resource	Type	Shared
21	Database table, index, view table	CSCBP_<class name>_CORRELATIONSET	T	Y
22		CSCBP_<class name>_CORREL_IDX1	I	Y
23		CSCBP_<class name>_CORREL_IDX2	I	Y
24		CSCBP_<class name>_STR_VARIABLE	T	Y
25		CSCBP_<class name>_STR_VAR_IDX	I	Y
26		CSCBP_<class name>_NUM_VARIABLE	T	Y
27		CSCBP_<class name>_NUM_VAR_IDX	I	Y
28		CSCBP_<class name>_BOOL_VARIABLE	T	Y
29		CSCBP_<class name>_BOOL_VAR_IDX	I	Y
30		CSCBP_<class name>_MSG_VARIABLE	T	Y
31		CSCBP_<class name>_MSG_VAR_IDX	I	Y
32		CSCBP_<class name>_MSG_RELATION	T	Y
33		CSCBP_<class name>_MSG_REL_IDX1	I	Y
34		CSCBP_<class name>_MSG_REL_IDX2	I	Y
35		CSCBP_<class name>_MSG_REL_IDX3	I	Y
36		CSCBP_<class name>_V_ACTIVITY	V	Y
37		CSCBP_<class name>_V_LINK	V	Y
38		CSCBP_<class name>_V_STR_VARIABLE	V	Y
39		CSCBP_<class name>_V_NUM_VARIABLE	V	Y
40		CSCBP_<class name>_V_BOOL_VARIABLE	V	Y
41		CSCBP_<class name>_V_MSG_VARIABLE	V	Y
42	Request reception queue (when cluster type is LB)	CSC<HCSC server name>ACPT_RCVQ	Q	N
43		CSC<HCSC server name>ACPT_DBQ	Q	N
44	Request reception queue (when cluster type is HA)	CSC<class name>ACPT_RCVQ	Q	Y
45		CSC<class name>ACPT_DBQ	Q	Y
46	Temporary file of HCSC server	ServerProperties_<HCSC server name>	F	N
47		ServerSetup_<HCSC server name>	F	N
48		ReceptionProperties_dbq_<HCSC server name>	F	N
49		ReceptionProperties_ejb_<HCSC server name>	F	N
50		ReceptionProperties_jms_<HCSC server name>	F	N
51		ReceptionProperties_soap_<HCSC server name>	F	N
52		UserReceptionProperties_<HCSC server name>_<Reception ID>	F	N
53		ServerProperties_<HCSC server name>.old	F	N
54		ServerSetup_<HCSC server name>.old	F	N
55		ReceptionProperties_dbq_<HCSC server name>.old	F	N
56		ReceptionProperties_ejb_<HCSC server name>.old	F	N

No.	Item	Resource	Type	Shared
57	Temporary file of HCSC server	ReceptionProperties_jms_<HCSC server name>.old	F	N
58		ReceptionProperties_soap_<HCSC server name>.old	F	N
59		UserReceptionProperties_<HCSC server name>_<Reception ID>.old	F	N
60		ServerPropertiesAct_<HCSC server name>	F	N
61		ReceptionPropertiesAct_dbq_<HCSC server name>	F	N
62		ReceptionPropertiesAct_ejb_<HCSC server name>	F	N
63		ReceptionPropertiesAct_jms_<HCSC server name>	F	N
64		ReceptionPropertiesAct_soap_<HCSC server name>	F	N
65		UserReceptionPropertiesAct_<HCSC server name>_< Reception ID>	F	N
66		ServerPropertiesAct_<HCSC server name>.old	F	N
67		ReceptionPropertiesAct_dbq_<HCSC server name>.old	F	N
68		ReceptionPropertiesAct_ejb_<HCSC server name>.old	F	N
69		ReceptionPropertiesAct_jms_<HCSC server name>.old	F	N
70		ReceptionPropertiesAct_soap_<HCSC server name>.old	F	N
71		UserReceptionPropertiesAct_<HCSC server name>_< Reception ID>.old	F	N
72		_cscmsg_cnfrqdbq_<HCSC server name>.xml	F	N
73		_cscmsg_cnfrqejb_<HCSC server name>.xml	F	N
74		_cscmsg_cnfrqjms_<HCSC server name>.xml	F	N
75		_cscmsg_cnfrqsoap_<HCSC server name>.xml	F	N
76		_cscmsg_cnfrqsorp_<HCSC server name>.xml	F	N
77		_cscmsg_cnfrq_<HCSC server name>_< Reception ID>.xml	F	N
78		inf	F2	N

Legend:

I: Indicates an index. #2

T: Indicates a database table #2

V: Indicates a view table #2

Q: Indicates Reliable Messaging.#3

F: Indicates an HCSC server temporary file.#4

F2: Indicates that it is the output destination directory for saving the system management information of the HCSC server #5

Y: Indicates that the resource is shared in the cluster.

N: Indicates that the resource is not shared in the cluster.

Note#1

Execute the following SQL statement to acquire the list of information set in the corresponding table:

```
SELECT * FROM CSCMSG_C<class name>_CLUSTER;
```

- When the acquired list does not contain information other than that of the HCSC server whose setup failed
  Run the following SQL and delete the corresponding table:

```
DROP TABLE CSCMSG_C<class name>_CLUSTER;
DROP TABLE CSCMSG_C<class name>_HA_ASYNC_ADP;
```

- When the acquired list contains information other than that of the HCSC server whose setup failed
  Run the following SQL and delete the corresponding record:

```
DELETE FROM CSCMSG_C<class name>_CLUSTER
WHERE CSC_SERVER_NAME='<HCSC server name that has failed in setup and unsetup>';
COMMIT;
```

Note#2

Delete the database table, index, and view table by executing the SQL command (DROP).

Note#3

To delete the Reliable Messaging queue, execute the hrmstop command to migrate to the management status, and then execute the hrmdelque command. For details about the command, see "8.3.8 hrmdelque (deleting queue) " in "Reliable Messaging".

Note#4

For the HCSC server temporary file, delete the files in "<Installation directory of Service Platform>\CSC\system\msg".

Note#5

Delete the resources in the directory specified in the hcscserver-data-filepath property of the HCSC server setup definition file. When a directory is not specified in the hcscserver-data-filepath property, delete the resources in the default directory of hcscserver-data-filepath property.

! Important note

- For deleting an HCSC server on the J2EE server, use the cscapputil command. You cannot delete with the J2EE server commands.
- Use the cscapputil command only when recovering from a failure. Do not use the command during normal operations and setup.
- The Service Platform system might collapse if you delete an application with the cscapputil command. Therefore, perform operations carefully.

7.5.4 How to recover when deploying and deleting HCSC Components

(1) Recovery procedure

If deployment of a service adapter, business process, or user-defined reception fails and the item cannot be re-deployed, or if a service adapter, business process or user-defined reception cannot be deleted even after repeated deletion attempts, perform the following procedure.

1. Execute the csccompoundeploy command by specifying the -ignore option, and delete the repository information.

```
csccompoundeploy -user <login user ID> -pass <login password> -csc <HCSC server name> -name
<Service ID or Reception ID> -ignore
```

The next steps you perform differ depending on whether deletion of applications is necessary:

- If deletion of applications is necessary, perform steps 2 to 5.
- If deletion of applications is unnecessary, perform step 5.

2. Execute the following command to confirm the name of the HCSC application that you want to delete:

```
cscapputil -user <login user ID> -pass <login password> -mng <Manager name> -j2ee <J2EE
server name> -operation list
```

The following table lists and describes the HCSC applications to be deleted. There are no shared resources between these applications within the cluster. Therefore, delete all applications.

Table 7–51: Table HCSC applications to be deleted (when there is a failure in deploying and deleting HCSC components)

Item	Application name
HCSC component (service adapter and business processes) applications	<Service ID>
HCSC component (user-defined reception) applications	<Reception ID>

3. Execute the following command to stop HCSC components to be deleted:

```
cscapputil -user <login user ID> -pass <login password> -mng <Manager name> -j2ee <J2EE
server name> -app <Application name> -operation stop
```

4. Execute the following command to delete HCSC components:

```
cscapputil -user <login user ID> -pass <login password> -mng <Manager name> -j2ee <J2EE
server name> -app <Application name> -operation delete
```

5. If there are resources (queue) that cannot be deleted, delete those resources in reference to "(2) Resources used by the HCSC server".

   However, for resources that are shared in the cluster, delete these resources when you are cancelling the setup of the last service adapter or business process in the cluster.

6. If there are resources (database table information) that cannot be deleted, delete in reference to the following procedure:

   Execute the following SQL statement and delete the remaining resources (database table information) that are not required.

```
DELETE FROM CSCMSG_C<class name>_HA_ASYNC_ADP
       WHERE CSC_SERVER_NAME='<HCSC server name>'
         AND ADAPTER_ID='<Service ID of asynchronous service adapter with failed deployment
or deletion>';

COMMIT;
```

   Do not delete resources (database table information), if all the following conditions are not met:

   - HCSC server is set up by specifying "HA" in cluster type.
   - Asynchronous service adapter with same service ID is not deployed within the cluster.

7. Restart the HCSC server.

(2) Resources used by the HCSC server

The following table lists and describes the resources used by the HCSC server (service adapters, business processes):

Table 7–52: Table List of resources used by the HCSC server (service adapters and business processes)

No.	Item	Resource	Type	Shared
1	Database table	Row where any of the following is stored in SERVICE_NAME column of CSCMSG_S<HCSC server name>_LC_DIRECTORY table: • Service names of service adapters to be deleted • Business process names to be deleted • The format of user-defined reception to be deleted is as follows: :Reception_*<Reception ID of user-defined reception to be deleted>*:*<Reception name of user defined reception to be deleted>*	T	N
2	Service adapter queue	CSC_<class name><Service ID>	Q	Y
3	Queue destination of MDB (WS-R) adapter	CSC<Service ID>	U	Y
4	HCSC server temporary file	UserReceptionProperties_<HCSC server name>_<Reception ID>	F	N
5		UserReceptionProperties_<HCSC server name>_<Reception ID>.old	F	N

No.	Item	Resource	Type	Shared
6	HCSC server temporary file	UserReceptionPropertiesAct_<HCSC server name>_<Reception ID>.old	F	N
7		_cscmsg_cnfrq_<HCSC server name>_<Reception ID>.xml	F	N
8		IAdapterName	F2	N
9		IServiceKind	F2	N
10		IServiceName	F2	N
11		R<Number>[#]	F2	N

Legend:

Y: Indicates that the resource is shared in the cluster.

N: Indicates that the resource is not shared in the cluster.

- "TYPE" column: Indicates respective content as follows:
- T: Indicates a database table.

  Execute the DELETE SQL command and delete one line each of database tables.
- Q: Indicates a Reliable Messaging queue.

  To delete Reliable Messaging queue, execute the hrmstop command to migrate to the management status, and then execute the hrmdelque command. For details on the command, see "8.3.26 hrmstop (Migrating to management status) " in "Reliable Messaging".
- U: Indicates address specified in the Reliable Messaging transfer queue.

  To delete the address specified in the Reliable Messaging transfer queue, execute the hrmstop command to migrate to the management status, and then execute the hrmdeladdr command. For details on the command, see"8.3.6 hrmdeladdr (Deleting address) " in "Reliable Messaging".
- F: Indicates HCSC server temporary file.

  When you want to delete file, delete the files in "<Installation directory of Service Platform>CSC\system\msg".
- F2: Indicates HCSC server temporary file.

  When you want to delete a file, delete resources (files) in the "directory-specified-in-hcscserver-data-filepath\inf\LC_DIRECTORY" directory specified in hcscserver-data-filepath property of the HCSC server setup definition file. When a directory is not specified in the hcscserver-data-filepath property, delete the resources (files) that in the "default-directory-of-hcscserver-data-filepath\inf\LC_DIRECTORY" directory.

Note#

The file in which any of the following items are stored in the SERVICE_NAME line within the file:

- Service name of the service adapter to be deleted
- Business process name to be deleted
- The format of the user-defined reception to be deleted is as follows:

  :Reception_<Reception ID of the user-defined reception to be deleted>:<Reception name of the user-defined reception to be deleted>

! Important note

- When deleting HCSC components on the J2EE server, use the cscapputil command. You cannot delete HCSC components with J2EE server commands.
- Use the cscapputil command only when recovering from a failure. Do not use the command during normal operations and setup.
- The Service Platform system might collapse if you delete an application with the cscapputil command. Therefore, perform operations with utmost care.

7.6 Troubleshooting during operation execution

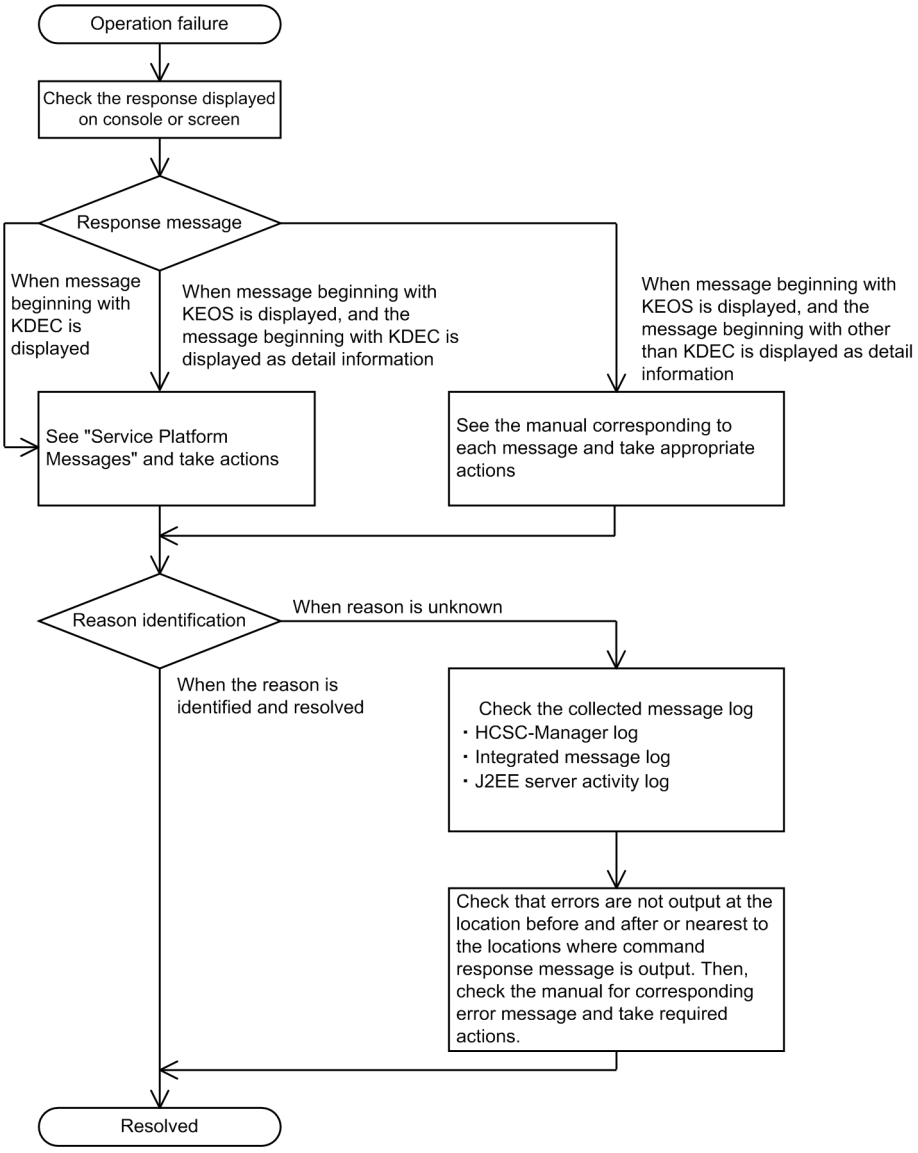
7.6.1 Investigating failures in screen operations of operating environment and command operations

When a failure occurs, check messages displayed on console or screens of the operating environment and investigate the failure. When the screens of operating environment are not operating, take actions so that the screens are restored to normal status.

(1) Methods for log analysis and classification of failure

The following figure shows the investigation procedure when a failure occurs when you perform command operations or screen operations of the operating environment:

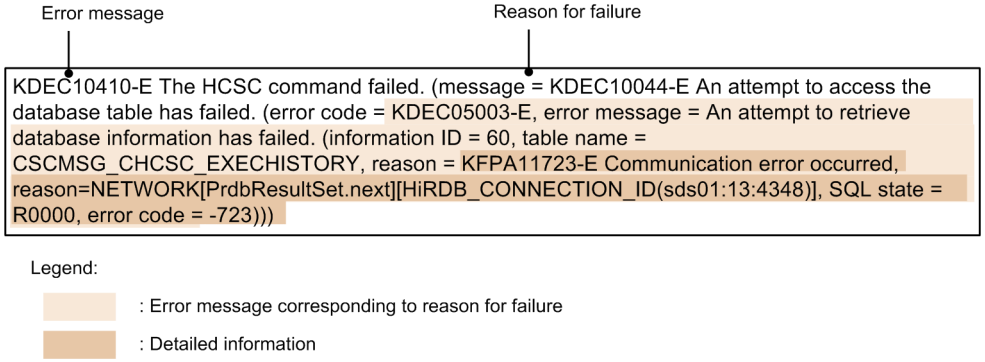
Figure 7–29: Figure Failure investigation procedure (Failure investigations when performing command operations or screen operations of the operating environment)



The description of the flow of investigation shown in Figure 7-29 is as follows:

1. When an error occurs in command operations or screen operations of the operating environment, first check messages output to the console as a response to the command.

   Also, check if messages are output as the detailed information of messages. The following figure shows output examples:



   - For KDEC or KEOS messages (messages related to HCSC - Manager) whose detained information includes a message whose ID begins with `KDEC`

     See the manual *uCosminexus Service Platform Messages*, and take countermeasures.

   - For KEOS messages (messages related to HCSC - Manager) whose detailed information includes a message whose ID does not begin with `KDEC`

     See the manual appropriate for the message. For example, if the detailed information includes a message whose ID begins with `KDJE`, see the manual *uCosminexus Application Server Messages*.

2. Reference the acquired message log when the cause cannot be specified. The following message logs are referenced as failure information when executing setup or unsetup. For details, see "*7.4.1 Message log*".

   - HCSC-Manager log
   - Integrated message log
   - Activity log of J2EE server

   The cause for occurrence of a failure might be due to environment settings or system status before command execution. Therefore, check locations where command response messages are output, and confirm that there are no other error messages and take appropriate actions.

Furthermore, the messages output to console are duplicated and output while checking the contents of message log. Therefore, check suitable execution time.

(2) Main failures and corresponding actions

The following table lists and describes the main failures and corresponding actions when executing command operations:

Table 7–53: TableMain failures and corresponding actions (Failure investigation when executing command operations and screen operations of the operating environment)

Operation	Main failures	Reason that can be considered	Troubleshooting	Reference
csm command execution when using Type4 driver	If the `csm` command is executed when the HCSC server is not running, the following error occurs: KDEC10410-E (KDEC10044-E) The following detailed information is output in the KDEC10044-E message: `(error code = KDEC05012-E, error`	Any one of the following directories is not set up: <Installation directory of Service Platform>\CSC\config\msg\cmdconf.bat <Installation directory of Service Platform>/CSC/config/msg/cmdconf <Installation directory of Service Platform>CSC/config/msg/cmdconf	Specify the path of jar file (pdjdbc2.jar) of HiRDB Type4 JDBC Driver in HCSC_ADDCLASSPATH of cmdconf (cmdconf.bat)	"HCSC-Messaging command definition file" in "Service Platform Reference Guide".

Operation	Main failures	Reason that can be considered	Troubleshooting	Reference
csm command execution when using Type4 driver	message = Database access initialization, before HCSC server startup, failed because loading of the JDBC driver failed. (JDBC name = JP.co.Hitachi.soft.HiRDB.JDBC.HiRDBDriver))	Any one of the following directories is not set up: <Installation directory of Service Platform>\CSC\config\msg\cmdconf.bat <Installation directory of Service Platform>/CSC/config/msg/cmdconf <Installation directory of Service Platform>CSC/config/msg/cmdconf	Specify the path of jar file (pdjdbc2.jar) of HiRDB Type4 JDBC Driver in HCSC_ADDCLASSPATH of cmdconf (cmdconf.bat)	"HCSC-Messaging command definition file" in "Service Platform Reference Guide".
csm command execution when using Oracle	If the csm command is executed when the HCSC server is not running, the following error occurs: KDEC10410-E (KDEC10044-E) The following detailed information is output in the KDEC10044-E message: (error code = KDEC05012-E, error message = Database access initialization, before HCSC server startup, failed because loading of the JDBC driver failed. (JDBC name = oracle.jdbc.driver.OracleDriver))		Specify the absolute path of jar file of Oracle JDBC Thin driver in HCSC_ADDCLASSPATH of cmdconf (cmdconf.bat).	
csm command execution in a status where HCSC server is not started	If the csm command is executed when the HCSC server is not running, the following error occurs: KDEC10410-E (KDEC10044-E) The following detailed information is output in the KDEC10044-E message: (error code = KDEC05001-E, error message = An attempt to open a connection to the database has failed. (reason = KFPA11724-E Environment definition error, variable=PDUSER, reason=NO VALUE[PrdbConnection.PrdbConnection], SQL state = R0000, error code = -724))	The user name and password of database are not specified in option of the csm command.	Specify the user name and password of database in the option of the csm command. When the HCSC server is offline, specify the user name and password of database without fail.	5. Commands (Operating environment and execution environment) " in "Service Platform Reference Guide".
csm command execution	The csm command fails, and the KFPA11912-E message (lack of work area for locks)	Insufficient working area due to mutual exclusion.	Increase the value specified for following operands of HiRDB system	" HiRDB Version 9 System Definition"

Operation	Main failures	Reason that can be considered	Troubleshooting	Reference
csm command execution	is output to the database (HiRDB) log and trace.	Insufficient working area due to mutual exclusion.	definition and restart HiRDB: • pd_max_access_tables • pd_lck_pool_size • pd_fes_lck_pool_size	" HiRDB Version 9 System Definition"

(3) How to take actions when screens of the operating environment cannot be operated

The actions to be taken when screens of the operating environment cannot be operated are as follows:

(a) When screen operations fail and you cannot click the button

Take actions as per the following procedure:

1. Investigate the cause of error output to the dialog box or screen console and take appropriate actions.
2. Perform any of the following operations:
   - Execute [Update to the latest information] from the HCSC-Manager menu
   - Close the editor and re-display
3. When you are unable to recover the screen with step 1 and 2, execute any of the following operations:
   - Execute commands for operations that ended in an error
   - Execute commands for operations that failed and operations opposite to the failed operations (Stop when the start procedure fails)

(b) When there is "No response" from the Eclipse screen

Take actions as per the following procedure:

1. Click the [Close] button of the Eclipse screen, and close the screen forcefully. When you cannot close the screen with the button, end the tasks of Eclipse from the [Application] tab of the [Task manager].
2. Investigate the cause of error and take actions.
3. Start the Eclipse screen, login to HCSC-Manager, and then re-execute the operations that ended with an error.

! Important note

On performing the above mentioned actions, the content that is being edited in the Eclipse same as the operating environment is lost. When you operate the screens of the operating environment, you must save or terminate contents that are being edited beforehand in Eclipse.

7.6.2 How to perform recovery when file input and output has failed

The error message KEOS50133-E is output at the time of operating commands, when file input and output has failed. When the KEOS50133-E is output once, KEOS50133-E is output at the time of command operations onwards, and commands cannot be executed.

Following are the actions to be taken when KEOS50133-E is output:

1. Reference the message log and investigate the reason for the failure in file input and output, and eliminate the cause of the error.

   Investigate the following and eliminate the cause of the error:
   - Whether there is any process being accessed incorrectly under the Repository root
   - Whether access permissions are allocated appropriately
   - Whether the disk is full

2. Restore the environment from backup files.

   Specify the output destination directory of the backup file from the backup type output to the KEOS50133-E message.

   Output the backup file to the following directory:

   `<Installation directory of Service Platform>\CSC\spool\manager\backup\<type>`

   The recovery methods differ as per the status at the time of error occurrence. The following table describes how to perform recovery according to the status at the time of error occurrence:

   Table 7–54: Table How to recover according to the status at the time of error occurrence

No	Type[#1]	Backup file name	Status at the time of error occurrence	How to perform recovery	Status after recovery
1	import	crt_mngenv.zip	During backup	Delete crt_mngenv.zip	Before executing the command in which an error has occurred
2		mngenv.zip	During file input output	1. Move mngenv.zip[#2]to any directory and empty the directory where mngenv.zip is stored. 2. Execute the following command: cscenvrestore -user <user ID> -pass <password> -restorefile <File name moved to 1.>	Before executing the command in which an error has occurred
3		del_mngenv.zip	After file input output (During backup file deletion)	Delete del_mngenv.zip.	After the command in which an error has occurred ends.
4	repository	crt_rep.zip	During backup	Delete crt_rep.zip.	Before executing the command in which an error has occurred
5		rep.zip	During file input and output	1. Delete the files under the following two directories[#3] and empty the directory: <repository root>\hirep\configs* <repository root>\manager* 2. Execute the following commands: cd <repository root> "<Installation directory of Service Platform>\jdk\bin\jar" xvf "<Installation directory of Service Platform>\CSC\spool\manager\backup\repository\rep.zip" 3. Delete rep.zip and empty the following directories where rep.zip is stored: <Installation directory of Service Platform>\CSC\spool\manager\backup\repository* 4. Execute the cscrepls command and confirm that it ends normally.	Before executing the command in which an error has occurred
6		del_rep.zip	After file input output (During backup file deletion)	Delete del_rep.zip.	After the command in which the error has occurred ends.

Note#1

Corresponds to the type described in the output destination directory of the backup file.

Note#2

mngenv.zip is a backup file the backup of is performed by the cscenvbackup command.

Note#3

rep.zip is a file in which files under the two directories (<repository root>\hirep\configs*and <repository root>\manager*) are zipped.

7.7 Troubleshooting during service component invocation request

When an error occurs while invoking service components from service requester, the error is returned to the service requester. This section describes how to report the places where error occurred to service requester and how to classify the reason for detected error.

Furthermore, the definition of development environment is running in execution environment via operating environment. However, the description about operating environment is omitted in this description.

7.7.1 Troubleshooting when executing Web service (SOAP communication)

For SOAP communication, if an error occurs when a service component is invoked from the service requester that error is returned to the service requester.

(1) Method of notifying an error in SOAP communication

The method of notifying an error differs in case of invoking a service component from the service requester using standard reception and in case of invoking a service component from the service requester using user-defined reception. Each of these notification methods is described here.

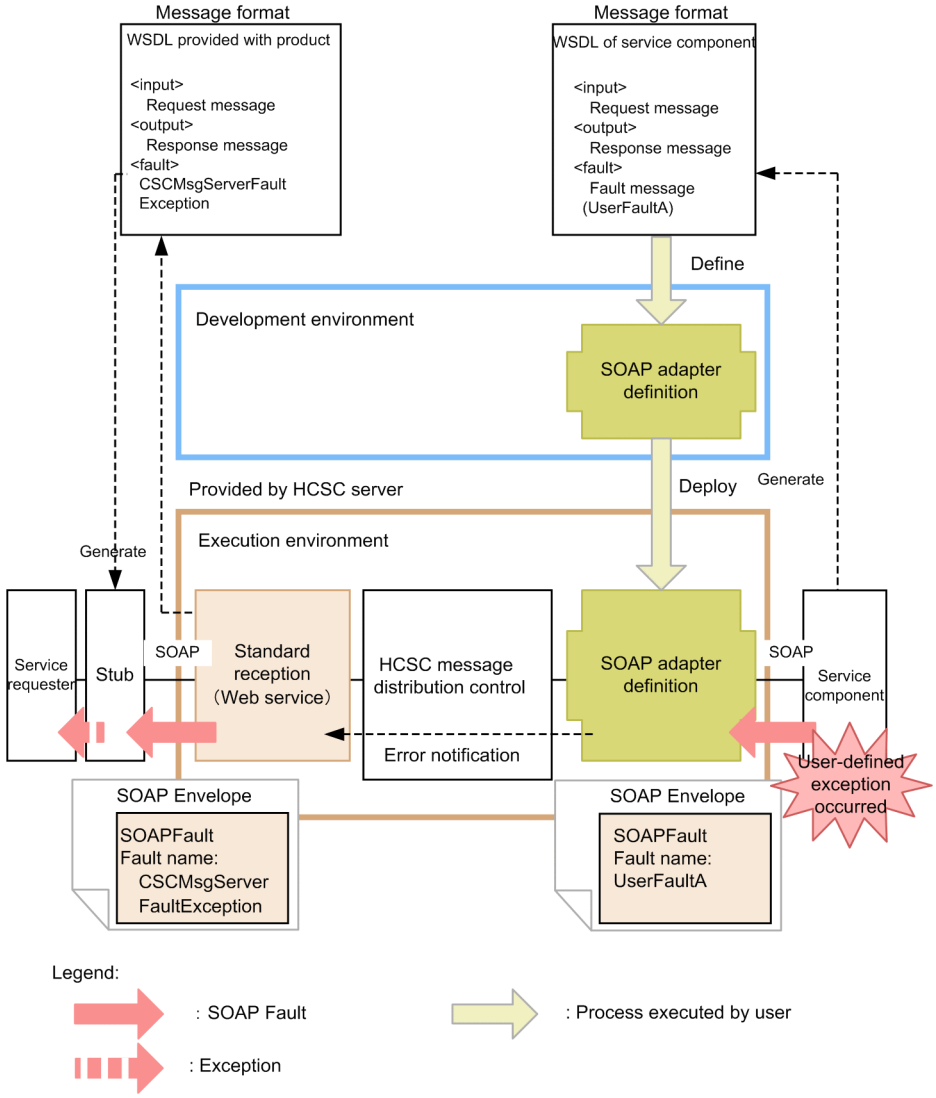
(a) For standard reception

The method of notifying an error differs according to error types and existence of the business process.

When an error other than the user-defined exception is returned from a service component (when you do not use a business process)

The following figure shows the method of notifying an error in SOAP communication, when an error of the user-defined exception is returned from a service component and a business process is not used:

Figure 7–30: Figure Method of notifying an error in SOAP communication (when you do not use a business process) when an error of the user-defined exception is returned from a service component



When you are using SOAP Communication Infrastructure or JAX-WS engine provided by Service Platform in the communication infrastructure of a service component, at the time of writing a code to throw an exception in the service component, a user-defined exception is defined using SOAP fault in WSDL of the service component. If a user-defined exception occurs in the service component, the contents of SOAP fault are returned from the standard reception to the service requester.

WSDL used by the service requester is provided by Service Platform. CSCMsgServerFaultException# is defined as SOAP fault in this WSDL. The service requester can catch SOAP fault returned by the HCSC server using the CSCMsgServerFaultException# object. You can acquire the name of the exception that occurs in a service component and the fault information (error details) by using getter of the exception object, which is caught. For details on CSCMsgServerFaultException#, see "8.3.8 Acquiring error information" in "Service Platform Basic Development Guide".

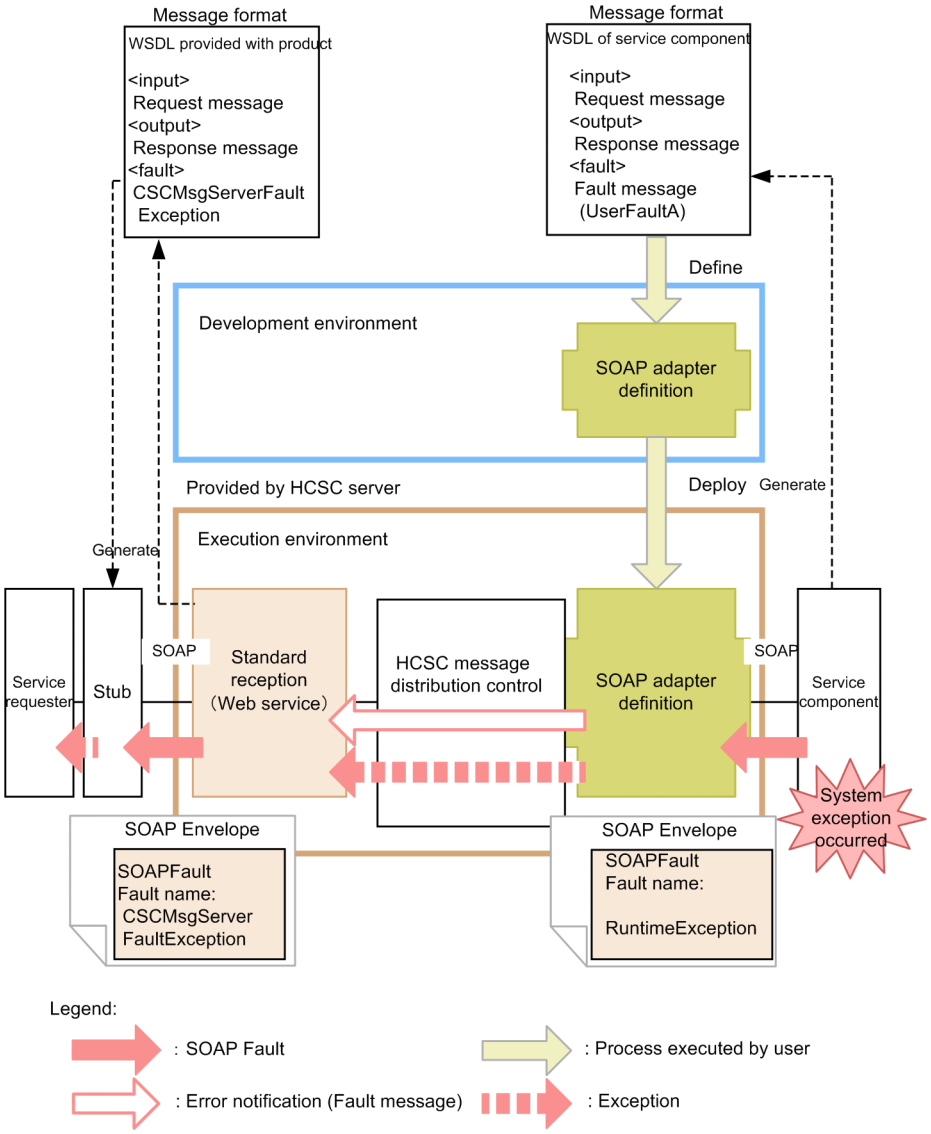
Note#

For SOAP1.2, the exception name will be CSCMsgServerFault12Exception.

When an error other than the user-defined exception is returned from a service component (when you do not use a business process)

The following figure shows the method of notifying an error in SOAP communication, when an error of the user-defined exception is returned from a service component and a business process is not used:

Figure 7–31: Figure Method of notifying an error in SOAP communication (when you do not use a business process) when an error other than the user-defined exception is returned from a service component



When you are using SOAP Communication Infrastructure or JAX-WS engine provided by Service Platform in the communication infrastructure of a service component, if an unexpected exception which is not defined in WSDL of the service component (system exception) occurs, the SOAP message is to be notified as RuntimeException. Moreover, this condition is to be handled as an exception in the HCSC server even if SOAP fault is defined in WSDL, when JAX-WS engine is used in the communication infrastructure of a service component and SOAP Communication Infrastructure provided by Service Platform is not used.

The system exception, which occurs when a service component is invoked from the service adapter can be transformed to a fault message using the service adapter. For details on how to transform a system exception into a fault message, see "*7.11 Selecting the errors to be acquired when an exception occurs*".

WSDL used by the service requester is provided by Service Platform. CSCMsgServerFaultException# is defined as SOAP fault in this WSDL. The service requester can catch the SOAP fault returned by the HCSC server using the CSCMsgServerFaultException# object. You can acquire information of the fault, which occurred (error details) using getter of the exception object, which is caught. For details on CSCMsgServerFaultException#, see "8.3.8 Acquiring error information" in "Service Platform Basic Development Guide".

When you want to notify the SOAP fault returned by a service component as is instead of an exception in the HCSC server, define it in SOAP Fault operation definition file. For details on SOAP Fault operation definition file, see "SOAP Fault operation definition file" in "Service Platform Reference Guide".

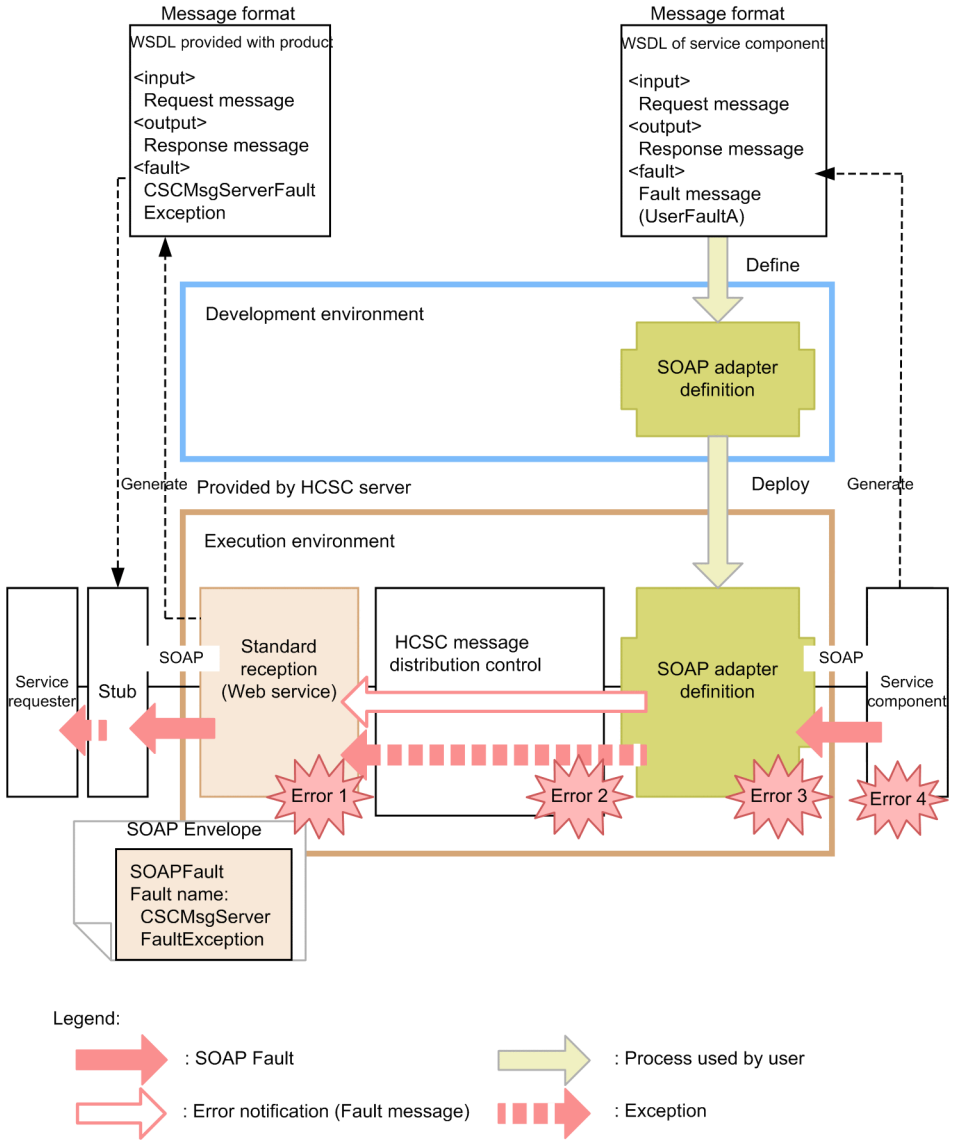
Note#

For SOAP1.2, the exception will be CSCMsgServerFault12Exception.

When an error is returned from the HCSC server (when you do not use a business process)

The following figure shows the method of notifying an error in SOAP communication, when an error is returned from the HCSC server and a business process is not used:

Figure 7–32: Figure Method of notifying an error in SOAP communication when an error is returned from the HCSC server (when you do not use a business process)



The following cases correspond to each of the errors shown in the figure:

- Error 1: Invalid request parameter, invalid specified character code, various invalid formats.
- Error 2: Address (location) is not found, the service adapter is stopped
- Error 3: A failure occurs in data transformation
- Error 4: Invalid address, stopping of a service component, communication failure

When any one of the errors from error 1 to error 3 shown in the figure is detected in the HCSC server, the exception of the error, which occurred is returned to the service requester.

If error 4 shown in the figure is detected, you can select whether to return the exception of error occurred as is to the service requester or whether to transform the exception of error into fault message in service adapter. For

details on how to select the error to be acquired when an exception occurs, see "*7.11 Selecting the errors to be acquired when an exception occurs*".

The service requester can catch the SOAP fault returned by the HCSC server using the CSCMsgServerFaultException# object. You can acquire information of the fault, which occurred (error details) using getter of the exception object, which is caught. For details on CSCMsgServerFaultException#, see "8.3.8 Acquiring error information" in "Service Platform Basic Development Guide".

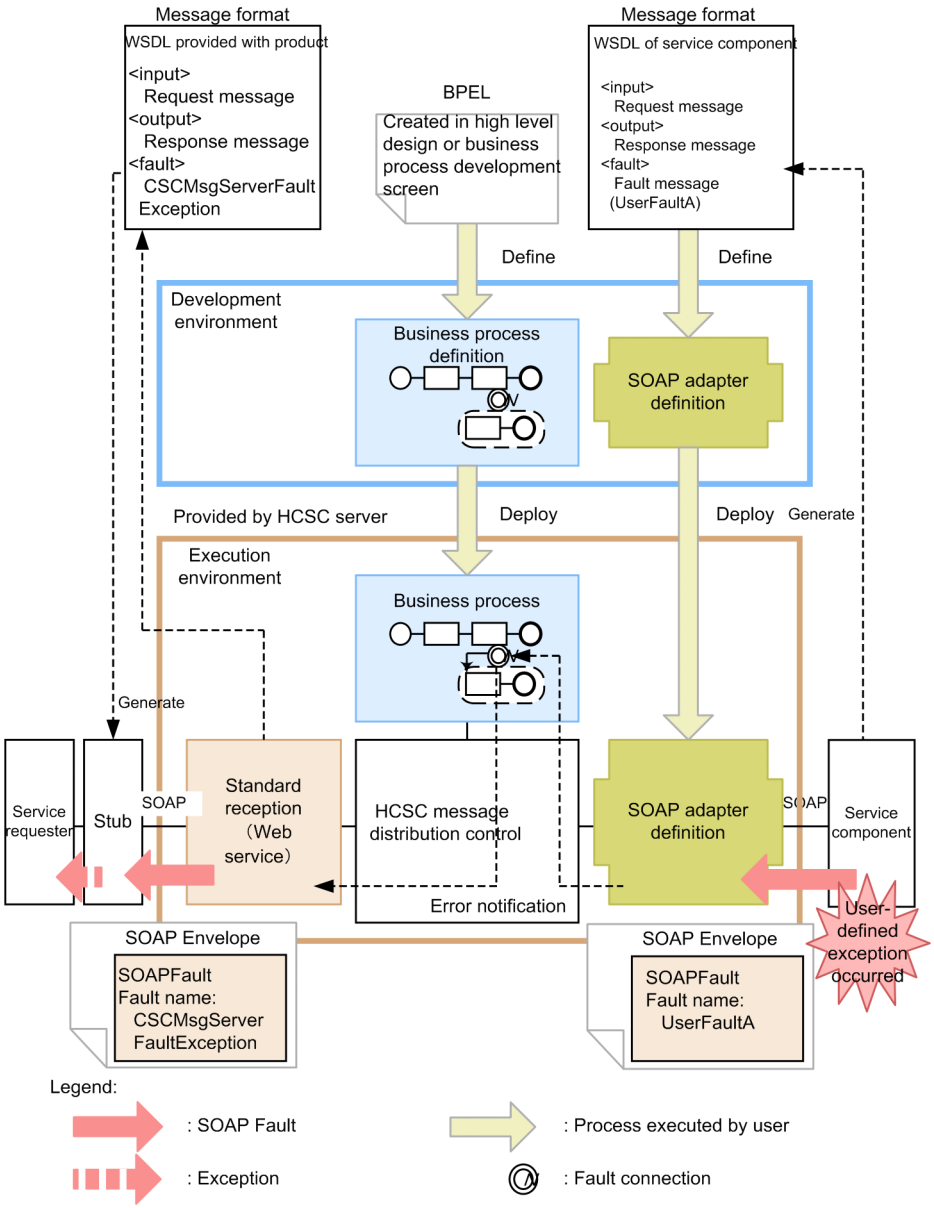
Note#

For SOAP1.2, the exception will be CSCMsgServerFault12Exception.

When an error other than user-defined exception is returned from a service component (when you use a business process)

The following figure shows the method of notifying an error in SOAP communication, when an error other than the user-defined exception is returned from the service component and a business process is used:

Figure 7–33: Figure Method of notifying an error in SOAP communication (when you use a business process) when an error of the user-defined exception is returned from a service component



When you are using SOAP Communication Infrastructure or JAX-WS engine provided by Service Platform in the communication infrastructure of a service component, at the time of writing a code to throw an exception in the

service component, a user-defined exception is defined using SOAP fault in WSDL of the service component. If a user-defined exception occurs in the service component, that error can be caught once in the business process.

The service requester can catch the SOAP fault returned by the HCSC server using the CSCMsgServerFaultException# object. You can acquire name of the exception or information of the fault (error details), which occurred using getter of the exception object, which is caught. It becomes easier to determine the exception, which occurs in the service requester by defining the fault name in the business process. For details on CSCMsgServerFaultException#, see "8.3.8 Acquiring error information" in "Service Platform Basic Development Guide".

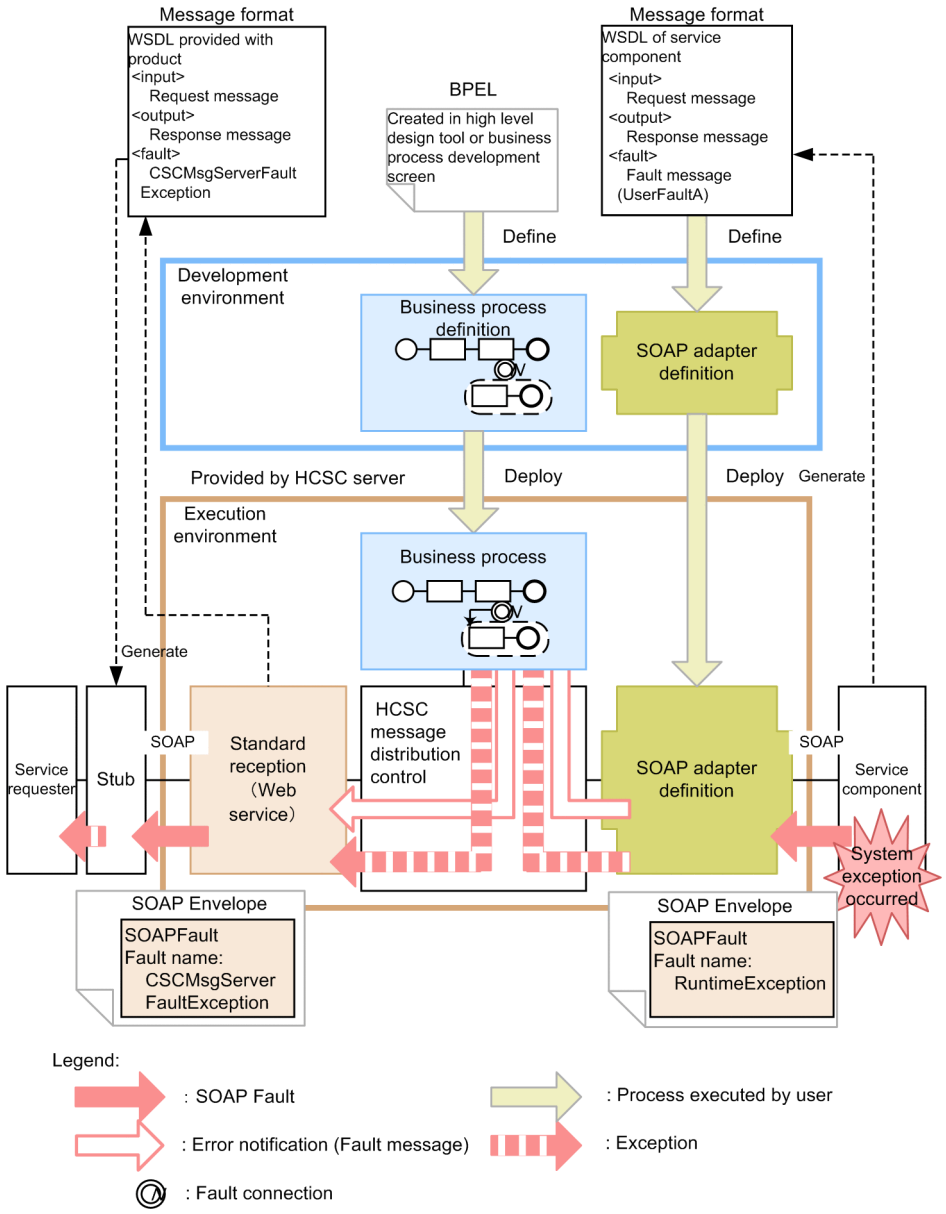
Note#

For SOAP1.2, the exception will be CSCMsgServerFault12Exception.

When an error other than the user-defined exception is returned from a service component (when you use a business process)

The following figure shows the method of notifying an error in SOAP communication, when an error other than the user-defined exception is returned from the service component and a business process is used:

Figure 7–34: Figure Method of notifying an error in SOAP communication (when you use a business process) when an error of user-defined exception is returned from a service component



When you are using SOAP Communication Infrastructure or JAX-WS engine provided by Service Platform in the communication infrastructure of a service component, if an unexpected exception (system exception), which is not defined in WSDL occurs in the service component, , the SOAP message is notified as RuntimeException. Moreover, if you use JAX-WS engine in the communication infrastructure of the service component or if you do not use SOAP communication infrastructure provided by Service Platform, even if you define SOAP fault in WSDL, it is handled as an exception in the HCSC server.

The system exception, which occurs when a service component is invoked from the service adapter, can be transformed into a fault message in the service adapter.

When you do not transform an exception into a fault message, process it as an exception in the business process and throw this exception into a standard reception. When you transform an exception into a fault message, it can be caught as a fault in the business process. For details on how to transform a system exception into a fault message, "*7.11 Selecting the errors to be acquired when an exception occurs*".

The service requester can catch the SOAP fault returned by the HCSC server using the CSCMsgServerFaultException# object. You can acquire information of the fault, which occurred (error details) using getter of the exception object, which is caught. For details on CSCMsgServerFaultException#, see "8.3.8 Acquiring error information" in "Service Platform Basic Development Guide".

When you want to notify the SOAP fault returned by a service component as is instead of an exception in the HCSC server, define it in SOAP Fault operation definition file. For details on SOAP Fault operation definition file, see "SOAP Fault operation definition file" in "Service Platform Reference Guide".

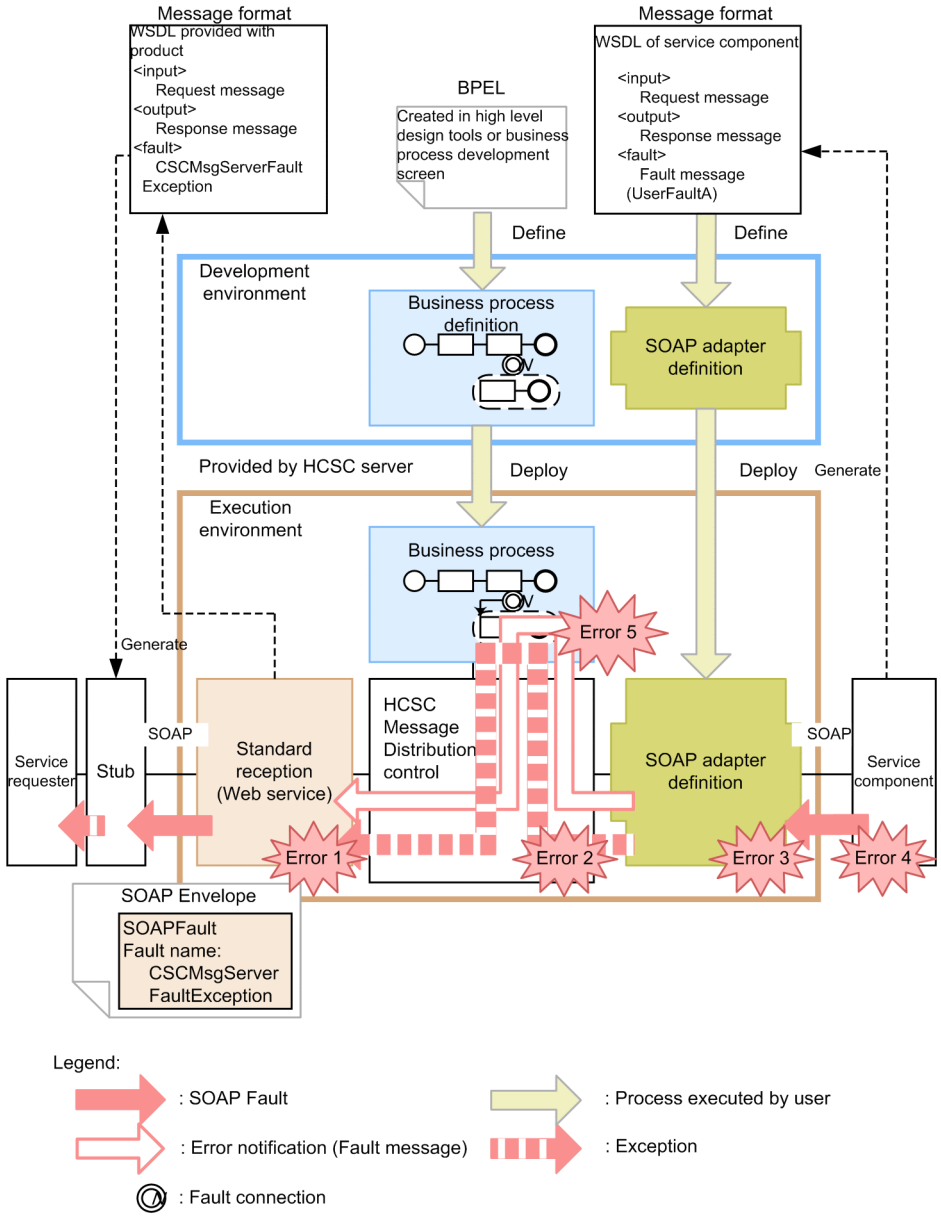
Note#

For SOAP1.2, the exception will be CSCMsgServerFault12Exception.

When an error is returned from the HCSC server (when you use a business process)

The following figure shows the method of notifying an error in SOAP communication, when an error is returned from the HCSC server and a business process is used:

Figure 7–35: Figure Method of notifying an error in SOAP communication (when you do not use a business process) when an error is returned from the HCSC server



The following cases correspond to each of the errors shown in the figure:

- Error 1: Invalid request parameter, invalid specified character code, various invalid formats
- Error 2: Address (location) is not found, the service adapter is stopped
- Error 3: A failure occurs in data transformation
- Error 4: Invalid address, stopping of a service component, communication failure
- Error 5: An exception error during processing of the business process

When any one of the errors from error 1 to error 3 and error 5 is detected in the HCSC server, the exception of the error, which occurred, is returned to the service requester. If error 4 shown in the figure is detected, you can select whether to return the exception of error occurred as is to the service requester or whether to transform the exception of error into fault message in service adapter. For details on how to select the error to be acquired when an exception occurs, see "*7.11 Selecting the errors to be acquired when an exception occurs*".

The service requester can catch the SOAP fault returned by the HCSC server using the CSCMsgServerFaultException# object. You can acquire information of the fault, which occurred (error details)

using getter of the exception object, which is caught. For details on CSCMsgServerFaultException#, see "8.3.8 Acquiring error information" in "Service Platform Basic Development Guide".

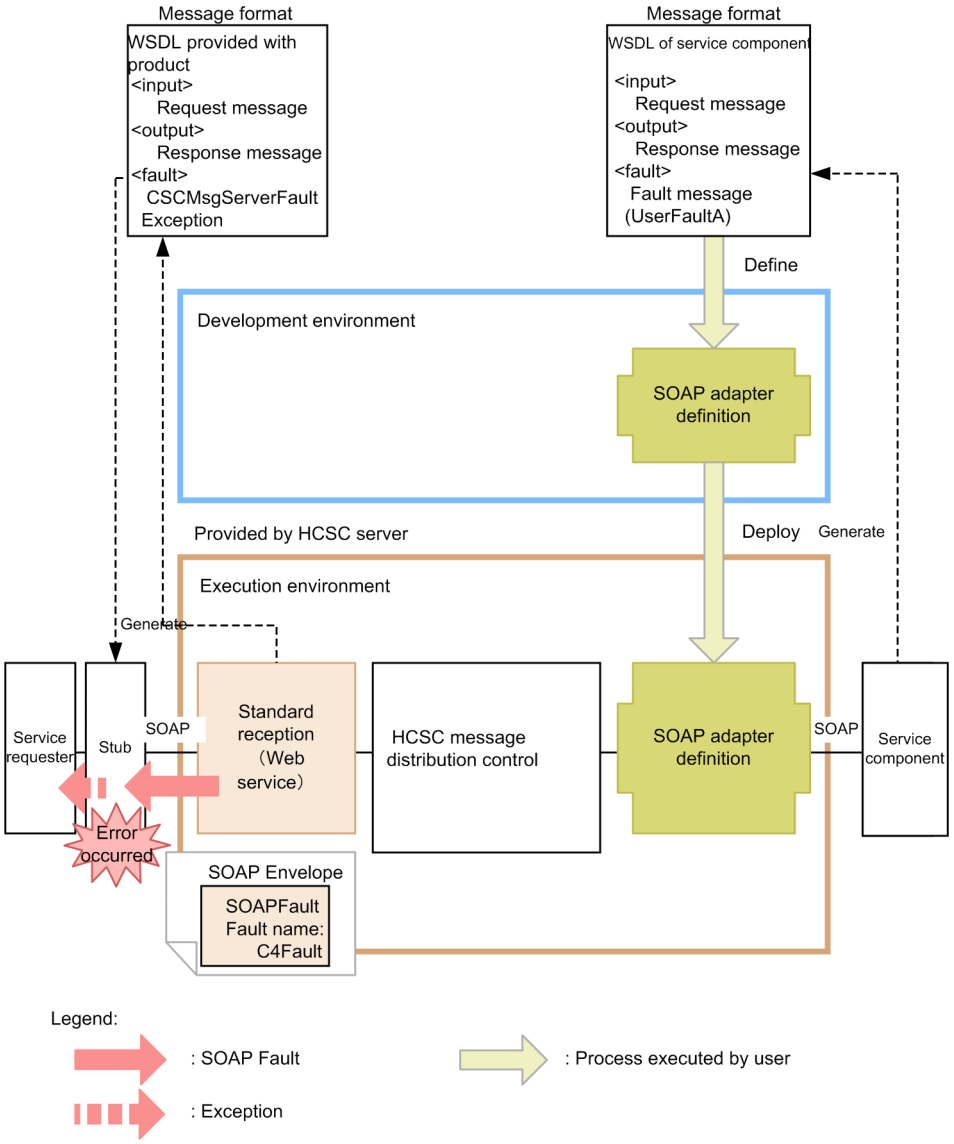
Note#

For SOAP1.2, the exception will be CSCMsgServerFault12Exception.

When an error is detected in the service requester

The following figure shows the method of notifying an error in SOAP communication, when an error is detected in the service requester:

Figure 7–36: Figure Method of notifying an error in SOAP communication when an error is detected in the service requester (for standard reception)



SOAP Communication Infrastructure or JAX-WS engine of the service requester (client side) returns an error in cases such as when the HCSC server is not invoked from the service requester or though invocation of the service component is completed, due to some reason, response was not returned from the HCSC server to the service requester.

When you are using SOAP Communication Infrastructure provided by Service Platform in the communication infrastructure of the service requester, the exception can be caught using the C4Fault object. Information of the fault, which occurred (error details) can be acquired using getter of the exception object, which is caught. For details on C4Fault, see "13.2 C4Fault class (Retaining SOAP Fault information) " in "Application Server SOAP Application Development Guide".

When you use JAX-WS engine in the communication infrastructure of the service requester, an exception can be caught in the SOAPFaultException object. Moreover, when you do not use SOAP Communication Infrastructure provided by Service Platform, catching of an exception depends on implementation of respective communication infrastructure.

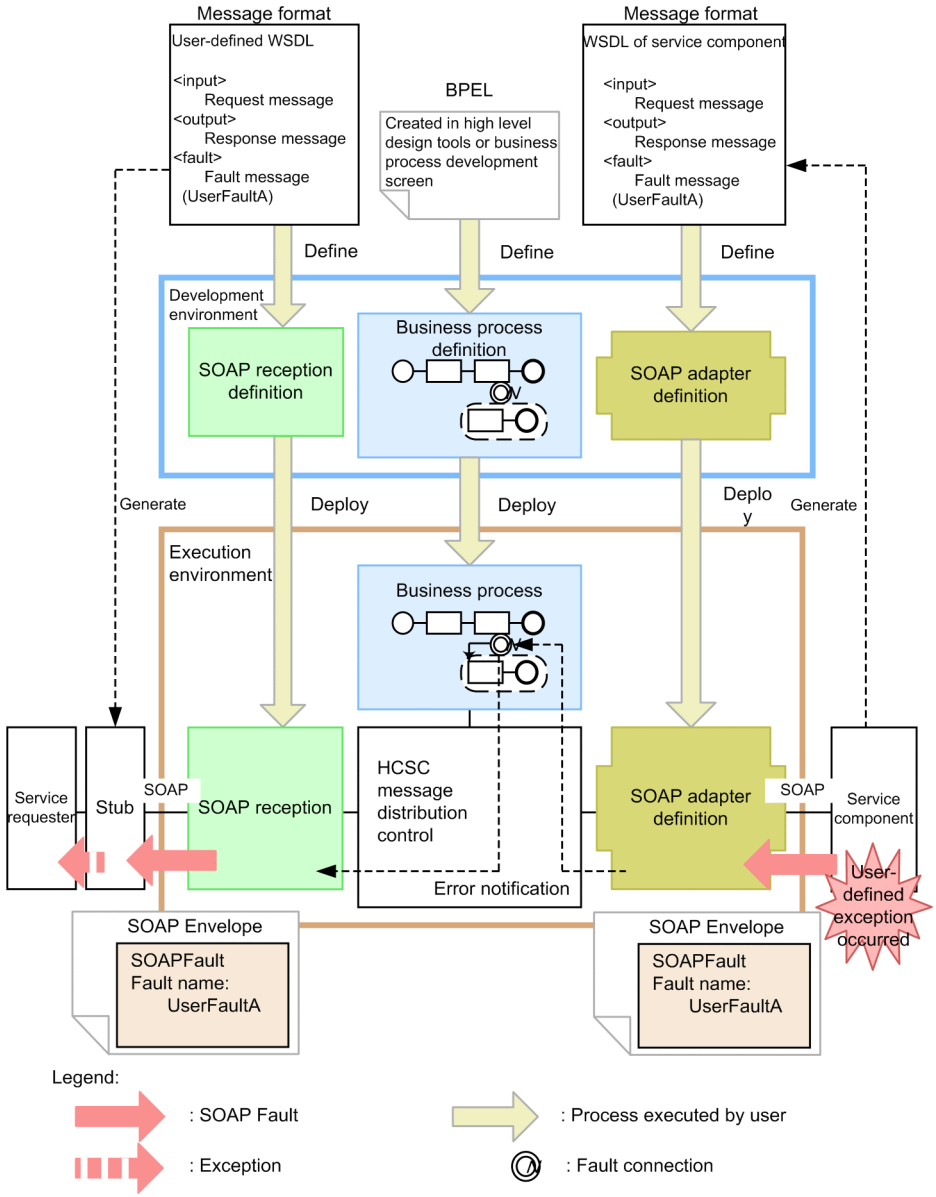
(b) For user-defined reception

The method of notifying an error differs according to error types and existence of the business process.

When an error of the user-defined exception is returned from a service component (when you use a business process)

The following figure shows the method of notifying an error in SOAP communication, when an error of the user-defined exception is returned from a service component and a business process is used:

Figure 7–37: Figure Method of notifying an error in SOAP communication when an error of the user-defined exception is returned from a service component (when you use a business process)



When you are using SOAP Communication Infrastructure or JAX-WS engine provided by Service Platform in the communication infrastructure of a service component and you are writing a code for throwing an exception in a

service component, a user-defined exception is defined in WSDL of a service component. If a user-defined exception occurs in the service component, that error can be caught once in the business process.

The service requester uses WSDL defined in the user-defined reception. However, the fault returned from a business process can be caught as the SOAP fault of user-defined exception even in the service requester by defining this fault in WSDL. With this, the fault can be caught with name and format same as the SOAP fault returned by a service component even in the service requester.

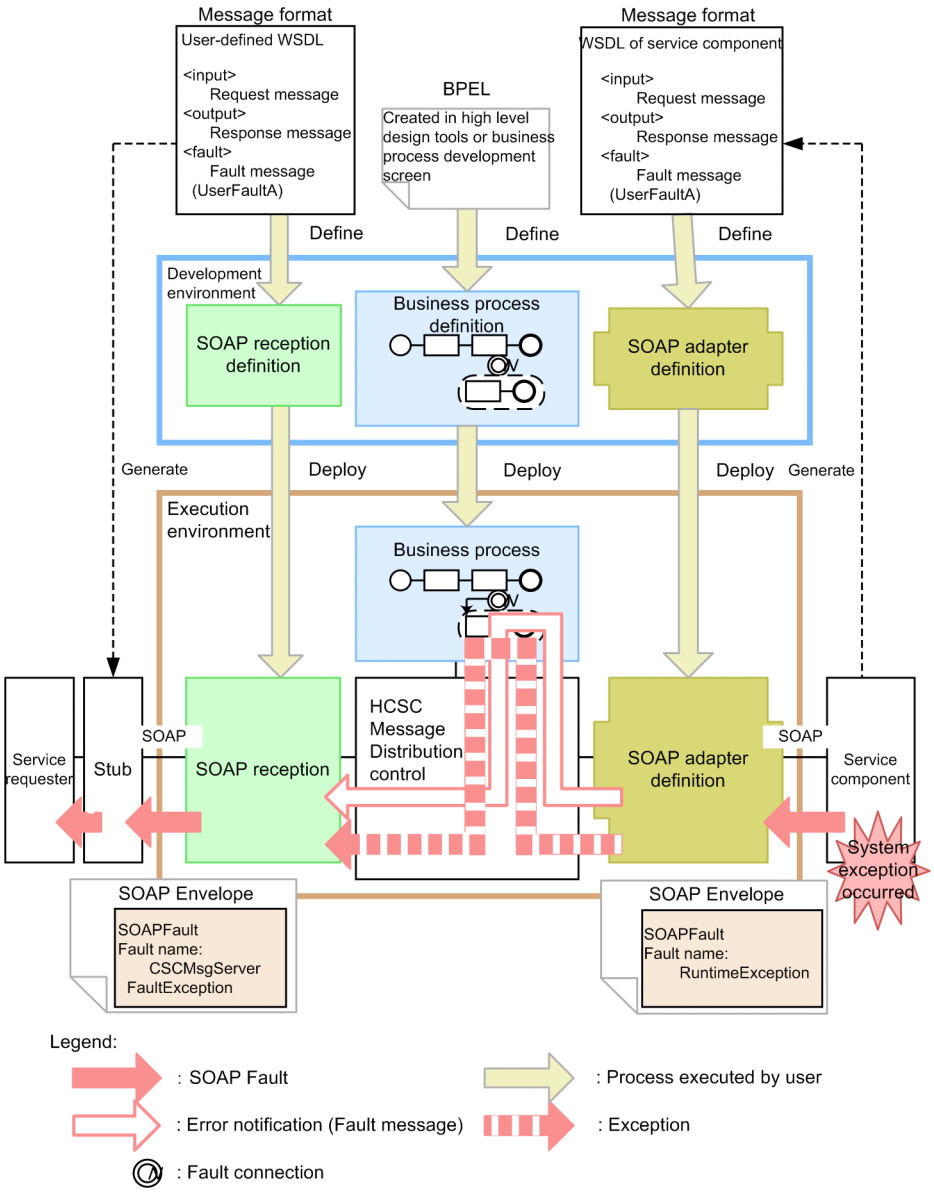
You must create the information required for analyzing the exception object which is caught using the program of a service component. Note that it becomes easier to determine the exception, which occurs in the service requester by defining the fault name in the business process.

For details on how to acquire the error information using the service requester that sends a request to SOAP reception, "8.7.6 Acquiring error information" in "Service Platform Basic Development Guide".

When an error other than the user-defined exception is returned from a service component (when you use a business process)

The following figure shows the method of notifying an error in SOAP communication, when an error other than user-defined exception is returned from a service component and a business process is used:

Figure 7–38: Figure Method of notifying an error in SOAP communication when an error other than user-defined exception is returned from a service component (when you use a business process)



When you are using SOAP Communication Infrastructure provided by Service Platform in the communication infrastructure of a service component, if an unexpected exception (system exception), which is not defined in WSDL, occurs in the service component, the SOAP message is notified as RuntimeException. Moreover, if you use JAX-WS engine in the communication infrastructure of the service component or if you do not use SOAP Communication Infrastructure provided by Service Platform, even if you define SOAP fault in WSDL, it is handled as an exception in the HCSC server.

The system exception, which occurs when a service component is invoked from the service adapter, can be transformed into a fault message in the service adapter.

When you do not transform an exception into a fault message, process it as an exception in the business process and throw this exception into the user-defined reception. When you transform an exception into a fault message, it can be caught as a fault in the business process. For details on how to transform a system exception into a fault message, see "*7.11 Selecting the errors to be acquired when an exception occurs*".

The HCSC server returns SOAP fault of CSCMsgServerFaultException to the service requester. However, WSDL used by the service requester is defined in the user-defined reception. CSCMsgServerFaultException is not defined in this WSDL. Therefore, when you are using SOAP Communication Infrastructure provided by Service Platform in the communication infrastructure of the service requester, an exception can be caught using the C4Fault object. Information of the fault, which occurred (error details) can be acquired using getter of the exception object, which is caught. For details on C4Fault, see, "13.2 C4Fault class (Retaining SOAP Fault information) " in "Application Server SOAP Application Development Guide".

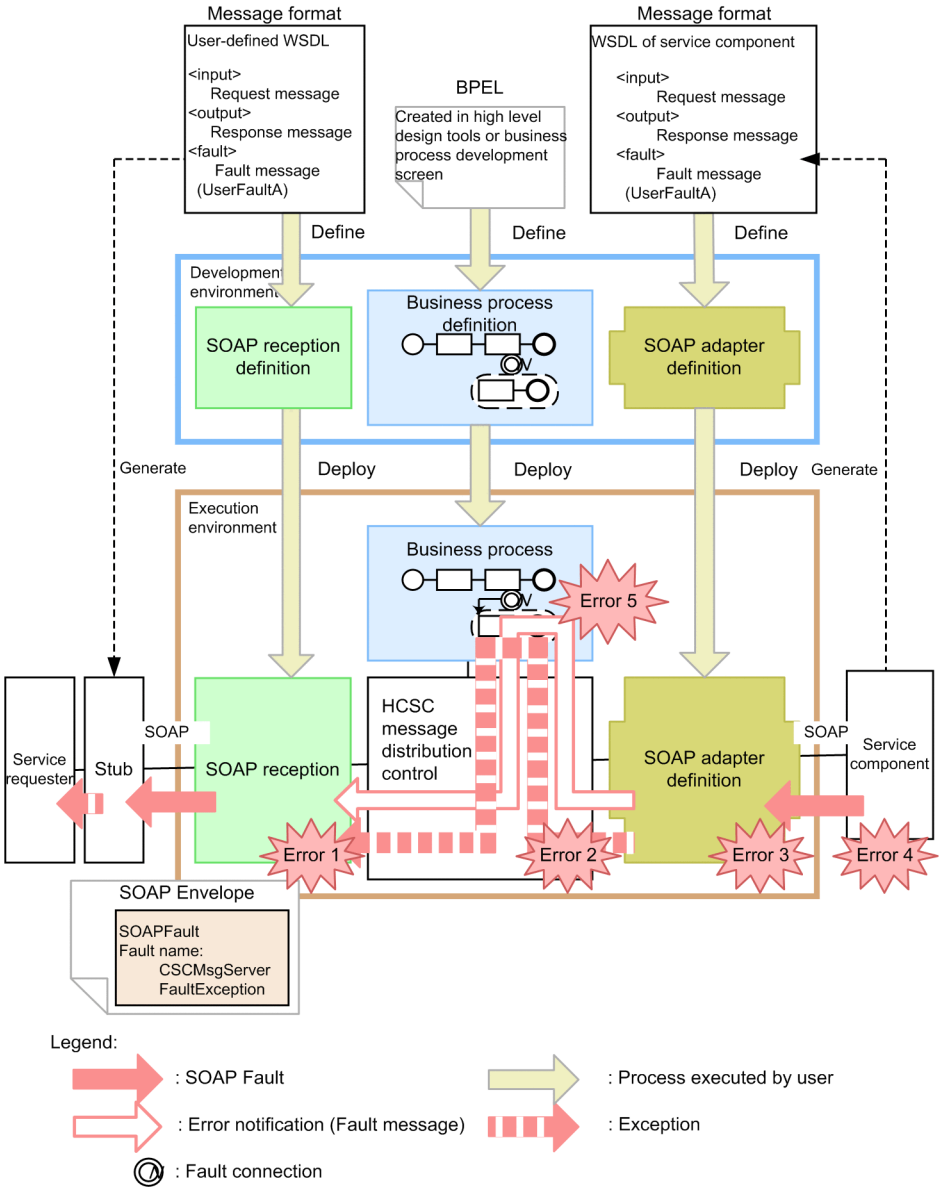
When you use JAX-WS engine in the communication infrastructure of the service requester, an exception can be caught using the SOAPFaultException object. Moreover, when you do not use SOAP Communication Infrastructure provided by Service Platform, catching of an exception depends on the implementation of respective communication infrastructure.

When you want to notify the SOAP fault returned by a service component as is instead of an exception in the HCSC server and catch a fault in the business process, define it in SOAP Fault operation definition file. For details on SOAP Fault operation definition file, see "SOAP Fault operation definition file" in "Service Platform Reference Guide".

When an error is returned from the HCSC server (when you use a business process)

The following figure shows the method of notifying an error in SOAP communication, when an error is returned from the HCSC server and a business process is used:

Figure 7–39: Figure Method of notifying an error in SOAP communication (when you do not use a business process) when an error is returned from the HCSC server



The following cases correspond to each of the errors shown in the figure:

- Error 1: Invalid specified character code, various invalid formats
- Error 2: Address (location) is not found, the service adapter is stopped
- Error 3: A failure occurs in data transformation
- Error 4: Invalid address, stopping of a service component, communication failure
- Error 5: An exception error during processing of the business process

When any one of the errors from error 1 to error 3 and error 5 is detected in the HCSC server, the exception of the error, which occurred, is returned to the service requester. If error 4 shown in the figure is detected, you can select whether to return the exception of the error occurred as is to the service requester or whether to transform the exception of the error into a fault message in the service adapter. For details on how to select the error to be acquired when an exception occurs, see "*7.11 Selecting the errors to be acquired when an exception occurs*".

The HCSC server returns SOAP fault of CSCMsgServerFaultException to the service requester. However, WSDL used by the service requester is defined in the user-defined reception. CSCMsgServerFaultException is not defined in this WSDL. Therefore, when you are using SOAP Communication Infrastructure provided by Service Platform in the communication infrastructure of the service requester, an exception is to be caught using the

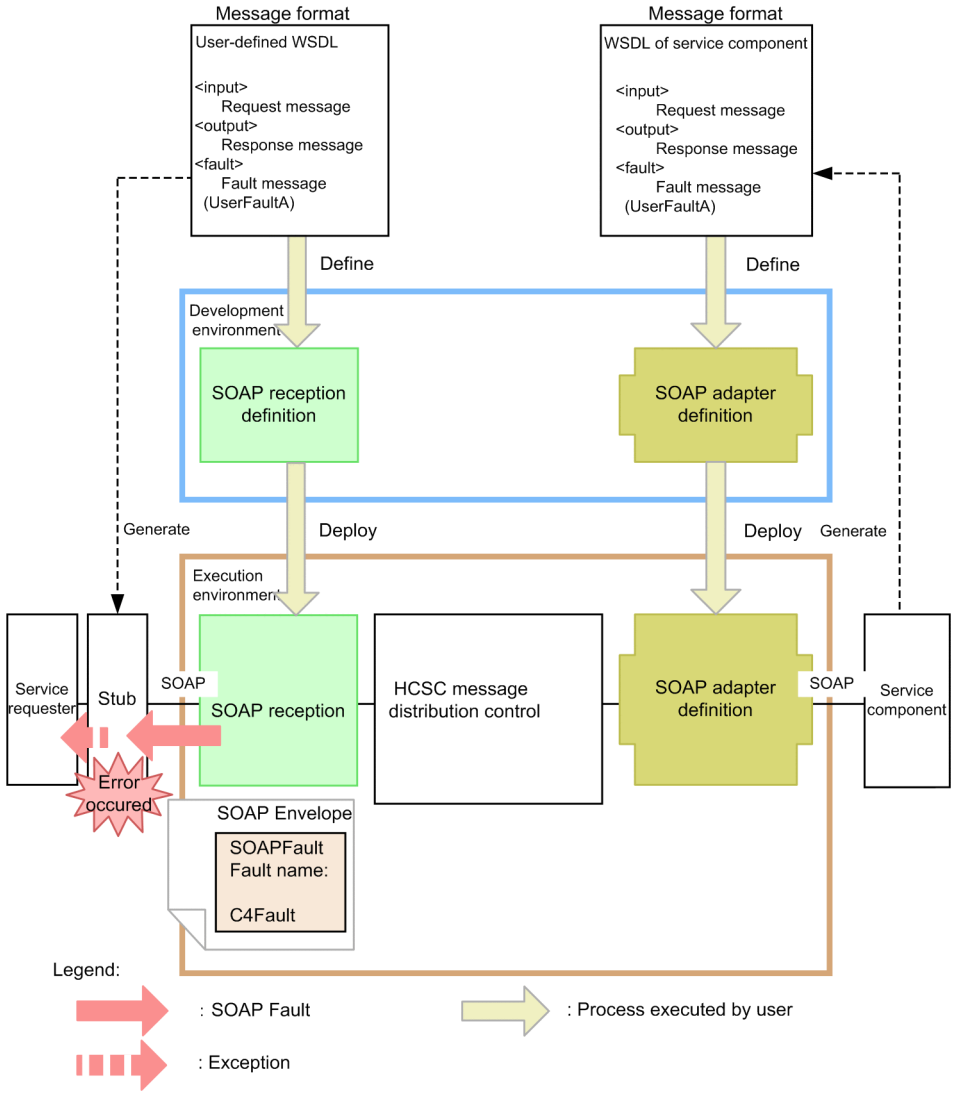
C4Fault object. Information of the fault, which occurred (error details) can be acquired using getter of the exception object, which is caught. For details on C4Fault, see "13.2 C4Fault class (Retaining SOAP Fault information) " in "Application Server SOAP Application Development Guide".

When you use JAX-WS engine in the communication infrastructure of the service requester, an exception can be caught using the SOAPFaultException object. Moreover, when you do not use SOAP Communication Infrastructure provided by Service Platform, catching of an exception depends on the implementation of respective communication infrastructure.

When an error is detected in the service requester

The following figure shows the method of notifying an error in SOAP communication, when an error is detected in the service requester:

Figure 7–40: Method of notifying an error in SOAP communication when an error is detected in the service requester (for user-defined reception)



SOAP Communication Infrastructure or JAX-WS engine of the service requester (client side) returns an error in cases such as when the HCSC server cannot be invoked from the service requester due to reasons such as invalid address, stopping of the HCSC server, and communication failure or though invocation of the service component is completed, due to some reason, response is not returned from the HCSC server to the service requester.

When you are using SOAP Communication Infrastructure provided by Service Platform in the communication infrastructure of the service requester, the exception can be caught using the C4Fault object. Information of the fault, which occurred (error details) can be acquired using getter of the exception object, which is caught. For details on C4Fault, see "13.2 C4Fault class (Retaining SOAP Fault information) " in "Application Server SOAP Application Development Guide".

When you use JAX-WS engine in the communication infrastructure of the service requester, an exception can be caught in the SOAPFaultException object. Moreover, when you do not use SOAP Communication Infrastructure provided by Service Platform, catching of an exception depends on implementation of respective communication infrastructure.

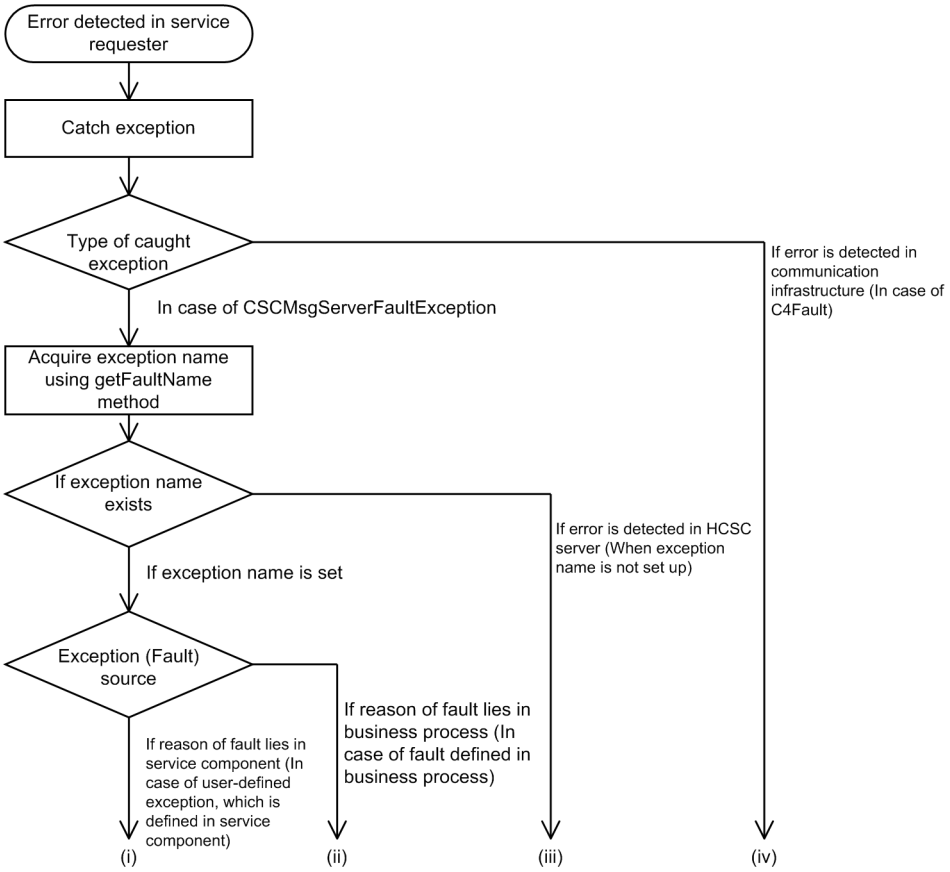
(2) Method of determining problem areas

The method of determining problem areas differs in case of standard reception and user-defined reception. For details on determining problem areas when communication is not possible using SOAP, see "14.3 Determining problem areas" in "Application Server SOAP Application Development Guide".

(a) For standard reception

The following figure shows the method of determining problem areas when a service component invoked from the service requester using standard reception (Web service):

Figure 7–41: Figure Method of determining problem areas (when a service component is invoked using the standard reception (Web service) from the service requester)



(i)When the cause of error is present in a service component (for user-defined exceptions defined in a service component)

The cause of error might be present in a service component. You can acquire the contents of SOAP Fault returned by a service component using the following methods:

<For SOAP1.1>

- getCscmsgFaultCode: Acquires FaultCode information.
- getCscmsgFaultString: Acquires FaultString information.
- getCscmsgFaultActor: Acquires FaultActor information.
- getCscmsgFaultDetail: Acquires FaultDetail information.

<For SOAP1.2>

- getCscmsgFaultCode: Acquires Code information.
- getCscmsgFaultReason: Acquires Reason information.
- getCscmsgFaultRole: Acquires Role information.
- getCscmsgFaultNode: Acquires Node information.
- getCscmsgFaultDetail: Acquires Detail information.

Check the causes using the following view-points:

- User message requested by the service requester
- Service component machine
- Program of a service component

Decision regarding whether to resend invocation of the service component depends on the agreement between the service requester and the service component (end-to-end) through the HCSC server.

(ii)When the cause of error is present in a business process (for faults defined in a business process)

The cause of error might be present in the processing of the activity executed by a business process (In case of invoke service activity, the cause of error might be present in the service component, which is invoked).

You can acquire the contents of SOAP Fault returned by the business process or the service component using the following methods:

<For SOAP1.1>

- getCscmsgFaultCode: Acquires FaultCode information.
- getCscmsgFaultString: Acquires FaultString information.
- getCscmsgFaultActor: Acquires FaultActor information.
- getCscmsgFaultDetail: Acquires FaultDetail information.

<For SOAP1.2>

- getCscmsgFaultCode: Acquires Code information.
- getCscmsgFaultReason: Acquires Reason information.
- getCscmsgFaultRole: Acquires Role information.
- getCscmsgFaultNode: Acquires Node information.
- getCscmsgFaultDetail: Acquires Detail information.

Check the causes using the following view-points:

- User message requested by the service requester
- Service component machine
- Program of a service component
- Definition contents of a business process

Decision regarding whether to resend invocation of the service component depends on the agreement between the service requester and the service component (end-to-end) through the HCSC server.

Moreover, depending on the type of the process in which the business process is designed, you must design the system containing a service requester that determines whether to resend (re-execution of a business process).

(iii)When an error is detected in the HCSC server (When the exception name is not set)

You can acquire the error contents using the following methods. Take action according to the countermeasures for the acquired error code and error message. Refer the message log output by Service Platform as well and check it.

- getErrorMessage: Acquires the error message of the error detected in the HCSC server.
- getErrorCode: Acquires the error code of the error detected in the HCSC server.

Check the cause based on the following viewpoints:

- Contents of the argument requested from the service requester
- Settings or status of the HCSC server
- Definition contents of the service adapter

- Definition contents of the business process
- User message requested from the service requester
- Service component machine
- Program of a service component
- Network status

Moreover, the problem areas can be narrowed down by verifying whether the following processes are always executed:

1. The SOAP message is correctly output from the service adapter (client).
2. The SOAP message has reached SOAP Communication Infrastructure or JAX-WS engine of the service component machine (server).
3. The message can be processed in the service component of the service component machine (server).
4. The SOAP message used as a reply from the service component of the service component machine (server) is correctly output.
5. The SOAP message used as a reply from the service component of the service component machine (server) has reached SOAP Communication Infrastructure or JAX-WS engine of the service adapter (client).

Refer the failure information output by SOAP Communication Infrastructure or JAX-WS engine at the time of verification. For details on how to acquire the failure information, see "*7.3.2(3) How to acquire the failure information output by SOAP Communication Infrastructure or JAX-WS engine*".

For the format of the failure information output by SOAP Communication Infrastructure, see "14. Troubleshooting" in "Application Server SOAP Application Development Guide". For the format of the failure information output by JAX-WS engine, see "39. Troubleshooting" in "Application Server Web Service Development Guide".

You can verify the message data sent and received between the service adapter and the service component by acquiring the application log output by SOAP Communication Infrastructure or JAX-WS engine.

Decision regarding whether to resend invocation of the service component differs as per the error contents. In case of temporary failure, you might succeed by trying to resend. However, in case of the following errors, even if you try to resend, an error occurs:

- If the contents of the argument requested from the service requester are incorrect
- If the settings of the HCSC server are incorrect
- If the definition of a service adapter and a business process is incorrect
- If the user message requested from the service requester is incorrect

(iv)When an error is detected in the communication infrastructure(for C4Fault)

You can acquire the error contents from C4Fault provided by SOAP Communication Infrastructure. Take action according the countermeasures for the acquired error codes and error messages.

For details on C4Fault, see "13.2 C4Fault class (Retaining SOAP Fault information) " in "Application Server SOAP Application Development Guide".

Check the cause based on the following viewpoints:

- WSDL used in the service requester
- Settings or status of SOAP Communication Infrastructure of the service requester machine
- Settings or status of the HCSC server
- Network status

Moreover, the problem areas can be narrowed down by verifying whether the following processes are always executed:

1. The SOAP message is correctly output from the service adapter (client).
2. The SOAP message has reached SOAP Communication Infrastructure of the HCSC server machine (server).
3. The SOAP message used as a reply from the service component of the HCSC server machine (server) is correctly output.
4. The SOAP message used as a reply from the service component of the HCSC server machine (server) has reached SOAP Communication Infrastructure of the service adapter (client).

Refer the failure information output by SOAP Communication Infrastructure at the time of verification. For details on how to acquire the failure information, see "*7.3.2(3) How to acquire the failure information output by SOAP Communication Infrastructure or JAX-WS engine*".

For the format of the failure information output by SOAP Communication Infrastructure, see "14. Troubleshooting" in "Application Server SOAP Application Development Guide"

You can verify the message data sent and received between the service requester and the HCSC server by acquiring the application log output by SOAP Communication Infrastructure.

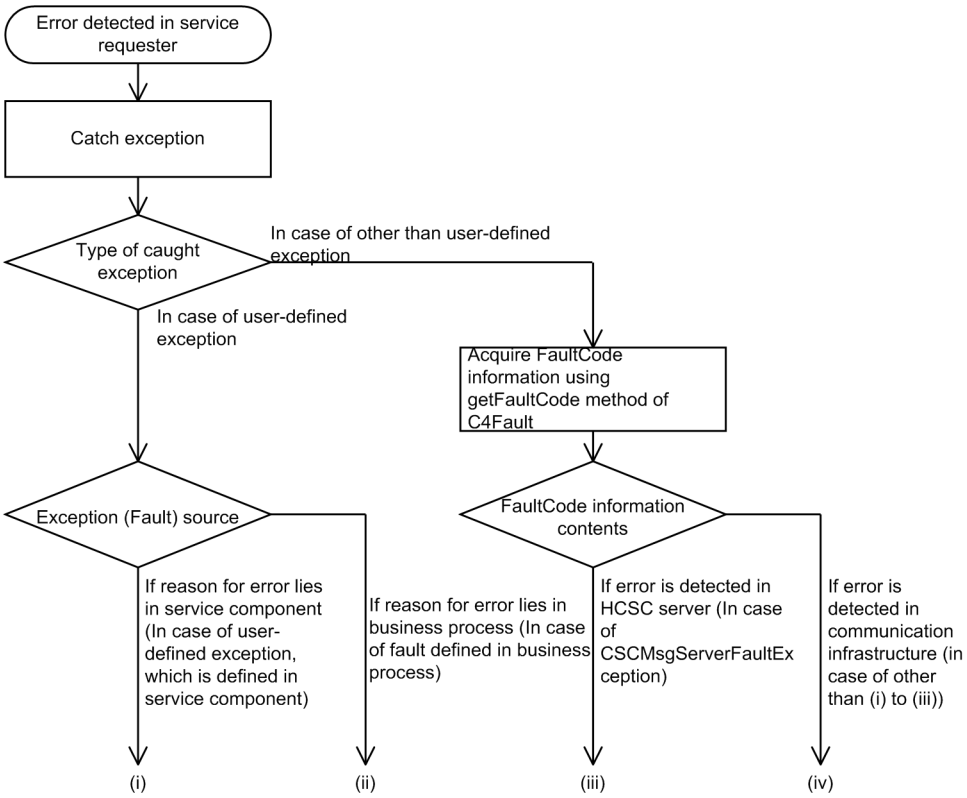
Decision regarding whether to resend invocation of the service component differs as per the error contents. In case of temporary failure, you might succeed by trying to resend. However, in case of the following errors, even if you try to resend, an error occurs:

- If WSDL used in the service requester is incorrect.
- Settings of SOAP Communication Infrastructure of the service requester machine are incorrect
- Settings of the HCSC server are incorrect

(b) For user-defined reception

The following figure shows the method of determining problem areas when a service component invoked from the service requester using SOAP reception:

Figure 7–42: Method of determining problem areas (when a service component is invoked from the service requester using SOAP reception)



(i) When the cause of error is present in a service component (for exceptions other than user-defined exceptions defined in a service component)

The cause of error might be present in a service component. The error information consists of the contents defined in the service component. (You must create the information required for analyzing the exception object, which is caught in the program of the service component).

Check the cause based on the following viewpoints:

- User message requested from the service requester
- Service component machine
- Program of the service component

Decision regarding whether to resend invocation of the service component depends on the agreement between the service requester and the service component (end-to-end) through the HCSC server.

(ii) When the cause of error is present in a business process (for faults defined in a business process)

The cause of error might be present in the processing of the activity executed by a business process (In case of invoke service activity, the cause of error might be present in the service component, which is invoked).

The error information will consists of contents of the fault defined in the business process (You must set the information required for analyzing the exception object, which is caught at the time of defining the business process).

Check the cause based on the following viewpoints:

- User message requested from the service requester
- Service component machine
- Program of the service component
- Definition contents of the business process

Decision regarding whether to resend invocation of the service component depends on the agreement between the service requester and the service component (end-to-end) through the HCSC server.

Moreover, you must design the system that determines whether to resend (re-execution of a business process) depending on the design contents of the business process.

(iii)When an error is detected in the HCSC server (for CSCMsgServerFaultException)

You can acquire the error contents from C4Fault provided by SOAP Communication Infrastructure. Take action according to the countermeasures for the acquired error code and error message. For the implementation method to be used when acquiring the error information from C4Fault in the service requester, see "8.7.6 Acquring Error Information" in "Service Platform Basic Development Guide". For details on C4Fault, see "13.2 C4Fault class (Retaining SOAP Fault information) " in "Application Server SOAP Application Development Guide". Refer the message log output by Service Platform as well and check it.

Check the cause based on the following viewpoints:

- Contents of the argument requested by the service requester
- Settings or status of the HCSC server
- Definition contents of the service adapter
- Definition contents of the business process
- User message requested from the service requester
- Service component machine
- Program of the service component
- Network status

Moreover, the problem areas can be narrowed down by verifying whether the following processes are always executed:

1. The SOAP message is correctly output from the service adapter (client).
2. The SOAP message has reached SOAP Communication Infrastructure of the service component machine (server).
3. The message can be processed in the service component of the service component machine (server).
4. The SOAP message used as a reply from the service component of the service component machine (server) is correctly output.
5. The SOAP message used as a reply from the service component of the service component machine (server) has reached SOAP Communication Infrastructure of the service adapter (client).

Refer the failure information output by SOAP Communication Infrastructure at the time of verification. For details on how to acquire the failure information, see "*7.3.2(3) How to acquire the failure information output by SOAP Communication Infrastructure or JAX-WS engine*".

For the format of the failure information output by SOAP Communication Infrastructure, see "14. Troubleshooting" in "Application Server SOAP Application Development Guide".

You can verify the message data sent and received between the service adapter and the service component by acquiring the application log output by SOAP Communication Infrastructure. Decision regarding whether to resend invocation of the service component differs as per the error contents. In case of temporary failure, you

might succeed by trying to resend. However, in case of the following errors, even if you try to resend, an error occurs:

- If the contents of the argument requested from the service requester are incorrect
- If the settings of the HCSC server are incorrect
- If the definition of a service adapter and a business process is incorrect
- If the user message requested from the service requester is incorrect

(iv)When an error is detected in the communication infrastructure (in cases other than (i) to (iii))

You can acquire the error contents from C4Fault provided by SOAP Communication Infrastructure. Take action according to the countermeasures for the acquired error code and error message.

For the implementation method to be used when acquiring the error information from C4Fault in the service requester, see "8.7.6 Acquiring Error Information" in "Service Platform Basic Development Guide". For details on C4Fault, see "13.2 C4Fault class (Retaining SOAP Fault information) " in "Application Server SOAP Application Development Guide". Refer the message log output by Service Platform as well and check it.

Check the cause based on the following viewpoints:

- WSDL used in the service requester
- Settings or status of SOAP Communication Infrastructure of the service requester machine
- Settings or status of the HCSC server
- Network status

Moreover, the problem areas can be narrowed down by verifying whether the following processes are always executed:

1. The SOAP message is correctly output from the service requester (client).
2. The SOAP message has reached SOAP Communication Infrastructure of the HCSC server machine (server).
3. The SOAP message used as a reply from the service component of the HCSC server machine (server) is correctly output.
4. The SOAP message used as a reply from the service component of the HCSC server machine (server) has reached SOAP Communication Infrastructure of the service requester (client).

Refer the failure information output by SOAP Communication Infrastructure at the time of verification. For details on how to acquire the failure information, see "*7.3.2(3) How to acquire the failure information output by SOAP Communication Infrastructure or JAX-WS engine*".

For the format of the failure information output by SOAP Communication Infrastructure, see "14. Troubleshooting" in "Application Server SOAP Application Development Guide".

You can verify the message data sent and received between the service requester and the HCSC server by acquiring the application log output by SOAP Communication Infrastructure. Decision regarding whether to resend invocation of the service component differs as per the error contents. In case of temporary failure, you might succeed by trying to resend. However, in case of the following errors, even if you try to resend, an error occurs:

- If WSDL used in the service requester is incorrect
- If settings of SOAP Communication Infrastructure of the service requester machine are incorrect
- If the settings of the HCSC server are incorrect

(3) Contents of SOAP Fault returned from the HCSC server

Regarding SOAP message returned from the HCSC server, the correspondence between the elements of SOAP Fault and information set up at the time of error is described here.

(a) For SOAP1.1

The following table describes the correspondence between the elements of SOAP fault and information set up at the time of error, when SOAP1.1 is in use:

The error case numbers are same as the numbers indicated in "*7.7.1(2) Method of determining problem areas*".

Table 7–55: Contents of SOAP Fault returned from the HCSC server (for SOAP1.1)

SOAP Fault returned from the HCSC server			Error case	
SOAP Fault element	SOAP Fault name	Fault name	For (i) and (ii) of standard reception	For (iii) of standard reception, (iii) of user-defined reception
faultcode	Fault code	-	The value depends on SOAP Communication Infrastructure and JAX-WS engine. In SOAP Communication Infrastructure, QCName referred by the message type attribute of message part is to be output. In JAX-WS engine, violation code is to be output.	
faultstring	Fault string	-	An error message is to be output.	
faultactor	Fault factor	-	The value depends on SOAP Communication Infrastructure and JAX-WS engine. There is no value in both SOAP Communication Infrastructure and JAX-WS engine.	
detail	Fault details	errorMessage	The error contents are as follows: An error detected in the HCSC server An error from a service component, a business process, and a service adapter#.	
		errorCode	The error codes correspond to the contents of the following exceptions: An error detected in the HCSC server An error from a service component, a business process, and a service adapter#	
		processInstanceID	Specifies information of the instance ID of the business process. The value is set when an error occurs in the business process.	
		cscmsgFaultCode	Specifies FaultCode information from a service component (Web service), a business process or a service adapter#.	There is no value.
		cscmsgFaultString	Specifies FaultString information from a service component (Web service), a business process or a service adapter#.	There is no value.
		cscmsgFaultActor	Specifies FaultActor information from a service component (Web service), a business process or a service adapter#.	There is no value.
		cscmsgFaultDetail	Specifies Detail information from a service component (Web service), a business process or a service adapter#.	There is no value.
		faultName	Specifies information of fault names (exception names) from a service component (Web service or SessionBean) or a business process. The value is set in the following cases: For SOAP Fault other than the user-defined exceptions from a service component (Web service or SessionBean) For faults from a business process	There is no value.

Legend:

-: Not applicable.

Note 1

In case of (i) and (ii) of the user-defined reception, SOAP Fault will be other than the user-defined exception.

Note 2

In case of (iv) of the standard reception or (iv) of the user-defined reception, an error is to be notified from SOAP Communication Infrastructure or JAX-WS engine of the service requester.

Note#

The following service adapters are not covered:

SOAP adapter

SessionBean adapter

MDB (WS-R) adapter

MDB (DB queue) adapter

For SOAP1.2

The following table describes the correspondence between the elements of SOAP Fault and information set up at the time of error, when SOAP1.2 is in use:

The error case numbers are same as the numbers indicated in "*7.7.1(2) Method of determining problem areas*".

Table 7–56: Contents of SOAP Fault returned from the HCSC server (for SOAP1.2)

SOAP Fault returned from the HCSC server			Error case	
SOAP Fault element	SOAP Fault name	Fault name	For (i) and (ii) of standard reception	For (iii) of standard reception, (iii) of user-defined reception
Code	Fault code	-	Violation code is to be output.	
Reason	Fault reason	-	An error message is to be output.	
Role	Fault factor	-	There is no value.	
Node	Fault node	-	There is no value.	
Detail	Fault details	errorMessage	The error contents are as follows: • An error detected in the HCSC server • An error from a service component, a business process, and a service adapter#.	
		errorCode	The error codes correspond to the contents of the following exceptions: • An error detected in the HCSC server • An error from a service component, a business process, and a service adapter#	
		processInstanceID	Specifies information of the instance ID of the business process. The value is set when an error occurs in the business process.	
		cscmsgFaultCode	Specifies Code information from a service component (Web service), a business process or a service adapter#.	There is no value.
		cscmsgFaultReason	Specifies Reason information from a service component (Web service), a business process or a service adapter#.	There is no value.
		cscmsgFaultRole	Specifies Role information from a service component (Web service), a business process or a service adapter#.	There is no value.
		cscmsgFaultNode	Specifies Node information from a service component (Web service), a business process or a service adapter#.	There is no value.

SOAP Fault returned from the HCSC server			Error case	
SOAP Fault element	SOAP Fault name	Fault name	For (i) and (ii) of standard reception	For (iii) of standard reception, (iii) of user-defined reception
Detail	Fault details	cscmsgFaultDetail	Specifies Detail information from a service component (Web service), a business process or a service adapter#.	There is no value.
		faultName	Specifies information of fault names (exception names) from a service component (Web service or SessionBean) or a business process. The value is set in the following cases: For SOAP Fault other than the user-defined exceptions from a service component (Web service or SessionBean) For faults from a business process	There is no value.

Legend:

-: Not applicable.

Note 1

In case of (i) and (ii) of the user-defined reception, SOAP Fault will be other than the user-defined exception.

Note 2

In case of (iv) of the standard reception or (iv) of the user-defined reception, an error is to be notified from JAX-WS engine of the service requester.

Note#

The following service adapters are not covered:

SOAP adapter

SessionBean adapter

MDB (WS-R) adapter

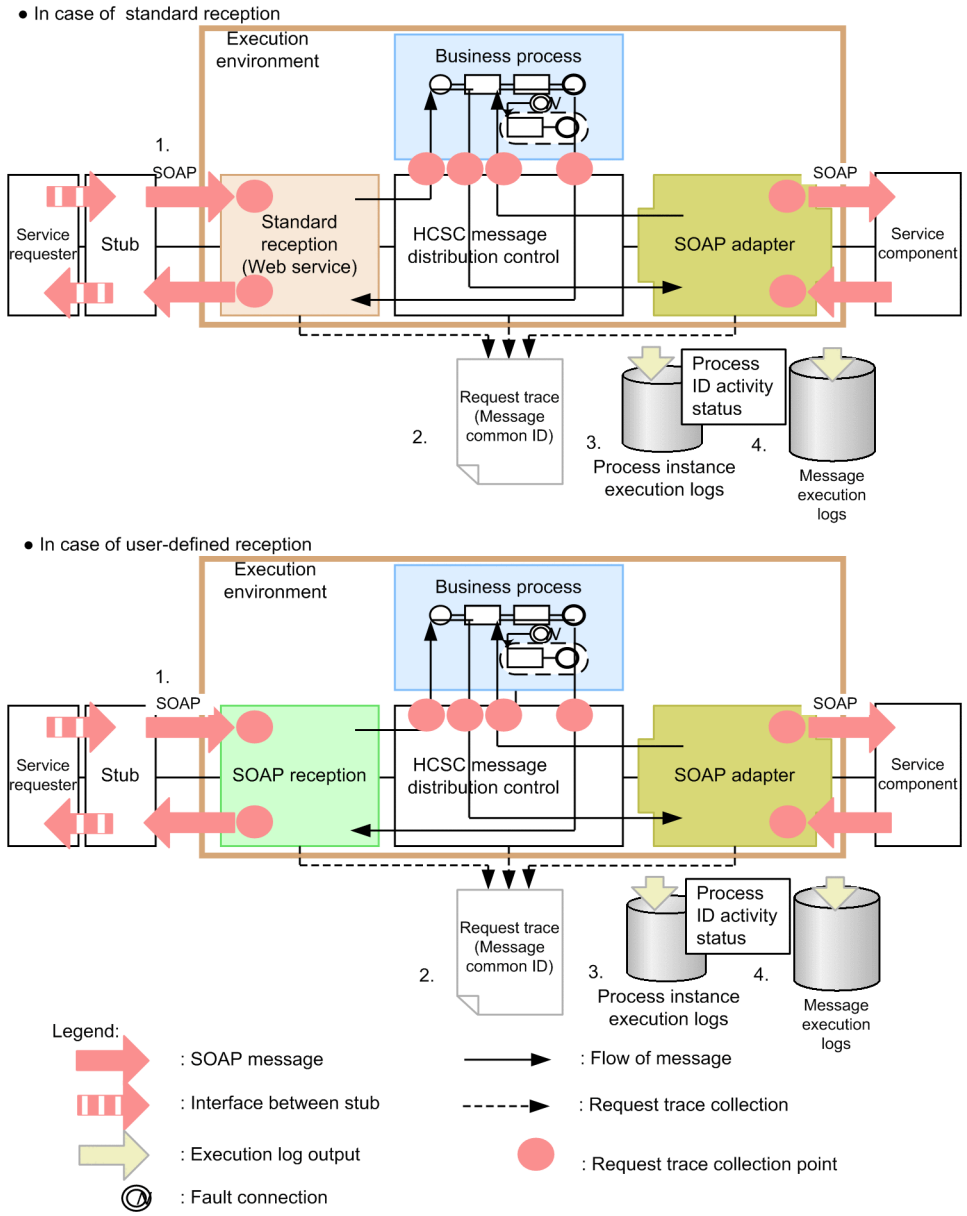
MDB (DB queue) adapter

Method of identifying other causes of failure (tracking the execution history of the invocation request of the service component)

When you use a business process, other than the method of determining the problem area from the exception and error message returned from the service requester, there is a method of identifying the problem area based on the client correlation ID or correlation set of the business process set in the service requester.

The procedure of tracking the execution history of the invocation request of the service component based on the client correlation ID or correlation set of the business process, when using the business process is described here. The following figure shows how to track the execution history of the invocation request of the service component:

Figure 7–43: Tracking the execution history of the service component (for Web service)



The basic flow of tracking the execution history is as follows:

1. Specify following items for each reception at the time of request:
   - For standard reception

     Specify client correlation ID in the parameter or specify correlation set in the request message at the time of request.
   - For user-defined reception

     Specify correlation set in the request message.
2. Identify the instance of the business process in which the failure occurred by acquiring the message common ID used when the error occurred.
3. Search the execution history of the process instance output to the database and acquire the process ID of the business process corresponding with the message common ID.

   You can know the status of an activity by using the process ID. Thus you can understand whether the activity has stopped anywhere in the process and how far has the process progressed.

4. Acquire the user message from the user message trace by using the message common ID.
   You can verify the message contents. The user message is useful for finding out the cause the failure investigation.

There are mainly 2 methods to tracking the execution history of the invocation request of the service component.

- Method of following the client correlation ID specified from the service requester
- Method of following from the business process correlation set specified in the user message

Method of following the client correlation ID specified from the service requester

The procedure followed from the client correlation ID specified from the service requester is as follows:

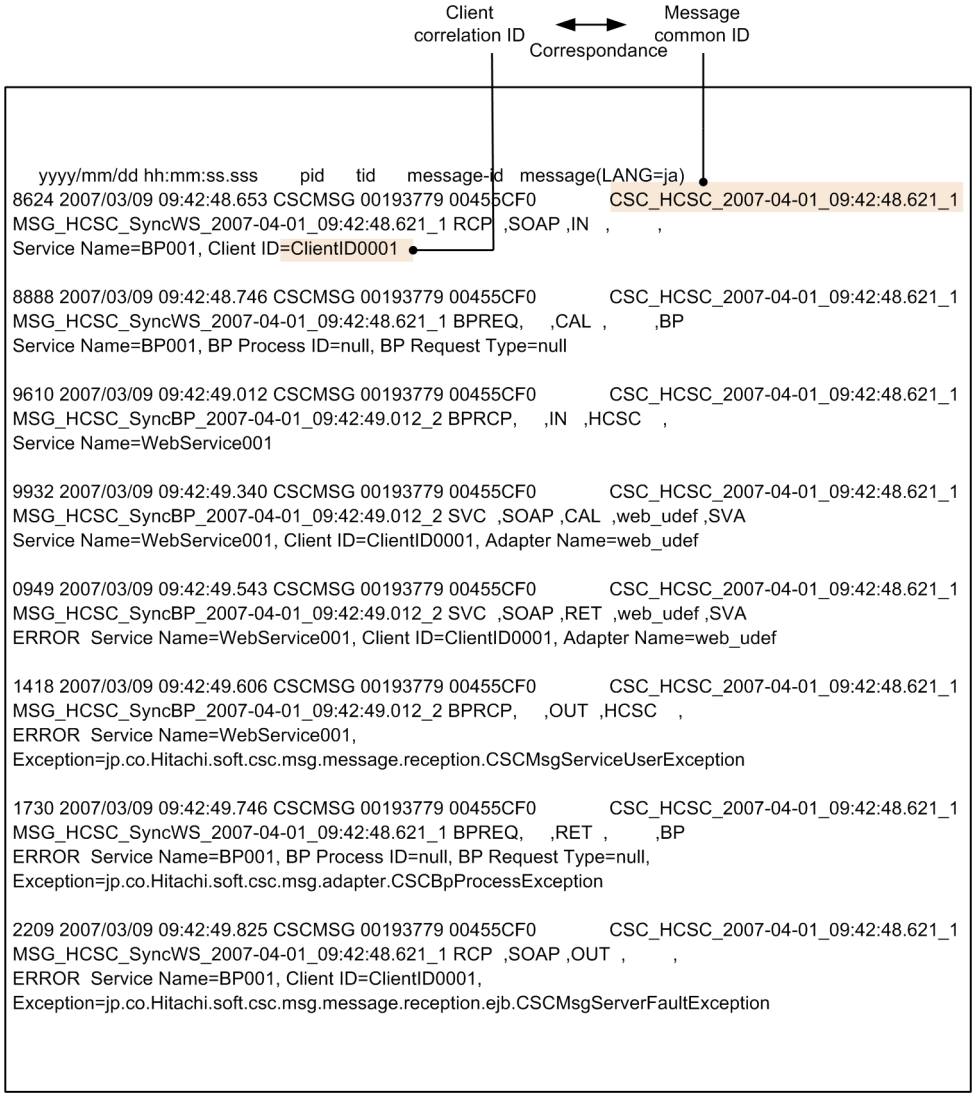
1. Check the client correlation ID.
   The client correlation ID is the information set at the time of request (at the time of invocation) in the program of the service requester, which requests for invocation of the service component. Use this ID to map request messages from the service requester with log and trace managed in the HCSC server. Therefore, it is recommended that you specify a different ID for each request sent to the HCSC server (You must specify it when creating a service requester).
   In case of tracking the execution history of the invocation request of the service component, when a request for failure investigation is made to the system administrator from the requester at service requester side, the client correlation ID is to be notified. Based on that information, the system administrator tracks the execution history.
   An example of coding that specifies the client correlation ID in the service requester is described here. The client correlation ID ("ClientID0001") is set in the argument when invoking the standard reception (Web service).

```
            :
      ((Omitted))
            :
CSCMsgSyncServiceDeliveryWSImplServiceLocator locator = new CSCMsgSyncServiceDeliveryWSImplServiceLocator();
CSCMsgSyncServiceDeliveryWSImpl ws = null;
try {
   ws = locator.getCSCMsgSyncServiceDeliveryWSImpl();
} catch (ServiceException e) {
   e.printStackTrace();
   return;
}

// Service method invocation
String result = ws.invokeXML(
      serviceName,       // Service name
      "ClientID0001",    // Client correlation ID
      null,              // Request format ID
      null,              // Response format ID
      operationName,     // Operation name
      userData);         // User message
```

Client correlation ID

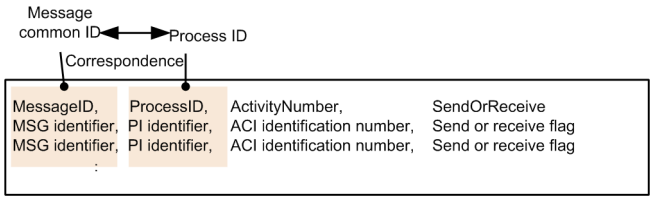
2. Check the request trace based on the client correlation ID and acquire the message common ID used when an error occurred. You can identify the instance of the business process in which a failure occurred according to the message common ID.
   The client correlation ID might be duplicated. Therefore, identify the corresponding locations by acquiring appropriate execution time and name of the business process (service name).
   An example of request trace is as follows. The client correlation ID and the business process name (service name) are present in the "message" raw of the request trace. The message common ID is output at first.



3. Based on the acquired message common ID, acquire the process ID of the business process by referring execution history of the process instance. Use search command of the process instance (cscpiselect) to acquire the process ID.

   In the cscpiselect command, search for the execution history of the process instance using start time and business process name (service name) in the condition.

   Moreover, specify "relation" in the -table option, specify SQL condition in the search condition (where clause), and display the corresponding message related information.



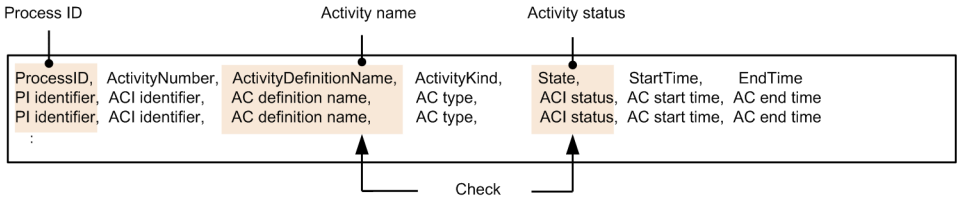
   For details on how to use the cscpiselect command, see "*6.1.2 Searching the execution log of a process instance*". For the syntax of the command, see "< cscpiselect (Searching a process instance) " in "Service Platform Reference Guide".

4. Based on the acquired process ID, acquire the activity of the business process and its status by referring execution history of the process instance. Use search command of the process instance (cscpiselect) to acquire the information of an activity.

In the cscpiselect command, search for the execution history of the process instance using start time and business process name (service name) in the condition.

Moreover, specify "activity" in the -table option, specify SQL condition in the search condition (where clause), and display the corresponding activity information.

The location whose status is "Executing" is an activity which is currently being executed. You can understand which activity has stopped by checking the status.



For details on how to use the cscpiselect command, see "*6.1.2 Searching the execution log of a process instance*". For the syntax of the command, see "cscpiselect (Searching a process instance) " in "Service Platform Reference Guide".

5. When the option to extract the user message trace is set, you can check the contents of the user message.

   Specify settings regarding extraction of the user message trace in the HCSC server runtime definition. For details, see "HCSC server runtime definition file" in "Service Platform Reference Guide".

   In the user message trace, search for the user message based on the message common ID(You can search even from the client correlation ID or time). For the output destination and output contents of the user message trace, see "*7.4.4 User message trace*".

(b) Method of following from the business process correlation set specified in the user message

The procedure for following from the business process correlation set specified in the user message is as follows:

1. Check the correlation set.

   The correlation set is the information to be set in the user message at the time of request in the program of the service requester, which requests for invocation of the service component. It is a string used for uniquely identifying a request message to be sent to a service component from the service requester through the HCSC server.

   As a response from the HCSC server, a response message containing the correlation set is to be sent to the service requester. As a result, the service requester can uniquely identify the mapping between the request messages and the received response messages.

   To use a correlation set, you must define it at the time of defining a business process in the development environment. For details, see "5.5.2 Defining Correlation Sets" in "Service Platform Basic Development Guide".

   In case of tracking the execution history of the invocation request of the service component, when a request for failure investigation is made to the system administrator from the requester at service requester side, the correlation set and name of the requested business process (service name) is to be notified. Based on that information, the system administrator tracks the execution history.

   ! Important note

   If the user of the service requester does not capture the value of the correlation set, the repository imported in the HCSC server must be referred in the development environment and the correlation set of the corresponding business process must be checked. Method of checking the correlation set is as follows:

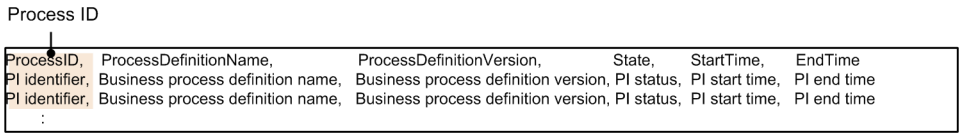
   1. Double-click the [Variables and correlation sets] icon of the business process definition screen.
      A dialog containing list of variables and correlation sets is displayed.
   2. Click the "View" button of the dialog containing list of variables and correlation sets.
      View variables dialog is displayed.
   3. Check the user message against XML schema of View variables dialog and acquire the path to the correlation set.
   4. Acquire variable names and part names from the path name using List of variables and correlation sets dialog. Search for correlation set having same variable name and part name from the List of variables and correlation sets dialog and acquire name of the correlation set.

2. Based on the acquired correlation set, refer the execution history of the process instance and acquire the process ID of the business process. To acquire the process ID, use search command (cscpiselect) of the process instance.

In the cscpiselect command, consider the correlation set as a condition and search for the execution history of the process instance.

Moreover, specify "process_set" in the -table option. Specify SQL condition in the search condition (where clause) and display overview of the corresponding process.

Result of search executed by considering correlation set as a key



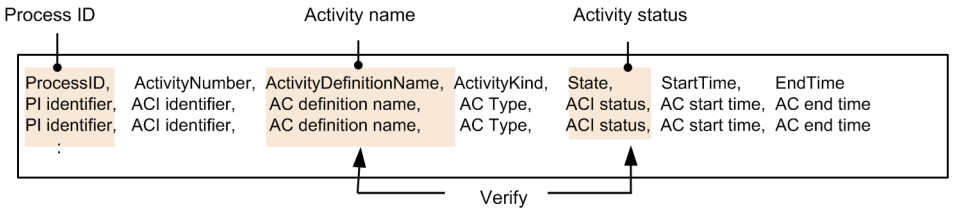
For details on how to use the cscpiselect command, see "*6.1.2 Searching the execution log of a process instance*". For the syntax of the command, see "cscpiselect (Searching a process instance) " in "Service Platform Reference Guide".

3. Based on the acquired process ID, acquire the activity of the business process and its status by referring execution history of the process instance. Use search command of the process instance (cscpiselect) to acquire the information of an activity.

   In the cscpiselect command, search for the execution history of the process instance using start time and business process name (service name) in the condition.

   Moreover, specify "activity" in the -table option and display the corresponding activity information in the search condition.

   The location whose status is "Executing" is an activity which is currently being executed. You can understand which activity has stopped by checking the status.



For details on how to use the cscpiselect command, see "*6.1.2 Searching the execution log of a process instance*". For the syntax of the command, see "cscpiselect (Searching a process instance) " in "Service Platform Reference Guide".

Points to be considered when using Web service of SOAP1.2

Format of SOAP Fault of SOAP1.1 and that of SOAP Fault of SOAP1.2 are different. Therefore, when Web service of SOAP1.2 returns an error response, the information is lost, if the request reception is EJB or SOAP1.1.

Either one of the following steps is required to verify the entire SOAP Fault information returned by Web service of SOAP1.2:

- Use the request reception of SOAP1.2 and implement the service requester.
- Verify in the user message trace (You must specify telegramtrace=ON and telegramtrace-trigger=FAULT in the HCSC server runtime definition).
- Verify the message log of the HCSC server (Fault information in which Detail information is removed, is output).

7.7.2 Troubleshootingwhen executing SessionBean

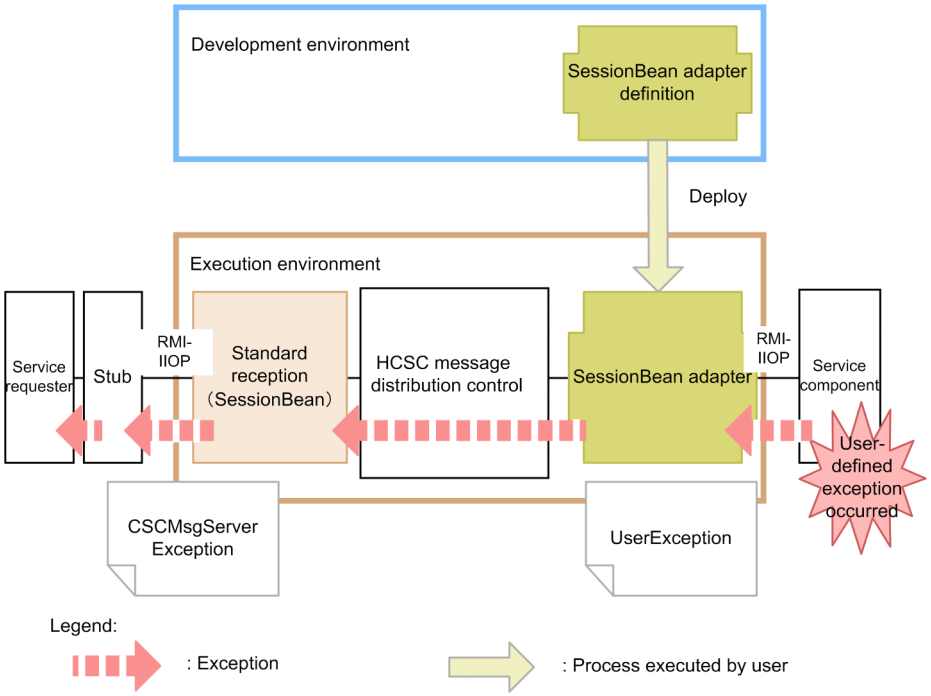
(1) Method of notifying an error in SessionBean communication

This section describes the method of notifying an error which occurs when you invoke the service component using the standard reception from the service requester. Note that the method of notifying an error differs according to the error or existence of a business process.

When an error of the user-defined exception is returned from a service component (when you do not use a business process)

The following figure shows the method of notifying an error in SessionBean communication, when an error of the user-defined exception is returned from the service component and a business process is not used:

Figure 7–44: Figure Method of notifying an error in SessionBean communication when an error of the user-defined exception is returned from a service component (**when you do not use a business process)**

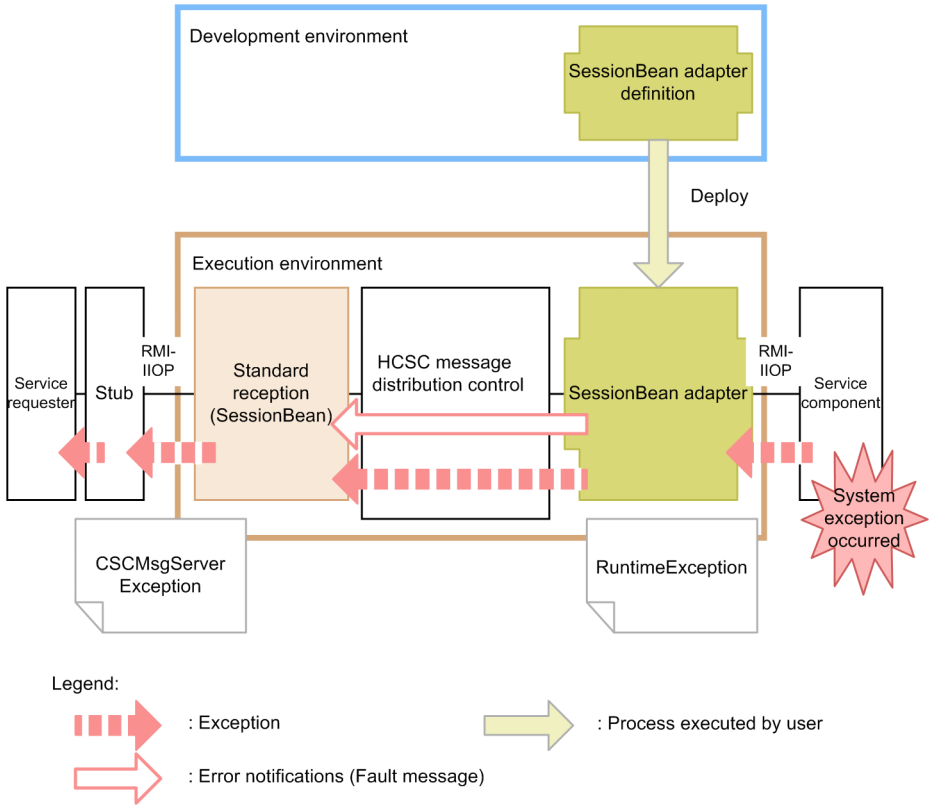


The exception which occurred in the service component is notified as-is to the HCSC server. The HCSC server that has caught the exception throws CSCMsgServerException to the service requester. You can acquire the name or contents of the exception (details of error) by using getter of the caught exception object. For details on CSCMsgServerException, see "8.4.7 Acquiring Error Information" in "Service Platform Basic Development Guide".

When an error other than the user-defined exception is returned from the service component (when you do not use a business process)

The following figure shows the method of notifying an error in SessionBean communication, when an error other than the user-defined exception is returned from the service component and a business process is not used:

Figure 7–45: Figure Method of notifying an error in SessionBean communication, when an error other than the user-defined exception is returned from a service component (when you do not use a business process)



When an unexpected exception occurs in the service component, it is notified as-is to the HCSC server as RuntimeException (System exception).

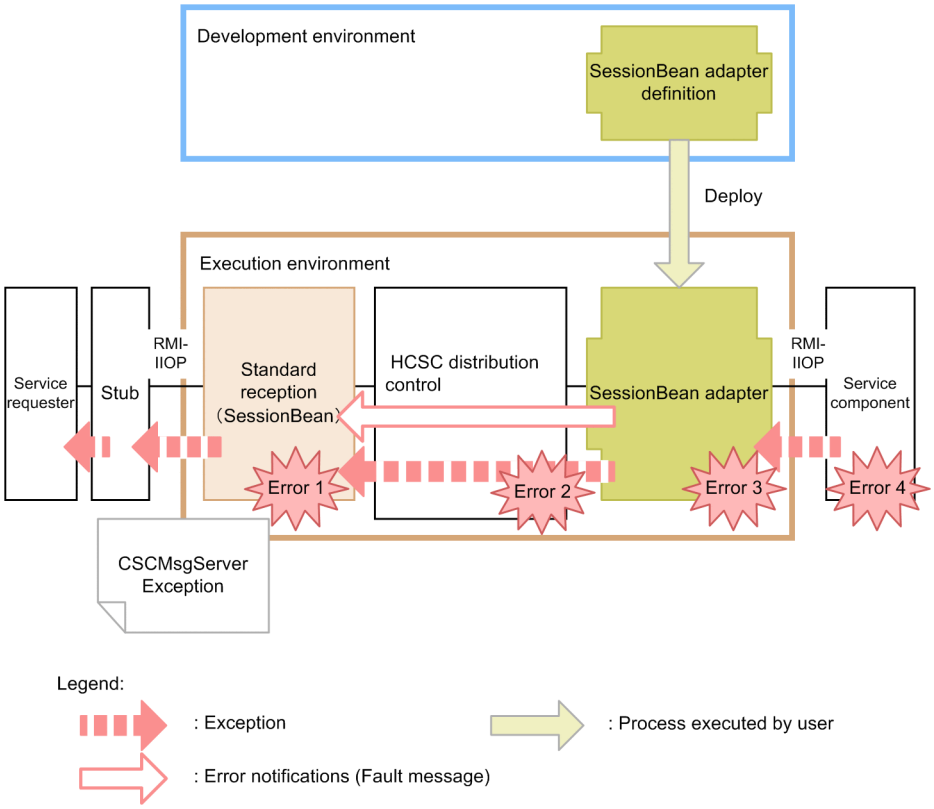
You can also transform the system exception which occurred when the service component is invoked from the service adapter to a fault message in the service adapter. For details on how to transform the system exception to a fault message, see "*7.11 Selecting the errors to be acquired when an exception occurs*".

The HCSC server that has caught the exception throws CSCMsgServerException to the service requester. You can acquire contents of the exception (Details of error) by using getter of the caught exception object. For details on CSCMsgServerException, see "8.4.7 Acquiring Error Information " in "Service Platform Basic Development Guide".

When an error is returned from the HCSC server (when you do not use a business process)

The following figure shows the method of notifying an error in SessionBean communication, when an error is returned from the HCSC server and a business process is not used:

Figure 7–46: Figure Method of notifying an error in SessionBean communication, when an error is returned from the HCSC server (when you do not use a business process)



The errors shown in figure 7-46 are as follows:

- Error 1:Invalid request parameter
- Error 2: Address (Location) not found, service adapter has stopped
- Error 3:Data transformation failed
- Error 4:Invalid address, service component has stopped, Communication failure

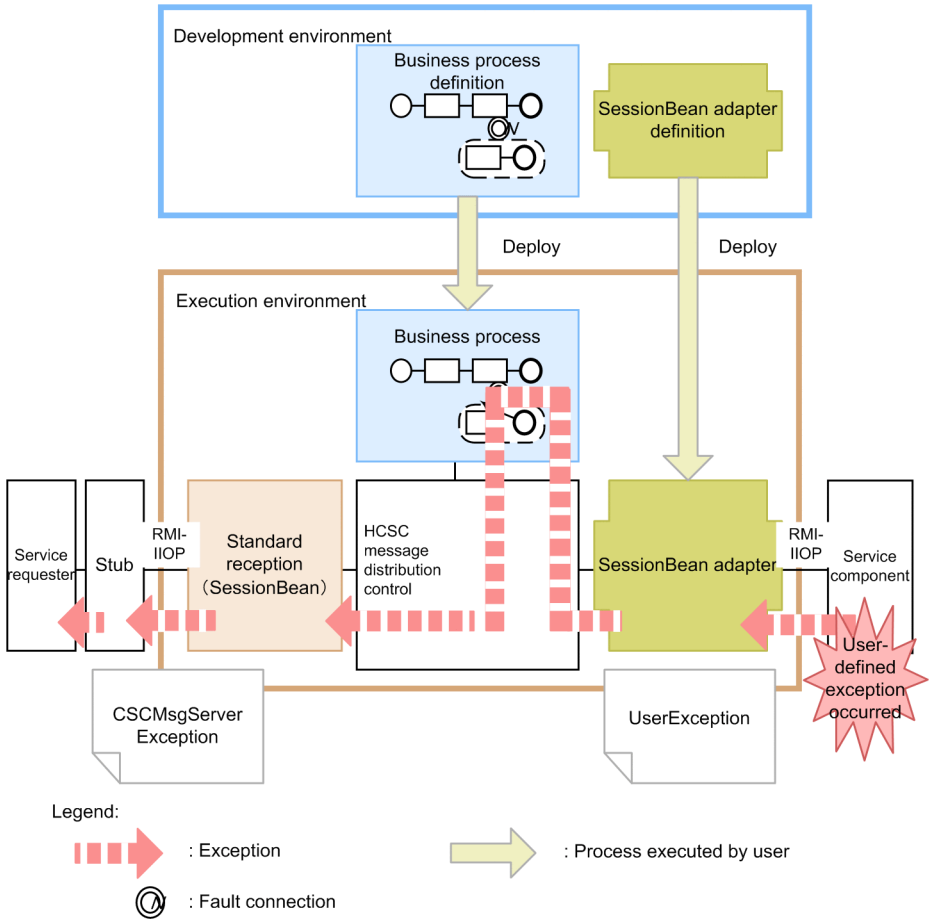
When any of Error 1~ Error 3 shown in the figure are detected in the HCSC server, the error information is thrown to the service requester as CSCMsgServerException. When Error 4 shown in the figure is detected, you can select whether to throw the exception of the error to the service requester as-is or to transform the error exception into a fault message in the service adapter. For details on how to select the error acquired when an exception occurs, see "*7.11 Selecting the errors to be acquired when an exception occurs*".

For the service requester, you can acquire the name or contents of the occurred exception (details of error) by using getter of the caught exception object For details on CSCMsgServerException, see "8.4.7Acquiring Error Information" in "Service Platform Basic Development Guide"

When an error of user-defined exception is returned from a service component (when you do use a business process)

The following figure shows the method of notifying an error in SessionBean communication, when an error of the user-defined exception is returned from the service component and a business process is used:

Figure 7–47: Figure Method of notifying an error in SessionBean communication when an error of user-defined exception is returned from a service component (when you use a business process)



If a user-defined exception occurs in the service component, the business process will process the error in following order:

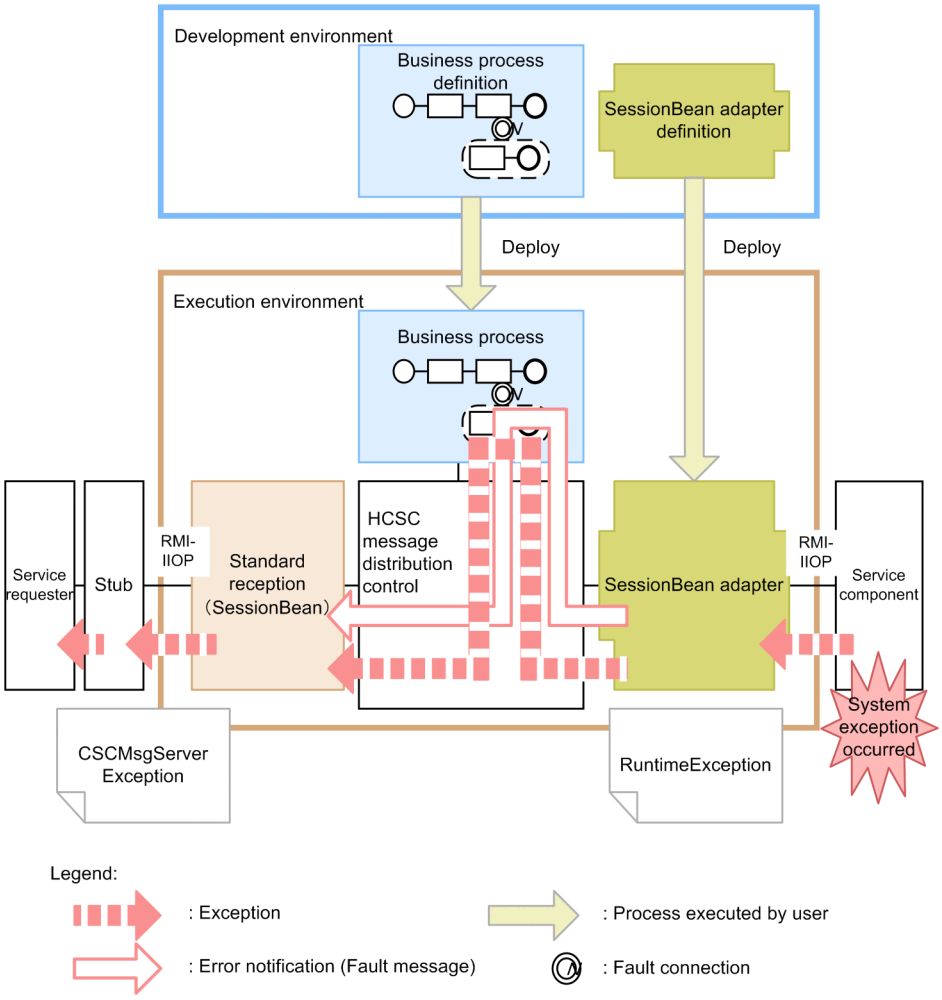
1. Error is caught in business process.
2. In the business process, the error is converted into an exception indicating the failure of the service component, and an exception is notified.
3. Business process throws CSCMsgServerException to the service requester.

You can acquire the contents of the exception (details of error) by using getter of the caught exception object. For details on CSCMsgServerException, see "8.4.7Acquiring Error Information" in "Service Platform Basic Development Guide".

When an error other than the user-defined exception is returned from a service component (when you use a business process)

The following figure shows the method of notifying an error in SessionBean communication, when an error other than the user-defined exception is returned from the service component and a business process is used:

Figure 7–48: Figure Method of notifying an error in SessionBean communication when an error other than the user -defined exception is returned from a service component (when you use a business process)



When an unexpected exception occurs in service component, you can select whether to return the exception as-is to the service requester or to transform the exception which occurred in the service adapter into a fault message. For details on how to transform an exception into a fault message, see "*7.11 Selecting the errors to be acquired when an exception occurs*".

When the exception is not to be converted into a fault message, the business process processes the error in the following order:

1. Error is caught in business process.
2. In the business process, the error is converted into an exception indicating the failure of the service component, and an exception is notified.

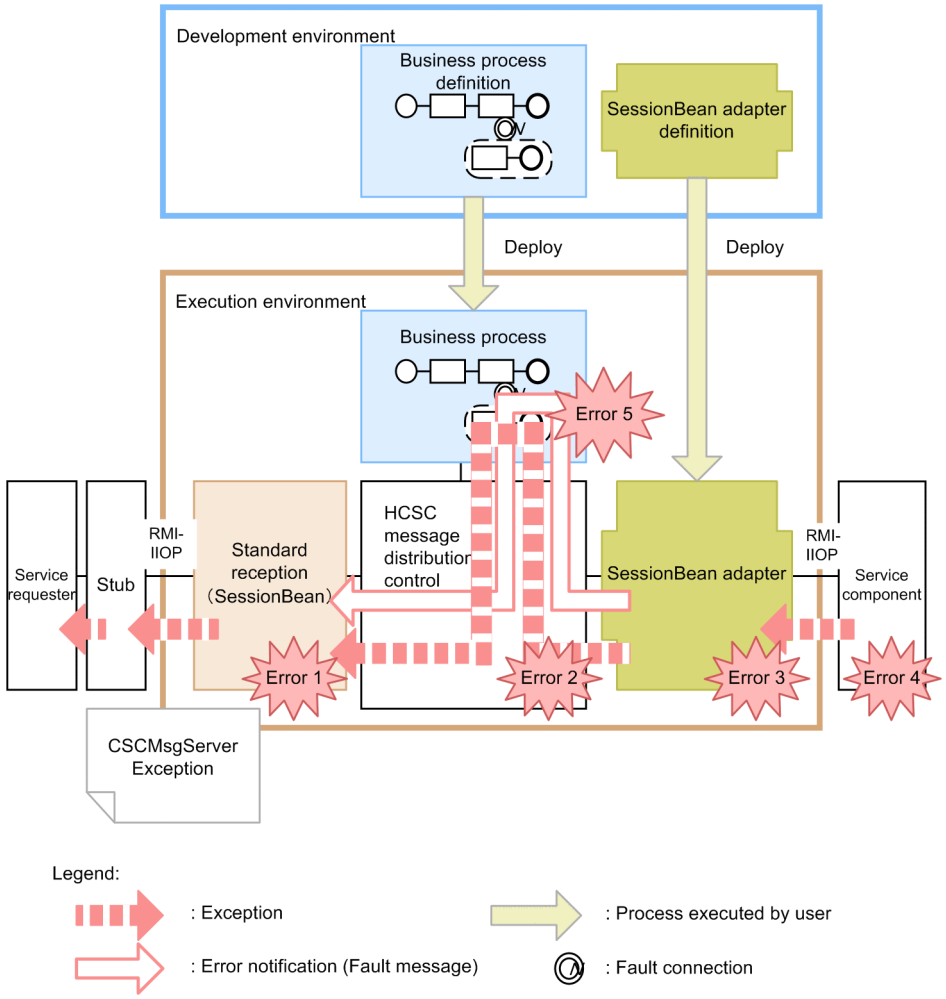
   When the exception is converted into a fault message, it can be caught in business process as a fault.
3. Business process throws CSCMsgServerException to the service requester.

You can acquire the contents of the exception (details of error) by using getter of the caught exception object. For details on CSCMsgServerException, see "8.4.7Acquiring Error Information" in "Service Platform Basic Development Guide".

When an error is returned from the HCSC server (when you use a business process)

The following figure shows the method of notifying an error in SessionBean communication, when an error of the user-defined exception is returned from the HCSC server, and a business process is used:

Figure 7–49: Figure Method of notifying an error in SessionBean communication when an error is returned from the HCSC server (when you use a business process)



The errors shown in figure are as follows:

- Error 1:Invalid request parameter
- Error 2: Address (Location) not found, service adapter has stopped
- Error 3:Data transformation failed
- Error 4:Invalid address, service component has stopped, Communication failure
- Error 5:Exception error in processing the business process

When any of Error 1~Error 3, and Error 5shown in figure are detected in the HCSC server, the error information is thrown to the service requester as CSCMsgServerException.

When Error 4 shown in the figure is detected, you can select whether to throw the exception of the error to the service requester as-is or to transform the exception of the error into a fault message in the service adapter.

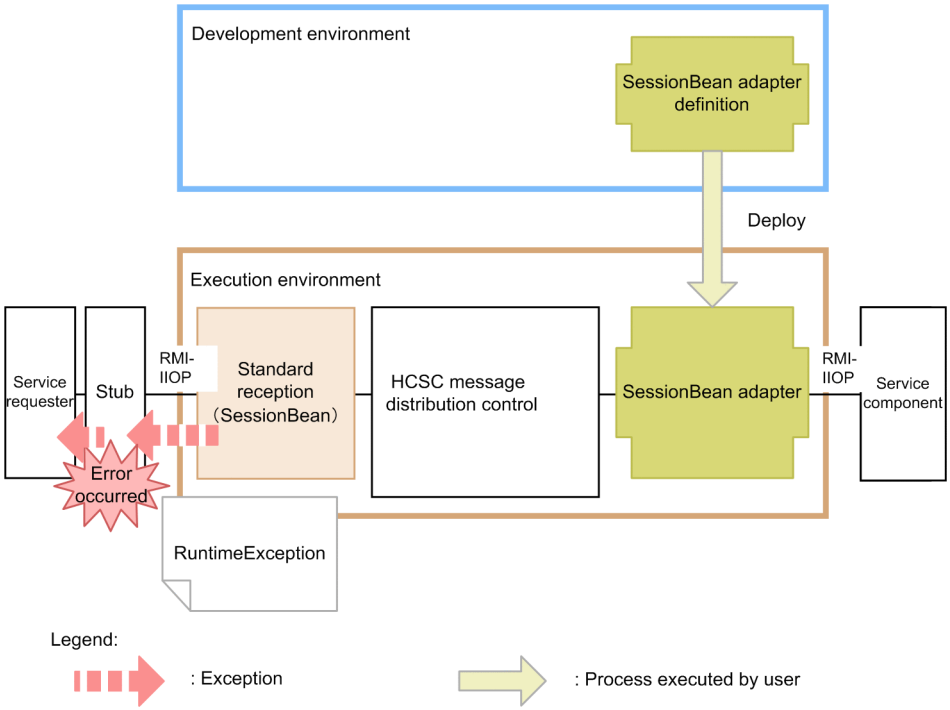
For details on how to select the error acquired when an exception occurs , see,"*7.11 Selecting the errors to be acquired when an exception occurs*".

For the service requester, you can acquire the contents of the exception (details of error) by using getter of the caught exception object. For details on CSCMsgServerException, see"8.4.7Acquiring Error Information" in "Service Platform Basic Development Guide"

When an error is detected in the service requester

The following figure shows the method of notifying an error in SessionBean communication when an error is detected in the service requester:

Figure 7–50: Figure Method of notifying an error in SessionBean communication when an error is detected in the service requester



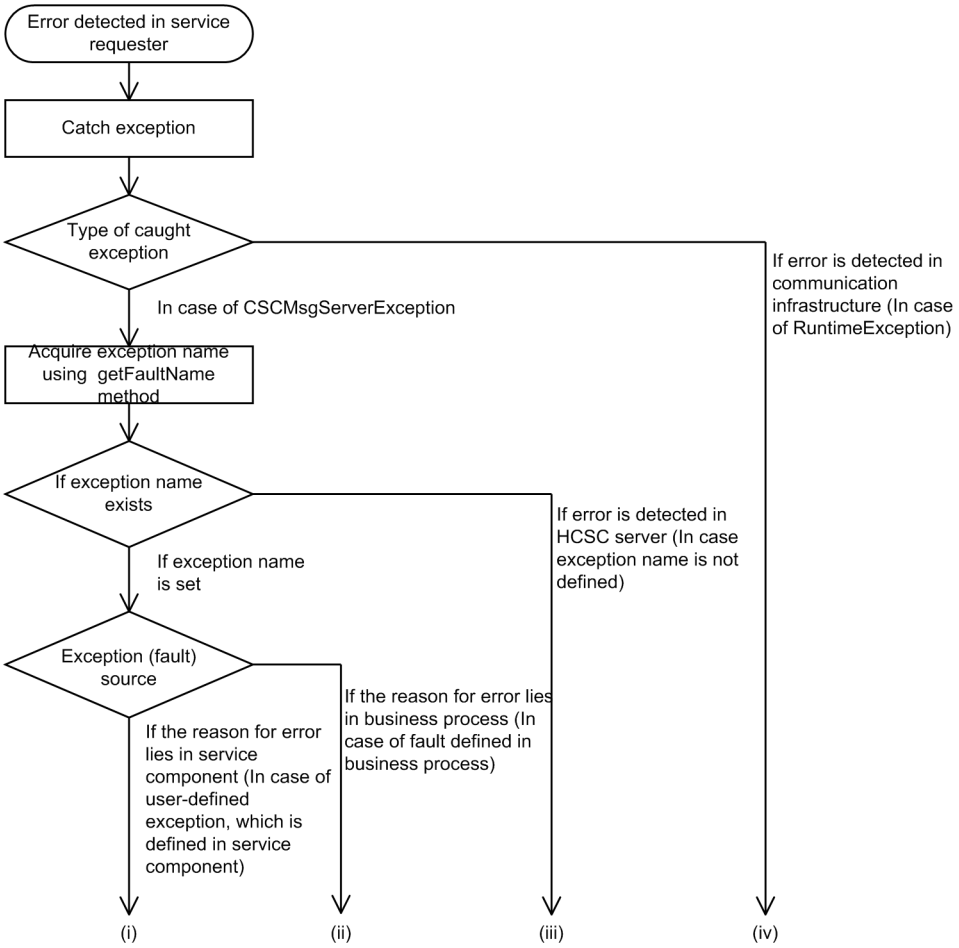
When the HCSC server could not be invoked from the service requester or, when invocation of a the service component is complete but there is no response from the HCSC server to the service requester due to some reason, the stub (J2EE container) at the service requester end (client end) returns an error.

The service requester can catch an exception in RuntimeException. You can acquire the information of fault (details of error) by using getter of the caught exception object.

(2) Method of determining a problem area

The method of determining an area where a problem has occurred when the service component is invoked from the service requester using standard reception (SessionBean) is described here. The following figure shows how to determine an area where the problem has occurred:

Figure 7–51: Figure Method of determining problem area (when the service component is invoked from the service requester using the standard reception (SessionBean)



When the cause of failure exists in the service component (for user-defined exception defined in the service component)

There is a possibility that the cause of failure exists in the service component. You can acquire contents of the exception returned by the service component by using the following method:

- getErrorMessage: Acquire contents of the exception from service component.
- getErrorCode: Acquire the error code corresponding to contents of the exception from service component.

Investigate the cause from the following perspective:

- User message requested from the service requester.
- Service component machine
- Service component program

Decision regarding whether to resend invocation of the service component depends on the agreement between the service requester and the service component (end-to-end) through the HCSC server.

(ii) When the cause of failure exists in business process (for a fault defined in the business process)

There is a possibility that the cause of failure exists in the activity processing executed in the business process (for service invocation activity, there is a possibility that the cause of failure exists in the invoked service component). You can acquire the contents of the fault returned by the business process using the following method:

- getErrorMessage: Acquire contents of the exception from the business process.
- getErrorCode: Acquire the error code corresponding to the contents of the exception from the business process.
- getCscmsgFaultCode: Acquire FaultCode information.

- getCscmsgFaultString: Acquire FaultString information.
- getCscmsgFaultActor: Acquire FaultActor information.
- getCscmsgFaultDetail: Acquire FaultDetail information.

Investigate the cause from the following perspective:

- User message requested from the service requester
- Service component machine
- Service component program
- Definition contents of business process

Decision regarding whether to resend invocation of the service component depends on the agreement between the service requester and the service component (end-to-end) through the HCSC server.

Furthermore, it is necessary to design a system which determines whether to resend (re-execution of business process) according to the design contents of the business process.

(iii) When an error is detected in the HCSC server (when the exception name is not set)

You can acquire the contents of the error by using the following method. Take action as per counter measures of the acquired error code and error message.

- getErrorMessage: Acquire message of the error detected within the HCSC server.
- getErrorCode: Acquire error code of the error detected within the HCSC server.

Investigate by referencing the message log output by Service platform.

Investigate the cause from the following perspective:

- Contents of the argument requested from the service requester.
- Settings or status of the HCSC server
- Definitional contents of service adapter.
- Definition contents of business process
- User message requested from the service requester
- Resending of the service component invocation differs according to the contents of the error.
- Service component machine
- Service component program
- Status of network

If resending fails temporarily, you can rectify it by trying the resend operation. However, in case of the following errors resending fails even if you try the resend operation and an error occurs:

- When there is error in the contents of the argument requested from the service requester.
- When there is an error in the settings of the HCSC server
- When there is an error in the definition of service adapter or business process
- When there is an error in the user message requested by the service requester

(iv) When error is detected in the communication board (for Runtime Exception)

You can acquire the contents of error from RuntimeException. Take action on the basis of the error information of the acquired exception.

Investigate the cause from the following perspective:

- Stub being used in the service requester
- Settings and status of J2EE container of the service requester machine
- Settings and status of the HCSC server
- Status of network

Whether to resend the invocation of the service component differs according to the contents of the error. If resending fails temporarily, you can rectify it by trying the resend operation. However, in the case of the following errors resending fails even if you try the resend operation, and an error occurs:

- When there is an error in stub being used in the service requester
- When there is an error in settings of J2EE server of the service requester machine

- When there is an error in settings of the HCSC server

(3) Contents of the exception returned from the HCSC server

This section describes the type of information to be set in a particular factor for SOAP Fault (SOAP message) returned from the HCSC server. The following table describes contents of an exception returned from the HCSC server.The error case number corresponds to the number shown in "*7.7.2(2) Method of determining a problem area*".

Table 7–57: Table Contents of the exception returned from the HCSC server

Fault name of CSCMsgServerException returned fromHCSC server	Error case	
	For (ii)	For (i), (iii)
errorMessage	This is the content of the following errors: • Error detected in the HCSC server • Error from service component, business process, and service adapter#	
errorCode	This is the error code corresponding to the contents of exception: • Error detected in HCSC server • Error from service component, business process, and service adapter#	
processInstanceID	This is the information of Instance ID of business process. Value is set when an error occurs in business process.	
cscmsgFaultCode	This is the FaultCode information from a service component (Web service), business process, or service adapter#	Value is not present.
cscmsgFaultString	This is the FaultString information from a service component (Web service), business process, or service adapter#	Value is not present.
cscmsgFaultActor	This is the FaultActor information from a service component (Web service), business process, or service adapter#	Value is not present.
cscmsgFaultDetail	This is the Detail information from a service component (Web service), business process, or service adapter#	Value is not present.
faultName	This is the Fault name (Exception name) information from a service component (Web service or SessionBean) or business process. Value will be set in following cases: • For SOAP Fault of the user-defined exception from a service component (Web service or SessionBean) • For fault from a business process	Value is not present.

#1

For (iv), throw RuntimeException from the stub of the service requester end (J2EE server).

#2

When the service component of the SOAP adapter is invoked from the standard reception (SessionBean), Fault information is set same as in (ii).

Note#

The following service adapters are out of scope:

SOAP adapter

SessionBean adapter

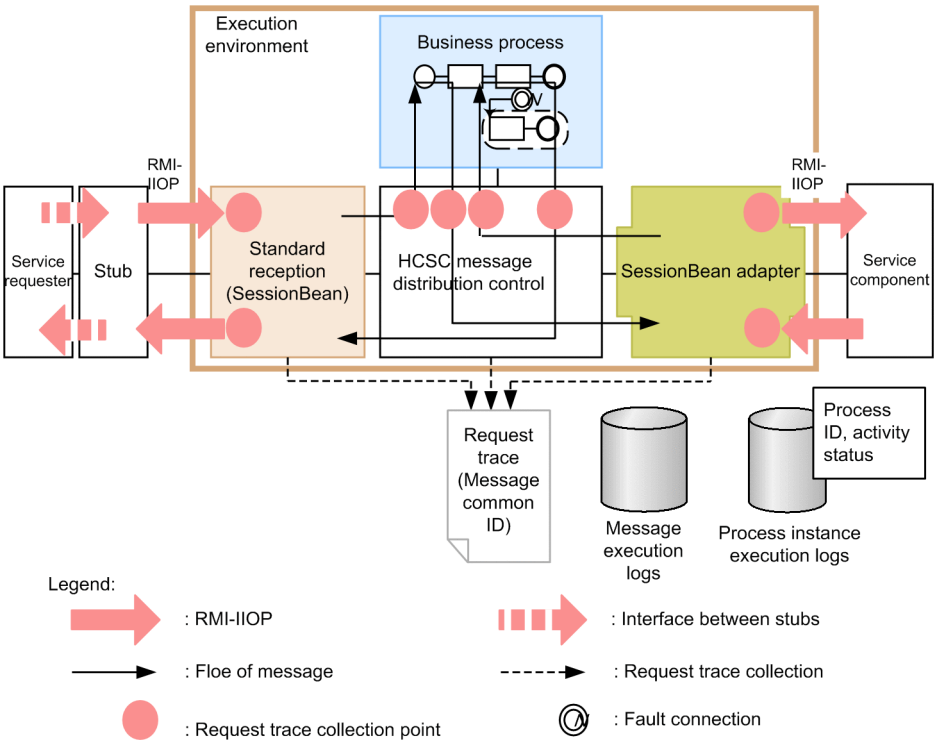
MDB (WS-R) adapter

MDB (DB queue) adapter

(4) Method of identifying other causes of failure (tracking the execution history of the invocation request of the service component)

Other than the method of determining the problem area from the exception and error message returned from the service requester, this section describes how to identify the problem area based on the client correlation ID or correlation set of the business process at the service requester end. The following figure shows how to track the execution history of the invocation request of the service component:

Figure 7–52: Figure Tracking the execution history of the service component (for SessionBean)



The method of identifying or the procedure when the business process is used is same as the procedure in Web service (SOAP communication).For details, see "*7.7.1 Troubleshooting when executing Web service (SOAP communication)*".

The procedure applicable for SessionBean is described here:

(a) Method of following the client correlation ID specified from the service requester

The procedure followed from the client correlation ID specified from the service requester is as follows:

1. Check the client correlation ID.
2. Acquire the common message ID.
3. Acquire the process ID of the business process.
4. Acquire the status of activity.
5. Check user message.

For details, see "7.7.1 Troubleshooting when Web service (SOAP communication) is executed"".

You can specify the problem area in more detail by investigating again using the performance analysis trace. You can check compatibility with the log of the sevice component machine by following the thread ID of the performance analysis trace.

1. Search for the row which has a character string matching with the common message ID

   Since the common message ID is output in the "ASCII" row at the entry of the request reception of HCSC server, first it is searched there.
2. Check the thread ID of the row which has matched in search, follow that thread ID, and check the problem area.

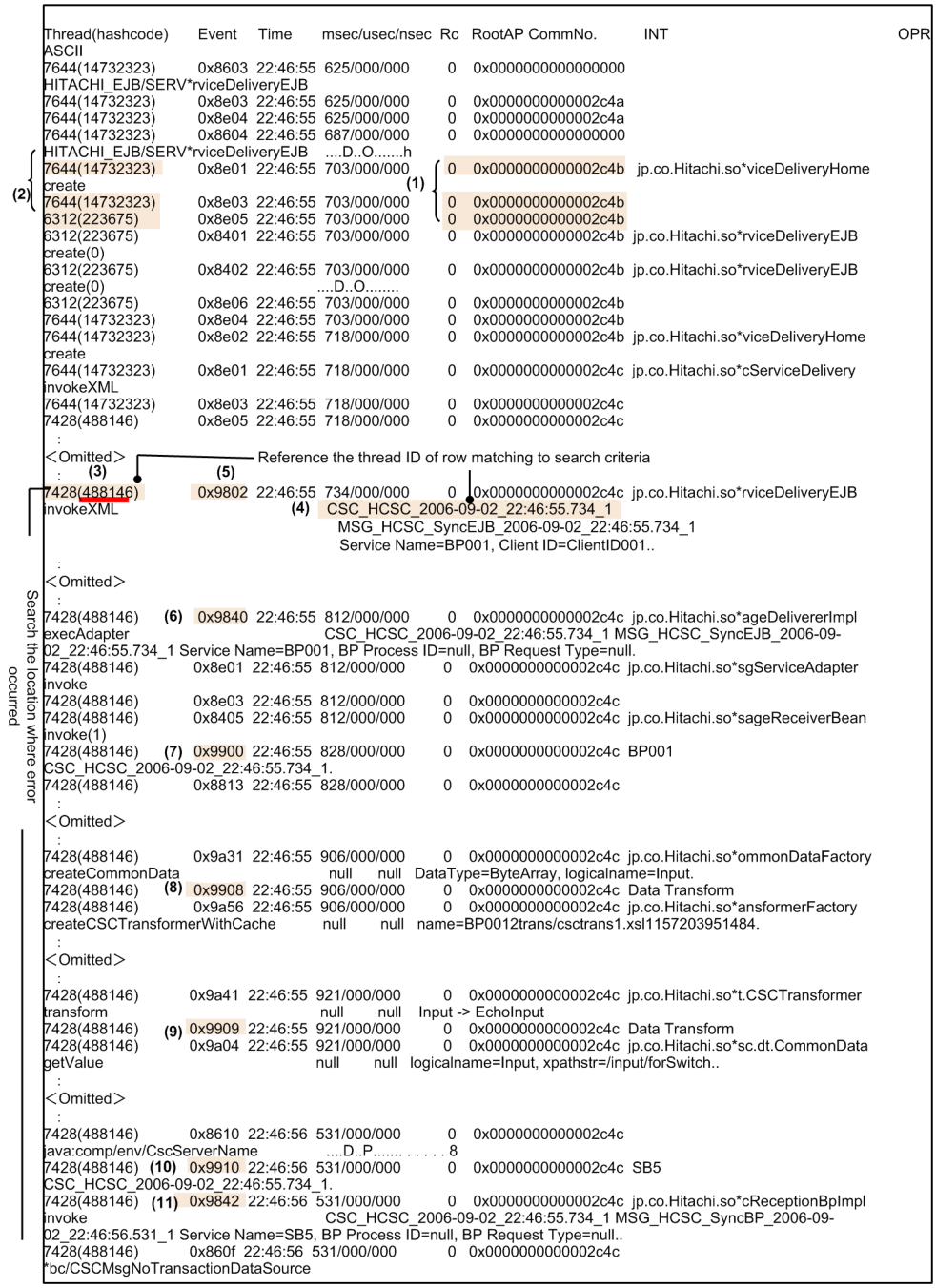
Thread ID is changed by invoking RMI-IIOP but you can understand the connection with "Root AP CommonNo" column.

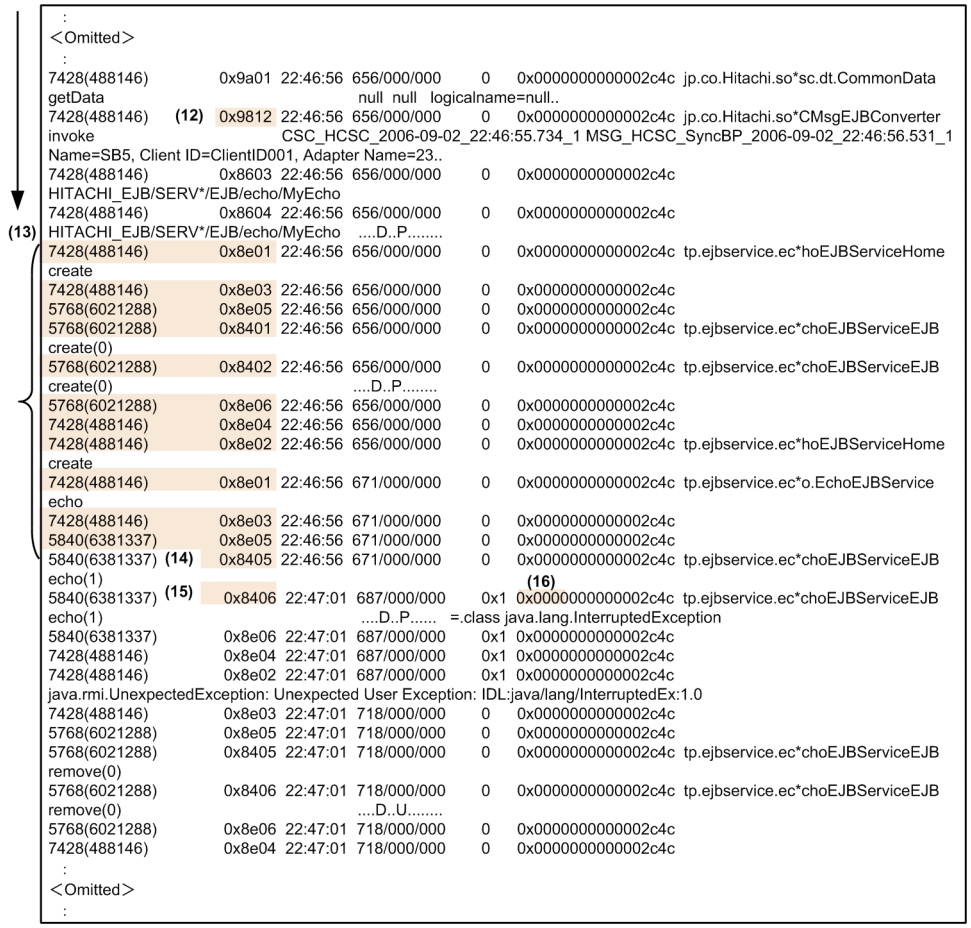
3. The error location is a location where a value other than 0 is specified in "Rc (Return code)" column. When the error location is identified, check the processing contents before and after that location and investigate the cause of error.

When you want to investigate again, use the log of the failure information output by the J2EE server and follow the thread ID of the location where error has occurred.

The following figure shows an example of performance analysis trace:

Figure 7–53: Figure Example of performance analysis trace





The numbers in "Figure 7-53 Example of performance analysis trace" indicate the following contents:

(1)This is a row which contains character strings matching with the common message ID. You can understand the connection since common IDs are assigned.

(2)Number changes since multiple threads are covered through RMI invocation.

(3)This is thread number that has matched in the search.

(4) This is thread ID of the thread number (Number 3).

(5) This is entry of standard reception (SessionBean).

(6) This is point of invocation of the business process.

(7) This is invocation of the execution request of the business process from the messaging board.

(8) This is invocation of the data transformation request.

(9) This is a response from the data transformation request.

(10) This is invocation of the service from the business process to the messaging board.

(11) This is the entry of the business process reception.

(12) This is invocation of the service component of SessionBean adapter.

(13) This is invocation of Service component machine from the HCSC server machine.

(14) This is immediately after an EJB container request.

(15) This is just before receiving an EJB container response.

(16) Error has occurred.

In this example, in point (13) shown in "*Figure 7-50 Example of performance analysis trace*", you can understand that RMI of the service component is invoked and the error has occurred immediately after the EJB container has received

a request (there are two extraction levels of performance analysis trace such as "Normal" and "Details", but "*Figure 7-50 Example of performance analysis trace*"shows trace collected at "Normal")

When Service component machine is using Application Server, you can investigate again by comparing the thread ID of the location where the error has occurred and the failure information at Service component machine end.

Note that, the thread ID of performance analysis trace has a decimal value but, since the failure information is output in hexadecimal value by the J2EE server, you must individually modify the thread ID to a hexadecimal value.

Regarding the invocation of the service component from the service adapter, thread ID is changed by invoking SessionBean, but you can understand the connection through Root AP CommonNo column. For details on how to use the performance analysis trace file, see "7.7.1 Overview of the analysis of process functionality" in "Application Server Maintenance and Migration Guide"

(b) Method of following from the business process correlation set specified in the user message

The procedure for following from the business process correlation set specified in user message is as follows:

1. Check the correlation set.
2. Acquire the process ID of business process.
3. Acquire status of activity.

For details, see "*7.7.1 Troubleshooting when executing Web service (SOAP communication)*".

7.7.3 Troubleshooting when executing MDB (WS-R)

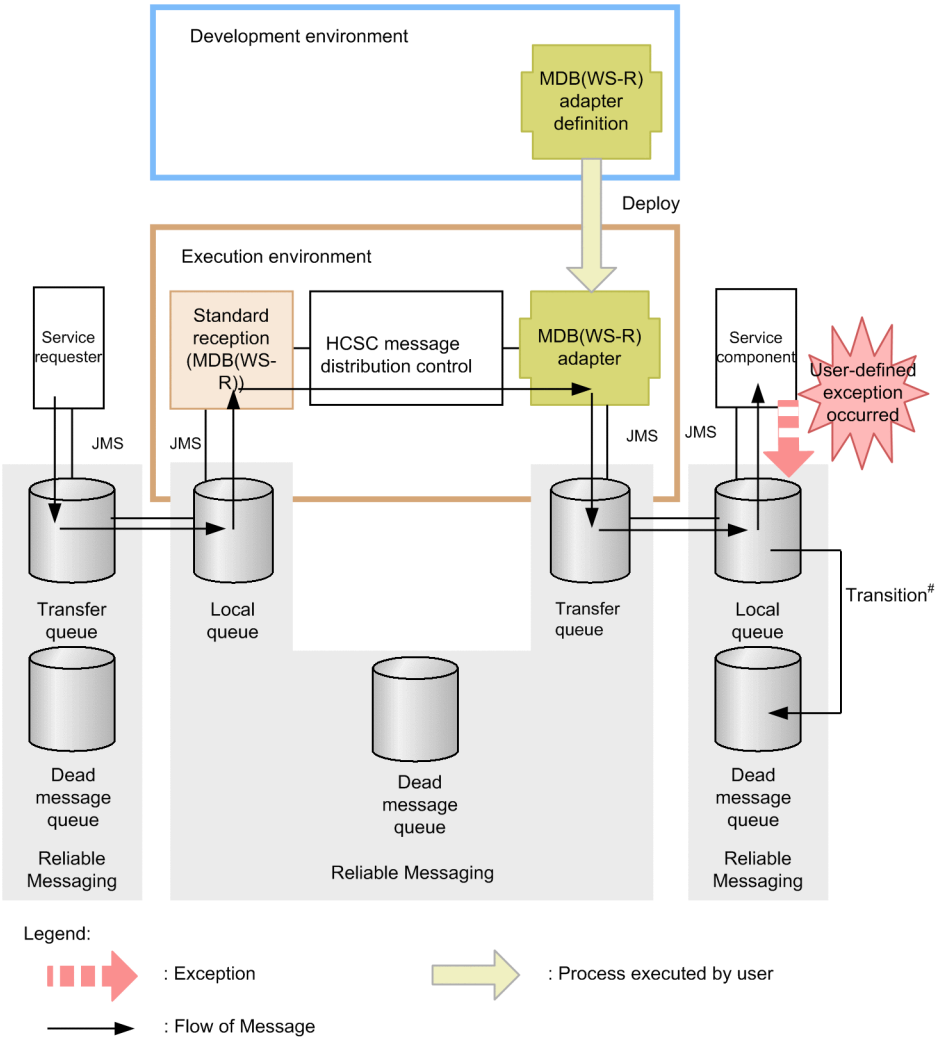
(1) Method of notifying an error in MDB (WS-R)

In the service component invocation of MDB (WS-R), the error which occurs between the service requester and the HCSC server, and the HCSC server and the service component is not notified. The types of failure that can be detected, output destination of logs and traces is described here.

When the error of user-defined exception is occurred in a service component

The following figure shows the method of notifying an error in MDB (WS-R) when an error of the user-defined exception occurs in a service component:

Figure 7–54: Figure Method of notifying an error in MDB (WS-R) when an error of the user-defined exception occurs in a service component



Transits when reached the maximum value of distribution count or reached the validity period.

The exception which occurred in the service component processes error in Reliable Messaging on the service component machine. Reliable Messaging on the service component machine outputs a message indicating the failure of fetching message from the local queue to the log on the service component machine.

Further, for user-defined exception (Application exception), whether to fetch message in the service component by again performing rollback depends on settings of Reliable Messaging at the service component machine end or creation of the service component program.

When you perform rollback in message fetching on the service component machine and frequency of rollback (frequency of message delivery) reaches the maximum value or when the message reaches to its expiry date, that message moves to the dead message queue. However, message is deleted in following cases:

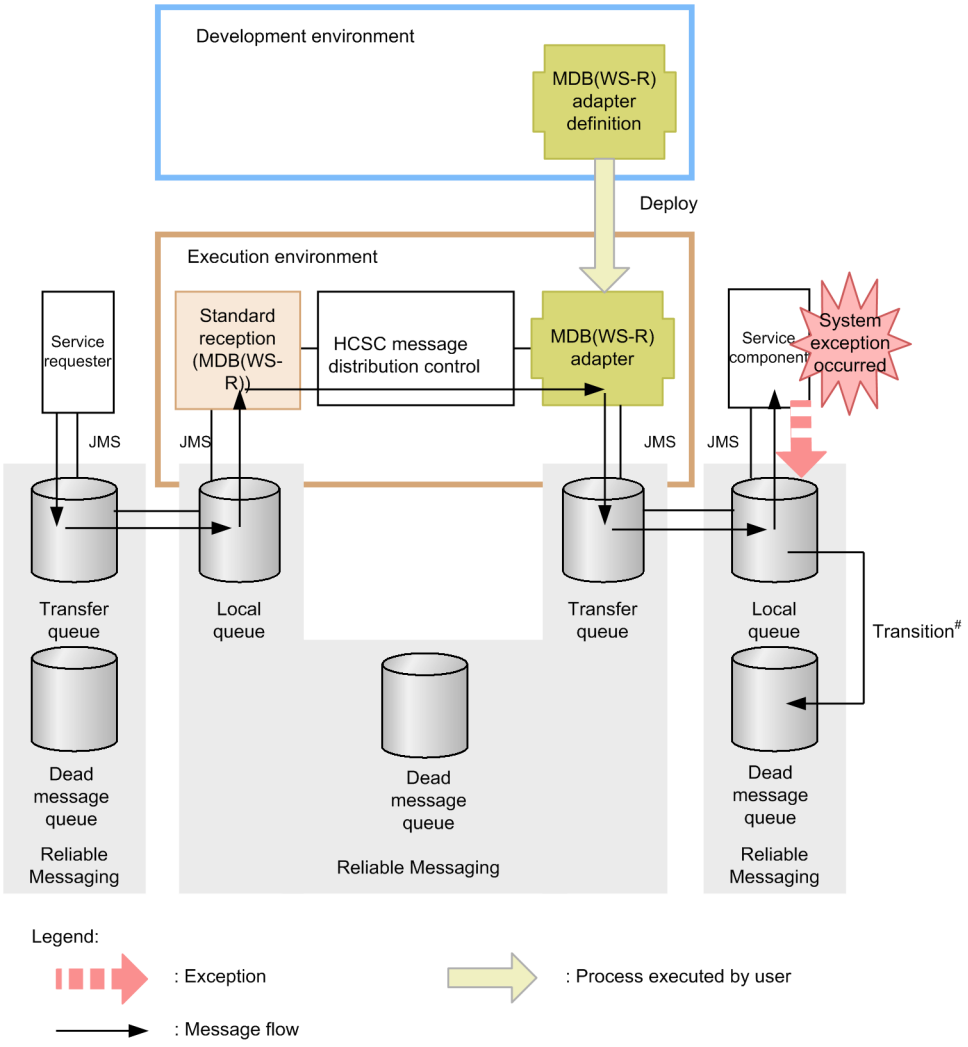
- When settings for the dead message queue are not performed
- When "Unlimited" is set in delivery frequency
- When number of messages in the dead message queue are in excess
- When failure occurs in database

For details on Reliable Messaging, see "Reliable Messaging".

When an error other than the user-defined exception occurs in the service component

The following figure shows the method of notifying an error in MDB (WS-R) when an error other than the user-defined exception occurs in a service component:

Figure 7–55: Figure Method of notifying an error in MDB (WS-R) when an error other than the user-defined exception occurs in service component



Transits when reached the maximum value of distribution count or reached the validity period.

The exception which occurred in the service component processes the error in Reliable Messaging on the service component machine. Reliable Messaging outputs a message indicating failure in message fetching from local queue in the log on the service component machine.

Furthermore, for system exception, perform rollback at the service component end and again try fetching message in Service component.

When you perform rollback in message fetching on the service component machine and rollback frequency (message delivery frequency) reaches the maximum value or when message reaches to its expiry date, the message moves to the dead message queue. However, the message is deleted in following cases:

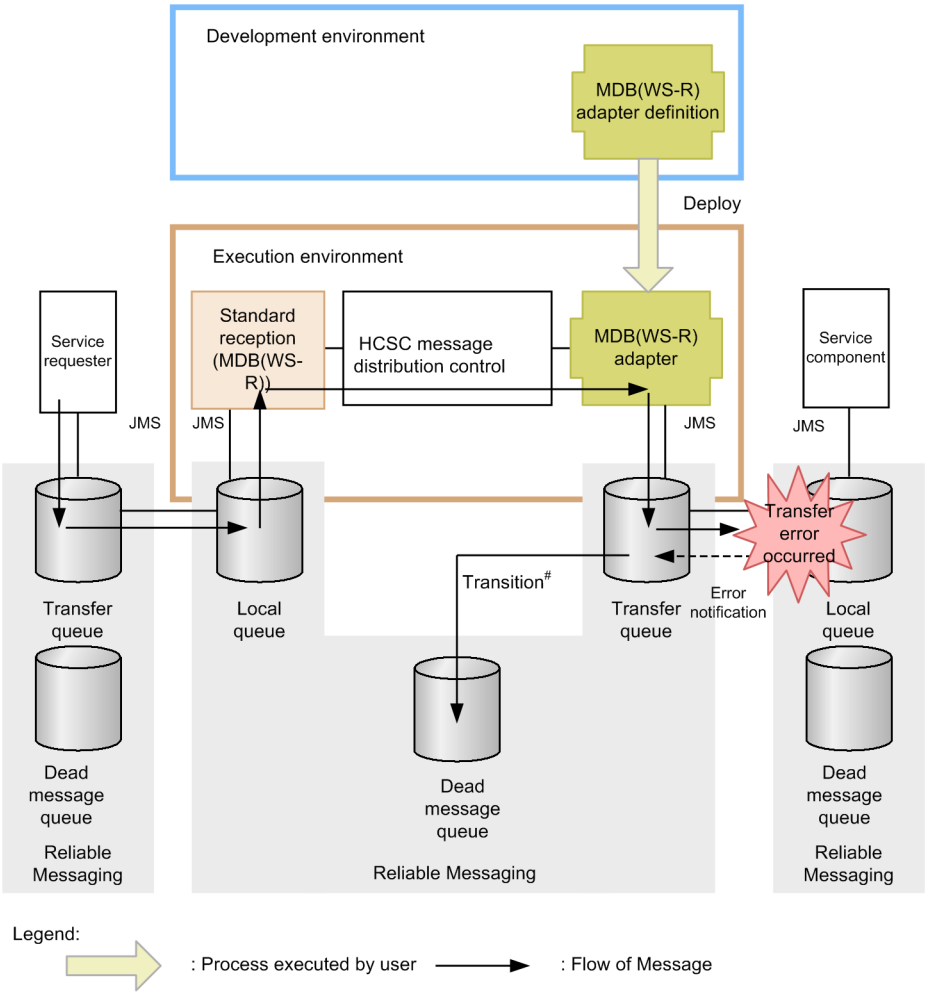
- When settings for the dead message queue are not performed.
- When "Unlimited" is set in delivery frequency
- When number of messages in the dead message queue are in excess.
- When a failure occurs in database.

For details on Reliable Messaging, see "Reliable Messaging".

When error occurs in transfer from the HCSC server machine to the service component machine

The following figure shows the method of notifying an error in MDB (WS-R) when error occurs in transfer from HCSC server machine to the service component machine:

Figure 7–56: Figure Method of notifying an error in MDB (WS-R) when an error occurs in transfer from HCSC server machine to the service component machine



Transits when reached the maximum value of distribution count or reached the validity period.

When message transfer from the HCSC server machine to the service component machine fails, error processing is to be performed in Reliable Messaging at the HCSC server end. Reliable Messaging outputs a message indicating the failure which has occurred in the message transfer to the log on the HCSC server machine.

Furthermore, when you detect an error in message transfer, perform rollback at the HCSC server end, and try to perform transfer again.

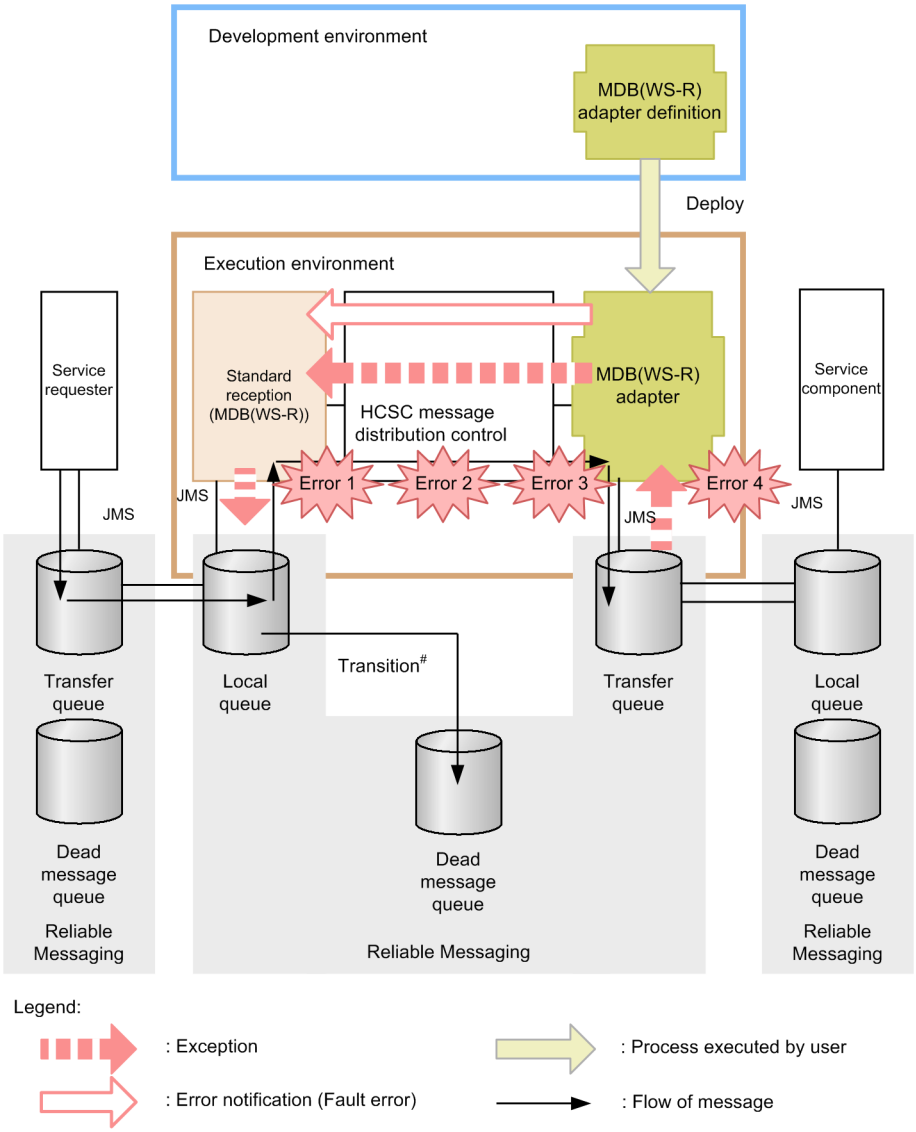
When you perform rollback in transfer from the HCSC server and rollback frequency (frequency of message delivery) reaches a maximum value or when "Unlimited" is set in delivery frequency, that message moves to the dead message queue. When the dead message queue name is not set or when the dead message queue is not created, the process of invoking the service component is re-executed without any limit. Therefore, you must set the dead message queue name or the dead message queue without fail.

For details on the setup of Reliable Messaging, see "*3.1.2 Setting up the software required for the execution environment*". For details on operations performed when the transfer between Reliable message queues fails, see "2.4.7 Operation when failure occurs in transfer between queues" in "Reliable Messaging".

When an error occurs from HCSC server

The following figure shows the method of notifying an error in MDB (WS-R) when an error occurs from HCSC server:

Figure 7–57: Figure Method of notifying an error in MDB (WS-R) when an error occurs from HCSC server



Transits when reached the maximum value of distribution count or reached the validity period.

The errors shown in Figure 7-57 are as follows:

- Error 1: Invalid request parameter
- Error 2: Address (Location) not found, service adapter has stopped.
- Error 3: Data transformation failed.
- Error 4: Failure in message sending

When any of Error 1~Error 3 shown in figure are detected in the HCSC server, the error processing is performed in Reliable Messaging on the HCSC server machine. When Error 4 shown in the above Figure is detected, you can select whether to throw an exception of the error to the standard reception as-is or to transform the exception of error into a fault message in the service adapter. For details on how to select the error acquired when an exception occurs, see "*7.11 Selecting the errors to be acquired when an exception occurs*".

Messages of error which have occurred are output to the message log. Reliable Messaging outputs the message indicating the failure in message fetching from the local queue to a log on the HCSC server machine.

Further, when an error is detected in the HCSC server, perform rollback at the HCSC server end and again try to fetch messages in the service component (invoking service component). When you perform rollback in message

fetching on the HCSC server machine, and when frequency of rollback (frequency of message delivery) reaches the maximum value, that message moves to the dead message queue.

When the dead message queue name is not set or when the dead message queue is not created, the process of invoking the service component is re-executed without any limit. Therefore, you must set the dead message queue name or the dead message queue.

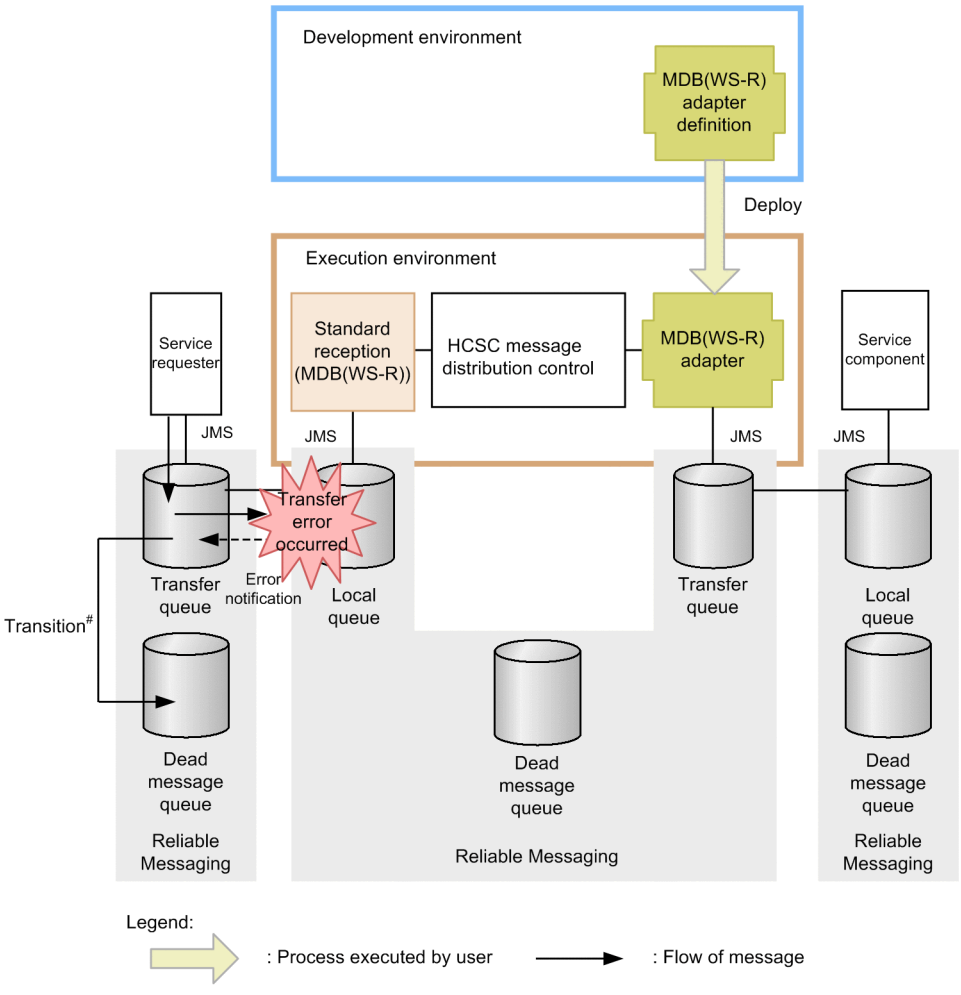
For details on setup of Reliable Messaging, see "*3.1.2 Setting up the software required for the execution environment*".

For details on Reliable Messaging, see "Reliable Messaging".

When an error occurs in the transfer between the service requester machine and the HCSC server machine.

The following figure shows the method of notifying an error in MDB (WS-R) when an error occurs in the transfer between the service requester machine and the HCSC server machine:

Figure 7–58: Figure Method of notifying an error in MDB (WS-R) when an error occurs in the transfer between the service requester machine and the HCSC server machine



Transits when reached the maximum value of distribution count or reached the validity period.

When message transfer between the service requester machine and the HCSC server machine fails, error processing is performed in Reliable Messaging at the service requester end. Reliable Messaging outputs a message indicating the failure in message transfer to a log on the service requester machine.

Furthermore, when an error is detected in message transfer, perform rollback at the service requester end and try to transfer the message one more time.

When you perform rollback in transfer from the service requester machine and frequency of rollback (frequency of message delivery) reaches the maximum value or when message reaches to its expiry date, that message moves to the dead message queue. However, the message is deleted in following cases:

- When settings for the dead message queue are not performed.

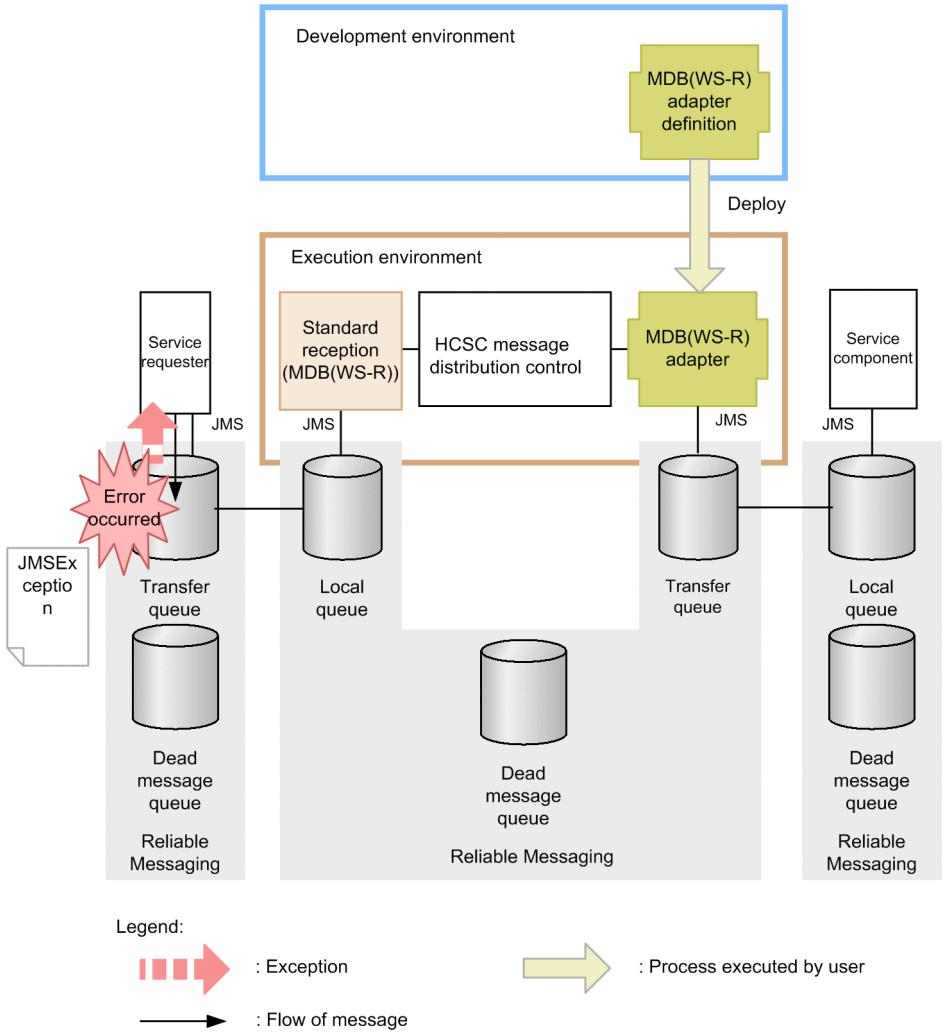
- When "Unlimited" is set in delivery frequency
- When number of messages in the dead message queue are in excess.
- When failure occurs in database.

For details on the operations performed when transfer between Reliable Messaging queues fails, see "2.4.7 Operation when failure occurs in transfer between queues" in "Reliable Messaging".

When an error is detected in the service requester

The following figure shows the method of notifying an error in MDB (WS-R) when an error is detected in the service requester:

Figure 7–59: Figure Method of notifying an error in MDB (WS-R) when an error is detected in the service requester

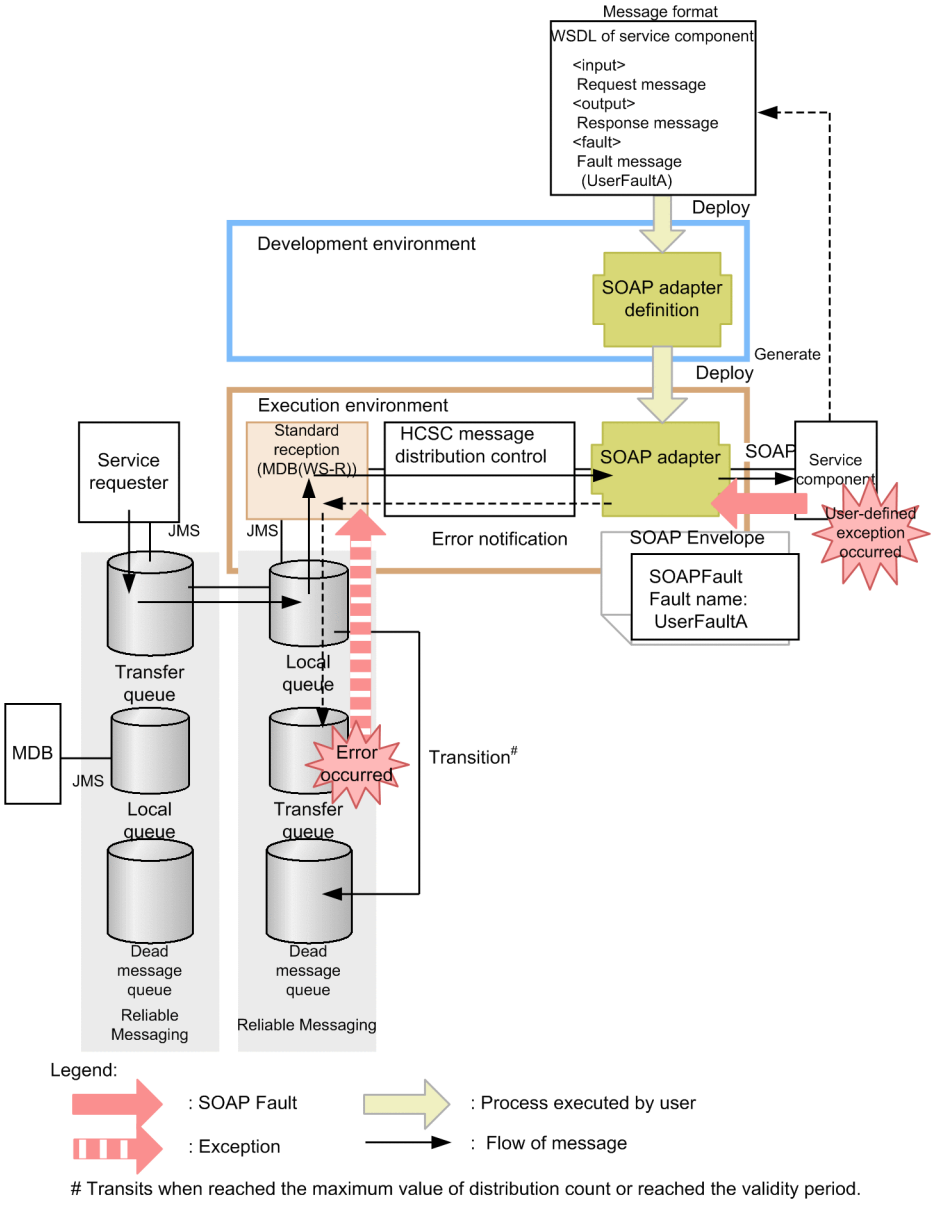


When you cannot send a message from the service requester to the transfer queue, exception (JMSException) is thrown to the service requester. The service requester catches the exception. You can acquire details of the error by using getter of the caught exception object. When message sending from service requester machine fails, message does not move to the dead message queue. For details on Reliable Messaging and JMS, see"Reliable Messaging" .

When the synchronous service component is invoked and an error of the user-defined exception occurs

The following figure shows the method of notifying an error in MDB (WS-R) when the synchronous service component is invoked, and an error of the user-defined exception occurs:

Figure 7–60: Figure Method of notifying error in MDB (WS-R) when the synchronous service component is invoked and an error of the user-defined exception occurs



Specify a queue for response when the service component is invoked for asynchronous standard reception (MDB (WS-R). The service component of synchronous SOAP adapter is invoked from asynchronous (MDB (WS-R). If a user-defined exception occurs at the service component end, the message of error information is sent to the queue for response (Transfer queue).

If you specify the destination of the transfer queue in the local queue at the service requester end, you can acquire contents of error by fetching the message from the destination of the transfer queue.

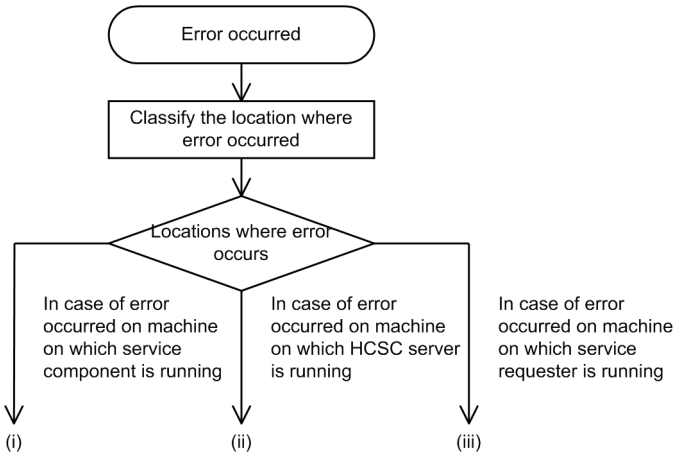
You must create a queue (Transfer queue) for response beforehand, but when there are no settings of the queue for sending a response, or when the number of messages in queue for response are in excess and sending to the queue fails, rollback the process within the HCSC server and message is resent from the local queue of standard reception (Rollback is not performed for process (Transaction) at the service component end).

When frequency of rollback (frequency of message delivery) reaches the maximum value that message moves to the dead message queue. When the dead message queue name is not set or when the dead message queue is not created, the process of invoking the service component is re-executed without any limit. Therefore, you must set the dead message queue name or the dead message queue.

(2) Method of determining a problem area

This section describes method of determining the problem area when the service component is invoked using standard reception (MDB (WS-R) from the service requester. The following figure shows the method of determining the problem area:

Figure 7–61: Figure Method of determining a problem area (when the service component is invoked)



When an error occurs in the service component machine

Investigate the failure by referencing the failure information output by Reliable Messaging at the service component machine end. Reference the user log of the J2EE server when error information is output to service component program.

Investigate the cause from the following perspective:

- User message requested from the service requester
- Service component machine
- Settings of Reliable Messaging of service component
- Service component program

(ii) When an error occurs in the HCSC server machine

Investigate the fault by referencing the failure information output by Reliable Messaging and message log at the HCSC server machine end.

Investigate the cause from the following perspective:

- Contents of argument requested from the service requester
- Settings and status of HCSC server
- Settings of Realizable Messaging of HCSC server
- Definition contents of service adapter
- Definition contents of business process
- User message requested from the service requester
- Status of network

(iii) When an error occurs in the service requester machine

You can acquire contents of error from exception caught by the service requester. Take action on the basis of the error information of acquired exception. Investigate the fault by referencing the error information output by Reliable Messaging at the service requester machine end.

Investigate the cause from the following perspective:

- Settings and status of J2EE container of the service requester
- Settings of Reliable Messaging of the service requester machine
- Status of network

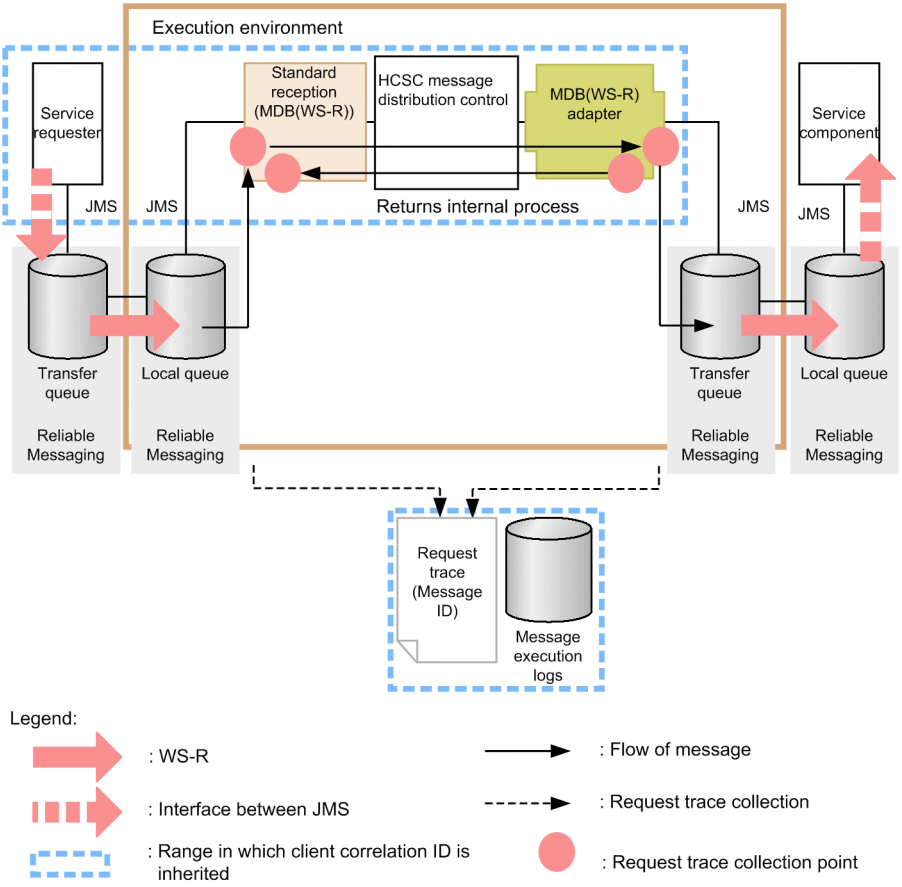
(3) Method of identifying other causes of failure (tracking execution history of the invocation request of service component)

You can track the progress of the service component invocation process on the basis of information identified from the service requester and information from the HCSC server. The information (ID) necessary to track execution history is described here.

(a) Client correlation ID

The client correlation ID is the information set in the program at the service requester end which requests the invocation of service component at the time of request. This ID is used to support request message from the service requester, logs and traces managed in HCSC server. Therefore, it is recommended to specify a different ID for each request sent to HCSC server. Specify the ID at the time of the service requester development. The following figure shows range inherited by the client correlation ID:

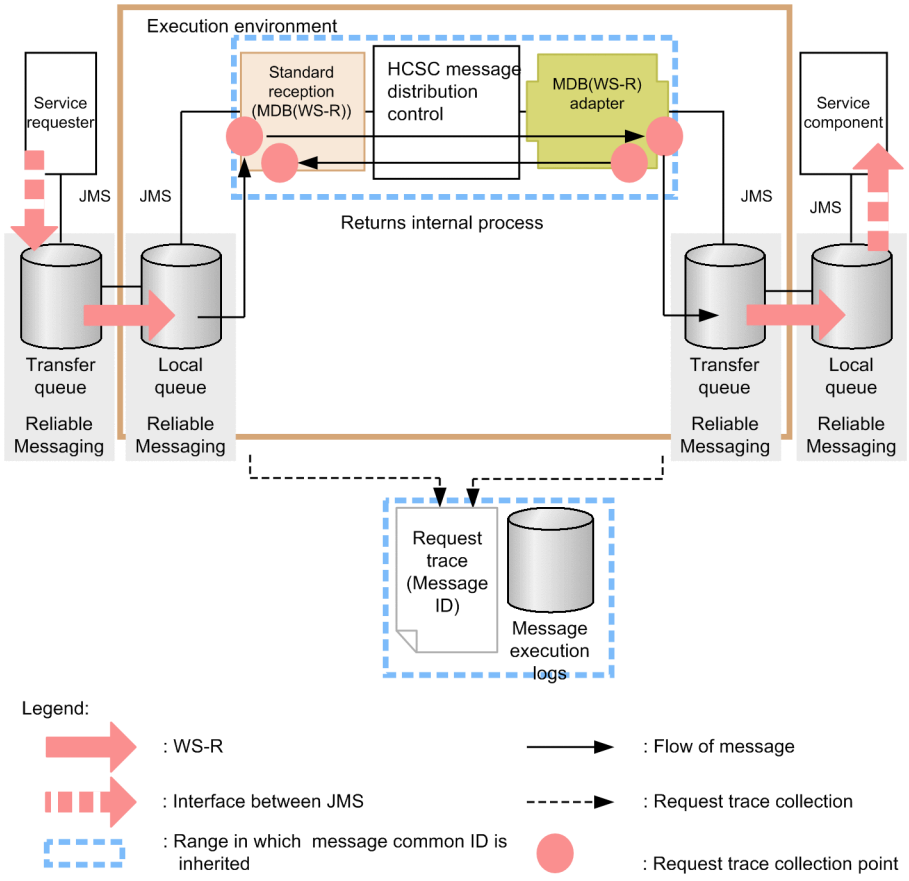
Figure 7–62: Figure Range inherited by the client correlation ID (MDB (when executing WS-R))



(b) Common message ID

This ID is assigned by the HCSC server. This ID is used to identify logs and traces within HCSC server. The following figure shows range inherited by the common message ID:

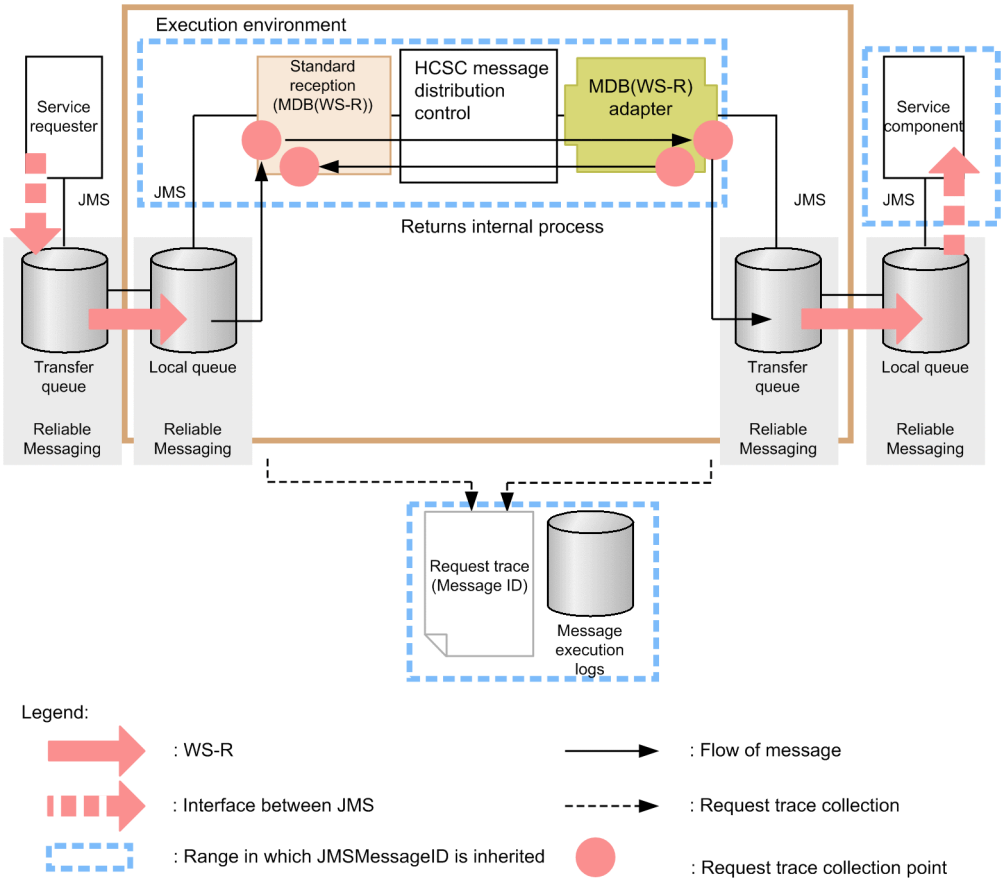
Figure 7–63: Figure Range inherited by the common message ID (when executing MDB (WS-R))



(c) JMS Message ID

This ID is assigned by Reliable Messaging. This ID is output to logs or traces within HCSC server. The following figure shows the range inherited by the JMSMessageID:

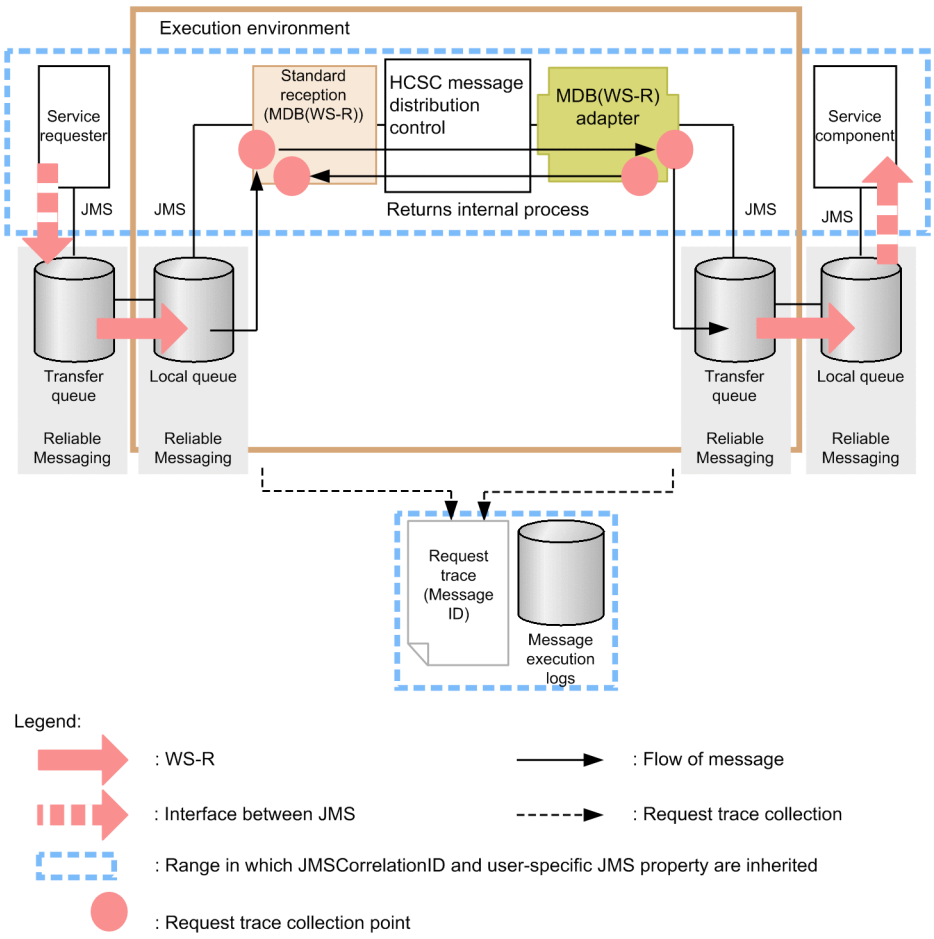
Figure 7–64: Figure Range inherited by the JMSMessageID (when executing MDB (WS-R))



(d) User specific JMSCorrelationID and JMS property

At the time of service component invocation request, if you set user specific JMSCorrelationID and JMS property in the service requester, that value is inherited to queue at the service component end. Messages are linked uniquely by acquiring them in program at the service component side. The following figure shows the range inherited by the JMSCorrelationID and user-specific JMS property:

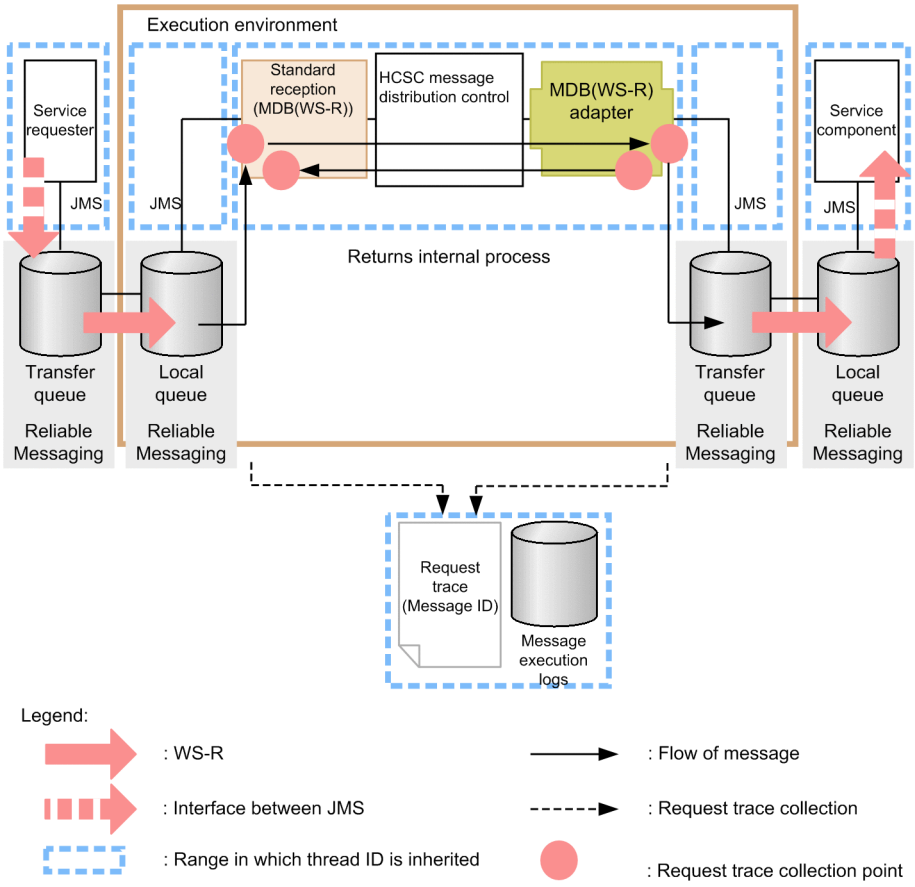
Figure 7–65: Figure Range inherited by JMSCorrelationID and user specific JMS property (when executing MDB (WS-R))



(e) Thread ID

Thread ID is an ID assigned to each thread processed using J2EE container. The following figure shows the range inherited by thread ID

Figure 7–66: Figure Range inherited by thread ID (when executing MDB (WS-R))



7.7.4 Troubleshooting when executing MDB (DB queue)

(1) Method of notifying an error in MDB (DB queue)

In the service component invocation of MDB (WS-R), the error which occurs between the service requester and the HCSC server, and the HCSC server and the service component is not notified. The types of failure that can be detected, output destination of logs and traces is described here.

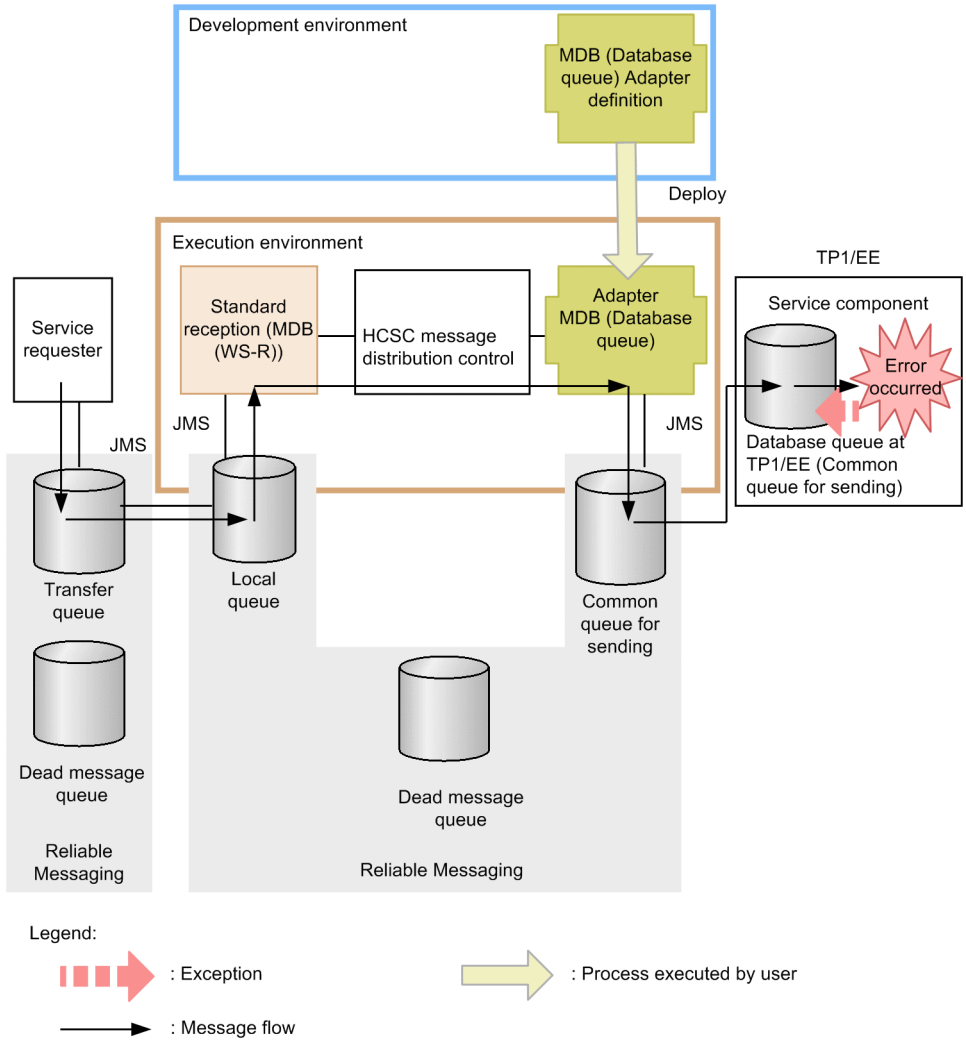
Note that, the service component cannot be invoked from asynchronous standard reception (MDB (DB queue) to the (MDB (DB queue) adapter. Therefore, a separate description is provided for the service component end for DB queue and the service requester end for DB queue.

(a) When DB queue exists at the service component end

When error occurs in service component

The error which has occurred at the service component is not notified to the HCSC server and the service requester as error information. Error information is output at the service component machine end. The following figure shows the method of notifying an error when error occurs in service component:

Figure 7–67: Figure Method of notifying an error when an error occurs in the service component

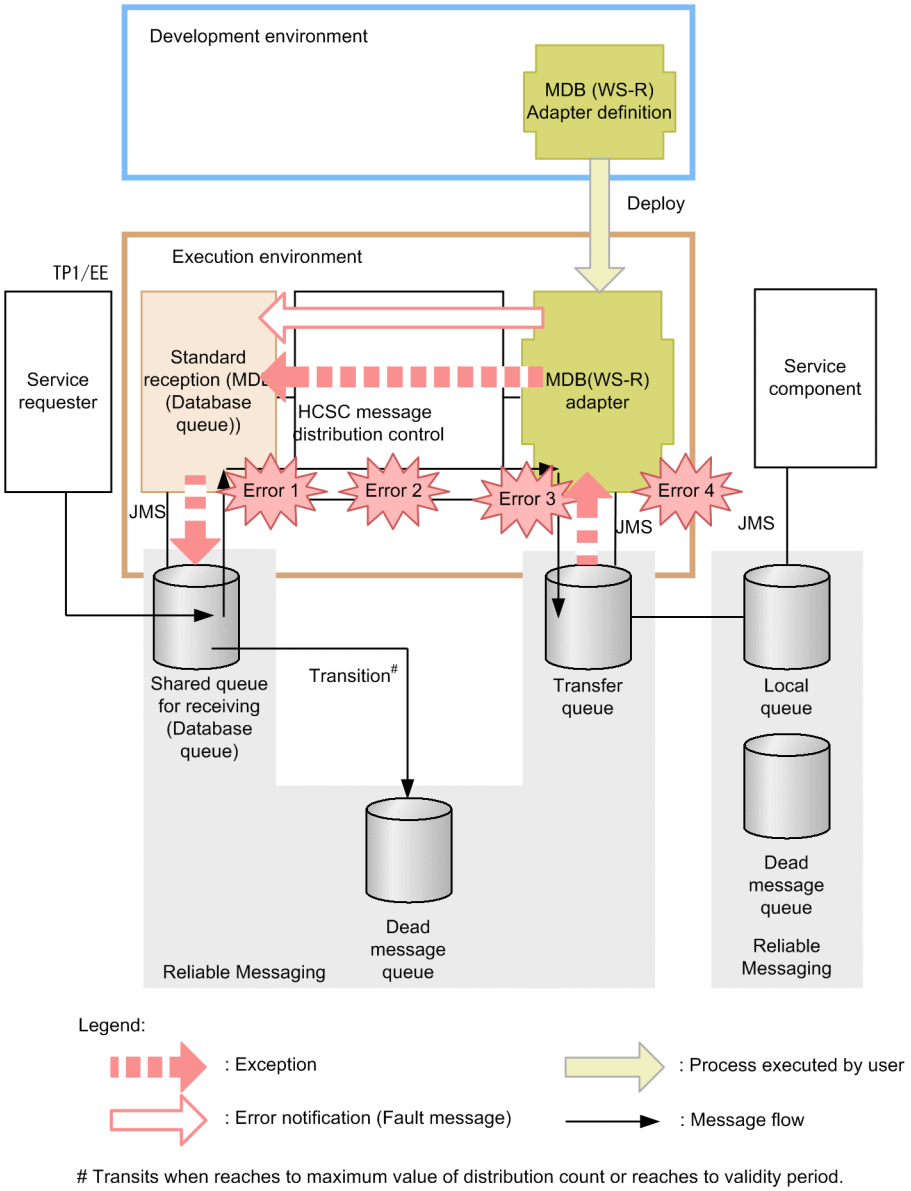


(b) When DB queue exists at the service requester end

When an error occurs from the HCSC server

The following figure shows the method of notifying an error when an error occurs from the HCSC server:

Figure 7–68: Figure Method of notifying an error when an error occurs from the HCSC server



Transits when reaches to maximum value of distribution count or reaches to validity period.

The errors shown in figure 7-68 are as follows:

- Error 1: Invalid request parameter
- Error 2: Address (Location) not found, service adapter has stopped
- Error 3: Data transformation failed
- Error 4: Message sending failed

When any of Error 1~Error3 shown in the figure are detected in HCSC server, the error is notified to Reliable messaging on the HCSC server machine.

When Error 4 shown in figure is detected, you can select whether to notify an error to Reliable Messaging on the HCSC server machine or to transform the exception of error into a fault message in the service adapter. For details on how to select an error acquired when an exception occurs, see "7.11 Selecting the errors to be acquired when an exception occurs".

Messages of an error are output to the message log. Reliable Messaging outputs a message indicating the failure in message fetching from the local queue to a log on the HCSC server machine.

When an error is detected in the HCSC server, perform rollback at HCSC server end and again try fetching a message in the service component (invocation of service component).

When you perform rollback in message fetching on the HCSC server machine and frequency of rollback (frequency of message delivery) reaches the maximum value, that message moves to the dead message queue. When the dead message queue name is not set or when the dead message queue is not created, process of invoking the service component is re-executed without any limit. Therefore set the dead message queue name or when the dead message queue without fail.

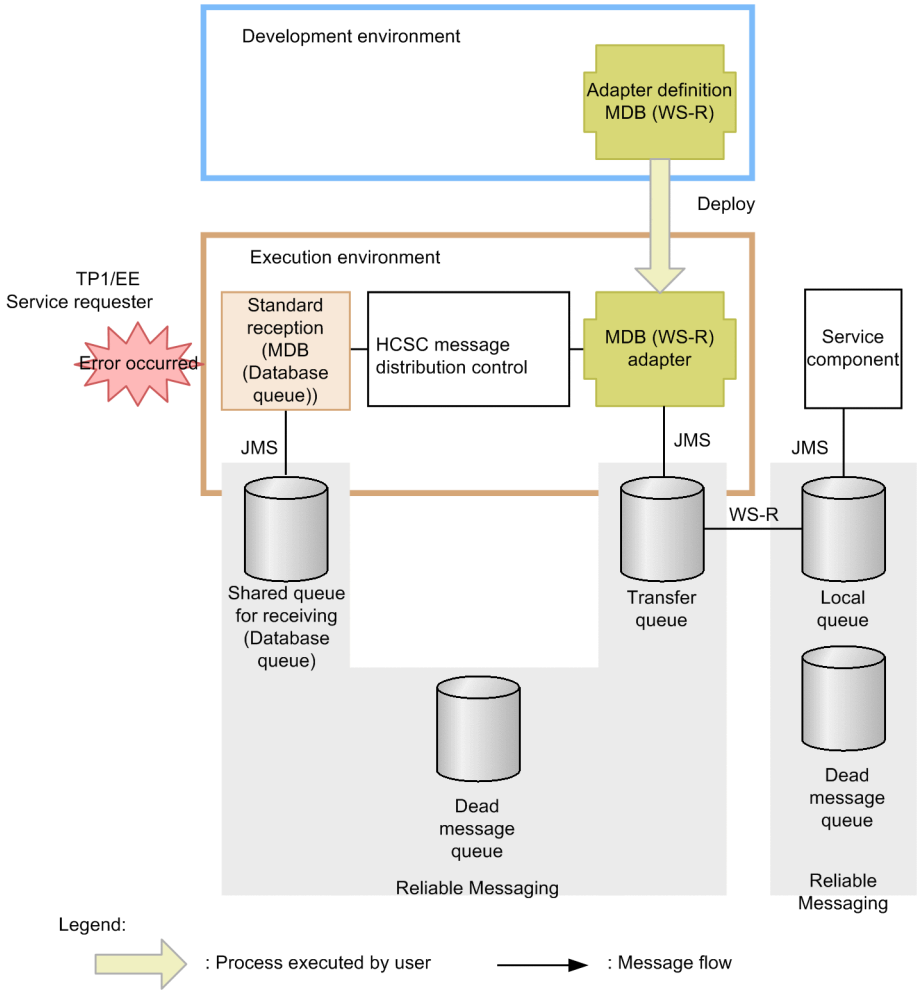
Further, when the frequency of process re-execution specified in request-jms.rollback-count property of the HCSC server runtime definition file is exceeded, warning message (KDEC00049-W) is output.

For details on setup of Reliable Messaging, see "3.1.2 Setting up the software required for the execution environment". For details on Reliable Messaging, see"Reliable Messaging".

When error is detected in the service requester

The following figure shows the method of notifying an error when an error is detected in the service requester:

Figure 7–69: Figure Method of notifying an error when an error is detected in the service requester

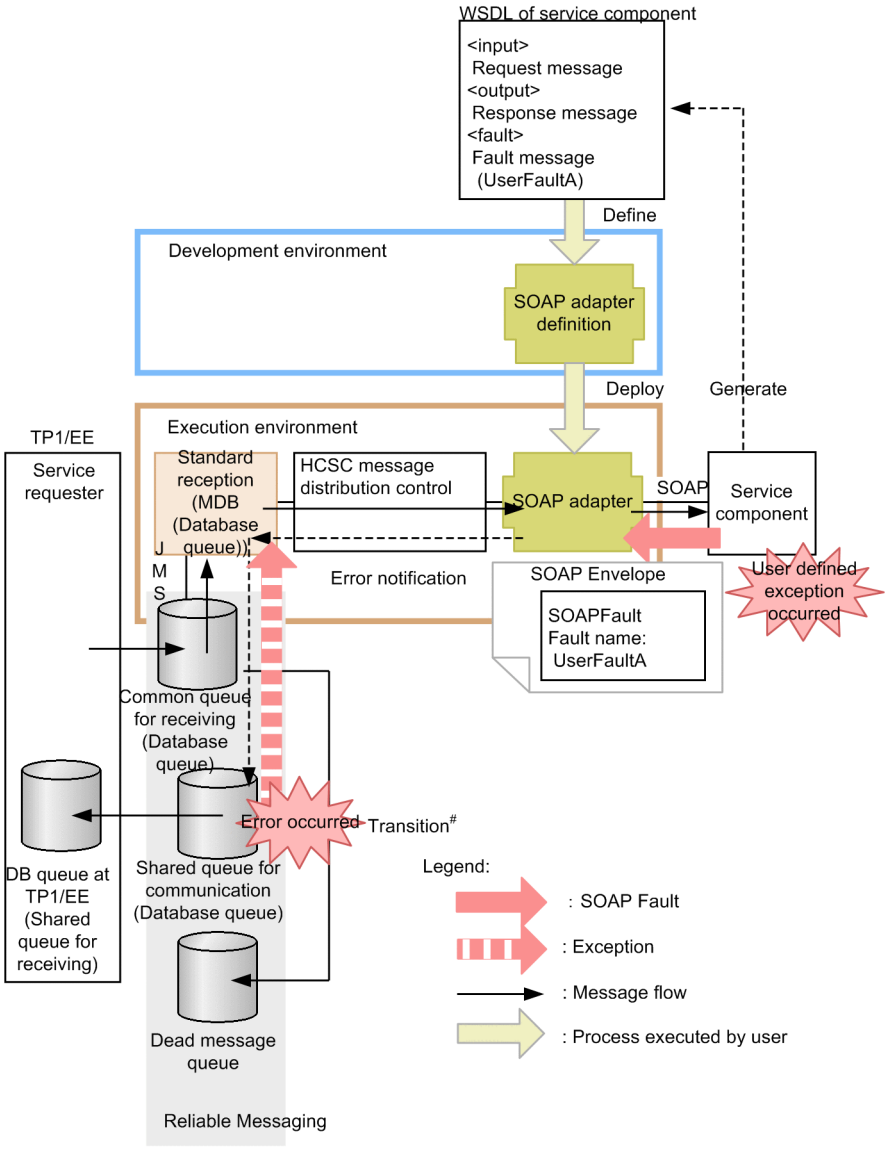


The error occurs when the service requester performs queuing of messages in DB queue is output at the service requester machine end.

When synchronous service component is invoked and error of user-defined exception occurs

The following figure shows the method of notifying an error when synchronous service component is invoked and error of user-defined exception occurs:

Figure 7–70: Figure Method of notifying an error when synchronous service component is invoked and error of user-defined exception occurs.



#
Transits when reaches to maximum value of distribution count or reaches to validity period.

Specify queue for response when the service component is invoked for standard reception of asynchronous (MDB (DB queue), the service component of synchronous SOAP adapter is invoked from standard reception of asynchronous (MDB (DB queue). If user-defined exception occurs at the service component end, message of error information is sent to queue for response (Common queue for sending). If you specify destination of common queue for sending in DB queue at the service requester end, you can acquire contents of error by fetching message from there.

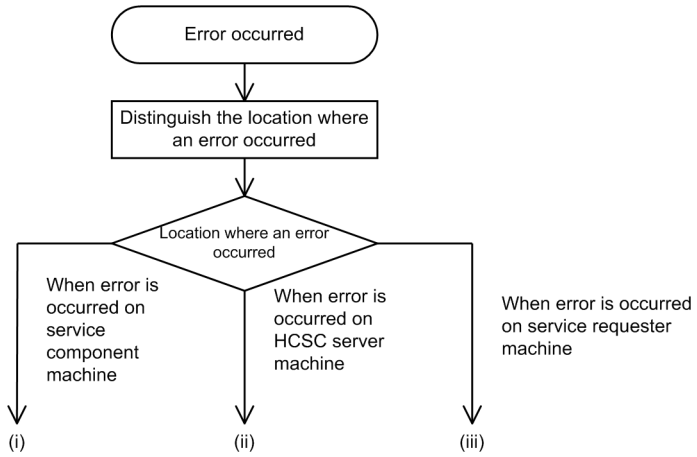
You must create queue for response (Common queue for sending) in advance but, when settings of queue for response are not performed or when number of messages in queue for response is in excess and sending to queue fails, perform rollback for process within the HCSC server and messages are resent from common queue for receiving standard reception. (However, rollback is not performed for process at the service component end (Transaction)).

When frequency of rollback (frequency of message delivery) reaches the maximum value, that message moves to the dead message queue. When the dead message queue name is not set or when the dead message queue is not created, process of invoking the service component is re-executed without any limit. Therefore you must set the dead message queue name or the dead message queue.

(2) Method of determining the problem area

This section describes method of determining the problem area when the service component is invoked using standard reception (MDB (DB queue)) from the service requester. The following figure shows flow of determining problem area:

Figure 7–71: Figure Flow of determining problem area (When the service component is invoked using standard reception (MDB (WS-R)) from the service requester)



When an error occurs in the service component machine

Investigate the cause of failure from failure information which is output to the service component machine end.

Investigate the cause from the following perspective:

- User message requested from the service requester
- Status of the service component machine
- Settings of the service component machine
- Service component program

(ii) When an error occurs in the HCSC server machine

Investigate the cause of failure by referencing the failure information output by message logs and Reliable Messaging at the HCSC server machine end.

Investigate the cause from the following perspective:

- Contents of binary data requested from the service requester
- Format of binary data requested from the service requester
- Settings and status of the HCSC server
- Settings of Reliable Messaging of the HCSC server
- Definition contents of service adapter
- Definition contents of business process
- User message requested from the service requester
- Status of network

(iii) When an error occurs in the service requester machine

Investigate the cause of failure from failure information output to the service requester machine end.

Investigate the cause from the following perspective:

- User message requested from the service requester
- Status of the service requester machine
- Settings of the service requester machine
- The service requester program

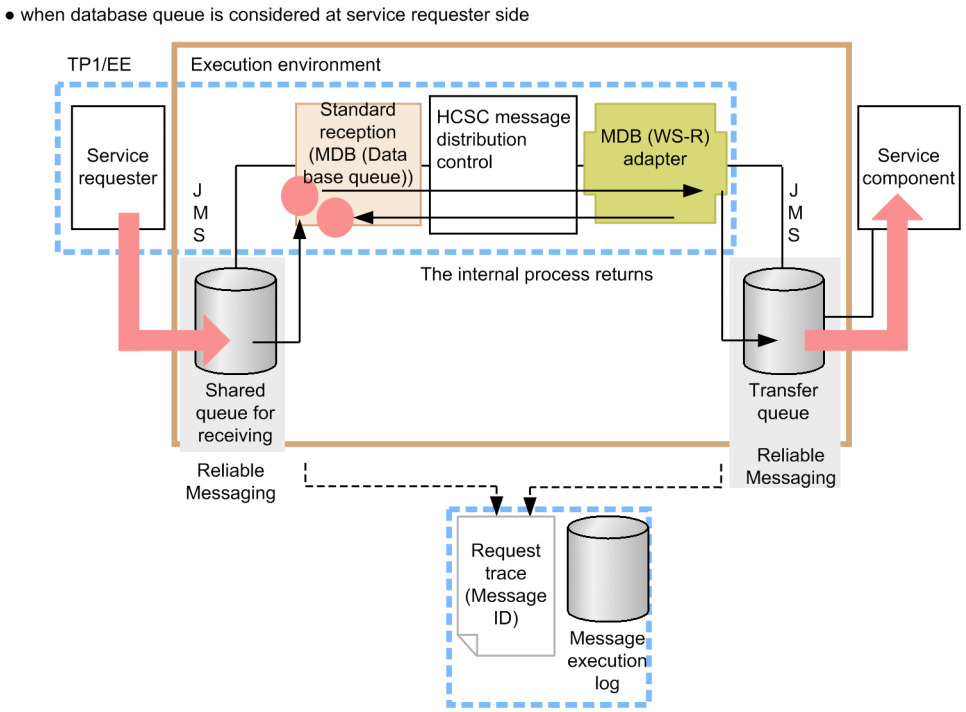
(3) Method of identifying other causes of failure (tracking execution history of the service component invocation request)

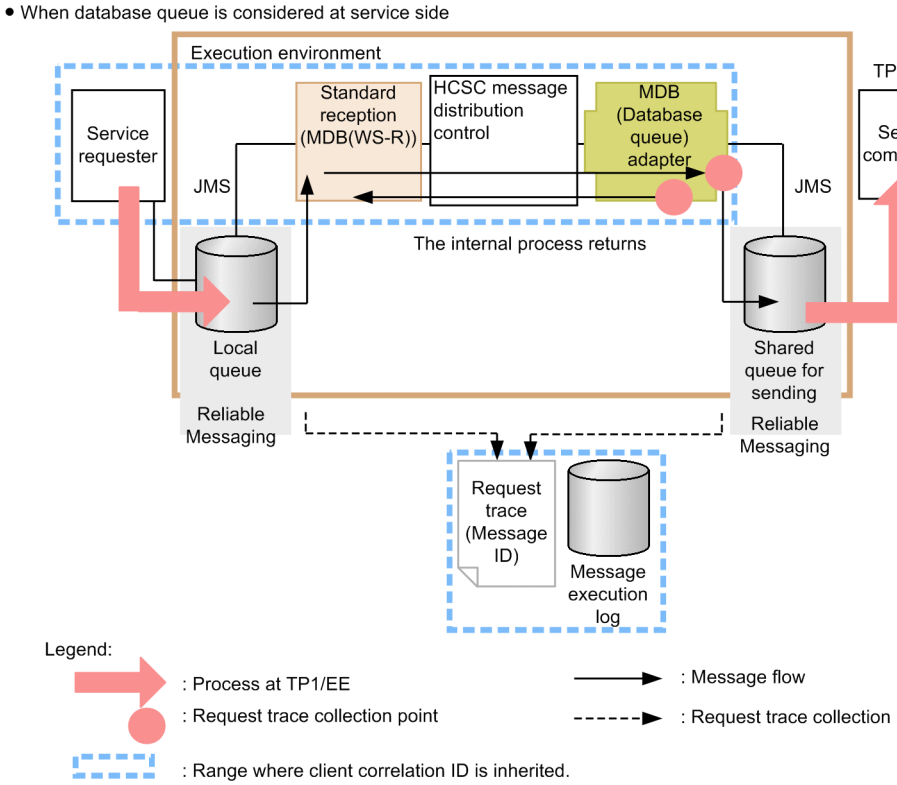
You can track the progress of the service component invocation process on the basis of information specified from the service requester or information from the HCSC server. The information (ID) necessary for tracking execution history is described here.

(a) Client correlation ID

The client correlation ID is information set in program at the service requester end which performs the invocation request of service component at the time of request. This ID is used to support request message from the service requester and logs and traces managed in the HCSC server. Therefore, it is recommended to specify different ID for each request sent to the HCSC server. (You must specify the ID when creating the service requester). The following figure shows range inherited by the client correlation ID:

Figure 7–72: Figure Range inherited by client correlation ID (When executing MDB (DB queue))

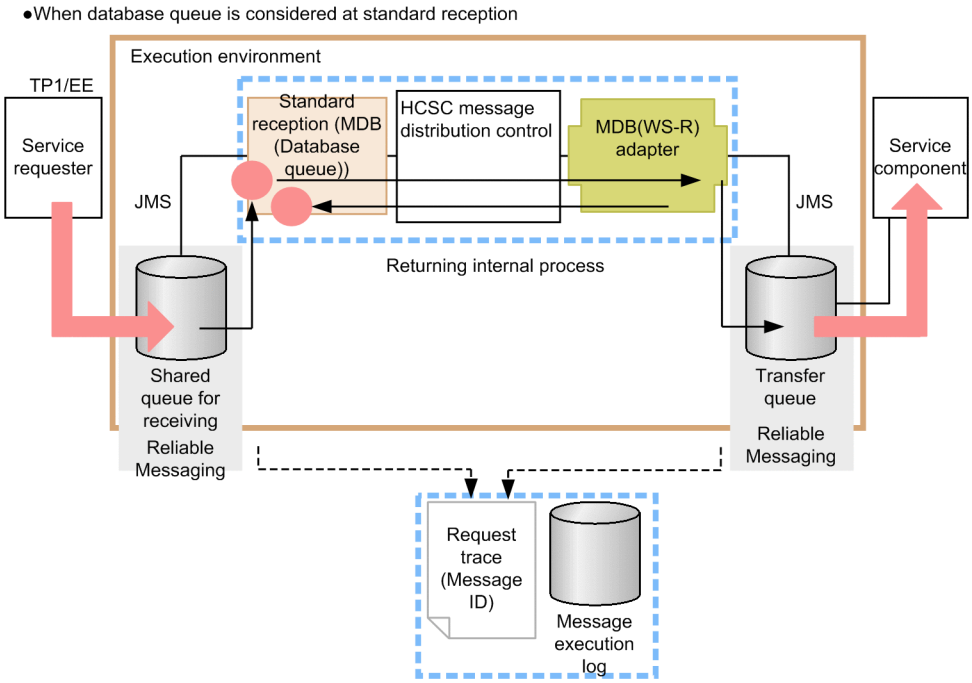


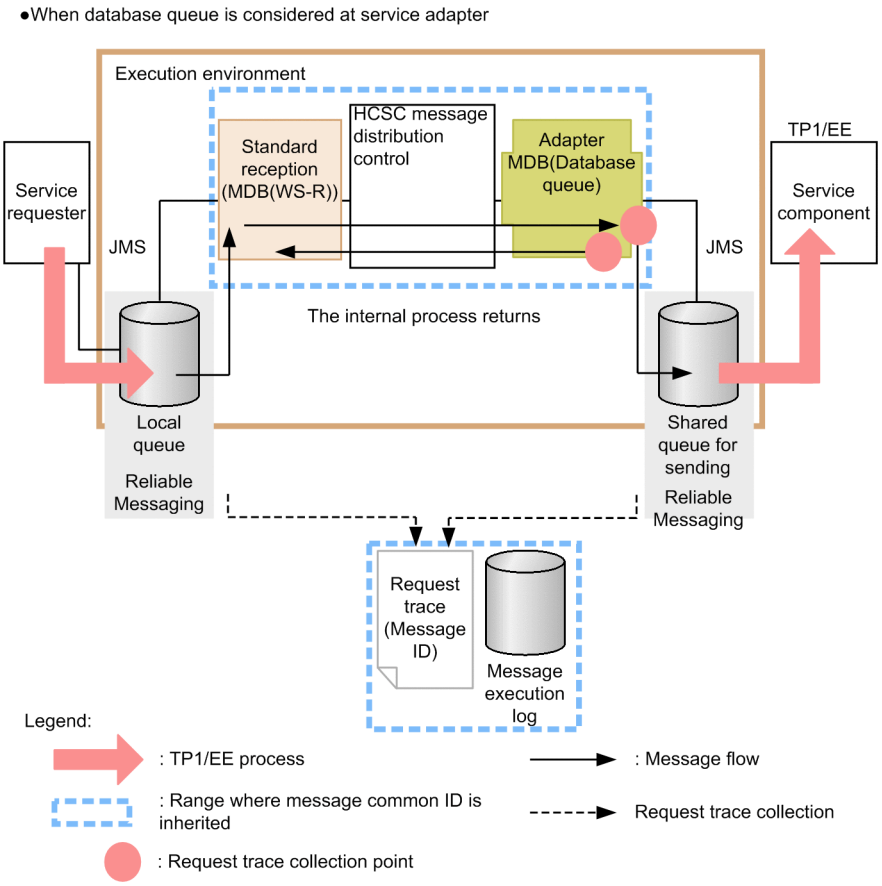


(b) Common message ID

This ID is assigned by HCSC server. This ID is used to identify logs or traces within HCSC server. The following figure shows range inherited by the common message ID:

Figure 7–73: Figure Range inherited by the common message ID (When executing MDB (DB queue))

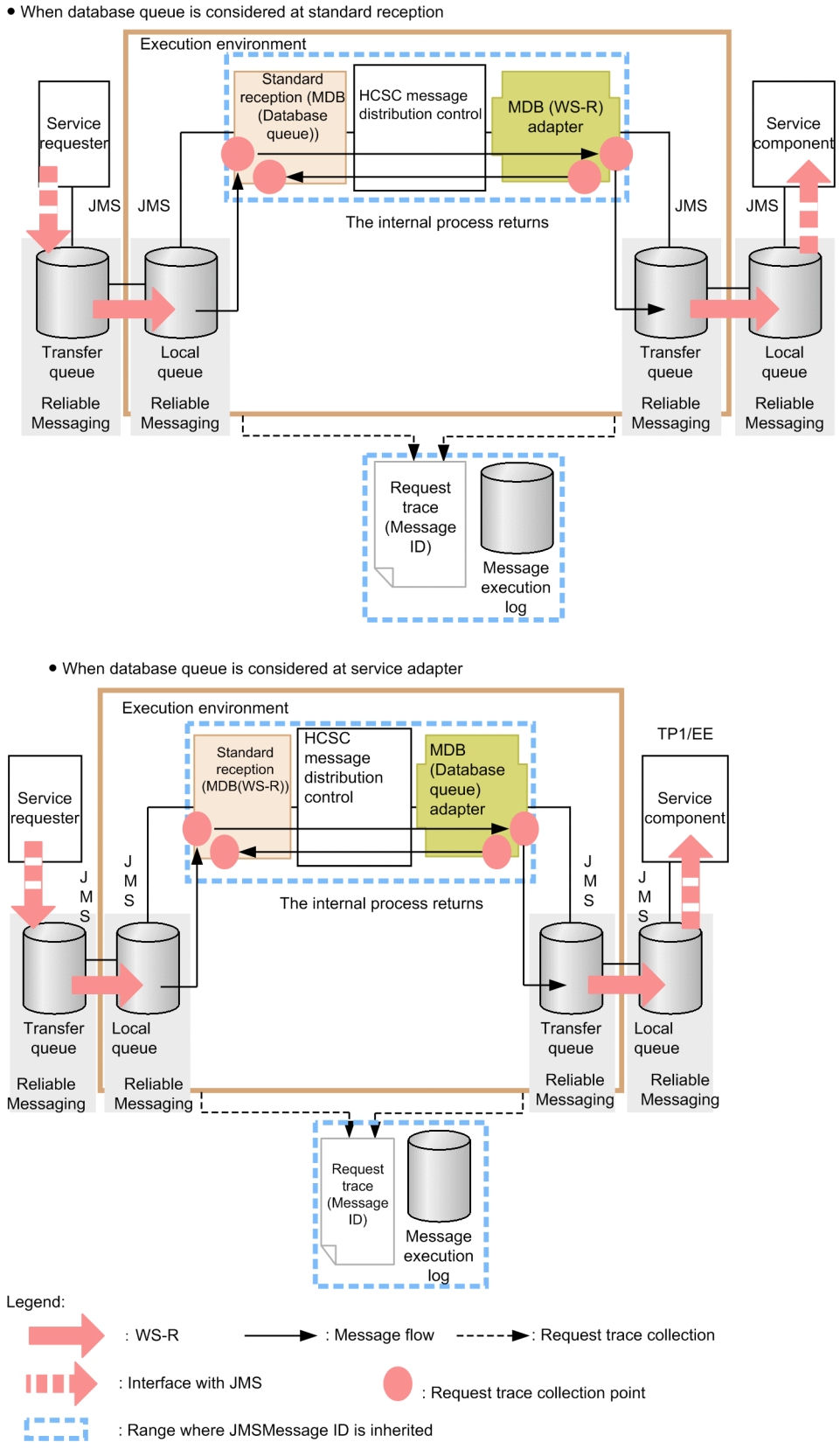




(c) JMSMessageID

JMSMessageID is assigned by Reliable Messaging. This ID is output to logs or traces within HCSC server. The following figure shows range inherited by JMSMessageID:

Figure 7–74: Figure Range inherited by JMSMessageID (When executing MDB (DB queue))

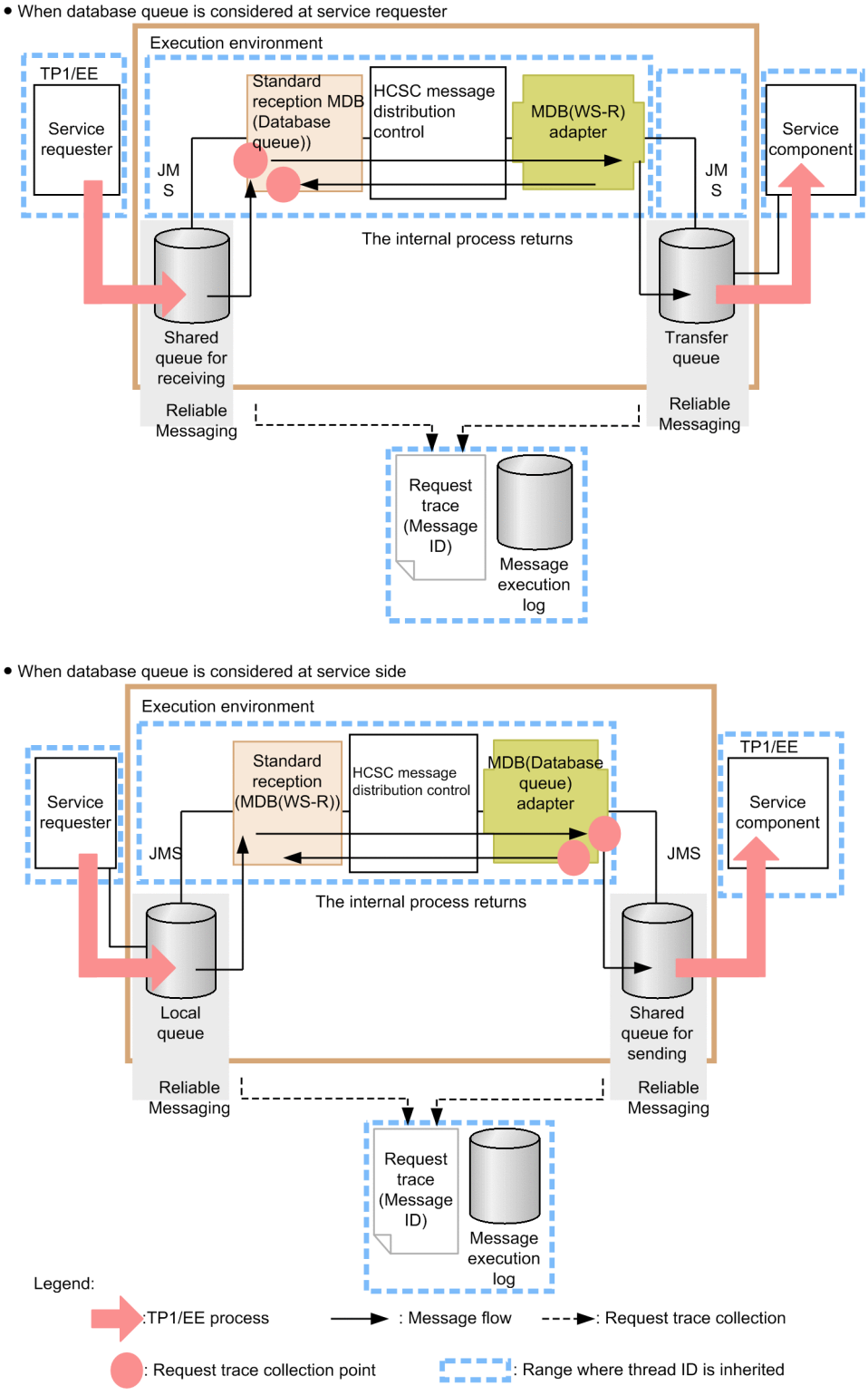


JMSCorrelationID or user specific information of property is not inherited.

(d) Thread ID

Thread ID is an ID assigned to each thread processed using J2EE container. The following figure shows range inherited by thread ID:

Figure 7–75: Figure Range inherited by thread ID (When executing MDB (DB queue))



#

You must embed information to link to user message when linking to program at the service component end.

7.7.5 INTENTIONALLY DELETED

INTENTIONALLY DELETED

7.7.6 INTENTIONALLY DELETED

INTENTIONALLY DELETED

7.7.7 Troubleshooting when executing file adapter

When failure occurs in the file adapter, information necessary for troubleshooting is output to log file and trace file. The following table lists type of logs and traces that you can acquire in the file adapter:

Table 7–58: Table Type of logs/traces (For file adapter)

Log/trace	Output information	Description
Message log	Each type of information in file adapter is output as message.	You can check operation information (Start/Stop/ Error) as message. You can check operational status of system in batch since the output destination of the message log is common for entire Application Server and Service Platform.
Method trace	The following information is output when you start or end an internal method of the file adapter: • Date • Time • Execution class name • Internal method name • Exception occurred • Information of specified argument	You can check the publication time and sequence of internal method.
Performance analysis trace (PRF trace)	The following information is output to the performance analysis trace collection point of the entire Application Server and Service Platform: • Date • Time • Request information • Trace collection source information The file adapter specific information is output in performance analysis trace collection point of file adapter.	You can validate the performance of Service Platform system on the basis of the performance analysis information output in the series of process starting from when you receive request from the service requester till the execution result is returned.

For details on points to be considered while outputting logs and traces, see ", *7.3.4(1) General notes*".

You can acquire the log and the trace of file adapter using the troubleshooting functionality of Application Server. The methods for acquiring logs and traces are as follows:

- Use the management command (mngsvrutil).
- For details, see "Application Server Command Reference Guide ".
- Using the management portal
  For details, see "Application Server Management Portal User Guide".
- Using the snapshotlog command

For details, see "Application Server Command Reference Guide ".

- Using the cprf command (Performance analysis trace only)
  For details, see "Application Server Command Reference Guide ".

Furthermore, if you acquire trace of HCSC server, troubleshooting of the entire Application Server becomes easy. The following table describes trace information that you can acquire in HCSC server. For details, see contents regarding collection of failure information in "Application Server Maintenance and Migration Guide".

Table 7–59: Trace information that you can acquire in HCSC server

Trace functionality	Description
Request trace	You can acquire information necessary to hold business process of requests received in standard reception, business process reception, or transfer reception between servers on messaging board, invocation destination of service adapter or its result.
Method trace	You can acquire method trace information provided by HCSC server.
Performance analysis trace	You can acquire information to analyze performance bottleneck of entire Application Server which includes J2EE application and entire Service Platform System

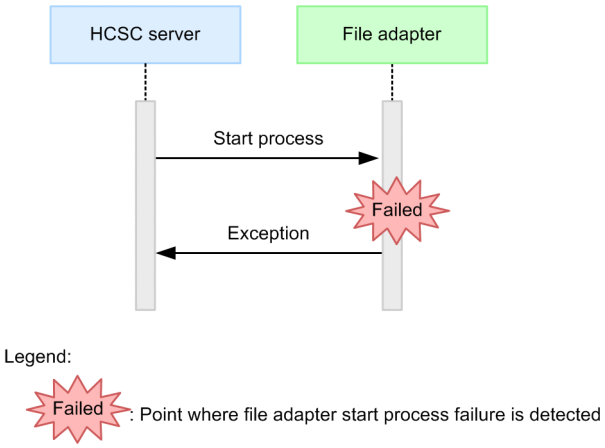
(1) Failure handling

When failure occurs in file adapter, exception is notified for the HCSC server excluding failure in stop process.

(a) Failure in start process

When start process of the file adapter fails, exception is notified to the HCSC server and process ends. Cause of failure in start process can be failure in analyzing file adapter execution environment property file.

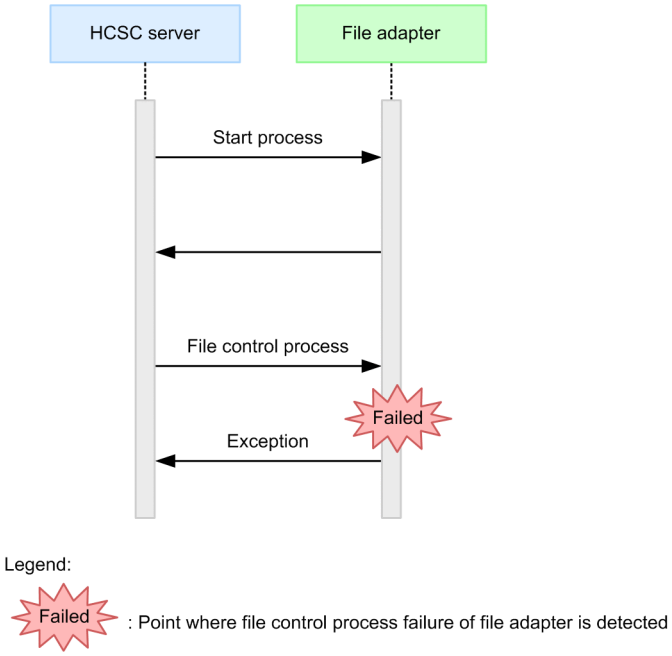
Figure 7–76: Figure Failure in start process



(b) Failure in file control process

When failure in file control process of file adapter is detected, exception is notified to the HCSC server and process ends.

Figure 7–77: Figure Failure in file control process



(c) Failure in stop process

When failure in stop process of file adapter is detected, stop process is continued till process ends. Exception is not notified for HCSC server. However, when an unexpected failure occurs, in some cases exception is notified.

(2) Message log

You can acquire information of start and stop of service and error information at the time of failure as message log, you can detect occurrence of failure and analyze cause of failure.

(a) Output destination

Output destination of the message log is as follows:

```
Path specified in output destination of J2EE server operation log
```

Specify the output destination of J2EE server operation log in the ejb.server.log.directory key of option definition file (usrconf.cfg) for the J2EE server on which the HCSC server is running. For details, see "2.4 usrconf.properties (User property file for J2EE server)" in "Application Server Definition Reference Guide".The following table lists log file name of message log:

Table 7–60: Table Log file name of message log

Output mode of log file	Log file name
For wraparound mode	cjmessage<Count>.log#
For shift mode	cjmessage.log#

#

Log file is common across entire Application Server and Service Platform. Message log of operational information and failure information of all the products on The HCSC server is to be output.

(b) Number of files

Specify the count of output files in the ejbserver.logger.channels.define.<Channel name>.filenum key of the user property file(usrconf.properties) for J2EE server on which the HCSC server is running. For details, see "2.4 usrconf.properties (User property file for J2EE server) " in "Application Server Definition Reference Guide".

(c) File size

Specify the output file size in the ejbserver.logger.channels.define.<channel name>.filesize key of the user property file (usrconf.properties) for J2EE server on which the HCSC server is running. For details, see "2.4 usrconf.properties (User property file for J2EE server) " in "Application Server Definition Reference Guide

(3) Method trace

You can validate the time and sequence of the internal method publication. Maintainance service uses method trace to analyze failure.

(a) Output destination

Output destination of method trace is as follows:

```
<Path specified in output destination of activity log of J2EE server>\CSCADP
\FFADP\maintenance\<Service adapter name>
```

Specify the output destination of J2EE server operation log in the ejb.server.log.directory key of the option definition file (usrconf.cfg) for J2EE server on which the HCSC server is running. For details, see "2.3 usrconf.cfg (Option definition file for J2EE server) " in "Application Server Definition Reference Guide".

The following table describes the trace file name of method trace.

Table 7–61: Table Trace file name of method trace

Output mode of trace file name	Trace file name
For wraparound mode	mtdtrace<Count>.log
For shift mode	mtdtrace.log

(b) Number of files

The default number of output files is 4. You can change number of output files using the methodtracefile.num key of file adapter execution environment property file.

For details on how to change, see description for creating the file adapter execution environment property file in "3.3.7 Defining file adapters " in "Service Platform Reception and Adapter Definition Guide".

(c) File size

The default size of the output file is 4MB. You can change the size of the output file with methodtracefile.size of file adapter execution environment property file.

For details on how to change, see description for creating the file adapter execution environment property file of "3.3.7 Defining file adapters " in "Service Platform Reception and Adapter Definition Guide".

(4) Performance analysis trace (PRF trace)

You can validate the performance of Application Server and Service Platform system on the basis of the performance analysis information output in the series of processes starting from when you receive a request from the service requester till the execution result is returned. File adapter specific information is output in performance analysis trace collection point of file adapter. Maintainance Service uses the information to analyze performance bottlenecks.

(a) Output destination

The following table describes the output destination of performance analysis trace and trace file name.

Table 7–62: Table Output destination of performance analysis trace and trace file name

Output destination path of trace	Trace file name
<Setting directory of environment variable PRFSPOOL>\utt\prf\<PRF Identifier>\dcopltrc#	prf_<n>

Legend:

N: Enter integar from 001 to maximum value of number of files.

Note#

The output destination of performance analysis trace is common for entire Application Server and Service Platform. For details, see "7.3 Collecting performance analysis trace file where Management Server is used " in "Application Server Maintenance and Migration Guide".

(b) Number of files

The default number of output files is 4. You can change the number of output files with the management portal or cprf command. For details on the management portal , see "Application Server Management Portal User Guide", For details on the cprf command, see "Application Server Command Reference Guide".

(c) File size

When file size is set in the management portal, the default file size is 32MB. When file size is set with the cprf command, the default file size is 8MB. You can change file size with the management portal of cprf command. For details on the management portal, see "Application Server Management Portal User Guide ", For details on the cprf command, see "Application Server Command Reference Guide".

(d) Output format

The format which is output to the performance analysis trace is same as the performance analysis trace of J2EE server. For details, see "7.3 Collecting performance analysis trace file where Management Server is used" in "Application Server Maintenance and Migration Guide".

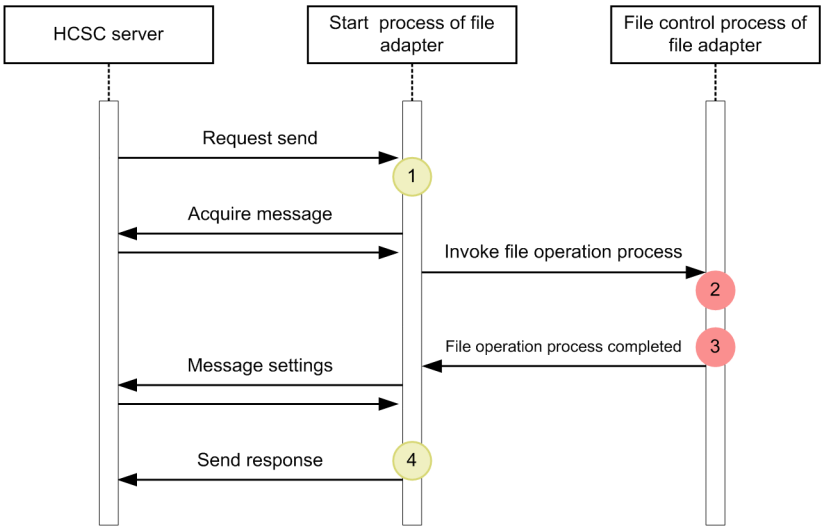
(e) Performance analysis trace collection point

In the performance analysis trace collection point of the file adapter, file adapter specific information is output.

●Overview

The following figure shows the performance analysis trace collection point of the file adapter:

Figure 7–78: Figure Performance analysis trace collection point of the file adapter



Legend:

: Trace collection point (Performance analysis trace collection level is "Standard")

: Trace collection point (Performance analysis trace collection level is "Detailed")

A point specific event ID is assigned in collection point of the performance analysis trace. Trace event ID output to file adapter is 0xA000~0xA0FF. The following table describes event ID, trace collection point, and performance analysis trace collection level. "Numbers in the figure" in the table correspond to numbers in "*Figure7-75 Performance analysis trace collection point of file adapter*"

Table 7–63: Table Performance analysis trace collection point

Event ID	Numbers in figure	Trace collection point	Level#1
0xA000	1	At the time of request reception	Details
0xA002	2	When invoking file operation process	Standard
0xA003	3	When file operation process ends.#2	Standard
0xA001	4	When sending response	Details

#1

For details on how to change level of performance analysis trace, see "Changing trace collection level", "Application Server Command Reference Guide", and "Application Server Maintenance and Migration Guide".

#2

Even when exception occurs during file operation process, trace collection point is same as when file operation process ends.

●Changing trace collection level

When you change PRF trace collection level, specify hexadecimal value (8 digits) of 4 bytes in -PrfChangeLevel option of the cprflevel command. Index number (Index 1, Index 2) is assigned in their respective hexadecimal values. The following table describes specified location when acquiring trace information:

Table 7–64: Table Specified location of trace collection level

Index	Digit	Upper layer	Lower layer
Index 1	1st digit	Redirect	Web container
	2nd digit	EJB container	JNDI
	3rd digit	JTA	JCA container
	4th digit	DB Connector	RMI
	5th digit	Web Services - Base	TP1 Connector, TP1/Client/J
	6th digit	TP1/Message Queue - Access	Reliable Messaging
	7th digit	OTS	-
	8th digit	CTM	-
Index 2	1st digit	HCSC server	Standard output/standard error output/User log
	2nd digit	DI	-
	3rd digit#	-	File adapter

Legend:

-: Not applicable.

#

When you change the trace collection level of the file adapter, value in lower layer of 3rd digit of Index 2 changes. The following table describes specified value:

Table 7–65: Table Specified value of trace collection level of file adapter

Specified value#	Trace collection level
0	Standard
1	Details

Note#

Convert in hexadecimal when specifying in -PrfChangeLevel option.

For details on the cprflevel command, see in "Application Server Command Reference Guide".

7.7.8 INTENTIONALLY DELETED

INTENTIONALLY DELETED

7.7.9 Troubleshootingwhen executing Message Queue reception

In Message Queue reception, performance analysis trace is output as failure information.

This section describes method of notifying an error when you execute Message Queue reception and performance analysis trace.

(1) Method of notifying an error when executing Message Queue reception

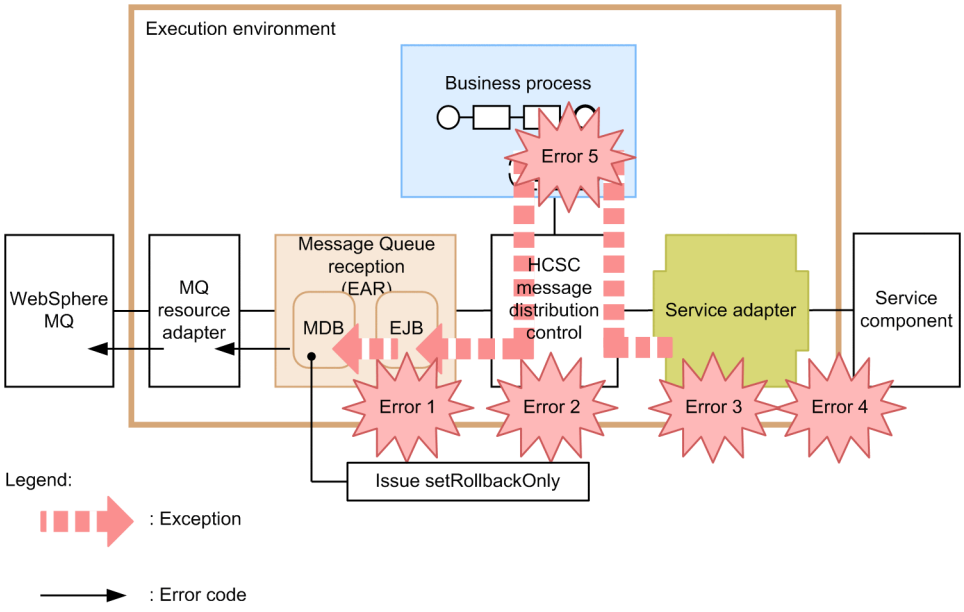
This section describes method of notifying an error when business process is invoked using Message Queue reception from JMS provider (WebSphere MQ).

The following figure shows the method of notifying an error when custom reception framework returns an error:

Reference note

When fault is to returned from the service component or service adapter, communication model cannot return fault from business process for asynchronous reception. Therefore, it returns an exception. The following figure shows the method of notifying an error:

Figure 7–79: Figure Method of notifying an error when custom reception framework returns an error (for reception of Message Queue)



The errors shown in figure are as follows:

- Error 1: Invalid request parameter.
- Error 2: Address (Location) not found, service adapter stop has stopped.
- Error 3: Data transformation failed.
- Error 4: Invalid address, the service component has stopped, communication failed.
- Error 5: Exception error on processing of business process

When any of Error 1- Error 5 occurs, custom reception framework in which exceptions are caught throws CSCMsgServerException for reception process of Message Queue reception. For details on CSCMsgServerException see "Appendix A.3 APIs of the custom reception framework" in "Service Platform Reception and Adapter Definition Guide".

In reception process of Message Queue reception, exception log is output on the basis of caught exceptions, respond normally to MQ resourse adapter after executing EJBContext#setRollbackOnly.

In MQ resourse adapter, normal response is returned as is for queue manager of JMS provider (WebSphere MQ).

The queue manager of JMS provider (WebSphere MQ) rolls back the transaction and resets the message at the beginning of the queue.

! Important note

When frequency of rollback increases due to settings of rollback frequency limit value, message is moved to dead letter queue. The maximum number of times rollback can be performed is described in detail in the manual *uCosminexus BPM/ESB Service Platform Overview*. See the description of the setting for the number of times a message can be rolled back in *2.10.1 Invoking service components using Message Queue reception* in that manual.

(2) Acquiring failure information (Message Queue reception)

When operation fails, the required troubleshooting information is output to log file as log, and to the trace file as trace.

This section describes how to acquire message log and each type of trace.

(a) Message log (Message Queue reception)

In the activity log of the J2EE server of message log, each type of information occurred in Message Queue reception is output as message.

For details on output contents or output destination of message log, see "*7.4.1 Message log*".

(b) Request trace (Message Queue reception)

Reuquest trace is used to analyze cause of failure occurred in request.

Output of request trace is not from Message Queue reception but from custom reception framework

(c) Performance analysis trace (Message Queue reception)

This section describes performance analysis trace (PRF trace) in Message Queue reception.

?Output format of performance analysis trace

The format to be output to performance analysis trace is same as format of performance analysis trace of J2EE server. For details on, see "7. Performance analysis wherein performance analysis trace is used" in "Application Server Maintenance and Migration Guide".

?Output contents

The following table describes contents to be output to performance analysis trace file:

Table 7–66: Table Contents to be output to performance analysis trace file (for Message Queue reception)

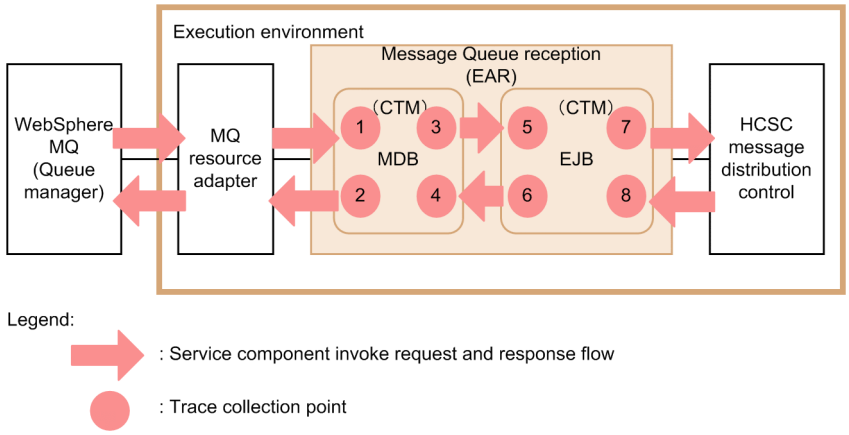
Item	Contents
Event ID	Event ID of collection point is output. For details on collection point, Item "*Performance analysis trace collection point*"
Return code	Collection point type is output. • 0: Normal end • 1: Abnormal end
Interface name	Class name is output.
Operation name	Method name is output
Operation information	Following operation information is to be output:

Item	Contents
Operation information	• JMS message ID • Reception name • Reception ID • Service name • Service operation name • Exception name (Only when failure occurs)

? Performance analysis trace collection point

The following figure shows the performance analysis trace collection point:

Figure 7–80: Figure Performance analysis trace collection point (for Message Queue reception)



The following table lists and describes the relationship between the event ID, trace collection point, and performance analysis trace collection level. The numbers in the *Number in figure* column of the table correspond to the numbers in the above figure.

Table 7–67: Table Performance analysis trace collection point (for Message Queue reception)

Event ID	Number in figure	Trace collection point	Level
0x98A0	1	Opening of Message Queue reception	A
0x98A1	2	Exit of Message Queue reception	A
0x98A2	3	Invocation of custom reception framework	B
0x98A3	4	Response reception of custom reception framework	B
0x9860	5	Entry to custom reception framework	A
0x9861	6	Exit to custom reception framework	A
0x9864	7	Invocation of HCSC message delivery control	A
0x9865	8	Response reception of HCSC message delivery control	A

Legend:

A: Indicates the "Standard" level.

B: Indicates the "Detailed" level.

? Collection method and output destination of performance analysis trace

Settings are important to acquire performance analysis trace. For details on settings, see "7. Performance analysis wherein performance analysis trace is used " in "Application Server Maintenance and Migration Guide".

(d) User message trace (Message Queue reception)

You can use the user message trace to check status of message.

User message trace is output from custom reception framework and not from Message Queue reception.

For details on user message trace, see explanation for request trace (custom reception) in "Appendix A.8 Acquiring the failure information (Custom reception) "in "Service Platform Reception and Adapter Definition Guide".

(3) Countermeasures to be taken when J2EE server becomes down during Message Queue reception process

When J2EE server is down during Message Queue reception process, realtime rollback is not performed for message in WebSphere MQ specification. Restart the WebSphere MQ server.

7.7.10 Troubleshootingwhen executing Message Queue

In the Message Queue adapter, the information to validate system performance and analyze the cause of failure is output to the log file or the trace file. The following table lists and describes the type of log and trace output to Message Queue:

Table 7–68: Table Type of log and trace (For Message Queue adapter)

Log/trace	Output information	Description
Message log	Each type of information in the Message Queue adapter is output as a message.	You can check operation information (start/stop/ error) as a message. You can check operation status of the system in a batch since the output destination of the message log is common for entire Application Server.
Method trace	The following information is output when you start or end an internal method of the Message Queue adapter: • Date • Time • Execution class name • Internal method name • Information of specified argument	You can check the publication time and sequence of internal method.
Data trace	The following information, sending and receiving messages between the Message Queue adapter and the resource adapter, Detail of fault response information is output: • Date • Time • I/O type of message • Contents of message	You can confirm the validity of message by acquiring contents of the message and information of the argument.
Performance analysis trace	The following information is output to the performance analysis trace collection point of the entire Application server: • Date • Time • Request information • Trace collection source information The Message Queue adapter specific information is output in the performance analysis trace collection point of the Message Queue adapter.	You can validate the performance of Application Server system on the basis of the performance analysis information output in the series of processes starting from when you receive a request from the service requester till the execution result is returned.
Exception log	Information of an exception which occurred in the method provided by Message Queue is output: • Date • Time	You can confirm the time when the exception occurred and the method

Log/trace	Output information	Description
Exception log	• Information of the exception (Stack race)	You can confirm the time when the exception occurred and the method

For details on points to be considered when a log or a trace is output, see "*7.3.4(1) General notes*".

In the troubleshooting functionality of the Message Queue adapter, a message is output to the console. When failure occurs, investigate the cause on the basis of the message information. When the cause of failure is not clear, collect the material regarding the definition of the Message Queue adapter and the message log, and contact the administrator.

You can acquire the log and the trace of Message Queue using the troubleshooting functionality of Application Server. The methods for acquiring the log and the trace are as follows:

- Using the management command of Management Server (mngsvrutil)
  For details, see "Application Server Command Reference Guide ".
- Using the management portal
  For details, see "Application Server Management Portal User Guide ".
- Using the snapshotlog command
  For details, see "Application Server Command Reference Guide ".

(1) Message log

Each type of information in the Message Queue adapter is output as a message in the activity log of the J2EE server of the message log.

For details on the output contents or the output destination of the message log, see "*7.4.1 Message log*".

(2) Method trace

You can check the publication time and the sequence of the internal method in method trace. Management service uses the method trace to analyze failure.

(a) Output destination

Output destination of the method trace of Message Queue is as follows:

<Working directory of J2EE server>\ejb\<J2EE server name>\logs\CSCADP\MQADP\maintenance\<Service ID>

Specify the output destination of the working directory in the ejb.public.directory key of the option definition file (usrconf.cfg) for the J2EE server on which the HCSC server is running.

For details, see "2.3 usrconf.cfg (option definition file for J2EE server) " in "Application Server Definition Reference Guide".

The following table lists the trace file name of method trace:

Table 7–69: Table Trace file name of method trace (Message Queue adapter)

Output mode of trace file	Trace file name
For wraparound mode	mtdtrace<Count>.log
For shift mode	mtdtrace.log

(b) Number of files

The default number of files is 4. You can change the number of files with the methodtracefile.num key of the Message Queue adapter execution environment.

For details on the Message Queue adapter runtime-environment property file, see "Message Queue adapter runtime-environment property file" in "Service Platform Reference Guide". For details on how to change, see the description for creating the Message Queue adapter runtime-environment property file in "3.3.9 Defining Message Queue adapters " in "Service Platform Reception and Adapter Definition Guide".

(c) File size

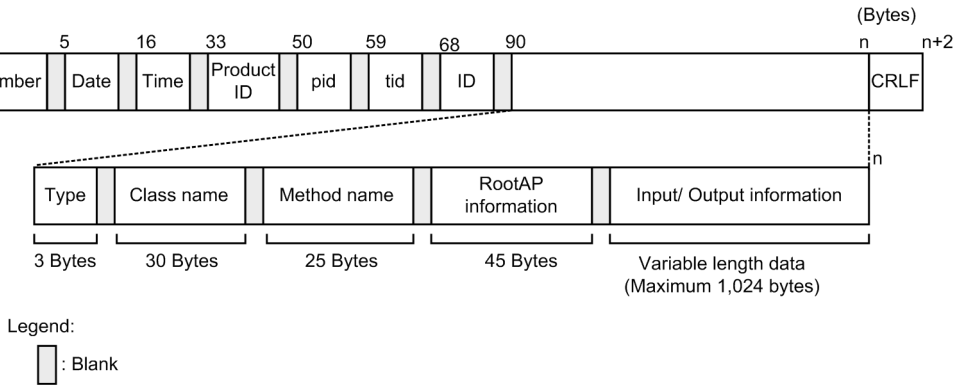
The default size of the output file is 4MB. You can change the file size using the methodtracefile.size key of the Message Queue adapter runtime-environment property file.

For details on the Message Queue adapter runtime-environment property file, see "Message Queue adapter runtime-environment property file " in "Service Platform Reference Guide". For details on how to change, see the description for creating the Message Queue adapter runtime-environment property file in "3.3.9 Defining Message Queue adapters " in "Service Platform Reception and Adapter Definition Guide".

(d) Output format

The following figure shows the output format of the method trace:

Figure 7–81: Figure Output format of method trace



(e) Output contents

The following table list and describes contents output in method trace:

Table 7–70: Table Items output to the method trace (Message Queue adapter)

Item	Contents
Number	The output serial number of the method trace is displayed.
Date	The collection date of the method trace is output in the yyyy/mm/dd format. • yyyy: Christian year • mm: Month • dd: Day
Time	The collection time of the method trace is output in hh:mm:ss.SSS format. • hh: hour • mm: minute • ss: second • SSS: milliseconds Time is shown in milliseconds in local time.
Product ID	"ADPMQ" indicating the Message Queue is displayed as the identifier used for identifying the product. Format of version information is as follows: • Regular edition product: VV-RR • Modified version product: VV-RR-SS
pid	The ID to identify the process is output.
tid	The ID to identify the thread is output.
ID	Blank

Item	Contents
Type	Type of trace collection point is output • BGN: Start Method • END: End Method • CAL: Invoke method • RET: Return method • THR: Throw exception • CTH: Catch exception
Class name	The class name to acquire trace is output. Perform left alignment when there are 30 or less characters, and replace with space in case of shortage of characters.
Method name	The method name to acquire trace is output. Perform left alignment when there are 25 or less characters, and replace with space in case of shortage of characters.
RootAP information	Character string wherein the information of RootAP such as IP address, process ID, communication number, which is output in the performance analysis trace is demarcated with "/ (slash)" is output.
I/O information	I/O information of method that acquires trace (Argument value or return value) is output.
CRLF	Record end code is output.

(3) Data trace

In data trace, you can check the message contents or I/O time of messages sent and received by the Message Queue adapter. The user recovers user data with the data trace, and Management Service analyzes failures with the data trace to analyze failures.

(a) Output destination

User messages sent and received in data trace are output. Therefore, specify an output destination for which security is ensured in the data trace.

The output destination of data trace is as follows:

<Working directory of J2EE server>\ejb\<J2EE server name>\logs\CSCADP\MQADP\maintenance\<Service ID>

Specify the output destination of the working directory in the ejb.public.directory key of the option definition file (usrconf.cfg) for the J2EE server on which the HCSC server is running. For details, see "Application Server Maintenance and Migration Guide" , "Application Server Definition Reference Guide".

The trace file name of data trace is as follows:

Table 7–71: Table Trace file name of data trace

Output mode of trace file	Trace file name
For wraparound mode	dattrace<number of files>.log
For shift mode	dattrace.log

(b) Number of files

The default number of files is 4. You can change number of files using the datatracefile.num key of the Message Queue adapter runtime-environment property file.

For details on the Message Queue adapter runtime-environment property file, see "Message Queue adapter runtime-environment property file" in "Service Platform Reference Guide". For details on how to change, see the description for creating the Message Queue adapter runtime-environment property file "3.3.9 Defining Message Queue adapters " in "Service Platform Reception and Adapter Definition Guide".

(c) File size

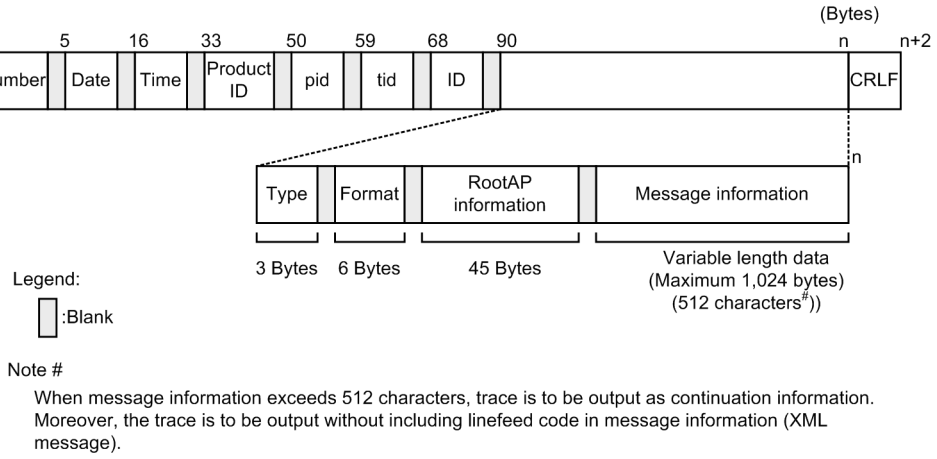
The default file size of the output file is 1MB. You can change the size of the output file with the datatracefile.size key of the Message Queue adapter runtime-environment property file.

For details on the Message Queue adapter runtime-environment property file, see "Message Queue adapter runtime-environment property file" in "Service Platform Reception and Adapter Definition Guide". For details on how to change, see the description for creating the Message Queue adapter runtime-environment property file in"3.3.9 Defining Message Queue adapters " in "Service Platform Reception and Adapter Definition Guide".

(d) Output format

The following figure shows the format output to the data trace:

Figure 7–82: Figure Format output to the data trace



Note #

When message information exceeds 512 characters, trace is to be output as continuation information. Moreover, the trace is to be output without including linefeed code in message information (XML message).

(e) Output contents

The following table lists and describes the items output to the data trace:

Table 7–72: Table Contents output to data trace (Message Queue adapter)

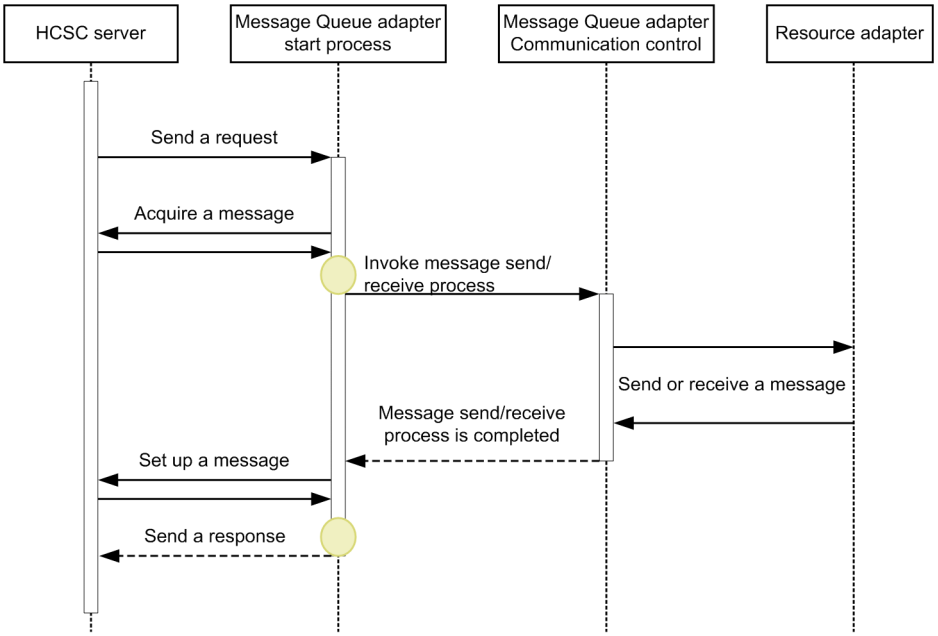
Item	Contents
Number	The output serial number of the data trace is displayed
Date	The collection date of data trace is output in the yyyy/mm/dd format. • yyyy: Christian year • mm: Month • dd: Day
Time	The collection time of the data trace is output in hh:mm:ss.SSS format. • hh: Hour • mm: Minute • ss: Second • SSS: Millisecond Time is shown in milliseconds in local time.
Product ID	"ADPMQ" and the version information indicating the Message Queue adapter is displayed as the identifier used for identifying the product. Format of version information is as follows: • Regular version product: VV-RR • Modified version of product: VV-RR-SS
pid	The ID to identify the process is output.
tid	The ID to identify the thread is output.
ID	Blank

Item	Contents
Type	I/O type of data is output: • REQ: Request message • RSP: Response message • FLT: Fault message • INF: JMS header information • ERR: Request/response message that has failed in sending and receiving • Space: Continuous data
Format	Format of data is output. • XML: XML format • BINARY: Binary format Perform left alignment when there are 6 or less characters, and replace with space in case of shortage of characters. For "INF" type, space for 6 characters is output.
RootAP information	Character string wherein the information of RootAP such as IP address, process ID, communication number, which is output in the performance analysis trace is demarcated with "/ (slash)" is output.
Message information	Sending and receiving of message information is output. • For "XML" format XML text is output. • For "BINARY" Hex dump format is output. • For "FLT" type Contents set in each element of fault information are output in "Element name= setting value" format. Demarcate each element with ", (Comma)". • For "INF" type JMS header information is output.
CRLF	Record end code is output.

(f) Collection point of data trace

In the data trace collection point of the Message Queue adapter, I/O message which is sent and received, and the Fault response information is output:

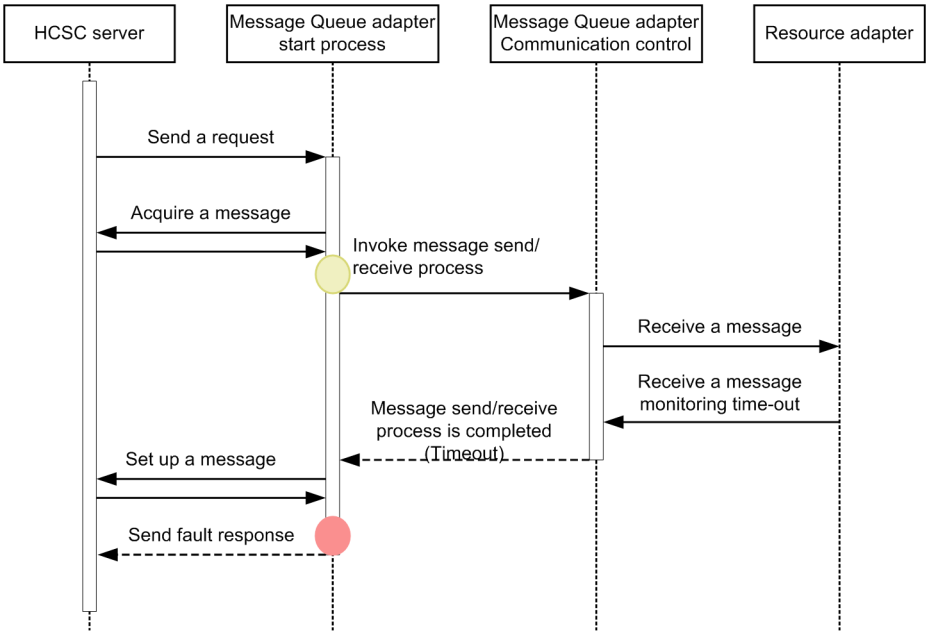
Figure 7–83: Figure Collection point of data trace (Normal end)



Legend:

: Indicates trace collection point. Acquire when data trace collection level is "30".

Figure 7–84: Figure Collection point of data trace (when sending Fault response)

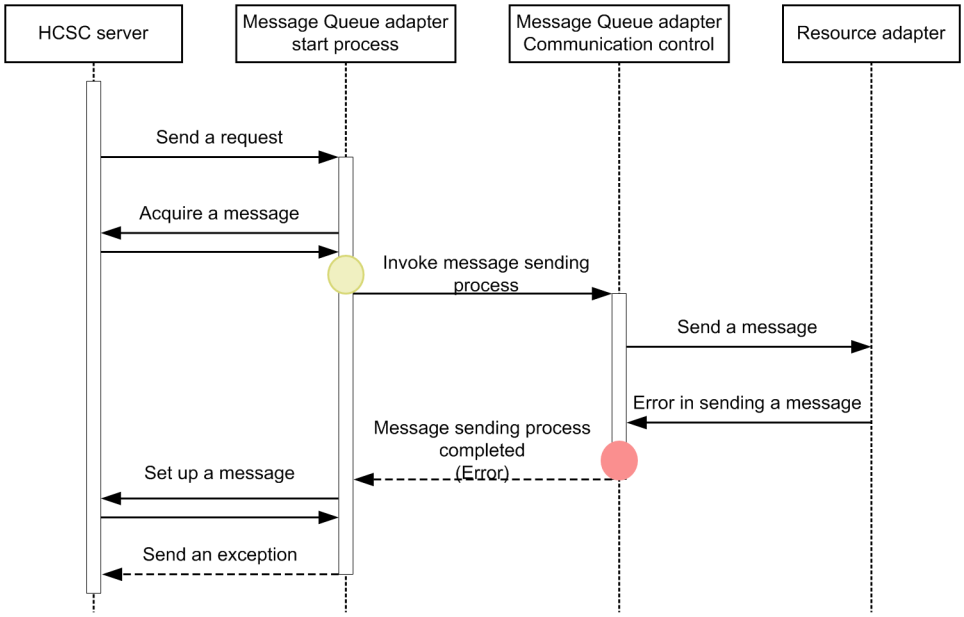


Legend:

: Indicates trace collection point. Acquire when data trace collection level as "10 (Default)"

: Indicates trace collection point. Acquire when data trace collection level is "30".

Figure 7–85: Figure Collection point of data trace (Message sending fails)

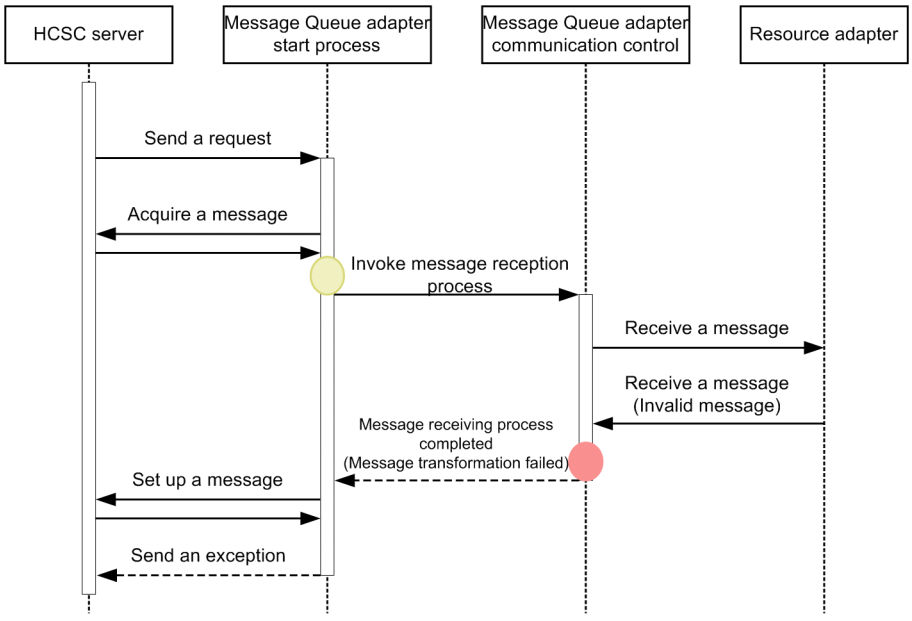


Legend:

: Indicates trace collection point. Acquire as data trace collection level is "10 (Default)".

: Indicates trace collection point. Acquire when data trace collection level is "30".

Figure 7–86: Figure Collection point of data trace (Message transformation fails)



Legend:

: Indicates trace collection point. Acquire as data trace collection level is "10 (Default)".

: Indicates trace collection point. Acquire when data trace collection level is "30".

(4) Performance analysis trace (PRF trace)

You can validate the performance of Application Server system on the basis of the performance analysis information output in the series of processes starting from when you receive a request from the service requester till the execution result is returned. Message queue specific information is output in the performance analysis trace collection point of the Message Queue adapter. Maintenance service uses the information to analyze performance bottlenecks.

(a) Output destination

The following table describes the output destination and trace file name of performance analysis trace:

Table 7–73: Table Output destination and trace file name of performance analysis trace

Path of output destination of trace	Trace file name
<Setting directory of environment variable PRFSPOOL>\utt\prf\<PRF identifier>\dcopltrc#	prf_<n>

Legend:

n: Enter integer from 001 to maximum value of number of files.

Note#

The output destination of performance analysis trace is common for entire Application Server. For details, see "7.3 Collecting performance analysis trace file in which Management Server is used" in "Application Server Maintenance and Migration Guide".

(b) Number of files

The default number of output files is 4. You can change the number of output files with the management portal or the cprfstart command. For details on management portal, see "Application Server Management Portal User Guide ". For details on the cprfstart command, see "Application Server Command Reference Guide ".

(c) File size

The default size of performance analysis trace (PRF trace) file is as follows:

- When file size is set in management portal: 32MB
- When file size is set using cprfstart command: 8MB

You can change the file size using the management portal or the cprfstart command. For details on management portal, see "Application Server Management Portal User Guide", and for details on the cprfstart command, see "Application Server Command Reference Guide "

(d) Output format

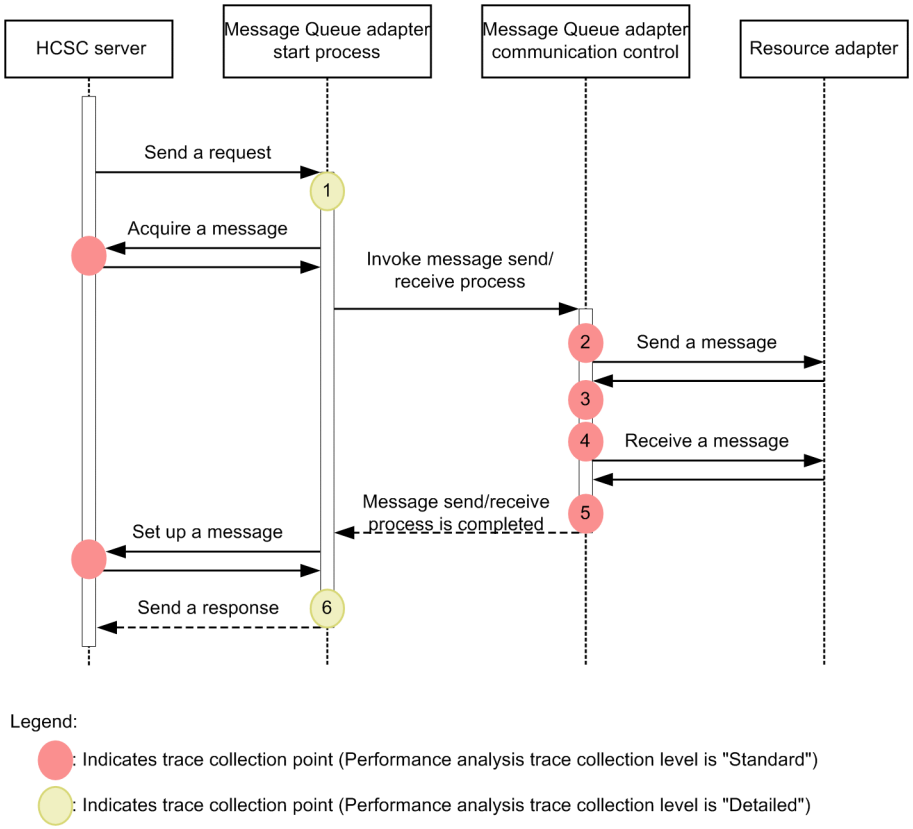
The format which is output to the performance analysis trace is same as the performance analysis trace of Application Server. For details, see "7. Performance Analysis Using Performance Analysis Trace" in "Application Server Maintenance and Migration Guide"

(e) Collection point of performance analysis trace

In the performance analysis trace collection point of the Message Queue adapter, the Message Queue adapter specific information is output.

The following figure shows the performance analysis trace collection point of the Message Queue adapter:

Figure 7–87: Figure Collection point of performance analysis trace



A point specific event ID is assigned in the collection point of the performance analysis trace. The Trace event ID output to the Message Queue adapter is 0xA200~0xA2FF.

The following table describes the event ID, trace collection point, and performance analysis trace collection point. The numbers in the *Number in figure* column of the table correspond to the numbers in the above figure.

Table 7–74: Table Performance analysis trace collection point(Message Queue adapter)

Event ID	Number in figure	Trace collection point	Level
0xA200	1	At the time of request reception	B
0xA202	2	When sending message	A
0xA203	3	When message sending ends	A
0xA204	4	When receiving message	A
0xA205	5	When message receiving ends	A
0xA201	6	When sending response	B

Legend:

A: Indicates the "Standard" level.

B: Indicates the "Detailed" level.

When you change collection level of PRF trace, specify 2 values in hexadecimal (8 digits) format of 4 bytes in the -PrfChangeLevel option of the cprflevel command. For details on how to specify the cprflevel command, see "cprflevel (displaying and changing PRF trace collection level) " in "Application Server Command Reference Guide.

Index number (Index 1, Index 2) is assigned in its respective hexadecimal value.

For details on how to change performance analysis trace level, see "Application Server Maintenance and Migration Guide".The default value is "Standard".

(5) Exception log

The exception information is output to the exception log. For details on the overview of the exception log, see "7.4.5(1) Exception log".

(a) Output destination

Output destination of exception log is as follows:

<Working directory of J2EE server>\ejb\<J2EE server name>\logs\CSCADP\MQADP\maintenance\<Service ID>

Specify the output destination of the working directory in the ejb.public.directory key of the option definition file (usrconf.cfg) for the J2EE server on which the HCSC server is running. The following table lists the log file name of the Exception log:

Table 7–75: Table Log file name of the Exception log (Message Queue adapter)

Output mode of log file	Log file name
For wraparound mode	exception<Count>.log
For shift mode	exception.log

(b) Number of files

The default number of output files is 4. You can change number of files using the exptracefile.num key of Message Queue adapter runtime-environment property file.

For details on the Message Queue adapter runtime-environment property file, see "Message Queue adapter runtime-environment property file" in "Service Platform Reference Guide". For details on how to change, see the description for creating the Message Queue adapter runtime-environment property file in "3.3.9 Defining Message Queue" in "Service Platform Reception and Adapter Definition Guide".

(c) File size

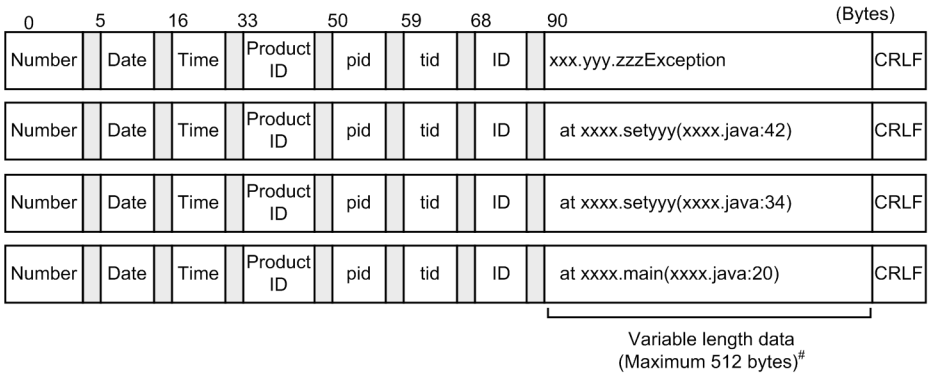
The default size of the output file is 4MB. You can change the file size using the exptracefile.size key of the Message Queue adapter runtime-environment property file.

For details on the Message Queue adapter runtime-environment property file, see "Message Queue adapter runtime-environment property file " in "Service Platform Reference Guide". For details on how to change, see the description for creating the Message Queue adapter runtime-environment property file in "3.3.9 Defining Message Queue" in "Service Platform Reception and Adapter Definition Guide".

(d) Output format

The following figure shows the format that is output in the Exception log:

Figure 7–88: Figure Format output in the Exception log



#
The upper limit value of trace length shows aimed value and even if upper limit value exceeds, it is possible to output without truncation. However, the length of a stack trace line is maximum 4,185 bytes and the information exceeding that limit is truncated.

(e) Output contents

The following table lists and describes the contents output in the exception log:

Table 7–76: Table Items output in the exception log (Message Queue adapter)

Item	Contents
Number	Output serial number of exception log is displayed.
Date	The collection date of the FTP protocol trace is output in the yyyy/mm/dd format. • yyyy: Christian year • mm: Month • dd: Day
Time	The collection time of the FTP protocol trace is output in hh:mm:ss.SSS format. • hh: Hour • mm: Minute • ss: Second • SSS: Millisecond Time is shown in milliseconds in local time.
Product ID	"ADPMQ" indicating the Message Queue adapter is output as the identifier used for identifying the product.
Pid	The ID to identify the process is output.
Tid	The ID to identify the thread is output.
ID	Blank
Stack trace information	Stack trace information is output.
CRLF	Record end code is output.

(6) Failure information of the Message Queue adapter

Message Queue adapter notifies failure using error information in the following cases:

- When timeout occurs in the message reception reponse monitoring time for the request to receive messages
- When a message does not exist in the reception queue for a request to browse and receive a message

The following table lists and describes each setting value of the error information:

Table 7–77: TableError information set by the Message Queue adapter

Element name	Form	Setting value	Description
faultCode	String	Server	Communication errors are errors at server side.
faultString	String	<Message text of message output by Message Queue adapter>	For details, see "2.12 Messages from KDEH20000 to KDEH30999" in "Service Platform Messages".
faultActor	String	<Service adapter name>	The name of the service adapter where error information is notified.
faultDetail	Document(XML)	Code:1 Message:"timeout"	When timeout occurs in monitoring time of received message or when received message does not exist.

(7) Points to be considered before setting Message Queue adapter

The following are the points to be considered before setting Message Queue adapter. Confirm that there is no problem when the system operates. If there is a problem then eliminate the cause of this problem.

- Message Queue adapter executes the connection release process for each request from the business process but, actually the connection between the resource adapter and WebSphere MQ is not disabled using the connection pool functionality of the resource adapter for a fixed period of time (5 minutes by default).

  Depends on specification in Connector property file (Not disconnected in default)
- When connection release of a Message Queue adapter fails, status of connection changes to "Released", but in some cases release of the connection is not detected in JMS provider system of connection destination. Due to this, there is a possibility that connection status may become inconsistent, and the next communication process may fail. Therefore, once initialize the established status of the connection in the connection destination JMS provider system.
- If failure occurs during Message Queue adapter operations and the stop process is not executed normally, in some cases the release of connection in the connection destination JMS provider system is not detected. Therefore, once initialize the established status of connection destination JMS provider system.
- Specify the request message with a value of one or more bytes. Error occurs if you specify 0 in the length of the request message.
- The user message in XML format which can be sent and received by the Message Queue adapter is as per the specification of XML Processor. For details, see support range of XML Processor in "XML Processor User's Guide".
- Specify the transaction support level provided in the resource adapter as "LocalTransaction" or "XATransaction". However, you can specify "LocalTransaction" only when the status in business process is not persistent. You cannot specify "NoTransaction".

  JTA user specification is affected since "LocalTransaction" and "XATransaction" specification is related to JTA (Java Transaction API). For example, when the monitoring time of the JTA message reception is less than the monitoring time (receive_timeout) of reception responseof the message of the Message Queue adapter communication-configuration definition file, timeout occurs in the monitoring time of JTA message reception.

(8) Actions to be taken when error occurs

This section explains actions to be taken when message sending, message receiving, and requests to browse, receive a message or send and receive a message fails.

When message sending, message receiving, and requests to browse, receive a message or send and receive a message fail, you can re-execute the business process or continue execution from a point at which any of these processes have failed. Select actions to be taken according to operating format.

Note that, when you re-execute a business process, take action after you return to a status prior to the failed request publication which includes status of transmission queue and reception queue, and the status of the partner system.

(a) Actions to be taken when message sending fails.

When a request to send message fails, check the message log and confirm whether message KDEH30111-E is output. As per result, cause and actions differ as shown in following table:

Validation result	Cause	Action
When KDEH30111-E is output	Message sending has failed	Reference the message output just before KDEH30111-E message, eliminate the cause of problem, and re-execute request for message sending. If you want check user data when message sending fails, see data trace.
When KDEH30111-E is not output	In some cases message sending is successful.	Check that message is stored in transmission queue.

(b) Actions to be taken when message reception or a request to browse and receive a message fails

When reception of message or a request to browse and receive a message fails, check the message log and confirm that KDEH30113-E message is output. As per result, cause and actions differ as shown in following table:

Validation result	Cause	Action
When KDEH30113-E is output	Message is removed from the reception queue	Reference the data trace and acquire the message. Confirm that the message received from the reception queue does not exist. For a request to browse and receive message, you need not check the reception queue.
When KDEH message is not output when KDEH30113-E message is not output and	Message is removed from the reception queue	Reference the data trace and acquire the message. Confirm that the message received from reception queue does not exist. For a request to browse and receive message you need not confirm reception queue. In this case, you need to set data trace level to 20.
When KDEH30113-E is not output.	Message receiving has failed	Confirm that KDEH30111-E is output. Reference the message output just before KDEH30111-E message, eliminate the cause of failure in message receiving, and re-execute the request to receive a message.
When KDEH30103-W is output	Message does not exist in reception queue.	Re-execute the request to receive a message according to operation status.

(c) Actions to be taken when send and receive of message fails

When send and receive of message fails, the causes and actions to be taken for failure in message sending and receiving are as follows:

- When message sending fails

  When a request to send message fails, check message log and confirm that KDEH30111-E message is output. As per the result, cause and actions differ as shown in following table:

Validity result	Cause	Action
When KDEH30111-E is output and the communication type is send	When message sending has failed	Reference the message that is output just before the KDEH30111-E message, eliminate the cause, and re-execute the request to send the message. If you want to check the user data when message sending fails, see the data trace.

- When receiving of message fails

  When the request to receive a message fails, check the message log and confirm that KDEH30113-E message is output. As per the result, cause and actions differ as shown in following table:

Validation Result	Cause	Action
When KDEH30113-E is output	Message sending is successful, and the message is removed from reception queue	Reference the data trace and acquire the receive message, and confirm that the message received from the reception queue does not exist.
When KDEH message is not output when KDEH30113-E is not output	Message sending is successful and message is removed from the reception queue	Reference the data trace and acquire the receive message, and confirm that the message received from reception queue does not exist. In this case, you must set data trace level as 20.
When KDEH30113-E is not output	When message sending is successful but message receiving has failed	KDEH30111-E is output, check that communication type is received. Eliminate the cause of failure in message receiving, execute a request to send and receive message, or execute a request to receive a message according to the operating format.
When KDEH30103-W is output	Message does not exist in reception queue. Message sending is successful.	Re-execute request to receive the message according to operation status.

7.7.11 Troubleshooting in FTP linkage system

This section describes the types of information that you can acquire for a failure which occurred at the time of FTP linkage operations.

(1) Acquiring failure information (FTP inbound adapter)

The failure information of the FTP inbound adapter can be classified as follows:

- Message log#
- Maintenance log#
- Protocol trace #
- Transfer history log#
- Common log between resource adapters#
- Maintenance log when executing operation command
- Performance analysis trace

The following is the description of the above mentioned failure information:

Note#

The following table describes the log file size required when you execute file transfer, or start and stop the FTP inbound adapter once for these logs. Reference values in this table and calculate the required log file size depending on the used environment:

Table 7–78: Table Required log file size

Type of log	Log file size required for single file transfer	Log file size required for single start and stop
Message log	1.0KB	1.5KB
Maintenance log	0.5KB	0.5KB
Protocol trace	2.0KB	0.0KB
Transfer history log	0.5KB	0.0KB
Common log between resource adapters	0.5KB	1.5KB

Furthermore, the FTP inbound adapter also includes the material output by the J2EE server and JavaVM on which the FTP inbound adapter is running other than the failure information described in this manual. For details on material output by the J2EE server and JavaVM, see "4.Output destination and output method for data required in troubleshooting " in "Application Server Maintenance and Migration Guide".

(a) Message log (FTP inbound adapter)

In the message log, a message showing the error information of the FTP inbound adapter and operating information is output. The message log in FTP inbound adapter is described here.

●Output format of message log

Output format of message log is as follows:

```
<Date> <Time> <pid> <tid> <Transfer ID> <Message ID> <Message text>
```

●Output contents

The following table lists and describes the contents output to the Message log:

Table 7–79: Table Contents output to the Message log (FTP inbound adapter)

Item	Contents
Date	The collection date of the Message log is output in the yyyy/mm/dd format. • yyyy: Christian year • mm: Month • dd: Day
Time	The collection time of the Message log is output in hh:mm:ss.SSS format. • hh: Hour • mm: Minute • ss: Second • SSS: Millisecond
pid	The ID to identify the process is output.
tid	The ID to identify the thread is output.
Transfer ID	Transfer ID is output.
Message ID	Message ID is output.
Message text	The content of the message is output.

● Output destination of message log

```
<Working directory of J2EE server>\ejb\<J2EE server name>\logs\csc\inbound-
adapter\ftp\FTP_Inbound_Resource_Adapter
```

The following table describes the log file name of the message log:

Table 7–80: Table Log file name of the Message log (FTP inbound adapter)

Type of file	Log file name
Current file	message.log
Backup file#	message<Count>.log

Note#

If the size of current file exceeds the size for each file, it is renamed to the backup file.

The number of backup files is included in the backup file name. The number increases for new log files. Once the log file is created, it cannot be deleted. Line feed code of file is "LF".

You can change <Working directory of J2EE server> in the ejb.public.directory key of usrconf.cfg (Option definition file for J2EE server). Default is <Installation directory of Service Platform>\CC\server\public. Note that you cannot change the output destination of the message log in the ejb.server.log.directory key. For details on

usrconf.cfg, see "2.3 usrconf.cfg (Option definition file for J2EE server)" in "Application Server Definition Reference Guide".

Furthermore, you can change the output level of the message log, file size, and number of files in the following properties of the connector property file that sets the property of RAR file:

- server_message_logLevel=output level of message log
- server_message_maxFileSize=file size of message log
- server_message_maxBackupIndex= number of backup files

For details on the procedure for setting, see "*3.2.3(3) Setting up the FTP inbound adapter*".

(b) Maintenance log (FTP inbound adapter)

In the maintenance log, the log when an error has occurred in the FTP inbound adapter is output. You need this log when you contact Maintenance Service. The log required for maintenance in the FTP inbound adapter is described here.

●Output format of the maintenance log

Output format of the maintenance log is as follows:

```
<Date> <Time> <pid> <tid> <Maintenance information>
```

●Output contents

The following table lists and describes the contents output to the maintenance log:

Table 7–81: Table Contents output to the maintenance log (FTP inbound adapter)

Items	Contents
Date	The collection date of the maintenance log is output in the yyyy/mm/dd format. • yyyy: Christian year • mm: Month • dd: Day
Time	The collection time of the maintenance log is output in the hh:mm:ss.SSS format. • hh: Hour • mm: Minute • ss: Second • SSS: Millisecond
pid	The ID to identify the process is output. It is different from the process ID managed by OS.
tid	The ID to identify the thread is output. It is different from the thread ID managed by OS.
Maintenance information	Maintenance information is output when you contact system administrator or maintenance service.

● Output destination of Maintenance log

```
<Working directory of J2EE server>\ejb\<J2EE server name>\logs\csc\inbound-adapter\ftp\FTP_Inbound_Resource_Adapter
```

The following table describes the log file name of the maintenance log:

Table 7–82: Table Log file name of the maintenance log (FTP inbound adapter)

Type of file	Log file name
Current file	maintenance.log
Backup file#	maintenance<Count>.log

Note#

If the size of current file exceeds the size for each file, it is renamed to backup file.

The number of backup files is included in the backup file name. The number increases for new log files. Once the log file is created, it cannot be deleted. Line feed code of file is "LF".

You can change <Working directory of J2EE server> in the ejb.public.directory key of usrconf.cfg (Option definition file for J2EE server).Default is <Installation directory of Service Platform>\CC\server\public. Note that you cannot change the output destination of the message log in the ejb.server.log.directory key. For details on usrconf.cfg, see "2.3 usrconf.cfg(Option definition file for J2EE server)" in "Application Server Definition Reference Guide".

Furthermore, you can change the output level of the maintenance log, file size, and number of files in the following properties of the connector property file that sets the property of RAR file:

- server_maintenance_logLevel= Output level of maintenance log
- server_maintenance_maxFileSize= File size of maintenance log
- server_maintenance_maxBackupIndex= Number of backup files

For details on procedure for settings, see "*3.2.3(3) Setting up the FTP inbound adapter*".

(c) FTP protocol trace (FTP inbound adapter)

In the FTP protocol trace, trace of the FTP protocol message which is sent and received from the FTP client is output. The FTP protocol trace of the FTP adapter is described here.

●Output format of FTP protocol trace

Output format of FTP protocol trace is as follows:

```
<Date> <Time> <pid> <tid> <Transfer ID> <Send and receive direction> <protocol message>
```

●Output Contents

The following table lists and describes contents output to the FTP protocol trace:

Table 7–83: Table Contents output to the FTP protocol trace (FTP inbound adapter)

Item	Contents
Date	The send and receive date of the protocol message is output in the yyyy/mm/dd format. • yyyy: Christian year • mm: Month • dd: Day
Time	The send and receive time of the protocol message is output in hh:mm:ss.SSS format. • hh: Hour • mm: Minute • ss: Second • SSS: Millisecond
pid	The ID to identify the process is output.
tid	The ID to identify the thread is output.
Transfer ID#	Transfer ID is output. However, it is not output to trace of first connection.
Direction of send and receive	Send and receive direction of protocol message is output. --->: when received from FTP client <---: when sent to FTP client
Protocol message	When character string of password which is argument of PASS command is output to the FTP protocol trace, "*****" is displayed instead of the character string of password.

Note#

You can understand the corresponding process thread (tid) from the record that outputs the transfer ID. You can refer the series of the FTP protocol trace for the transfer process by searching tid.

● **Output destination of FTP protocol trace**

```
<Working directory of J2EE server>\ejb\<J2EE server name>\logs\csc\inbound-
adapter\ftp\FTP_Inbound_Resource_Adapter
```

The following table describes the trace file name of FTP protocol trace:

Table 7–84: Table File name of FTP protocol trace (FTP inbound adapter)

Type of file	Trace file name
Current file	protocol.log
Backup file#	protocol<Count>.log

Note #

If the size of current file exceeds the size for each file, it is renamed to the backup file.

The number of backup files is included in the backup file name. The number increases for new log files. Once the log file is created, it cannot be deleted. Line feed code of file is "LF".

You can change <Working directory of J2EE server> in the ejb.public.directory key of usrconf.cfg (Option definition file for J2EE server). Default is <Installation directory of Service Platform>\CC\server\public. Note that you cannot change the output destination of the FTP protocol trace in the ejb.server.log.directory key. For details on usrconf.cfg, see "2.3usrconf.cfg(Option definition file for J2EE server) " in "Application Server Definition Reference Guide".

You can change the output level of the FTP protocol trace, file size, and number of files in the following properties of the connector property file that sets the property in the RAR file.

- server_protocol_logLevel= Output level of FTP protocol trace
- server_protocol_maxFileSize= File size of FTP protocol trace
- server_protocol_maxBackupIndex=Number of backup files

For details on procedure of setting, see "*3.2.3(3) Setting up the FTP inbound adapter*".

●**Example of output of FTP protocol trace**

Example of executing RETR command and output of FTP protocol trace when acquiring file from server is as follows:

```
2010/10/29 21:50:15.346    <pid>    <tid>                    ---> connection from
10.209.12.244
2010/10/29 21:50:15.346    <pid>    <tid> <Transfer ID>           ---> OPENED
2010/10/29 21:50:15.346    <pid>    <tid> <Transfer ID>           <--- 220 Service ready
for new user.
2010/10/29 21:50:15.346    <pid>    <tid> <Transfer ID>           ---> USER admin
2010/10/29 21:50:15.346    <pid>    <tid> <Transfer ID>           <--- 331 User name okay,
need password for admin.
2010/10/29 21:50:15.346    <pid>    <tid> <Transfer ID>           ---> PASS *****
2010/10/29 21:50:15.346    <pid>    <tid> <Transfer ID>           <--- 230 User logged in,
proceed.
2010/10/29 21:50:15.346    <pid>    <tid> <Transfer ID>           ---> TYPE A
2010/10/29 21:50:15.346    <pid>    <tid> <Transfer ID>           <--- 200 Command TYPE
okay.
2010/10/29 21:50:15.346    <pid>    <tid> <Transfer ID>           ---> PORT
10,209,12,244,17,28
2010/10/29 21:50:15.346    <pid>    <tid> <Transfer ID>           <--- 200 Command PORT
okay.
2010/10/29 21:50:15.346    <pid>    <tid> <Transfer ID>           ---> RETR /sample1/
hoge.txt
2010/10/29 21:50:15.361    <pid>    <tid> <Transfer ID>           <--- 150 Opening ASCII
mode data connection for /sample1/hoge.txt.
2010/10/29 21:50:15.533    <pid>    <tid> <Transfer ID>           <--- 226 Transfer
Complete.
2010/10/29 21:50:15.533    <pid>    <tid> <Transfer ID>           ---> QUIT
2010/10/29 21:50:15.533    <pid>    <tid> <Transfer ID>           <--- 221 Goodbye.
2010/10/29 21:50:15.533    <pid>    <tid> <Transfer ID>           ---> CLOSED
```

(d) Transfer history log (FTP inbound adapter)

In the transfer history log, the transfer history in FTP linkage system is output to following location:

```
<Working directory of J2EE server>\ejb\<J2EE server name>\logs\csc\inbound-
adapter\ftp\FTP_Inbound_Resource_Adapter
```

The following table describes the log file name of the transfer history log:

Table 7–85: Table File name of transfer history log (FTP inbound adapter)

Type of file	Log file name
Current file	history.log
Backup file#	history<Count>.log

Note#

If the size of current file exceeds the size for each file, it is renamed to the backup file.

The number of backup files is included in the backup file name. The number increases for new log files. Once the log file is created, it cannot be deleted. Line feed code of file is "LF".

You can change <Working directory of J2EE server> in the ejb.public.directory key of the usrconf.cfg (option definition file of J2EE server). Default is <Installation directory of Service Platform>\CC\server\public. Note that you cannot change the output destination of the transfer history log in the ejb.server.log.directory key. For details on usrconf.cfg, see "2.3 usrconf.cfg(Option definition file for J2EE server) " in "Application Server Definition Reference Guide".

Furthermore, you can change the output level of the transfer history log, file size, and number of files in the following properties of connector property file that sets the property in the RAR file.

- server_history_logLevel=output level of transfer history log
- server_history_maxFileSize= file size of transfer history log
- server_history_maxBackupIndex= number of backup files

For details on procedure for setting, see "*3.2.3(3) Setting up the FTP inbound adapter*".

(e) Common log between resource adapters (FTP inbound adapter)

The information regarding the process from the start of the FTP inbound adapter till the decision regarding the resource adapter name and the process of the network control and log output is output in the common log between resource adapters. The common log between the resource adapters of the FTP inbound adapter is described here.

●Output format of the common log between resource adapters and output contents

The common log between resource adapters is output as the message and maintenance information.

Output format

The output format of the common log between resource adapters is as follows:

- **For message**

```
<Date> <Time> <pid> <tid> <Transfer ID> <Message ID> <Message text>
```

- **For Maintenance information**

```
<Date> <Time> <pid> <tid> <Maintenance information>
```

Output contents

The following table list and describes output contents to the common log between resource adapters:

- **For message**

Table 7–86: Table Output contents to the common log between resource adapters (FTP inbound adapter) (For message)

Item	Contents
Date	The collection date of the common log between resource adapters is output in the yyyy/mm/dd format. • yyyy: Christian year • mm: Month • dd: Day
Time	The collection time of the common log between resource adapters is output in hh:mm:ss.SSS format.

Item	Contents
Time	• hh: Hour • mm: Minute • ss: Second • SSS: Millisecond
pid	The ID to identify the process is output.
tid	The ID to identify the thread is output.
Transfer ID	Transfer ID is output.
Message ID	Message ID is output
Message text	Content of the message is output.

- **For Maintenance information**

  Table 7–87: Table Output contents to the common log between resource adapters (FTP inbound adapter) (For maintenance information)

Items	Contents
Date	The collection date of the common log between resource adapters is output in yyyy/mm/dd format. • yyyy: Christian year • mm: Month • dd: Day
Time	The collection time of the common log between resource adapters is output in hh:mm:ss.SSS format. • hh: Hour • mm: Minute • ss: Second • SSS: Millisecond
pid	The ID to identify the process is output.
tid	The ID to identify the thread is output.
Maintenance information	Maintenance information required when you contact system administrator and maintenance service is output.

● Output destination of the common log between resource adapters

```
<Working directory of J2EE server>\ejb\<J2EE server name>\logs\csc\inbound-adapter\ftp\common
```

The following table describes the log file name of the common log between resource adapters:

Table 7–88: Table File name of the common log between resource adapters (FTP inbound adapter)

Type of file	Log file name
Current file	ftpd.log
Backup file#	ftpd<Count>.log

Note#

If the size of current file exceeds the size for each file, it is renamed to the backup file.

The number of backup files is included in the backup file name. The number increases for new log files. Once the log file is created, it cannot be deleted. Line feed code of file is "LF".

You can change <Working directory of J2EE server> in the ejb.public.directory key of usrconf.cfg (option definition file for J2EE server) Default is <Installation directory of Service platform>\CC\server\public. Note that you cannot change the output destination of the common log between resource adapters in the

ejb.server.log.directory key. For details on usrconf.cfg, see "2.3 usrconf.cfg (Option definition file for J2EE server) " in "Application Server Definition Reference Guide".

You can change the output level of the common log between resource adapters, file size and number of files in properties of the connector property file that sets property in RAR file.

- server_common_logLevel=Output level of the common log between resource adapters
- server_common_maxFileSize= File size of the common log between resource adapters
- server_common_maxBackupIndex= number of backup files

For details on procedure of settings, see "*3.2.3(3) Setting up the FTP inbound adapter*"

(f) Maintenance log when executing the operations command (FTP inbound adapter)

The log at the time of error occurrence is output to the maintenance log when you execute the operations command. This log is required when you contact maintenance service.

●Output destination of the maintenance log when executing operations command

```
<Installation directory of Service platform>\CSC\inbound-adapter\ftp\logs
\FTP_Inbound_Resource_Adapter
```

When you execute the operations command, to change the output destination of the log, specify the output destination directory after making the change in the environment variable (CSCFTP_CMD_LOG) with a full path. If a specified path does not exist, the directory is created when you execute the operations command. When an environment variable is not set or when null character is specified as the value of the environment variable, the default output destination is output.

Output destination of log when specifying environment variable CSCFTP_CMD_LOG

<Specified value of environment variable CSCFTP_CMD_LOG>\logs\FTP_Inbound_Resource_Adapter

The path that fulfills the following conditions can be specified in the environment variable (CSCFTP_CMD_LOG):

- "Path should not contain "//", "/./", or "/../"
- Use one-byte alphanumeric character, single byte space, file separator ("\" or "/") and ":".
- Length of the path must be128 bytes (128 single byte characters) or less

For Linux, when there is space in the directory path, you must to enclose the path with double quotation (").

Log file name of maintenance log when executing the operations command

The following table lists and describes log file names of the maintenance log when executing the operations command. Note that the maximum file size and maximum number of files of these maintenance logs are fixed and cannot be changed.

Table 7–89: Table File name of maintenance log when executing operations command (FTP inbound adapter)

File type	Log file name	Maximum file size	Maximum number of files
Message log	• Current file message.log • Backup file# message<Count>.log	5MB	7
Maintenance log	• Current file maintenance.log • Backup file# maintenance<Count>.log		
Common log	• Current file ftpd.log • Backup file# ftpd<Count>.log		

Note#

If the size of current file exceeds the size for each file, it is renamed to the backup file.

The number of backup files is included in the backup file name. The number increases for new log files. Once the log file is created, it cannot be deleted. Line feed code of file is "LF".

(g) Performance analysis trace (FTP inbound adapter)

The performance analysis trace in the FTP inbound adapter is described here.

●Output format of performance analysis trace

The format output in the performance analysis trace is same as the performance analysis trace of the J2EE server. For details, see "7. Performance Analysis Using the Performance Analysis Trace" in "Application Server Maintenance and Migration Guide".

●Output contents

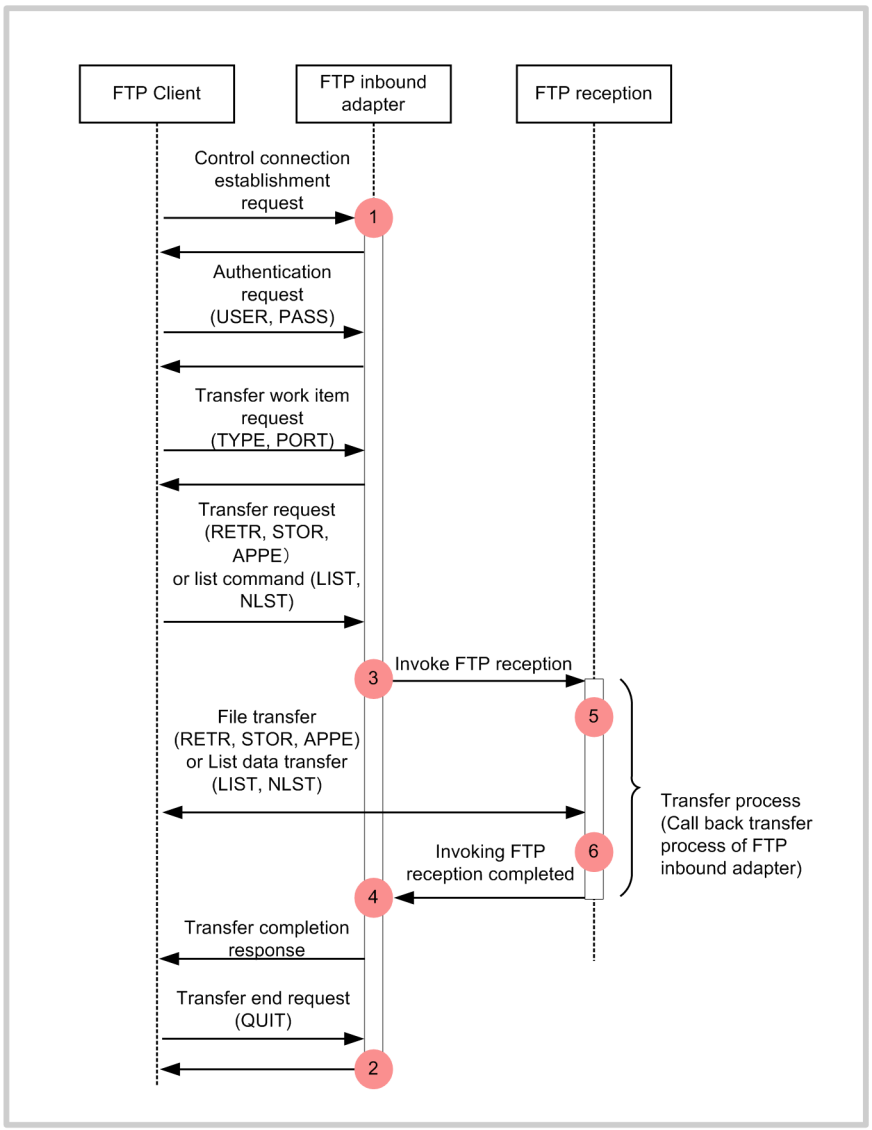
The following table lists and describes contents output to the performance analysis trace file:

Table 7–90: Table Contents output to the Performance analysis trace file (FTP inbound adapter)

Item	Contents
Event ID	The Event ID of collection point is output. For details on the collection point, see "*Performance analysis trace collection point*".
Return code	The type of the collection point is output. • 0:Normal end • 1:Abnormal end
Interface name	Class name is output.
Operation name	Method name is output.
Option information	Maintenance information is output. In some cases, collection point is not used to perform output.

●Performance analysis trace collection point

Figure 7–89: Figure Performance analysis trace collection point (FTP inbound adapter)



Legend:

: Indicates trace collection point (Performance analysis trace collection level is "Standard")

The following table lists the event ID, trace collection point, and the performance analysis trace collection level. The numbers in the *Number in figure* column of the table correspond to the numbers in the above figure.

Table 7–91: Table Performance analysis trace collection point (FTP inbound adapter)

Event ID	Number in figure	Trace collection point	Level
0x9950	1	Location where a new request is received from FTP client	A
0x9951	2	Location wherein series of requests from FTP client are completed and session ends	A
0x9952	3	Prior to the location where a transfer request is received, and request for sorting to FTP reception is done	A
0x9953	4	After the location where a transfer request is received, and request for sorting to FTP reception is done	A

Event ID	Number in figure	Trace collection point	Level
0x9954	5	Location before the transfer process is executed in FTP reception	A
0x9956		Location before the list data transfer process is executed in FTP reception	A
0x9955	6	Location after the transfer process is executed in FTP reception	A
0x9957		Location after the list data transfer process is executed in FTP reception	A

Legend:

A: Indicates the "Standard" level.

●How to acquire performance analysis trace and output destination

Settings are required to acquire performance analysis trace. For details on settings, see "7.Performance Analysis Using the Performance Analysis Trace " in "Application Server Maintenance and Migration Guide".

(2) Acquiring the failure information (FTP adapter)

The failure information of the FTP adapter can be classified as follows:

- Message log
- Maintenance log
- Performance analysis trace
- FTP protocol trace
- Exception log
- FTP command message log

The following is the description of the above mentioned failure information:

(a) Message log (FTP adapter)

For details on the message log, see "*7.4.1 Message log*".

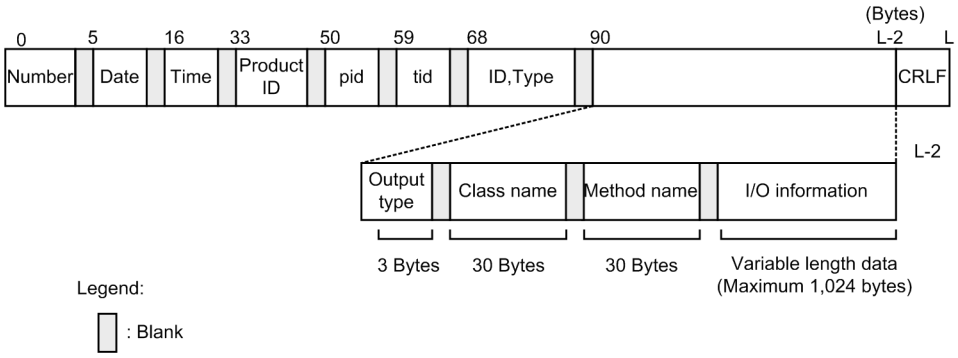
(b) Maintenance log (FTP adapter)

The maintenance log of the FTP adapter is described here.

● Output format of Maintenance log

The following figure shows the output format of the maintenance log:

Figure 7–90: Figure Output format of Maintenance log (FTP adapter)



●Output contents to be output

The following table lists and describes the contents output to the Maintenance log:

Table 7–92: Table Contents output to the Maintenance log (FTP adapter)

Item	Contents
Number	The output serial number of the Maintenance log is output.
Date	Collection date of maintenance log is output in yyyy/mm/dd format. • yyyy: Christian year • mm: Month • dd: Day
Time	The collection time of the Maintenance log is output in hh:mm:ss.SSS format. • hh: Hour • mm: Minute • ss: Second • SSS: Millisecond
Product ID	"FTPADP" indicating the FTP adapter is output as the identifier used for identifying the product. Version information is output.
pid	The ID to identify the process is output.
tid	The ID to identify the thread is output.
ID,type	Not displayed.
Output type	Collection point information of the Maintenance log (Collection location) is output. • BGN: Start method • END: End method • CAL: Invoke method • RET: Return method • THR: Throw exception • CTH: Catch exception
Class name	Class name to acquire Maintenance log is output.
Method name	Method name to acquire Maintenance log is output.
I/O information	I/O information of the method to acquire the Maintenance log (value of argument, return value, and exception name) is output.
CRLF	Record end code is output.

●Output destination of maintenance log

```
<Path specified in ftpadp.methodtrace.filepath property of FTP-adapter
runtime-environment property file>\<Service ID>
```

The following table describes the log file name of the maintenance log:

Table 7–93: Table File name of maintenance log (FTP adapter)

Output mode of log file	Log file name
For Wraparound mode	cscftpadpmtd_<HCSC server name>_<Count>.log
For shift mode	cscftpadpmtd_<HCSC server name>_.log

Specify the number of log files in the ftpadp.methodtrace.filenum property of the FTP-adapter runtime-environment property file. Specify the log file size in the ftpadp.methodtrace.filesize property of the FTP-adapter runtime-environment property file.

For details on the FTP-adapter runtime-environment property file, see "FTP-adapter runtime-environment property file" in "Service Platform Reference Guide".

(c) Performance analysis trace (FTP adapter)

The performance analysis trace of the FTP adapter is described here.

● Output format of Performance analysis trace

The format output in the performance analysis trace file is same as the performance analysis trace of the J2EE server. For details, see "7. Performance Analysis Using the Performance Analysis Trace" in "Application Server Maintenance and Migration Guide".

●Output contents

The following table lists and describes contents output to the performance analysis trace file:

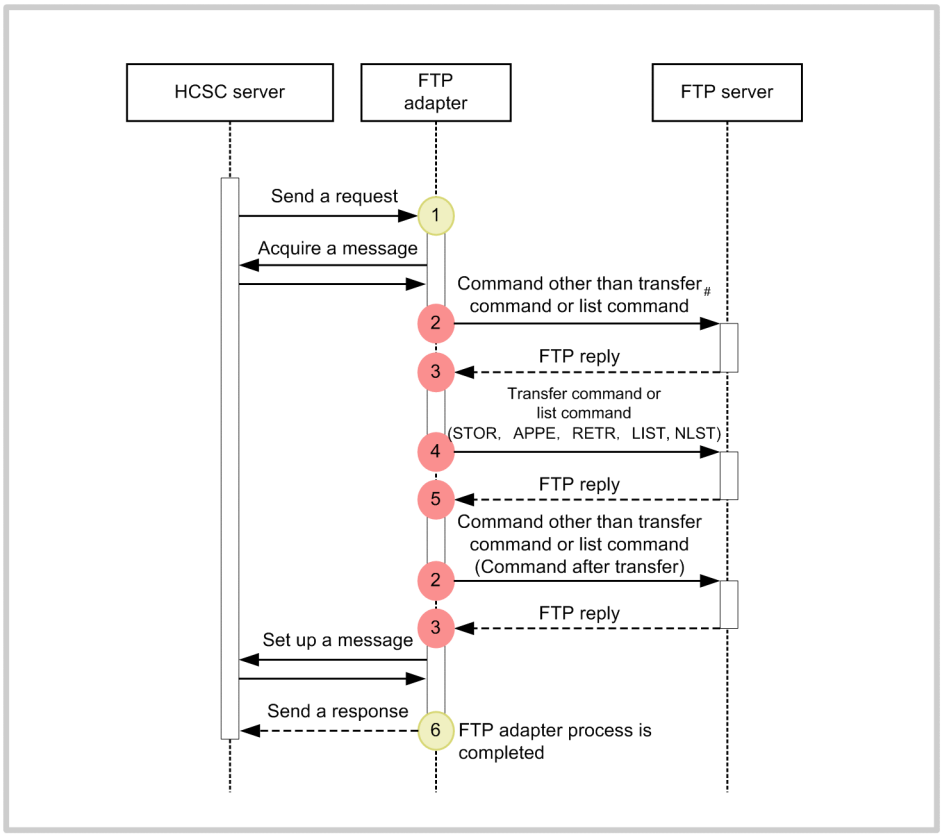
Table 7–94: Table Contents output to performance analysis trace file (FTP adapter)

Item		Contents
Event ID		The Event ID of the collection point is output. For details on the collection point, see the item "*Performance analysis trace collection point*".
Return code		The type of the collection point is output. • 0:Normal end • 1:Abnormal end
Interface name		Class name is output.
Operation name		Method name is output.
Option information	Service ID	Service ID of HCSC components is output
	Operation	Any of the following is output: • PUT • GET • GETINFO
	FTP command name	STOR, APPE, RETR, LIST, NLST, TYPE are output.
	Transfer file name or path	Local file name is output when the FTP command name is STOR or APPE. Remote file name is output when the FTP command name is RETR. Remote path is output when the FTP command name is LIST or NLST.
	Transfer size	Size of the transfer file and the list data is output in bytes.
	Nano seconds from any time	Return value of nano time method of java.lang.System class is output.
	Exception class name	Class name when exception occurred is output.

●Performance analysis trace collection point

The following figure shows the performance analysis trace collection point:

Figure 7–91: Figure Performance analysis trace collection point (FTP adapter)



Legend:

: Indicates trace collection point (Performance analysis trace collection level is "Standard")

: Indicates trace collection point (Performance analysis trace collection level is "Detailed")

#
It indicates USER/ PASS authentication, TYPE/Mode of transfer settings, SITE FSIZE, MDTM/SIZE/STST before transfer command.

The following table lists and describes the event ID, trace collection point, and performance analysis trace collection level. The numbers in the *Number in figure* column of the table correspond to the numbers in the above figure.

Table 7–95: Table Performance analysis trace collection point (FTP adapter)

Event ID	Number in figure	Trace collection point	Level
0xAB00	1	At the time of request reception	B
0xAB02	2	When executing FTP commands other than transfer or list	A
0xAB03	3	When replying to an FTP command other than transfer or list	A
0xAB04	4	When executing a transfer command or a list command (STOR, APPE, RETR, LIST, or NLST)	A
0xAB05	5	When replying to a transfer command or a list command (STOR, APPE, RETR, LIST, or NLST)	A
0xAB01	6	When sending a response	B

Legend:
A: Indicates the "Standard" level.

B: Indicates the "Detailed" level.

●How to acquire performance analysis trace collection and output destination

Settings are required to acquire performance analysis trace. For details on settings, see "7. Performance Analysis Using the Performance Analysis Trace" in "Application Server Maintenance and Migration Guide".

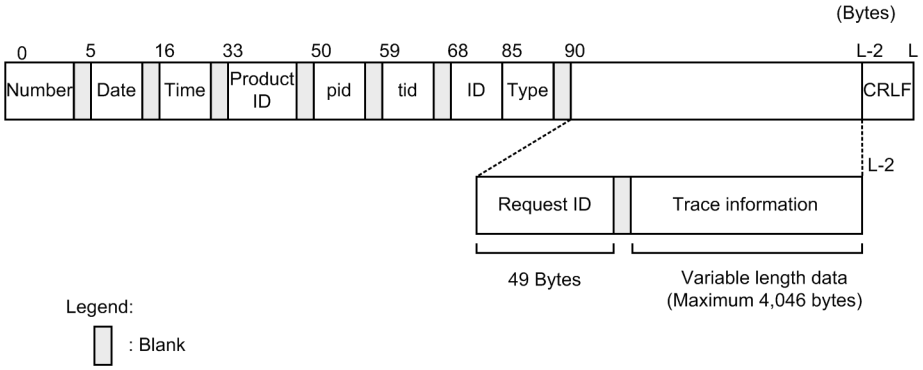
(d) FTP protocol trace (FTP adapter)

The protocol trace of the FTP adapter is described here.

●Output format of FTP protocol trace

The following figure shows the output format of the FTP protocol trace:

Figure 7–92: FigureOutput format of FTP protocol trace (FTP adapter)



●Output contents

The following table lists and describes the contents output in the FTP protocol trace:

Table 7–96: TableContents output in the FTP protocol trace (FTP adapter)

Item	Contents
Number	The output serial number of the FTP protocol trace is output.
Date	The collection date of the FTP protocol trace is output in the yyyy/mm/dd format. • yyyy: Christian year • mm: Month • dd: Day
Time	The collection time of the FTP protocol trace is output in hh:mm:ss.SSS format. • hh: Hour • mm: Minute • ss: Second • SSS: Millisecond
Product ID	"FTPADP" indicating the FTP adapter is output as the identifier used for identifying the product.
pid	The ID to identify the process is output.
tid	The ID to identify the thread is output.
ID	Not output.
Type	FTP protocol trace type is output: • CMD: Command execution • REP: Response row
Request ID	The request ID created on reception is output. If you are using a common folder, "****" will be output since the request ID does not exist.

Item	Contents
Trace information	If the type is CMD, FTP command name is output. If the type is REP, the command message is output.
CRLF	Record end code is output.

●Output destination of the FTP protocol trace

```
<value specified in the ejb.public.directory key of usrconf.cfg (option
definition file for J2EE server)>\ejb\<J2EE server name>\logs\CSCADP\FTPADP
\<Service ID>
```

The following table lists trace file names of the FTP protocol trace:

Table 7–97: Table Trace file names of the FTP protocol trace (FTP adapter)

Output mode of trace file	Trace file name
For Wraparound mode	ftpprotocoltrace_<number of files>.log
For Shift mode	ftpprotocoltrace_.log

For details on usrconf.cfg, see "2.3 usrconf.cfg (option definition file for J2EE server) " in "Application Server Definition Reference".

Specify the number of log files with the ftpadp.ftpprotocoltrace.filenum property of the FTP-adapter runtime-environment property file. Specify the log file size with the ftpadp.ftpprotocoltrace.filesize property of the FTP-adapter runtime-environment property file.

For details, see "FTP-adapter runtime-environment property file" in "Service Platform Reference Guide".

●Output example of FTP protocol trace

The following is an output example of the FTP protocol trace in the FTP adapter:

```
CMD RCP01---0102000300000420100602144121012000/HCSC Connected to 10.208.180.254.
REP RCP01---0102000300000420100602144121012000/HCSC 220 (vsFTPd 2.0.1)
CMD RCP01---0102000300000420100602144121012000/HCSC USER user1
REP RCP01---0102000300000420100602144121012000/HCSC 331 Please specify the password.
CMD RCP01---0102000300000420100602144121012000/HCSC PASS ********
REP RCP01---0102000300000420100602144121012000/HCSC 230 Login successful.
CMD RCP01---0102000300000420100602144121012000/HCSC TYPE I
REP RCP01---0102000300000420100602144121012000/HCSC 200 Switching to Binary mode.
CMD RCP01---0102000300000420100602144121012000/HCSC PORT 10,210,182,27,8,173
REP RCP01---0102000300000420100602144121012000/HCSC 200 PORT command successful. Consider
using PASV.
CMD RCP01---0102000300000420100602144121012000/HCSC STOR test.txt
REP RCP01---0102000300000420100602144121012000/HCSC 150 Ok to send data.
REP RCP01---0102000300000420100602144121012000/HCSC 226 File receive OK.
CMD RCP01---0102000300000420100602144121012000/HCSC QUIT
REP RCP01---0102000300000420100602144121012000/HCSC 221 Goodbye.
```

(e) Exception log (FTP adapter)

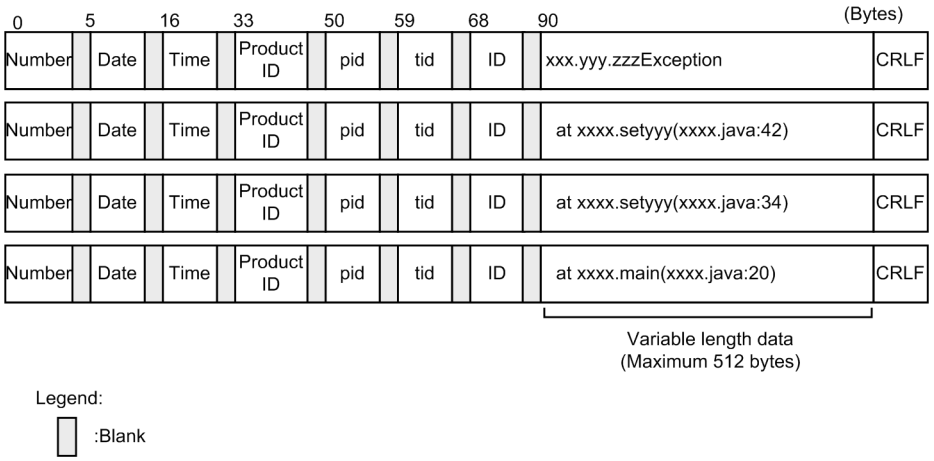
The exception information that has occurred after the start of the trace (stack trace) is output to a different file as an exception log. In the exception log, you can set the size and numbers of the output file without setting the path and output level of the output file,. In addition, the exception log file will be output to the same directory as the Maintenance log

The exception logs of the FTP adapter are described here:

●Output format of Exception log

The following figure shows the output format of the Exception log:

Figure 7–93: FigureOutput format of the Exception log (FTP adapter)



●Output contents

The following table lists and describes the contents output in the exception log:

Table 7–98: Table Contents output in the exception log (FTP adapter)

Item	Contents
Number	The output serial number of the Exception log is displayed.
Date	The collection date of the Exception log is output in the yyyy/mm/dd format. • yyyy: Christian year • mm: Month • dd: Day
Time	The collection time of the Exception log is output in hh:mm:ss.SSS format. • hh: Hour • mm: Minute • ss: Second • SSS: Millisecond
Product ID	"FTPADP" indicating the FTP adapter is output as the identifier used for identifying the product.
pid	The ID to identify the process is output.
tid	The ID to identify the thread is output.
ID	Blank
Stack trace information	Stack trace information is output.
CRLF	Record end code is output.

●Output destination of Exception log

The following is the output destination of Exception log. The path is same as Maintenance log.

```
< Path specified in the ftpadp.methodtrace.filepath property of the FTP-
adapter runtime-environment property file>\<Service ID>
```

The following table lists the log file names of the Exception log:

Table 7–99: Table Log file names of the Exception log (FTP adapter)

Output mode of log file	Log file name
For Wraparound mode	cscftpadpexp_<HCSC server name>_<number of files>.log

Output mode of log file	Log file name
For Shift mode	cscftpadpexp_<HCSC server name>_.log

Specify the log file number with the ftpadp.exptrace.filenum property of the FTP-adapter runtime-environment property file. Specify the log file size, with the ftpadp.exptrace.filesize of the FTP-adapter runtime-environment property file.

For details on the FTP-adapter runtime-environment property file, see"FTP-adapter runtime-environment property file" in "Service Platform Reference Guide".

(f) Command message log (FTP adapter)

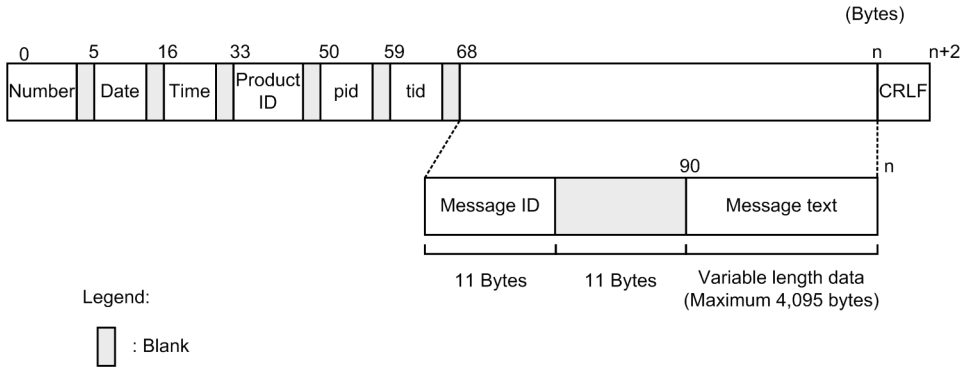
The command message log of the FTP adapter is described here.

The information at the time of starting and stopping the user management commands of the FTP adapter, error messages when a failure occurs during command execution is output to the command message log as a log file. By referencing the command message log, you can check the failure information and the running information of the command that was executed in the past.

●Output format of the Command message log

The following figure shows the output format of the Command message log:

Figure 7–94: FigureOutput format of the Command message log (FTP adapter)



●Output contents

The following table lists and describes the contents output to the Command message log:

Table 7–100: Table Contents output to the Command message log (FTP adapter)

Item	Contents
Number	The output serial number of the Command message log is displayed.
Date	The collection date of the Command message log is output in the yyyy/mm/dd format. • yyyy: Christian year • mm: Month • dd: Day
Time	The collection time of the Command message log is output in hh:mm:ss.SSS format. • hh: Hour • mm: Minute • ss: Second • SSS: Millisecond
Product ID	"add","del", or "ls" indicating the name of executed command is output after "FTPADP" indicating the FTP adapter is output as the identifier used for identifying the product. • FTPADP:add • FTPADP:del

Item	Contents
Product ID	• FTPADP:ls
pid	The ID to identify the process is output.
tid	The ID to identify the thread is output.
Message ID	Message ID is output in the "KDEKnnnnn-X" format.
Message text	Content of the message is output.
CRLF	Record end code is output.

●Output destination of the Command message log

The following table lists and describes the output destination and log file name of the Command message log:

```
< Path specified in the ftpadp.command.messagelog.filepath key of the FTP
adapter command definition file>\message<number of files>.log
```

Specify the number of log files with ftpadp.command.messagelog.filenum key of the FTP adapter command definition file. Specify the log file size, with the ftpadp.command.messagelog.filesize key of the FTP adapter command definition file.

(3) Acquiring failure information (file operations adapter)

The failure information of the file operations adapter can be classified as follows:

- Message log
- Maintenance log
- Performance analysis trace
- Exception log

The types of failure information are described here.

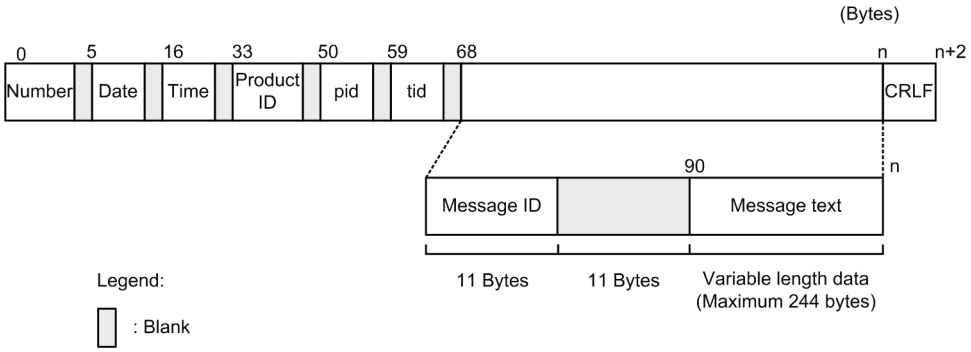
(a) Message log (file operations adapter)

The message log of the file operations adapter is described here.

●Output format of Message log

The following figure shows the output format of the Message log:

Figure 7–95: FigureOutput format of Message log (file operations adapter)



●Output contents

The following table lists and describes the contents output to the Message log:

Table 7–101: TableContents output to the Message log (file operations adapter)

Item	Contents
Number	The output serial number of the Message log is displayed.

Item	Contents
Date	The collection date of the Message log is output in the yyyy/mm/dd format. • yyyy: Christian year • mm: Month • dd: Day
Time	The collection time of the Message log is output in hh:mm:ss.SSS format. • hh: Hour • mm: Minute • ss: Second • SSS: Millisecond
Product ID	"HEJB" indicating Component Container is output as the identifier used for identifying the product.
pid	The ID to identify the process is output.
tid	The ID to identify the thread is output.
Message ID	Message ID is output in the "KDECnnnnn-X" format.
Message text	Content of the message is output.
CRLF	Record end code is output.

●Output destination of the Message log

The message log is output to the path specified in the output destination of the activity log of the J2EE server.

Specify the output destination of the activity log of the J2EE server with the ejb.server.log.directory key of usrconf.cfg (option definition file for J2EE server).The default output destination is <Installation directory of Service Platform>\CC\server\public\ejb\<J2EE server name>\logs. For details on usrconf.cfg, see " 2.3 usrconf.cfg (option definition file for J2EE server) " in "Application Server Definition Reference".

The following table lists the Log file name of the Message log:

Table 7–102: Table Log file name of Message log (file operations adapter)

Output mode of log file	Log file name
For Wraparound mode	cjmessage<number of files>.log
For Shift mode	cjmessage.log

Specify the number of log files with the ejbserver.logger.channels.define.<channel name>.filenum key of the user property file (usrconf.properties) for the J2EE server that is operating on the HCSC server. Specify the log file size with the ejbserver.logger.channels.define.<channel name>.filesize key of the user property file (usrconf.properties) for the J2EE server that is operating on the HCSC server.

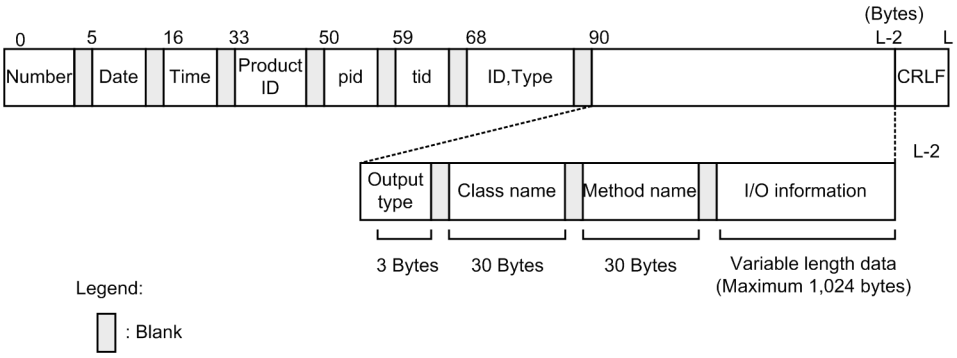
(b) Maintenance log(file operations adapter)

The maintenance log of the file operations adapter is described here.

●Output format of Maintenance log

The following figure shows the output format of the maintenance log:

Figure 7–96: FigureOutput format of Maintenance log (File operations adapter)



●Output contents

The following table lists and describes the contents output to the Maintenance log:

Table 7–103: TableContents output to the Maintenance log (File operations adapter)

Item	Contents
Number	The output serial number of the Maintenance log is output.
Date	The collection date of the Maintenance log is output in the (yyyy/mm/dd format). • yyyy: Christian year • mm: Month • dd: Day
Time	The collection time of the Maintenance log is output in hh:mm:ss.SSS format. • hh: Hour • mm: Minute • ss: Second • SSS: Millisecond
Product ID	"FOPADP" indicating the File operations adapter is output as the identifier used for identifying the product. Also, the version information is output.
pid	The ID to identify the process is output.
tid	The ID to identify the thread is output.
ID, Type	Not displayed.
Type of output	Collection point information of the Maintenance log (Collection location) is output. • BGN: Start Method • END: End Method • CAL: Invoke method • RET: Return method • THR: Throw exception • CTH: Catch exception
Class name	Class name to acquire Maintenance log is output.
Method name	Method name to acquire Maintenance log is output.
Input output information#	Input and output information of the method to acquire the Maintenance log (value of argument, return value, and exception name) is output.
CRLF	Record end code is output.

Note#

- At the time of starting the file conversion operation
  The information is output in the following format:
  <Input file path> , file type = < Input file format> , file size = < Input file size>
  The following table describes the meaning of each item:

Information to be added	Description
<Path of Input file>	Absolute path of the Input file
<Input file format>	For binary format: non-xml For XML format: xml
<Input file size>	Output in bytes

- At the time of completion of the output of file conversion operation
- The information is output in the following format:
  <Path of Output file> , file type = <Output file format> , file size = <Output filesize> , record count = <Number of input records>
  The following table describes the meaning of each item:

Information to be added	Description
<Path of Output file>	Absolute path of the Output file
<Output file format>	For binary format:non-xml For XML format: xml
<Output file size>	Output in bytes
<Number of input records>	For segmentation method: Outputs the input records For batch processing method: Normally outputs "-1"

●Output destination of Maintenance log

```
<Log output directory of J2EE server>\CSCADP\ADPFOP\maintenance\<Service ID
of File operations adapter>
```

The following table lists Log file name of the Maintenance log:

Table 7–104: TableLog file name of Maintenance log(File operations adapter)

Output mode of log file	Log file name
For Wraparound mode	cscadpfopmnt_<HCSC server name>_<number of files>.log
For Shift mode	cscadpfopmnt_<HCSC server name>_.log

Specify the number of log files with the methodtrace-filenum property of the HCSC server runtime definition file.
Specify the log file size with the methodtrace-filesize property of the HCSC server runtime definition file.

For details on the HCSC server runtime definition file, see "HCSC server runtime definition file" in "Service Platform Reference Guide".

(c) Performance analysis trace(file operations adapter)

The performance analysis trace of the file operations adapter is described here.

●Output format of Performance analysis trace

The format output in the performance analysis trace file is same as the performance analysis trace of J2EEserver. For details, see "7. Performance Analysis Using the Performance Analysis Trace" in "Application Server Maintenance and Migration Guide".

●Output contents

The following table lists and describes contents output to the performance analysis trace file.

Table 7–105: TableContents output to the Performance analysis trace file (File operations adapter)

Item		Contents
Event ID		The Event ID of the collection point is output. For details on the collection point, seethe item "*Performance analysis trace collection point*".
Return code		The type of the collection point is output. • 0:Normal end • 1:Abnormal end
Interface name		Class name is output.
Operation name		Method name is output.
Additional information	Data (Hexadecimal format)	The information (hexadecimal format) that differs for each collection point is output. Data in excess of 512 characters is truncated.
	Data (ASCII format)#	Contents of Data (Hexadecimal format) are output in the ASCII format. Data in excess of 512 characters is truncated.

Note#

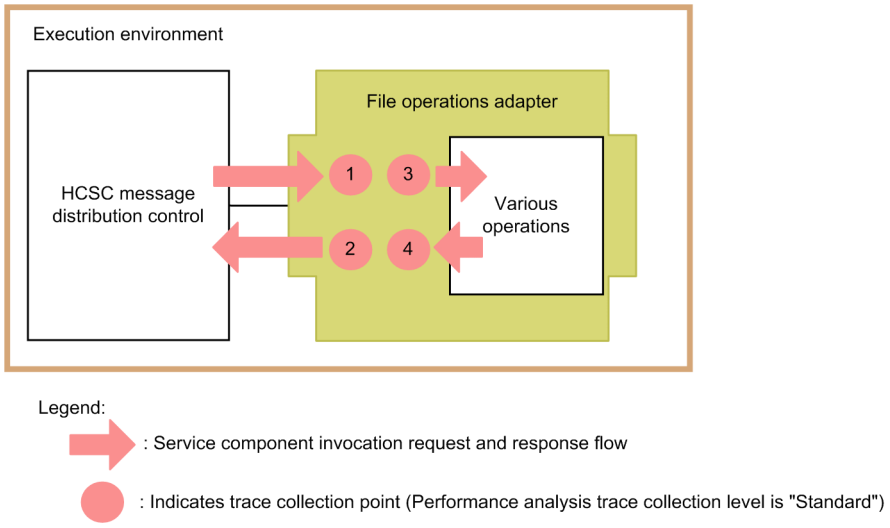
The example of the output format of Data (ASCII format) is as follows:

```
Service ID=<Service ID>, Operation Name=<Service operation name>, Time=<Nano seconds from
any time>, Exception=<Exception class name>
```

●Performance analysis trace collection point

The following figure shows the performance analysis trace collection point:

Figure 7–97: FigurePerformance analysis trace collection point(file operations adapter)



The following table lists the event ID, trace collection point, and the performance analysis trace collection level. The numbers in the *Number in figure* column of the table correspond to the numbers in the above figure.

Table 7–106: TablePerformance analysis trace collection point(File operations adapter)

Event ID	Number in Figure	Trace collection point	Level
0x9B80	1	Entry to File operations adapter	A
0x9B81	2	Exit from File operations adapter	A
0x9B82	3	Invocation of the operations of file operations adapter	A
0x9B83	4	Point of receiving the results of the operations of file operations adapter	A

Legend:

A:Indicates the "Standard" level.

●How to acquire Performance analysis trace and output destination

Settings are required to acquire performance analysis trace. For details on settings, see "7. Performance Analysis Using the Performance Analysis Trace" in "Application Server Maintenance and Migration Guide".

(d) Exception log(File operations adapter)

Exception information is output to the exception log. For the overview of the exception log, see "*7.4.5(1) Exception log*".The output contents of the exception log are same as the Maintenance log.

●Output destination

The output destination of the exception log is as follows:

```
<Log output directory of J2EE server >\CSCADP\ADPFOP\maintenance\<Service
ID of File operations adapter>
```

The following table lists the log file names of the Exception log:。

Table 7–107: TableLog file name of the Exception log(File operations adapter)

Output mode of log file	Log file name
For Wraparound mode	cscadpfopexp_<HCSC server name>_<number of files>.log
For Shift mode	cscadpfopexp_<HCSC server name>_.log

●Number of files

The default number of files of the output file is 8. You can change the number of files with the exptrace-filenum key of the File operations adapter runtime-environment property file. Specify the size of the log file with the exptrace-filesize property of the File operations adapter runtime-environment property file.

For details on the File operations adapter runtime-environment property file, see " File operations adapter runtime-environment property" in "Service Platform Reference Guide".

(4) Acquiring the failure information (FTP reception)

Performance analysis trace is output in the FTP reception as the failure information.

The method to notify an error that has occurred at the time of executing FTP reception and performance analysis trace is described here:

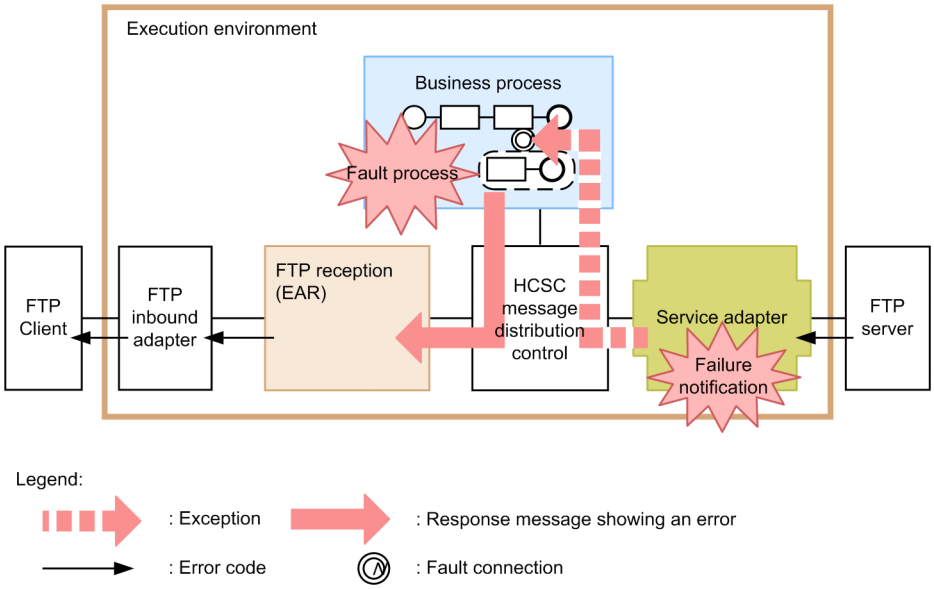
(a) Method to notify an error that has occurred at the time of executing FTP reception

The method to notify the error when you invoke the business process using the FTP reception from the FTP client is described here. Note that the method of notification depends on the type of error.

When the response message indicating an error in the FTP reception is returned

The following figure shows the method to notify an error when the response message indicating an error in the FTP reception is returned:

Figure 7–98: Figure Method to notify an error when the response message indicating an error in the FTP reception is returned



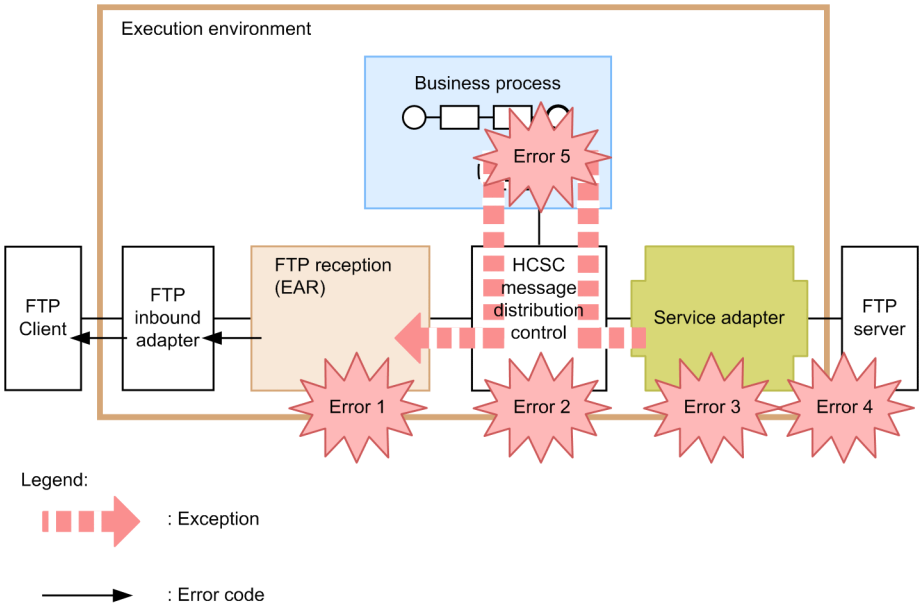
The fault message returned from the service adapter is notified to the fault processing of business processes. In the fault processing of business processes, the error information is converted to a response message (response message that was set to false in the <success> tag of response message) ,and is returned to the FTP reception. At this time, the response message indicating the error is returned to the FTP reception via the message delivery infrastructure and custom reception framework.

In the FTP reception, the message text set in the response message is returned as-is to the FTP inbound adapter. In the FTP inbound adapter, the received message text responds to the FTP client as the transfer command of FTP or response of the list command.

When the custom reception framework returns an error

The following figure shows the method to notify an error when the custom reception framework returns an error. Note that when a fault message is returned from a service adapter that is invoked from the business process, even if the fault process corresponding to this fault is not defined in the business process, the flow will be same as the flow shown in the following figure.

Figure 7–99: FigureMethod to notify an error when the custom reception framework returns an error



The causes for the occurrence of Error 1~ Error 5 shown in Figure 7-117 are as follows:

- Error 1:Invalid request parameter
- Error 2: Address (Location) not found, service adapter has stopped
- Error 3:Data transformation failed
- Error 4:Invalid address, Service component has stopped, Communication failure
- Error 5:Exception error in processing the business process

When any of the errors mentioned in Error 1~ Error 5 occur, the custom reception framework that has caught the exception throws CSCMsgServerException to the reception processing of the FTP reception.

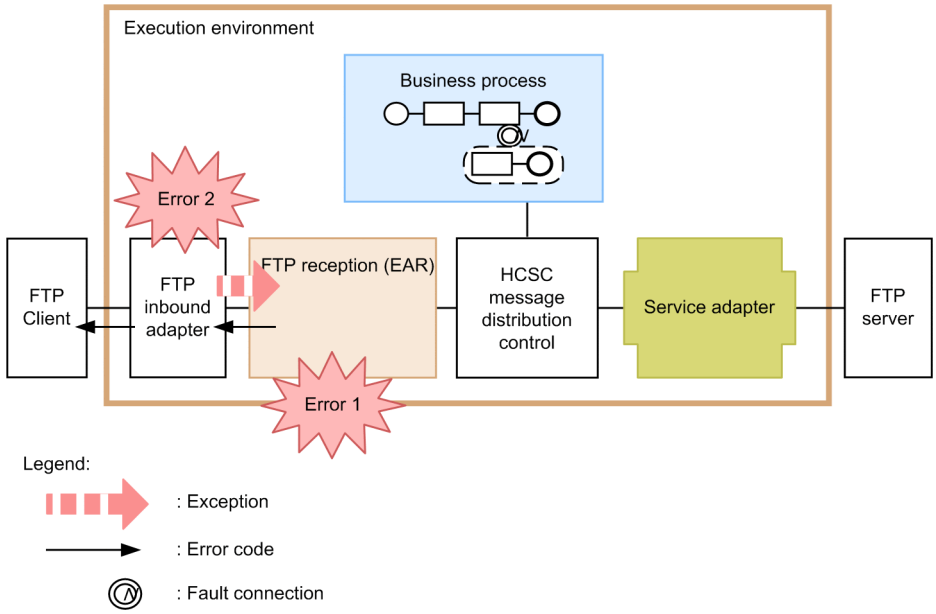
In the reception processing of the FTP reception, a message text of KDEC00386-E~KDEC00410-W is generated on the basis of the caught exception, and a response is sent to the inbound FTP adapter. In the FTP inbound adapter, the received message text is sent as a response of the transfer command or the list command of FTP to the FTP client.

For details on CSCMsgServerException, see "AppendixA.3 APIs of the custom adapter development framework" in "Service Platform Reception and Adapter Definition Guide".

When the FTP reception detects an error

The following figure shows the method to notify an error when the FTP reception detects an error:

Figure 7–100: Figure Method to notify an error when the FTP reception detects an error



The causes for the occurrence of Error 1 and Error 2 shown in the Figure 7-118 are as follows:

- Error 1:Failure in creation of working folder
- Error 2: Occurrence of failure during the transfer of file data or list data in the FTP inbound adapter

In the FTP reception, the message text of KDEC00386-E~KDEC00410-W is generated on the basis of the detected failure, and a response is sent to the inbound FTP adapter. In the FTP inbound adapter, the received message text is sent as a response of the transfer command or list command of FTP to the FTP client.

(b) Performance analysis trace (FTP reception)

The performance analysis trace in the FTP reception is described here:

●Output format of Performance analysis trace

The format that is output to the performance analysis trace file is same as the performance analysis trace of the J2EE server. For details, see "7. Performance Analysis Using the Performance Analysis Trace" in "Application Server Maintenance and Migration Guide".

●Output contents

The following table lists and describes contents output to the performance analysis trace file:

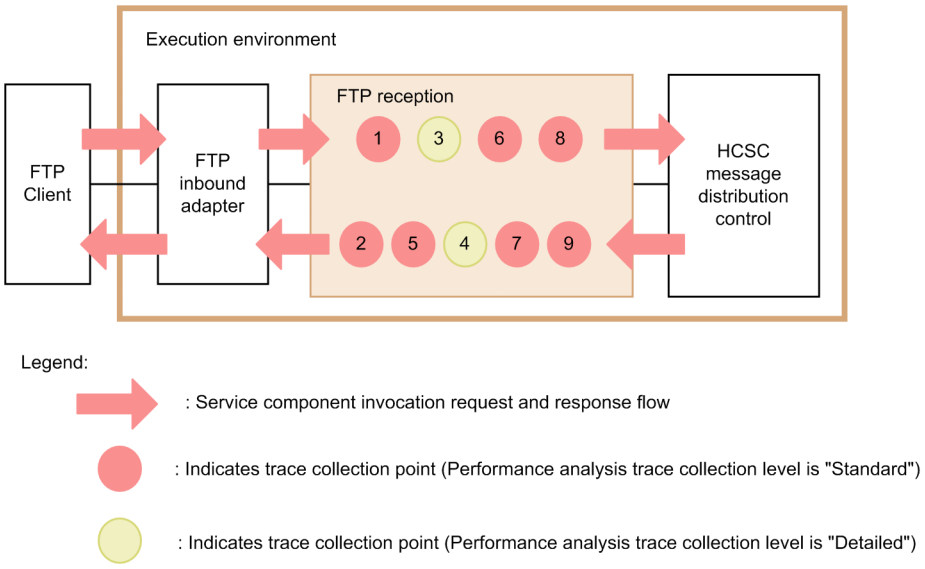
Table 7–108: TableContents output to the Performance analysis trace file (FTP reception)

Item	Content
Event ID	The Event ID of the collection point is output. For details on the collection point, see the item "Performance analysis trace collection point"
Return code	The type of the collection point is output. • 0:Normal end • 1:Abnormal end
Interface name	Class name is output.
Operation name	Method name is output.
Option information	The following option information is output: • Reception name • Reception ID • Request ID • Service name • Service operation name • Exception name (only at the time of failure occurrence)

●Performance analysis trace collection point

The following figure shows the performance analysis trace collection point:

Figure 7–101: FigurePerformance analysis trace collection point (FTP reception)



The following table lists the event ID, trace collection point, and the performance analysis trace collection level. The numbers in the *Number in figure* column of the table correspond to the numbers in the above figure.

Table 7–109: TablePerformance analysis trace collection point (FTP reception)

Event ID	Number in Figure	Trace collection point	Level
0x9870	1	Entry to custom reception	A
0x9871	2	Exit from custom reception	A
0x9872	3	Invocation of custom reception framework	B
0x9873	4	Point for receiving response of custom reception framework	B

Event ID	Number in Figure	Trace collection point	Level
0x9874	5	For PUT operation After invoking business process and before deleting working directory For GET operation After transferring file data to FTP client and before deleting working directory For GETINFO operation After transferring list data to FTP client and deleting working directory	A
0x9860	6	Entry to custom reception framework	A
0x9861	7	Exit from custom reception framework	A
0x9864	8	Invocation of HCSC message delivery control	A
0x9865	9	Point for receiving response of HCSC message delivery control	A

Legend:

A: Indicates the "Standard" level.

B: Indicates the "Detailed" level.

●How to acquire Performance analysis trace and output destination

Settings are required to acquire performance analysis trace. For details on settings, see "7. Performance Analysis Using the Performance Analysis Trace" in "Application Server Maintenance and Migration Guide".

7.7.12 Troubleshooting when executing the mail adapter

In mail adapter, the information to verify system performance and analyze the cause of failure is output in log file or trace file. The following table describes the types of logs and traces which are generated in mail adapter:

Table 7–110: Table Types of logs and traces (in mail adapter)

Logs and traces	Output information	Description
Message log	All kinds of information generated in mail adapter is output as messages.	You can check operating information (Start, Stop and Failure) as messages. Note that the output destination of message logs is common for Application Server and entire Service Platform and therefore, you can check system operating status in a batch.
Maintenance log	The following information is output as the maintenance information of internal mail adapter. • Date • Time • Execution class name • Internal method name • Exception that occurred • Information of the specified argument	You can check the time of issuance and sequence of internal method.
Performance analysis trace	The following information is output at the performance analysis trace collection point of the entire Service Platform system. • Date • Time • Request information	Based on the performance analysis information which is output from a series of processes, right from receiving request from service requester to returning the execution result, you can check the performance of Service Platform system.

Logs and traces	Output information	Description
Performance analysis trace	• Trace collection source information At the performance analysis trace collection point of mail adapter, mail adapter specific information is output.	Based on the performance analysis information which is output from a series of processes, right from receiving request from service requester to returning the execution result, you can check the performance of Service Platform system.
Exception log	Information of exception which occurred in mail adapter (stack trace) is output.	You can check the information of exceptions in mail adapter. You can use it to analyze the cause of failure.
Command message log	All kinds of information which is generated at the time of executing mail adapter commands, is output.	You can check the information that is generated during the start, stop and when an error occurs at the time of executing mail adapter command.

The following table shows the mail information which is output to message log, maintenance log and performance analysis trace.

Table 7–111: Table Mail information output to log and trace

Classification	Item	Message log	Maintenance log			Performance analysis trace
			Output level 3 and below	Output level 4	Output level 5	
Server information	Host name of mail server	Y	Y	Y	Y	Y
	Port number of mail server	Y	Y	Y	Y	Y
Email address	TO	N	N	Y	Y	N
	CC	N	N	Y	Y	N
	BCC	N	N	Y	Y	N
	FROM	N	N	Y	Y	N
File path	Path for email body	Y	Y	Y	Y	Y
	Path for attached file	Y	Y	Y	Y	Y
	Path for mail adapter account definition file	Y	Y	Y	Y	Y
	Path for mail header definition file	Y	Y	Y	Y	Y
Mail format	--	Y	Y	Y	Y	Y
Mail contents	Subject line	N	N	N	N	N
	Mail body	N	N	N	N	N
	Attached file	N	N	N	N	N
Encoding	--	Y	Y	Y	Y	Y
Authentication information	Authentication format	Y	Y	Y	Y	Y
	User name	Y	Y	Y	Y	Y
	Password	Y#	Y#	Y#	Y#	Y#
Message ID	--	Y	Y	Y	Y	Y

Legend:

Y: Output.

N: No output.

--: No corresponding item.

Note #

8 digit asterisks are output.

In addition to this, error messages and traces which are output in JavaMail of Application Server are also required at the time of troubleshooting. For details on how to get failure information output by Application Server, see "Application Server Maintenance and Migration Guide".

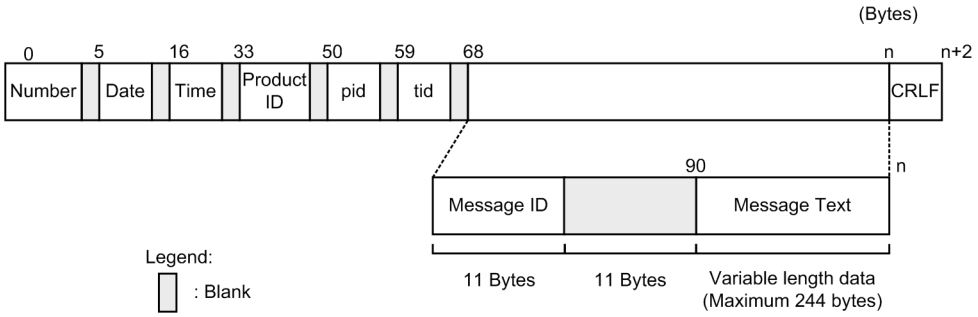
The following points describe the method to acquire logs and traces and the contents that are output:

(1) Message log

(a) Output format

The following figure shows the output format of message log:

Figure 7–102: Figure Output format of message log (Mail adapter)



(b) Output contents

The following table described the contents output in message log:

Table 7–112: Table Contents output in message log (Mail adapter)

Item	Description
Number	The output serial number of message log is displayed.
Date	The date of acquiring message log is output in the yyyy/mm/dd format. • yyyy: Year • mm: Month • dd: Day
Time	The message log acquisition time is output in hh:mm:ss.SSS format. • hh: Hour • mm: Minutes • ss: Seconds • SSS: Milliseconds
Product ID	"HEJB" showing Component Container is output as an identifier for identifying product.
pid	ID for identifying process is output.
tid	The ID for identifying thread is output.
Message ID	Message ID in "KDECnnnnn-X" format is output.

Item	Description
Message text	The content of message is output.
CRLF	Terminal symbol of record is output.

(c) Output destination

The output destination of message log is as follows:

```
Path specified in the output destination of the operating log of J2EE server
```

Specify the output destination of the operating log of J2EE server in the ejb.server.log.directory key of usrconf.cfg (Option definition file for J2EE server). The default destination is <Installation directory of Service Platform>\CC\server\public\ejb\<J2EE server name>\logs. For details about usrconf.cfg, see "2.3 usrconf.cfg (Option definition file for J2EE server) " in "Application Server Definition Reference Guide".

The following table shows the log file name of message log:

Table 7–113: Table Log file name of message log (Mail adapter)

Output mode of log file	Log file name
For wrap around mode	cjmessage<Number of files>.log
For shift mode	cjmessage.log

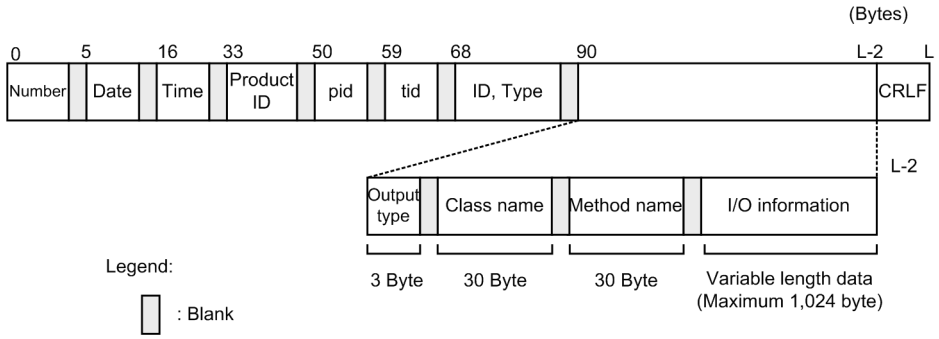
Specify the number of log files in the ejbserver.logger.channels.define.<channel name>.filenum key of the option definition file (usrconf.cfg) for the J2EE server on which the HCSC server is running. Specify the size of log files in the ejbserver.logger.channels.define.<channel name>.filesize key of the option definition file (usrconf.cfg) for the J2EE server on which the HCSC server is running.

(2) Maintenance log

(a) Output format

The following figure shows the output format of maintenance log:

Figure 7–103: Figure Output format of maintenance log (Mail adapter)



(b) Output contents

The following table describes the contents that are output in maintenance log:

Table 7–114: Table Contents output in maintenance log (Mail adapter)

Item	Description
Number	The output serial number of maintenance log is displayed.
Date	The maintenance log collection date is displayed in yyyy/mm/dd format.

Item	Description
Date	• yyyy: Year • mm: month • dd: Day
Time	The maintenance log collection time is displayed in hh:mm:ss.SSS format. • hh: Hour • mm: Minutes • ss: Seconds • SSS: Milliseconds
Product ID	"MAILADP" indicating mail adapter is output as the identifier to identify the product.
pid	ID to identify process is output.
tid	ID to identify thread is output.
ID, Type	Not displayed.
Output type	Maintenance log trace collection point information (collection position) is displayed. • BGN: Start method • END: End method • CAL: Invoke method • RET: Return method • THR: Throw exception • CTH: Catch exception
Class name	Class name to collect maintenance log is output.
Method name	Method to name to collect maintenance log is output.
Input and output information	Input and output information of method to collect maintenance log is output.
CRLF	Record end code is output.

(c) Output destination

The output destination of maintenance log is as follows:

```
Path specified in the mailadp.methodtrace.filepath key of the mail adapter
execution environment property file
```

The following table shows the log file name of maintenance log:

Table 7–115: Table Log file name of maintenance log (Mail adapter)

Output mode of log file	Log file name
For wrap around mode	cscmailadpmtd_<HCSC server name>_<Number of files>.log
For shift mode	cscmailadpmtd_<HCSC server name >_.log

Specify the number of log files by using the mailadp.methodtrace.filenum key of mail adapter execution environment property file. Specify the size of log files by using the mailadp.methodtrace.filesize key of mail adapter execution environment property file.

For details on the mail adapter execution environment property file, see "Mail adapter execution environment property file" in "Service Platform Reference Guide".

(3) Performance analysis trace

(a) Output format

The format which is output in performance analysis trace file is similar to that of performance analysis trace of J2EE server. For details see "7. Performance analysis using performance analysis trace" in "Application Server Maintenance and Migration Guide".

(b) Output contents

The following table describes the contents that are output in performance analysis trace file:

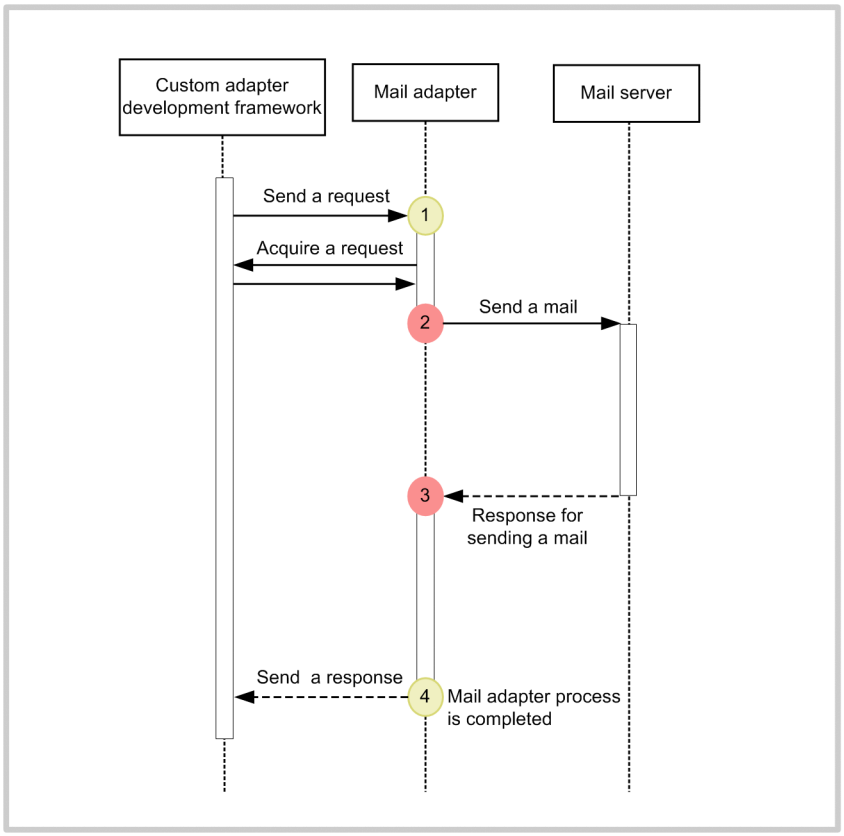
Table 7–116: Table Contents output in performance analysis trace file (Mail adapter)

Item		Description
Event ID		Event ID of collection point id output. For details on collection point, see "(c) Performance analysis trace collection point".
Return code		Collection point type is output. • 0: Normal end • 1: Abnormal end
Interface name		Class name is output.
Operation name		Method name is output.
Option information	Service ID	Service ID of HCSC component is output.
	Operation	SEND is output.
	Send mail (includes the connection to mail server and sending mail)	The host name, port number of destination mail server, date, message ID, etc. output.
	Exception class name	Class name where exception occurred is output.

(c) Performance analysis trace collection point

The following figure shows the performance analysis trace collection point:

Figure 7–104: Figure Performance analysis trace collection point (Mail adapter)



Legend:

: Indicates trace collection point (Performance analysis trace collection level is "Standard")

: Indicates trace collection point (Performance analysis trace collection level is "Detailed")

The following table describes the event ID, trace collection point and performance analysis trace collection level. The "Number in Figure" corresponds to the numbers in the above figure.

Table 7–117: Table Performance analysis trace collection point (Mail adapter)

Event ID	Number in Figure	Trace collection point	Level
0x9B90	1	When receiving request	B
0x9B92	2	When sending mail (Includes connection to mail server)	A
0x9B93	3	When responding to send mail (includes the connection mail server)	A
0x9B91	4	When sending response	B

Legend:

A: Indicates that the process/level is "Standard".

B: Indicates that the process/level is "Details".

(d) Performance analysis trace collection method and output destination

Settings are required for collecting performance analysis trace. For details about these settings, see "7. Performance analysis using performance analysis trace" in "Application Server Maintenance and Migration Guide".

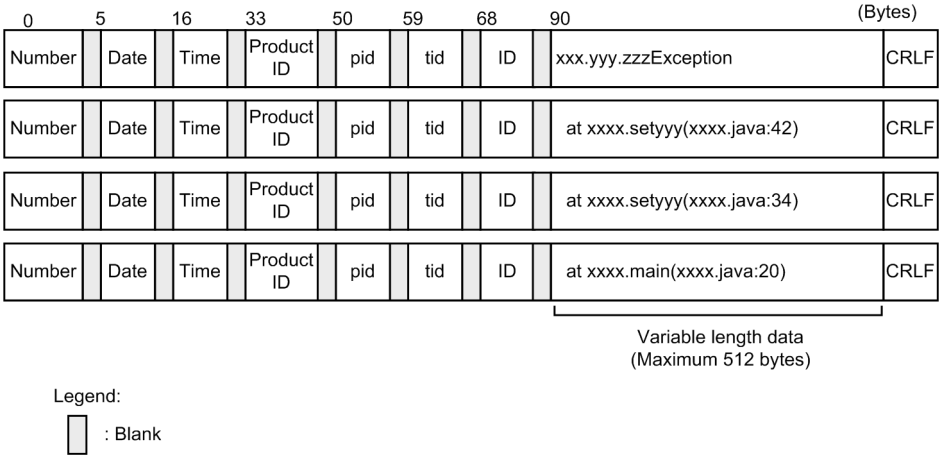
(4) Exception log

Exception log starts/stops at the same time of maintenance log, and then, captures exception information (stack trace) and outputs the same to a file. As the output destination of exception log is the same directory as that of maintenance log, you cannot change it separately.

(a) Output format

The following figure shows the output format of exception log:

Figure 7–105: Figure Output format of exception log (mail adapter)



(b) Output contents

The following table describes the contents output in exception log:

Item	Description
Number	The output serial number of exception log is displayed.
Date	The exception log collection date is output in format yyyy/mm/dd. • yyyy: Year • mm: Month • dd: Day
Time	The exception log collection time is output in format hh:mm:ss.SSS. • hh: Hour • mm: Minutes • ss: Seconds • SSS: Milliseconds
Product ID	"MAILADP" indicating mail adapter is output to identify product.
pid	ID to identify process is output.
tid	ID to identify thread is output.
ID	Blank
Stack trace information	Stack trace information is output.
CRLF	Record end code is output.

(c) Output destination

Following is the output destination of exception log. The path is same as that of maintenance log.

```
<Path specified in the mailadp.methodtrace.filepath property of mail adapter
execution environment property file>\<Service ID>
```

The following table shows the log file name of exception log.

Table 7–118: Table Log file name of exception log (Mail adapter)

Output mode of log file	Log file name
For wrap around mode	cscmailadpexp_<HCSC server name>_<number of files>.log
For shift mode	cscmailadpexp_<HCSC server name>_.log

Specify the number of log files in the mailadp.exptrace.filenum property of mail adapter execution environment property file. Specify the size of log files in the mailadp.exptrace.filesize property of mail adapter execution environment property file.

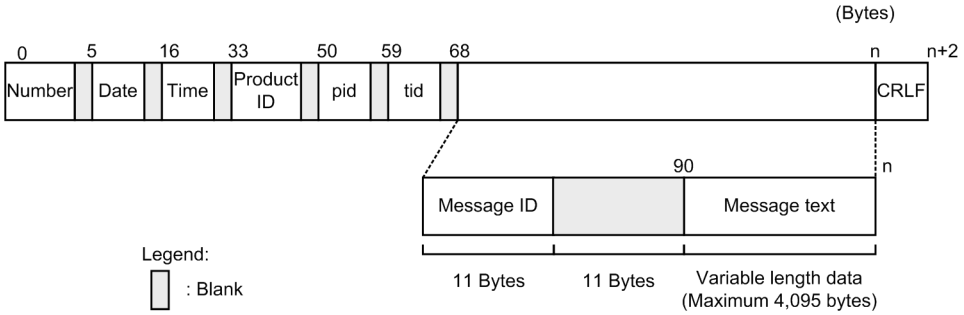
For details about the mail adapter execution environment property file, see "Mail adapter execution environment property file" in "Service Platform Reference Guide".

(5) Command message log

(a) Output format

The following figure shows the output format of command message log.

Figure 7–106: Figure Output format of command message log (Mail adapter)



(b) Output contents

The following table describes the contents output in command message log.

Table 7–119: Table Contents output in command message log (Mail adapter)

Item	Description
Number	The output serial number of command message log is displayed.
Date	The collection date of command message log is output in format yyyy/mm/dd. • yyyy: Year • mm: Month • dd: Day
Time	The collection time of command message log is output in format hh:mm:ss.SSS. • hh: Hour • mm: Minutes • ss: Seconds • SSS: Milliseconds
Product ID	"MAILADP" along with the name indicating the command to be executed like "add", "del" or "ls", is output as an identifier to identify the product.

Item	Description
Product ID	• MAILADP:add • MAILADP:del • MAILADP:ls
pid	ID for identifying process is output.
tid	The ID for identifying thread is output.
Message ID	Message ID in "KDECnnnnn-X" format is output.
Message text	The content of message is output.
CRLF	Terminal symbol of record is output.

(c) Output destination

Following is the output destination and log file name of command message log.

```
<Path specified in the mailadp.command.messagelog.filepath key of mail adapter
command definition file>\adpmailcommand<Number of files>.log
```

Specify the number of log files in the mailadp.command.messagelog.filenum key of mail adapter command definition file. Specify the size of log files in the mailadp.command.messagelog.filesize key of mail adapter command definition file.

7.7.13 Troubleshooting when executing the HTTP reception

This sub-section describes the kinds of failure information which is output when HTTP reception is operating. Following are the types of failure information related to HTTP reception.

- Message log
  The information details during the start and stop of HTTP reception and error information of errors such a transfer error is output in log files.
- Method trace
  Maintenance information is output in trace files.
- Performance analysis trace
  Trace information for executing performance analysis of Service Platform system is output.

The following points describe the collection method, output format and output destination of the logs and traces which are output by Service Platform during the execution of HTTP reception.

(1) Message log

The message log of HTTP reception outputs the operating log of J2EE server from among the message log outputted by Service Platform.

For details about the output contents of message log, see "2.6 Messages from KDEC80400 to KDEC80499" in "Service Platform Messages".

For details about output contents and output destination of message log, see "*7.4.1 Message log*".

(2) Method trace

The method trace of HTTP reception is as per the specifications of the method trace output by Service Platform.

For details about output contents and output destination of method trace, see "*7.4.5(3) Method trace*".

(3) Performance analysis trace

This sub-section describes the performance analysis trace in HTTP reception. By using Performance Tracer, Performance analysis trace (PRF trace function) outputs performance analysis information at any point in the series of processes right from receiving requests from service requester to returning the service execution result. Thus, you can check the performance of the entire system.

(a) Output format

The format which is output in performance analysis trace file is the same as that of performance analysis trace of Application Server. For details, see "7. Performance analysis using performance analysis trace" in "Application Server Maintenance and Migration Guide".

(b) Output contents

The following table describes the contents which are output in performance analysis trace file.

Table 7–120: Table Contents that are output in performance analysis trace file (HTTP reception)

Item	Description
Event ID	Event ID of collection point is output. For details about collection point, see "*(c) Performance analysis trace collection point*".
Return code	Collection point type is output. • 0: Normal end • 1: Abnormal end
Interface name	Class name is output.
Operation name	Method name is output.
Option information	Only the following option information is output. • Reception name • Reception ID • Request ID • Service name • Service operation name • Exception name#

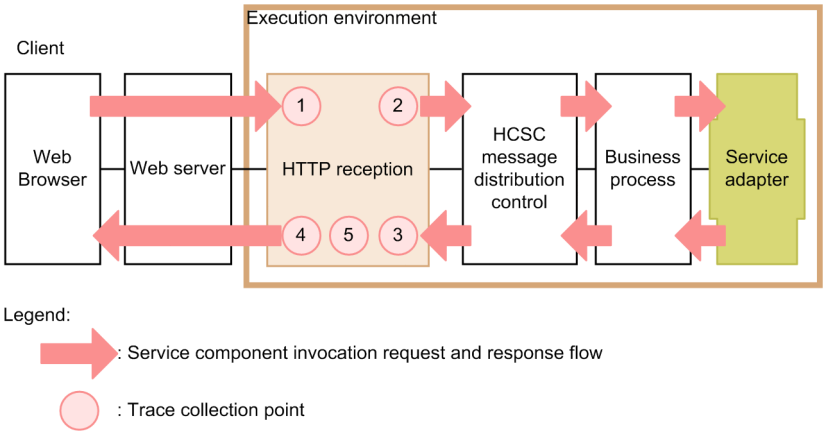
Note #

This item is output only when error is generated.

(c) Performance analysis trace collection point

The following figure shows the collection point of performance analysis trace.

Figure 7–107: Figure Performance analysis trace collection point (HTTP reception)



The following table shows event ID, trace collection point and performance analysis trace collection level. The "Number in figure" in the table, corresponds to the numbers shown in the above figure.

Table 7–121: Table Performance analysis trace collection point (HTTP reception)

Event ID	Number in figure	Trace collection point	Level
0x9880	1	Entry to HTTP reception	A
0x9882	2	Invocation of custom reception framework	A
0x9883	3	Reception of response from custom reception framework	A
0x9881	4	Exit from HTTP reception	A
0x9884	5	Before deletion of work folder#	A

Legend:

A: Indicates that the process/level is "Standard".

Note #

When you want to download file to HTTP client, in HTTP response, you will be able to do so after sending data to HTTP client.

(d) Performance analysis trace collection method and output destination

Settings are required for collecting performance analysis trace. For details about these settings, see "7. Performance analysis using performance analysis trace" in "Application Server Maintenance and Migration Guide".

7.7.14 Troubleshooting when executing the HTTP adapter

The information for checking system performance and analyzing causes of failure is output in log files and trace files in HTTP adapter. The following table describes the log files and trace files which are output in HTTP adapter:

Table 7–122: Table Types of logs and traces (in HTTP adapter)

Logs and traces	Output information	Description
Message log	All type of information that occurs in HTTP adapter is output as messages.	You can check operating information (Start, Stop and Failure) as messages. Note that the output destination of message log is common for Application Server and Service Platform as a whole and therefore, you can check system operating status in a batch.
Maintenance log	The following information is output as the maintenance information inside HTTP adapter. • Date	You can check the time of publication and sequence of internal method.

Logs and traces	Output information	Description
Maintenance log	• Time • Execution class name • Internal method name • Exception that occurred • Information of the specified argument	You can check the time of publication and sequence of internal method.
Performance analysis trace	The following information is output in the performance analysis trace collection point of the entire Service Platform system. • Date • Time • Request information • Trace collection source information HTTP adapter specific information is output in the performance analysis trace collection point of HTTP adapter.	Based on the performance analysis information which is output from a series of processes, right from receiving request from service requester to returning the execution result, you can check the performance of Service Platform system.
Exception log	Information of exception which occurred in HTTP adapter (stack trace) is output.	You can check the information of exceptions in HTTP adapter. You can use it to analyze the cause of failure.
Communication log	Messages sent and received in HTTP communication are output.	Used for checking the sent and received contents such as when investigating failure.

See the following points for details about the collection method and output contents of logs and trace.

(1) Message log

The message log of HTTP adapter outputs the operating log of J2EE server from among the message log outputted by Service Platform.

For details about the output contents of message log, see "2.8 Messages from KDEC81000 to KDEC81499" in "Service Platform Messages".

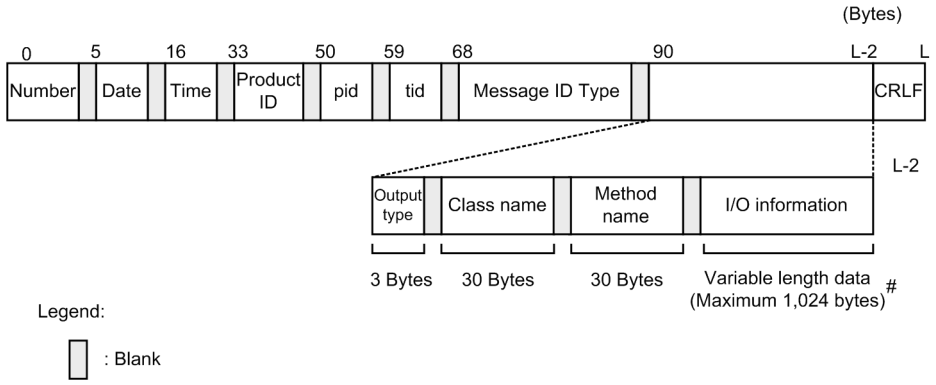
For details about output contents and output destination of message log, see "*7.4.1 Message log*".

(2) Maintenance log

(a) Output format

The following figure shows the output format of maintenance log:

Figure 7–108: Figure Output format of maintenance log (HTTP adapter)



#
The upper limit value of trace length indicated here is aimed value. Even if the upper limit value is exceeded it output without being truncated.

(b) Output contents

The following table describes the contents that are output in maintenance log:

Table 7–123: Table Contents output in maintenance log (HTTP adapter)

Item	Description
Number	The output serial number of maintenance log is displayed.
Date	The maintenance log collection date is displayed in yyyy/mm/dd format. • yyyy: Year • mm: month • dd: Day
Time	The maintenance log collection time is displayed in hh:mm:ss.SSS format. • hh: Hour • mm: Minutes • ss: Seconds • SSS: Milliseconds
Product ID	"ADPHTTP" indicating HTTP adapter and version information is output as the identifier to identify the product. Version information format is as follows: • Regular version: VV-RR • Fixed version: VV-RR-SS
pid	ID to identify process is output.
tid	ID to identify thread is output.
Message ID type	Not displayed.
Output type	Maintenance log trace collection point information (collection position) is displayed. • BGN: Start method • END: End method • CAL: Invoke method • RET: Return method • THR: Throw exception • CTH: Catch exception

Item	Description
Class name	Class name to collect maintenance log is output.
Method name	Method to name to collect maintenance log is output.
Input and output information	Input and output information of method to collect maintenance log is output.
CRLF	Record end code is output.

(c) Output destination

The output destination of maintenance log is as follows:

```
<Path specified in the adphttp.config.trace.path property>\CSCADP\ADPHTTP
\maintenance\<Service ID>
```

Note #

Specify the adphttp.config.trace.path property in HTTP adapter execution environment property file or HTTP adapter execution environment common property file.

The following table shows the log file name of maintenance log:

Table 7–124: Table Log file name of maintenance log (HTTP adapter)

Output mode of log file	Log file name
For wrap around mode	cscadphttpmnt_<HCSC server name>_<number of files>.log
For shift mode	cscadphttpmnt_<HCSC server name>_.log

Specify the number of log files with the adphttp.config.methodtrace.filenum property and specify the log file size with the adphttp.config.methodtrace.file size property in HTTP adapter execution environment property file or HTTP adapter execution environment common property file.

For details about the HTTP adapter execution environment property file, see "HTTP adapter execution environment property file" in "Service Platform reference Guide". For details about the HTTP adapter execution environment common property file, see "HTTP adapter execution environment common property file" in "Service Platform reference Guide".

(3) Performance analysis trace

(a) Output format

The format which is output in performance analysis trace file is similar to that of performance analysis trace of J2EE server. For details, see "7. Performance analysis using performance analysis trace " in "Application Server Maintenance and Migration Guide".

(b) Output contents

The following table describes the contents that are output in performance analysis trace file:

Table 7–125: Table Contents output in performance analysis trace file (HTTP adapter)

Item	Description
Event ID	Event ID of collection point id output. For details about the collection point, see "*(c) Performance analysis trace collection point*".
Return code	Collection point type is output. • 0: Normal end • 1: Abnormal end

Item		Description
Interface name		Class name is output.
Operation name		Method name is output.
Option information	Service ID	Service ID of HCSC component is output.
	Operation	Operation name defined in HTTP adapter is output.
	Request ID[#1]	The request ID which is specified in request message (header) is output.
	Nanoseconds from any time	Return value of the nanoTime method of java.lang.System class is output.
	Exception class name	Class name where exception occurred is output.
	Transfer sixe[#2#3]	The received data size is output (unit: bytes).
	HTTP method[#4]	HTTP method of the invoked HTTP request is output.
	URI[#4#5]	The URI at the time of sending request is output.

Note #1

Nothing is output if request ID is not specified in request message (header) or if an error occurs before collection of value.

Note #2

If the event ID is 0x9894, the value collected from HTTP response header is output as is. The number may be 0 or less than 0, if system is unable to collect a value from HTTP response header, or if the value is in an invalid format. Nothing is output when value cannot be collected due to an error.

Note #3

If the event ID is 0x9893, the value received by HTTP adapter is output. Nothing is output when a value cannot be collected due to an error.

Note #4

If nothing is specified in request message (header), HTTP adapter execution environment property file and HTTP adapter execution environment common property file, or if an error occurs before collection of value, nothing is output.

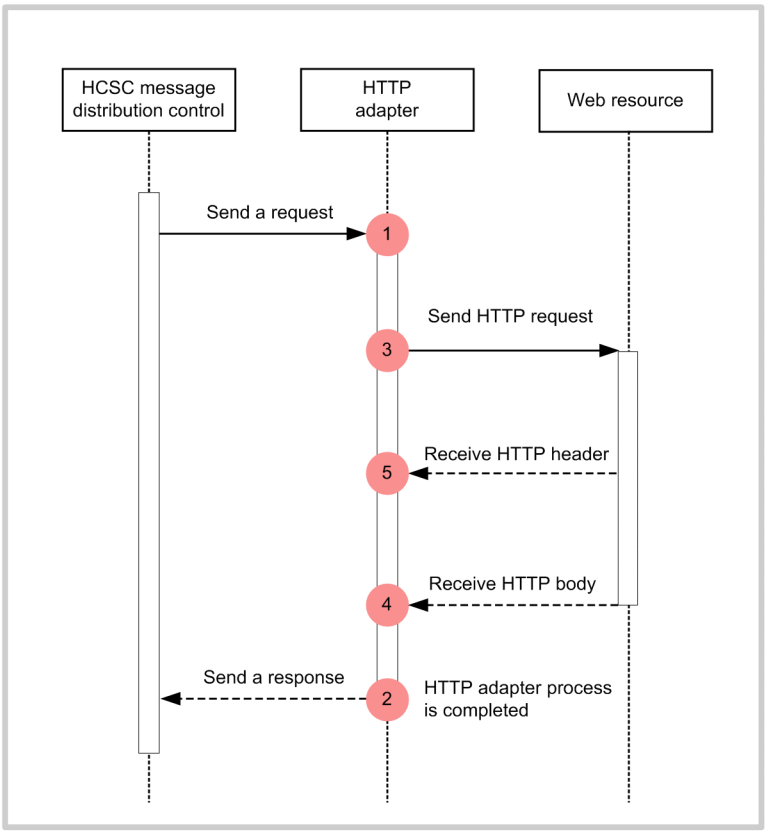
Note #5

Only the path part and schema and authority (except user information), which is specified in request message (header), HTTP adapter execution environment property file and HTTP adapter execution environment common property file is output.

(c) Performance analysis trace collection point

The following figure shows the performance analysis trace collection point:

Figure 7–109: Figure Performance analysis trace collection point (HTTP adapter)



Legend:

: Indicates trace collection point (Performance analysis trace collection level is "Standard")

The following table describes the event ID, trace collection point and performance analysis trace collection level. The "Number in Figure" corresponds to the numbers in the above figure.

Table 7–126: Table Performance analysis trace collection point (HTTP adapter)

Event ID	Number in Figure	Trace collection point	Level
0x9890	1	When receiving request	A
0x9891	2	When sending response	A
0x9892	3	When sending HTTP request	A
0x9893	4	When HTTP response is received	A
0x9894	5	When HTTP	A

Event ID	Number in Figure	Trace collection point	Level
0x9894	5	response header is received.	A

Legend:

A: Indicates that the process/level is "Standard".

(d) Performance analysis trace collection method and output destination

Settings are required for collecting performance analysis trace. For details about these settings, see "7. Performance analysis using performance analysis trace" in "Application Server Maintenance and Migration Guide".

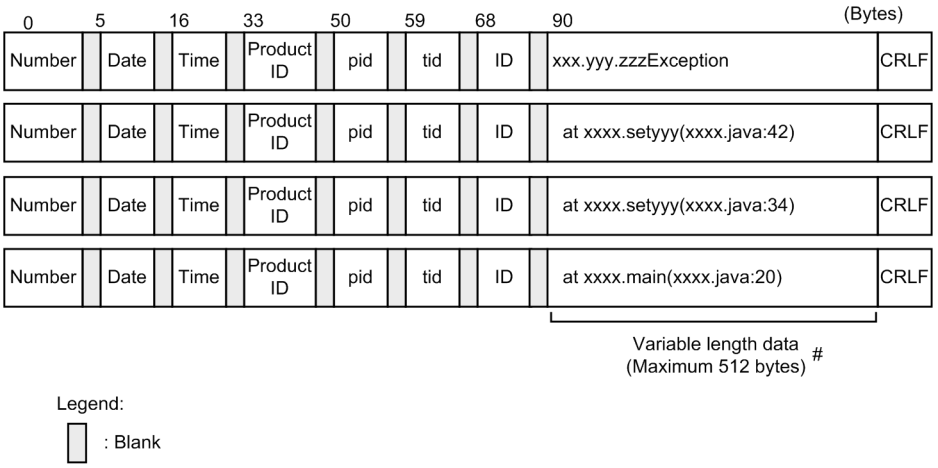
(4) Exception log

Exception log starts/stops at the same time of maintenance log, and then, captures exception information (stack trace) and outputs the same to a file. As the output destination of exception log is the same directory as that of HTTP adapter maintenance log, you cannot change it separately.

(a) Output format

The following figure shows the output format of exception log:

Figure 7–110: Figure Output format of exception log (HTTP adapter)



#
The upper limit value of trace length indicated here is aimed value. Even if the upper limit value is exceeded it output without truncated.

(b) Output contents

The following table describes the contents output in exception log:

Item	Description
Number	The output serial number of exception log is displayed.
Date	The exception log collection date is output in format yyyy/mm/dd. • yyyy: Year • mm: Month • dd: Day
Time	The exception log collection time is output in format hh:mm:ss.SSS.

Item	Description
Time	• hh: Hour • mm: Minutes • ss: Seconds • SSS: Milliseconds
Product ID	"ADPHTTP" indicating HTTP adapter and version information is output as the identifier to identify the product. Version information format is as follows: • Regular version: VV-RR • Fixed version: VV-RR-SS
pid	ID to identify process is output.
tid	ID to identify thread is output.
ID	Blank
Stack trace information	Stack trace information is output.
CRLF	Record end code is output.

(c) Output destination

Following is the output destination of exception log. The path is same as that of maintenance log.

```
<Path specified in the adphttp.config.trace.path property#>\CSCADP\ADPHTTP
\maintenance\<Service ID>
```

Note #

Specify the adphttp.config.trace.path property in HTTP adapter execution environment property file or HTTP adapter execution environment common property file.

The following table shows the log file name of exception log:

Table 7–127: Table Log file name of exception log (HTTP adapter)

Output mode of log file	Log file name
For wrap around mode	cscadphttpexp_<HCSC server name>_<number of files>.log
For shift mode	cscadphttpexp_<HCSC server name>_.log

Specify the number of log files with the adphttp.config.exptrace.filenum property and specify the log file size with the adphttp.config.exptrace.file size property in HTTP adapter execution environment property file or HTTP adapter execution environment common property file.

For details about the HTTP adapter execution environment property file, see "HTTP adapter execution environment property file" in "Service Platform reference Guide". For details about the HTTP adapter execution environment common property file, see " HTTP adapter execution environment common property file" in "Service Platform reference Guide".

(5) Communication log

HTTP adapter processes HTTP communication using the JAX-RS function of application server. The data which is sent and received in HTTP communication is output as communication log by Jax-RS function.

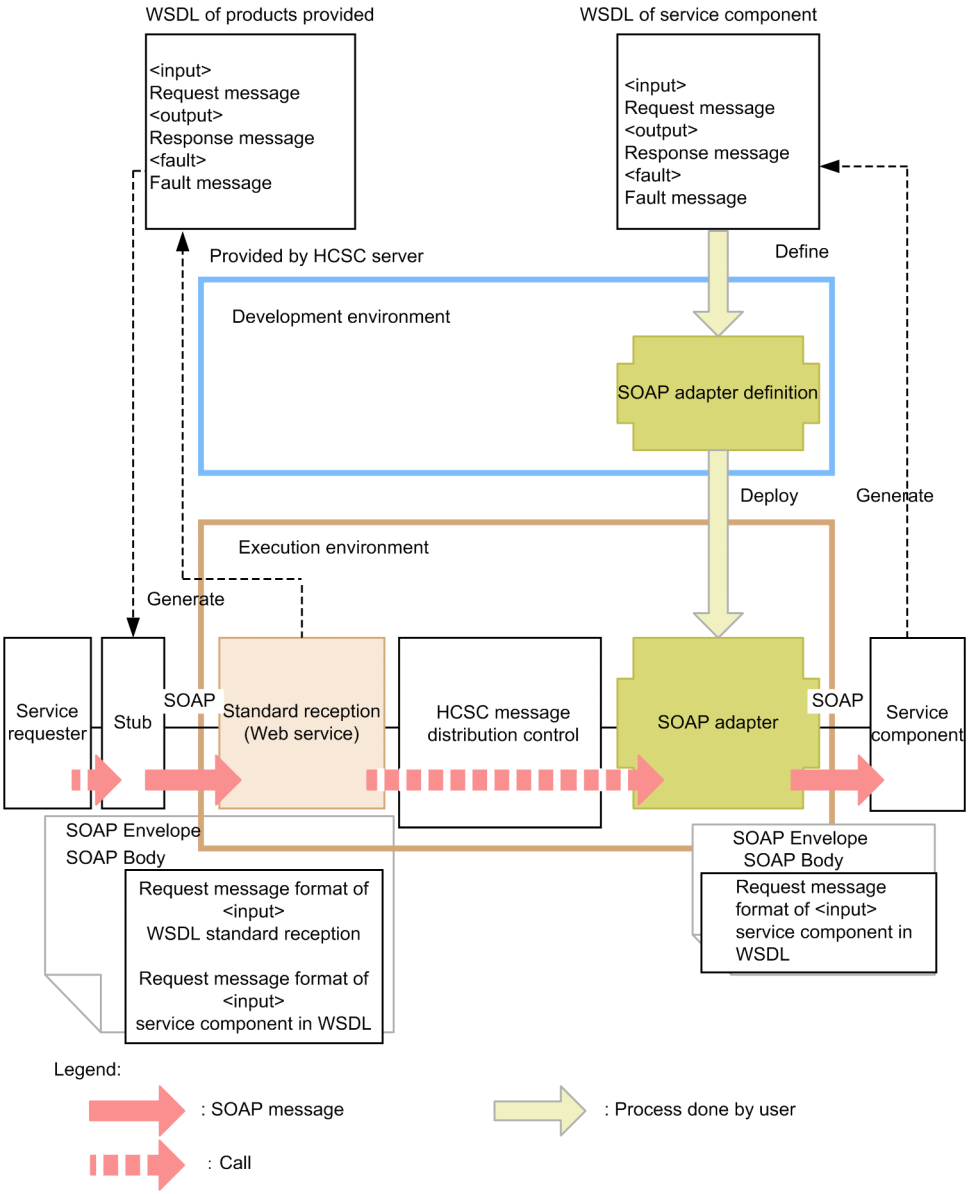
You can set the output level, number of files, maximum size and character encoding of communication log, in the application server common definition file. For details about communication log settings, see "13.1.2 Setting items in common definition file" in "Application Server Web Service Development Guide".

7.7.15 Troubleshooting when there is a mistake in user message

(1) Error when there is a mistake in user message

When directly invoking service components of service adapter from standard reception, you must create the user message (XML document) that requests service components in service requester. Thus, if there is a mistake in the XML created in service requester, system cannot invoke the correct service component. The following figure shows the relationship between the SOAP message in SOAP communication and user message.

Figure 7–111: Figure Relationship between SOAP message in SOAP and user message



When there is a mistake in user message (when you execute a message in a format which is different than the format of format definition), the error contents will differ depending on the difference in the protocol of service adapter.

Note that depending on the format of the message, there may be instances wherein, instead of an error in service adapter, there may be an exception in service component; or instead of an error in service component, an unexpected response may be returned.

(a) For an error due to wrong user message when executing Web service (SOAP reception)

The specifications of service components that can be called from SOAP adapter must meet the application scope which is given in "2.6.1 Applicability of the service components that use Web service" in "Service Platform Basic Development Guide". Operation of service components which are out of the application scope cannot be guaranteed.

(b) For an error due to wrong user message when executing SessionBean

The specifications of service components which can be invoked from SessionBean adapter, must meet the application scope, indicated in"2.6.2 Application Scopes of Service Components That Use SessionBean" in "Service Platform Basic Development Guide". Operation of service components which are out of the application scope cannot be guaranteed.

(c) For an error due to wrong user message when executing MDB (WS-R/DB queue)

There is no error in the service adapter of MDB (WS-R/DB queue), in case of an error in the user message which is requested from service requester. Schema is defined at the time of defining in the development environment, but normally, even the messages that are not in the format defined in this schema are sent to the asynchronous queue. If you create such that the user message is received and validated in service component, error is detected in service component.

(2) How to validate messages in service adapter

You can validate if the user message (XML document) and format definition (XML schema) which is specified in service adapter are according to the specifications of XML schema.

Set the telegram-validation property in HCSC server runtime definition file for using the service adapter message validation function. For details about the HCSC server runtime definition file, see "HCSC server runtime definition file" in "Service Platform Reference Guide".

! Important note

When a message which is invalid as per the defined format definition but successfully invokes service components; if the message format is determined to be invalid by using message validation function, there will be an error in service adapter.

The following table shows the service adapters of the entire HCSC server, where message validation function will be valid. You cannot set the function for each service adapter. Also, the function will be effective for the request messages which invoke service components and for response messages.

Table 7–128: Table Service adapters in which message validation function is effective

Adapter type	Direction	Data transformation definition pattern	Format definition to be validated	Message type	Effectiveness of validation function
SOAP adapter, SessionBean adapter, MDB (WS-R) adapter, MDB (DB queue) adapter	Request	No data transformation	Service component message	XML	Y
				Binary	N #1
		Standard - service components Data transformation	Standard message	XML	Y
				Binary	N #1
			Service component message	XML	Y
				Binary	N #1
	Response	No data transformation	Service component message	XML	Y
				Binary	N #1
		Service component - Standard data transformation	Standard message	XML	Y
				Binary	N #1

Adapter type	Direction	Data transformation definition pattern	Format definition to be validated	Message type	Effective ness of validation function
SOAP adapter, SessionBean adapter, MDB (WS-R) adapter, MDB (DB queue) adapter	Response	Service component - Standard data transformation	Service component message	XML	Y
				Binary	N [#1]
	Fault	No data transformation	N	XML	N
DB adapter	Request	No data transformation	Service component message	XML	N [#2]
		Standard - service components Data transformation	Standard message	XML	N
				Binary	N
			Service component message	XML	N[#2]
	Response	No data transformation	Service component message	XML	N[#2]
		Service component - Standard data transformation	Standard message	XML	N
				Binary	N
			Service component message	XML	N[#2]
TP1 adapter	Request	No data transformation	Service component message	Binary	N[#1]
		Standard - service components Data transformation	Standard message	XML	Y
				Binary	N[#1]
			Service component message	Binary	N[#1]
	Response	No data transformation	Service component message	Binary	N[#1]
		Service component - Standard data transformation	Standard message	XML	Y
				Binary	N[#1]
			Service component message	Binary	N[#1]
File adapter	Request	No data transformation	Service component message	XML	Y
				Binary	N[#1]
		Standard - service components Data transformation	Standard message	XML	Y
				Binary	N[#1]
			Service component message	XML	Y
				Binary	N[#1]
	Response	No data transformation	Service component message	XML	Y
				Binary	N[#1]
		Service component - Standard data transformation	Standard message	XML	Y
				Binary	N[#1]

Adapter type	Direction	Data transformation definition pattern	Format definition to be validated	Message type	Effective ness of validation function
File adapter	Response	Service component - Standard data transformation	Service component message	XML	Y
				Binary	N[#1]
Object Access adapter	Request	No data transformation	Service component message	XML	Y
		Standard - service components Data transformation	Standard message	XML	Y
				Binary	N[#1]
			Service component message	XML	Y
	Response	No data transformation	Service component message	XML	Y
		Service component - Standard data transformation	Standard message	XML	Y
				Binary	N[#1]
			Service component message	XML	Y

Legend:

Y: Validation function is effective.

N: Validation function is not effective.

Request: Indicates that a message is directed from service adapter to service components.

Response: Indicates that a message is directed from service components to service adapter.

Fault: Indicates that a message is directed from service component to service adapter when there is an error.

Note #1

On the basis of set format definition, transformation to DOM (path processing) is performed when invoking service components of binary message. Therefore, if you send a binary message, which is invalid as per the format definition, an exception occurs and the following message is displayed:

KDEC05504-E an attempt to specify format definition settings has failed. (Information1 = maintenance information, information2 = maintenance information)

The settings of format definition failed.

Note #2

DB adapter validates message format with functions other than telegram-validation property. For example, at the time of request when you convert "Requester (binary) - Standard (XML) - Service components (binary)" in service adapter, DB adapter converts and validates request message in the following flow:

1. Validate request message as per requester format definition (Same when binary message function is OFF).
2. If the result of validation performed in Step 1 is valid, convert message from requester message format to standard message format.
3. After conversion, validate the standard message format as per the format definition of standard message.
4. If the result of validation performed in Step 3 is valid, convert message from standard message format to service component message format.
5. Validate the converted message as per the format definition of service component (same even when binary message function is OFF).
6. If the result of the validation performed in Step 5 is valid, then invoke service component.

(3) Analyze by collecting user message trace

Based on the collected user message trace, you can check if the message is flowing as per the design, at the requester side and service side and you can also check the message at all points such as business process activity and data transformation.

For collecting user message trace, perform settings in the following properties of HCSC server runtime definition file:

- telegramtrace property
- telegramtrace-filepath property
- telegramtrace-filesize property
- telegramtrace-filenum property
- telegramtrace-trigger property

For details about the HCSC server runtime definition file, see "HCSC server runtime definition file" in "Service Platform Reference Guide".

For details about user message trace, see "*7.4.4 User message trace*".

! Important note

- There are security issues (concerns like information leaks) for outputting user message contents to a file. Therefore, do not acquire user message contents in normal operation including production operation.
- You cannot collect user message trace for collection position SVC and collection position CNVST, in the DB adapter which is created by using the "<Installation directory of Service Platform>>\CSC\lib\cscdba.ear" prior to 01-60.

7.7.16 Analyzing failure in entire system

(1) Process hang up

When there is no response, the service component invocation requests from service requester or to the command requests, the process in HCSC server (J2EE server) may be hung up. Following points describe the flow of analysis when process hangs up:

(a) For service component invocation requests from service requester

The analysis procedure when process hangs up for service component invocation request from service requester is as follows:

1. Analyze till what point, the service component invocation requesting process is complete and where exactly has the process hung up. Tracking execution log of the service component invocation process is different for each protocol.

   For details on troubleshooting during the execution of requests in each protocol, see "*7.7.1 Troubleshooting when executing Web service (SOAP communication)*" , "*7.7.2 Troubleshooting when executing SessionBean*", "*7.7.3 Troubleshooting when executing MDB (WS-R)*" and "*7.7.4 Troubleshooting when executing MDB (DB queue)*".
2. With reference to the results after analyzing till what point, the service component invocation request is processed, analyze the CPU usage for the corresponding processes in service requester machine, HCSC server machine, service component machine and database machine.

   When CPU usage is near 100%, there is a possibility that the process has fallen into an infinite loop or recurring invocation.

   When CPU usage is near 0%, there may be a deadlock or cases wherein there is no response from back process.
3. Check the "J2EE server, redirector, server management command log" of Service Platform, for any invalid error output.
4. Collect performance analysis trace and analyze the same. You can identify the location of hang up by identifying the location where the process takes longer time.
5. Acquire a thread dump multiple times, observing in chronological order, perform a comparative analysis of the stack traces of same thread as tid in the corresponding thread dumps.

(b) For command requests

When the process for command requests hangs up, analyze with the following steps:

1. Investigate the CPU usage of respective processes on machines on which operating environment, HCSC server and database are running for command requests.

   When the CPU usage is about 100%, the process might go in an infinite loop or restart invocation.

   When the CPU usage status is about 0%, there are cases such as no response from back process or deadlock.
2. Confirm the message log of Service Platform or "logs of J2EE server, redirector, and server management commands" or "logs of Administration Agent, Management Agent or Management Server" of Cosminexus and investigate that no invalid errors are output.
3. Acquire the thread dump for multiple times and observe it as per time-series and compare the stack trace of similar threads of tid in respective thread dump.

(2) Process slow down

If there service component invocation request from service requester slows down or if the response time is slow, use performance analysis trace to identify the location where the execution time is long.

You can identify the exact location where slow down occurs by identifying the place where process takes more time, by collecting performance analysis trace and analyzing the same.

(3) Timeout

Following points describe the flow when a timeout occurs, in service component invocation request from service requester and in response to command requests.

(a) In case of a service component invocation request from service requester

The investigation procedure for timeout in case of a service component invocation request from service requester is as follows:

1. Investigate the error messages output when timeout occurs.
2. Check the error information output by J2EE server of Service Platform for any other error messages that are output in addition to the timeout error messages.
3. Check till what point is the service invocation request process is complete and, where exactly has the process hung up. The trace of execution logs of service component invocation process differs for each protocol.

   For troubleshooting during request execution in each protocol, see "*7.7.1 Troubleshooting when executing Web service (SOAP communication)*", "*7.7.2 Troubleshooting when executing SessionBean*", "*7.7.3 Troubleshooting when executing MDB (WS-R)*" and "*7.7.4 Troubleshooting when executing MDB (DB queue)*".
4. Investigate the request trace or performance analysis trace.

   Reference the results of investigations for process completion of service component invocation request and specify the places that take longer time for executing processes and thereby find out the reason for timeout.

(b) For command requests

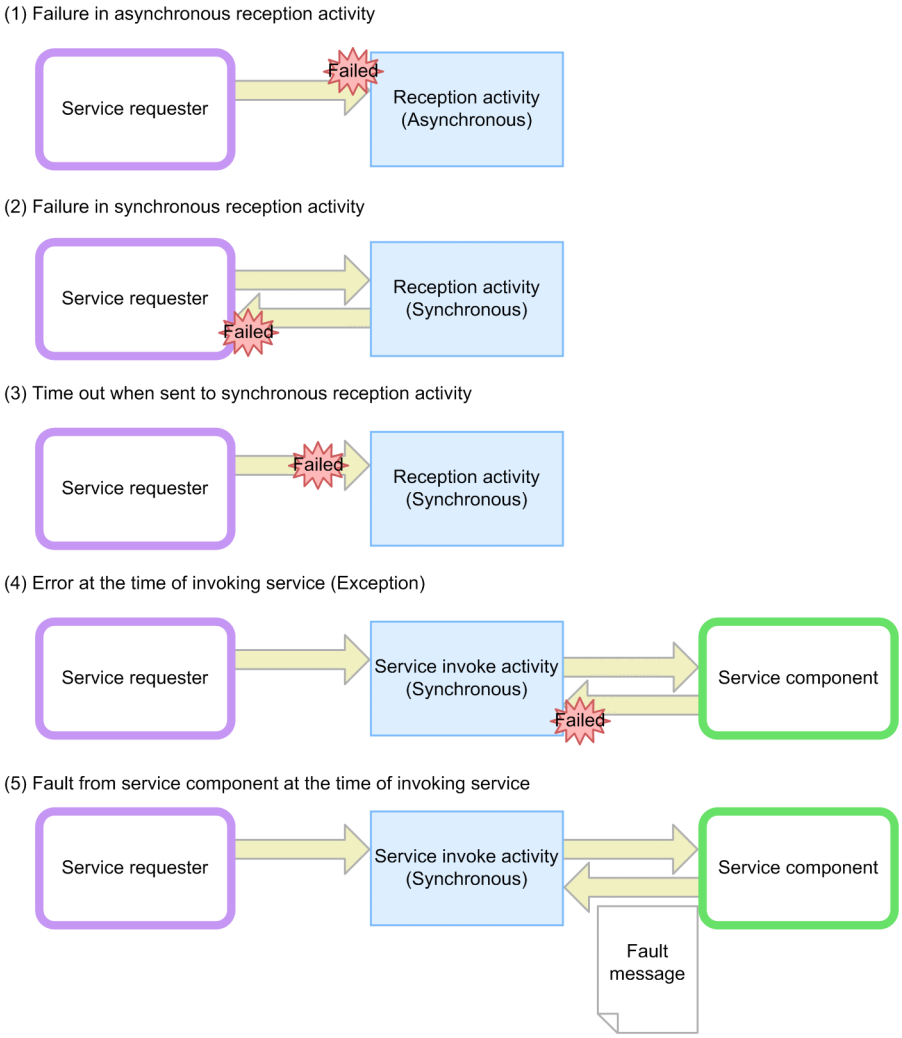
This point describes the procedure when timeout occurs in command request.

1. Investigate the error messages output when timeout occurs.
2. Check the "J2EE server, redirector, server management command logs" of Service Platform for any other error messages are output in addition to the timeout error messages and check "logs of Administration Agent, Management Agent and Management Server" of Cosminexus for any invalid error output.

7.7.17 Troubleshooting when executing the business process

While a business process is executing, the failures shown in the figure below may occur. This subsection describes how to handle these failures.

Figure 7–112: Figure Failures during business process execution



(1) Failure in an asynchronous receive activity

If an error occurs when a message is sent from the service requester to an asynchronous receive activity, the HCSC server is placed in a status in which it can no longer accept messages. The actions in such cases are as follows:

1. Eliminate the cause of error.
2. Resend the same message from service requester.

(2) Failure in a synchronous receive activity

To handle an error that occurs while a message is being sent from the service requester to a synchronous receive activity:

1. See the error message which is output in message log.
2. Eliminate the cause of the error (this is required for certain types of errors).
3. Resend the message from service requester.

(3) Timeout when sending a message to a synchronous receive activity

The following describes how to handle a timeout that occurs while a message is being sent from the service requester to a synchronous receive activity.

Action

Since it is unknown whether or not the message sent from the service requester was executed, check if the error message output to the message log.

When an error message is output

1. If an error message has been output, take appropriate action according to the error message.

When no error message is output

1. Use the cscpiselect command to check the process instance status in the correlation set of the corresponding message.
2. If the process instance is still executing, take one of the following actions:

   Re-execute the process instance using the cscpireexec command.

   Delete the process instance execution log, using the cscpidelete command and, resend the same message from service requester.

   If the process instance status cannot be acquired, reception of the corresponding message has failed. In this case, resend the same message from the service requester.

(4) Error during service invocation (Exception)

When you invoke service in the invoke service activity of business process, if the following errors occur, the execution of process instance will stop.

- The service adapter invoked from invoke service activity is not running
- The service adapter invoked from invoke service activity is not deployed
- Data transformation process in the service adapter invoked from invoke service activity, has failed
- Errors in the processing of synchronous service component invocation (errors such as invalid service component address, HTTP error due to stopping of service component, communication timeout, communication failure)
- Errors in the processing of asynchronous service component invocation, when usage of business process compatibility is OFF (errors such as invalid queue address and failure in the queue send process)
- Errors in the processing of DB access using DB adapter (errors such as DB access error, SQL error, invalid DB Connector settings)
- The fault messages responded from Web service in the service invocation process of SOAP, does not satisfy conditions for handling as a fault in HCSC server

  For details about the conditions for handling fault messages returned from service components as faults, see "4.3 Catching a fault with the SOAP fault operation definition file" in "Service Platform Overview".

Note that the status of the applicable invoke service activity, remains Error or Executing, when the usage of business process compatibility is OFF (bp-status-compatible in HCSC server setup definition) and; remains Executing when the usage of business process compatibility is ON.

Following are the steps to be taken in case an error occurs:

1. Eliminate the cause of error in the service adapter or service components, according to the error information.
2. Re-execute the process instance with the cscpireexec command and invoke the service component again. In this case, you will be invoking service component with the same message for the second time. Therefore, service component must be able to perform duplicate check and process the second call without any conflict.

(5) Fault from service components during service invocation

If a service component responds with a fault message when HCSC server executes synchronous execution, perform the following:

Steps

When fault connection is defined

Process is executed as per the defined fault connection.

When fault connection is not defined

The process instance is placed in fault termination status and stops executing. Service component resends any messages that do not result in a fault respond.

! Important note

You cannot re-execute a process instance with the cscpireexec command, if SOAF Fault returned from service component during service invocation, is a fault. This is because the status of business process does not remain as interrupted, as business process is executed as per the defined fault connection and process instance execution stops.

7.7.18 Troubleshootingwhen executing the data transformation

This sub-section describes the major faults that occur during data transformation execution, and how to deal with those faults. The following table describes the major failures that occur during data transformation execution and how to handle those failures:

Table 7–129: Table Major failures and their solutions (analyzing the failures that occur during data transformation execution)

Operation	Major failure	Possible cause	Solution	Reference manual
Executing data transformation for XML message	When executing data transformation for XML message, KDEC40463-E is output and data transformation fails	Incorrect namespace in XML message (such as when declaration between the namespace and prefix added to the tag name of XML is incorrect)	Review the namespace of XML message. Correct the XML message and then execute service invocation again.	• Service Platform Basic Development Guide • Service Platform Reception and Adapter Definition Guide

7.8 Automatic operations when error occurred

This section describes about the functionality for executing automatic operations when error occurred.

7.8.1 Monitoring errors using the JP1 linkage functionality

(1) Monitoring messages by JP1

Service platform notifies JP1 of the failure messages that occur as JP1 events. You can thereby collect the error messages that are output and centrally monitor these messages on JP1 integrated console.

Along with receiving JP1 specific events (error messages) at JP1 side, you can automate system operations such as executing commands automatically and notifying error occurrence to system administrator and executing commands for recovery.

For details about the settings for monitoring on JP1 integrated console, see "*2.8 Environment setup while using JP1 integrated functionality*". For details about the message mapping file (system log mapping file for JP1/IM linkage) see "10.19 System log message mapping file for JP1/IM linkage" in "Application Server Definition Reference Guide".

(2) How to check JP1 events

INTENTIONALLY DELETED

(3) Process for which monitoring in JP1 is recommended

The following table lists the processes for which monitoring in JP1 is recommended:

Table 7–130: Table Process for which monitoring in JP1 is recommended

Process for which monitoring is recommended	Process name	
	In Windows	In UNIX
Management Server	mngsvr.exe	Cjstartsv#
Administration Agent	adminagentsv.exe	adminagent

Note #

Monitor in command line name (ps -ef suitable). Following is an execution example:

/opt/Cosminexus/CC/server/bin/cjstartsv cosmi_m

"cosmi_m" is default server name. When you change the server name to something other than "cosmi_m", you also need to change the command line name that you want to monitor.

When you use database, JP1 monitoring is also recommended for the processes in the database in use. For details about these process names, see the manual for each database.

For details about process monitoring by JP1, see "7.1.2 Monitoring processes through JP1" in "Service Platform Overview".

7.8.2 JP1 event detail information notified from Service platform

This sub-section describes the values which are specific to Service Platform from the detail information of JP1 event.

(1) Event ID

This value indicates the issued application program and contents of the event. The following table shows the values that are displayed as per severity:

Table 7–131: Table Severity and Event ID

Severity	Event ID
Error	0x00012093
Warning	0x00012094
Information	0x00012096

(2) Severity

Indicates the urgency of the JP1 event. Following are the values that are displayed, in a descending order of urgency:

1. Error
2. Warning
3. Information

(3) Object ID

"<Logical server name>: <J2EE application name>" is displayed.

Logical server name

Displays the J2EE server name that was set up at the time of configuring Service Platform.

J2EE application name

Displays the J2EE application name if the J2EE application that issued the message can be identified.

From the J2EE application name, you can locate the failure on the Service Platform. The following table lists and describes J2EE application names and locations of failure on the Service Platform.

Table 7–132: Table J2EE application names and locations of failure on Service Platform

J2EE application name	Location of failure
CSCMessaging	Execution environment (operation control)
CSCMsgAsyncServiceDelivery	Execution environment (Standard asynchronous reception (MDB (WS-R)))
CSCMsgAsyncServiceDeliveryDBQ	Execution environment (Standard asynchronous reception (MDB (DB queue)))
CSCMsgSyncServiceDelivery	Execution environment (Standard synchronous reception (SessionBean))
CSCMsgSyncServiceDeliveryWS	Execution environment (Standard synchronous reception (Web service and SOAP1.1)) or Execution environment (standard synchronous reception (Web service and SOAP1.2))
cscmsg_async	Execution environment (Asynchronous EJB of business process)
Service ID	Corresponding business process or service adapter

(4) Message ID

The message ID on the Service Platform that was issued as a JP1 event is displayed. This message ID begins with KDEC.

7.9 Restoration methods when HCSC server error occurred

7.9.1 Restoration methods when system operations of HCSC server cannot be executed

If a HCSC server failure occurs and system operations are disabled, take the actions described below.

(1) Information needed for recovery

To recover the HCSC server, you need the following information.

- Repository information for the operating environment:
  This is the repository information for the operating environment at the time of failure.
- HCSC server configuration definition file
  This information was set in the `-propfile` option of the `cscsvsetup` command when the HCSC server was set up.
- HCSC server setup definition file
  This information was required for HCSC server setup.
- HCSC server runtime definition file:
  This information was set in the `-propfile` option of the `cscsvconfig` command.

(2) Recovery procedure

1. To recover the HCSC server: Execute the `cscrepctl` command to export the repository and back up the current repository information.

```
cscrepctl -user login-user-ID -pass login-password -export file-name
```

2. Execute the `cscsvunsetup` command to cancel setup of the HCSC server on which the failure occurred.

```
cscsvunsetup -user login-user-ID -pass login-password -csc HCSC-server-name-for-unsetup
```

   If an error occurs in the execution of the `cscsvunsetup` command, execute step 3. If error does not occur, execute step 4.

3. Execute the command as per the failure contents.
   - **When a communication failure occurs in a machine with an HCSC server**
     Execute the `cscsvunsetup` command to cancel setup of the HCSC server on which the failure occurred.

```
cscsvunsetup -user login-user-ID -pass login-password -csc HCSC-server-name-to-be-unsetup -ignore
```

   - **When a version mismatch occurs in the repository or system configuration definition**
     Manually delete the files and directories under the repository root.

4. Check for any unneeded resources and if there are any, manually delete them.
   For details about checking for unneeded resources, see *7.5.3 How to recover when executing HCSC server setup and unsetup*.

5. Execute the `cscsvsetup` command and set up the HCSC server.
   In the `-propfile` option of the `cscsvsetup` command, specify the HCSC server configuration definition file for the HCSC server on which the failure occurred.

```
cscsvsetup -user login-user-ID -pass login-password -csc HCSC-server-name -cluster cluster-name -propfile HCSC-server-configuration-definition-file-name
```

6. Execute the `cscrepctl` command to import the repository information you backed up in step 1.

```
cscrepctl -user login-user-ID -pass login-password -import file-name
```

7. Execute the `csccompodeploy` command, if necessary, to deploy a business process and a service adapter.
   - To deploy a business process:

```
csccompodeploy -user login-user-ID -pass login-password-csc HCSC-server-name -
name service-ID-of-business-process
```

   - To deploy a service adapter:

```
csccompodeploy -user login-user-ID -pass login-password -csc HCSC-server-name -
name service-ID-of-service-adapter
```

7.9.2 How to recover during cluster configuration

The troubleshooting methods for an error which occurs during cluster configuration are described by separately for load-balancing cluster configuration and for HA cluster configuration.

(1) Failure and recovery in load-balancing cluster configuration

By arranging the HCSC server machines having space in load-balancing cluster, as a preparation in case the HCSC server on which load-balancing cluster is configured fails, you can maintain a fixed quantity of load of HCSC server operating with load-balancing cluster.

! Important note

Every HCSC server has a reception queue for standard asynchronous reception (MDB (WS-R)/MDB (DB queue)). Therefore, you cannot send messages that are retained in the reception queue for standard asynchronous reception (MDB (WS-R)/MDB (DB queue)), when there is a failure in load-balancing cluster configuration.

(a) Disconnecting HCSC server with a failure

When there is a failure in an HCSC server that configures load-balancing cluster, disconnect the HCSC server in which the failure has occurred from the load-balancing cluster. After disconnecting, eliminate the failure in HCSC server so that service component execution requests can be received. Recover by operating the HCSC server from which you eliminated failure, in load-balancing cluster.

(b) Restoring HCSC server with a failure

The following points describe the steps to disconnect and restore HCSC server in which a failure has occurred:

1. Set the load-balancer such that when a failure occurs, service component execution requests are not sent to the HCSC server in which the failure has occurred.

   Control the service component execution requests by setting the load-balancer. The setting method is different as per the specifications of each load-balancer.

2. If you are using CTM, lock queue.

   For details about how to lock queue, see "3.7.4 Lock control for schedule queue" in "Application Server Expansion Guide".

3. Eliminate the fault from the HCSC server, in which the failure has occurred so that service component execution requests can be received.

4. If you are using CTM, release the lock for queue.

   For details about how to release the queue lock, see "5.4.2 How to lock services which can be executed in each system and how to stop J2EE application" in "Application Server Operation, Monitoring, and Linkage Guide".

5. Set the load-balancer to send service component execution requests to the HCSC server from which the fault was eliminated.

   The setting method is different as per the specifications of every load-balancer.

(2) Failure and recovery in HA cluster configuration

When a failure occurs in the executing node, the process is switched to standby node by the cluster software. After switching to standby node, eliminate the fault in executing node and, resume the operations in executing node.

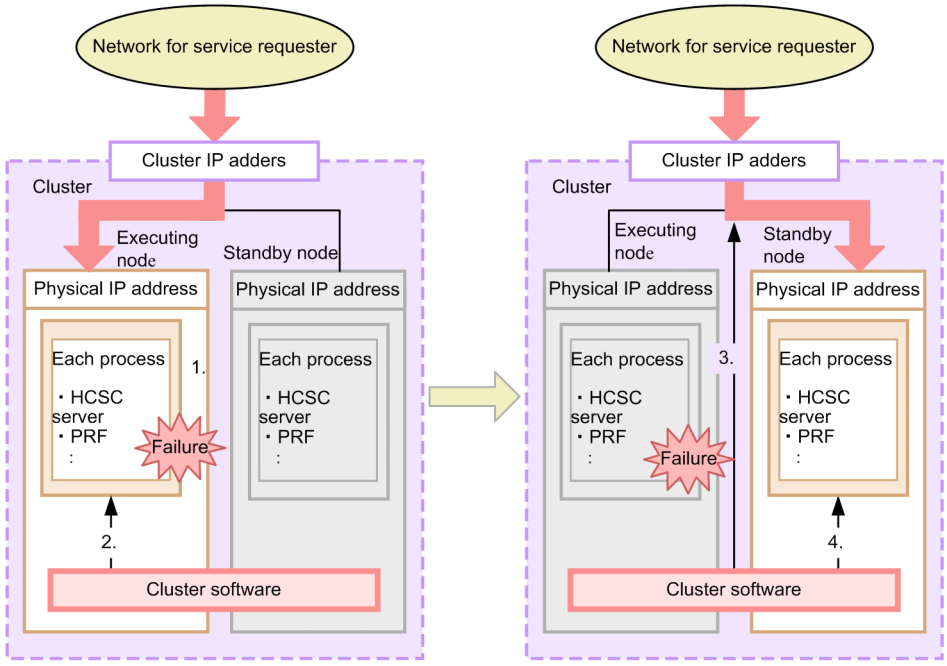
Important note

When there is a failure in executing node and operations are switched to standby node, you must eliminate the fault in executing node and return to the operations in executing node. You can neither use the standby node as an executing node and nor can you use the node with failure as a standby node by eliminating the fault.

(a) Disconnecting node

The following figure shows the operation when process is switched to standby node by cluster software, in case of a failure in executing node:

Figure 7–113: Figure Switching to standby node when a failure occurs (HA cluster)



1. A failure occurs in the executing node and the process is down.

2. Cluster software detects the failure in the executing node.

3. Cluster software disconnects the network to the executing node and switches the connection to the standby node.

4. Cluster software executes the script that is used to invoke or start the required process.

(b) Recovering executing node

When a failure occurs in executing node and operation are switched to standby node, you must eliminate the fault in executing node and, return to the operation in executing node.

The following points describe the steps to eliminate the fault in executing node and, return operation to executing node:

1. Disconnect the executing node and standby node from the network for service requester so that execution requests from service requester are not received.
2. Stop the standby node reception (Standard reception and user-defined reception).
   For details about how to stop standard reception, see "*5.3.28 Terminating the Standard Reception*".
   For details about how to stop user-defined reception, see "*5.3.29 Stopping the user -defined reception*".
3. Stop the standby node HCSC server.

For details about how to stop HCSC server, see "*5.3.33 Terminating the HCSC Server*".

4. Restore the fault in the HCSC server of executing node.
   For details about how to collect failure information and how to recover from the failure, see "*7. Troubleshooting*".
5. Start the executing node HCSC server.
   For details about how to start HCSC server, see "*5.3.4 Starting HCSC server*".
6. Start the executing node reception (standard reception and user-defined reception).
   For details about how to start standard reception, see "*5.3.9 Starting standard receptions*".
   For details about how to start user-defined reception, "*5.3.8 Starting user-defined receptions*".
7. Restore operation by connecting the executing node and standby node to the network for service requester so that execution requests from service requester can be received in executing node.

7.9.3 Backup and recovery of operating environment

When recovering from a failure that has occurred in the operating environment or when migrating the environment by migrating the machine along with the expansion in system scale, you can take the backup of the files required for restoring the environment.

(1) Backup of operating environment

Execute the cscenvbackup command as follows to take the backup of the latest files required to restore the operating environment.

```
cscenvbackup -user <login user ID> -pass <login password> -backupdir  <Backup files output destination directory>
```

If the backup files output destination directory is specified in HCSC-Manager definition file, execute the cscenvbackup command as follows:

```
cscenvbackup -user <login user ID> -pass <login password>
```

Reference note

You can acquire the operating environment backup files even in the case of automatic backup. The operating environment backup files acquired during the automatic backup are stored at the following directories:

- Output destination of the environment backup files specified in the HCSC-Manager definition file
- <Installation directory of Service Platform>\CSC\spool\manager (if the output destination is not specified in the HCSC-Manager definition file (cscmng.properties))

You can check the repository information in the backup files for the acquired operating environment backup files with the following command:

```
cscrepls -user <login user ID> -pass <login password> -envbackfile <Operating environment backup file name>
```

(2) Restoring the operating environment

You can restore the operating environment from the operating environment back files, by using the cscenvrestore command.

Reference note

The restoration using the cscenvrestore command is suitable in the cases when the operating environment is built on a machine different from the machine with an execution environment.

Important note

Only the operating environment can be restored using the cscenvrestore command. The execution environment cannot be recovered with this command. To recover the execution environment, following the steps specified in the section described below, remove the environment repository information and resources and, re-build the execution environment.

- *7.5.3 How to recover when executing HCSC server setup and unsetup*
- *7.5.4 How to recover when deploying and deleting HCSC Components*

(a) Procedure for recovery from a disk failure

The steps are as follows:

1. Prepare a machine with an installed Service Platform. Install software as needed.
2. Save the acquired operating environment backup files in a location that can be recognized by the computer to be restored.
3. Execute the cscrepls command to check the environment that will be restored by the operating environment backup files.

```
cscrepls -user <login user ID> -pass <login password> -envbackfile <Operating environment
backup file name>
```

4. Execute the cscenvrestore command to restore environment using the operating environment backup files.

```
cscenvrestore -user <login user ID> -pass <login password> -restorefile <Operating
environment backup file name>
```

(b) Procedure for migrating the operating machine

The steps are as follows:

1. As needed, use the cscenvbackup command to acquire operating environment backup files that exist before the environment is restored.

   If you restore the operating environment with the cscenvrestore command, the operating environment before restoration is destroyed. The content of the environment backup files may differ when the backup is taken automatically and when the backup is taken just before recovery.
2. Prepare a machine with an installed Service platform. Save the acquired operating environment backup files in a location that can be recognized by the machine after migration.
3. Execute the cscrepls command to heck the environment that will be restored by the operating environment backup files.

```
cscrepls -user <login user ID> -pass <login password> -envbackfile <Operating environment
backup file name>
```

4. Execute the cscenvrestore command to restore the environment using the operating environment backup files.

```
cscenvrestore -user < login user ID > -pass < login password > -restorefile < Operating
environment backup file name >
```

Important note

The HCSC-Manager definition file (cscmng.properties) is saved in the environment backup acquired by executing the cscenvbackup command or cscrepctl command (-import option). However, when the operating environment is restored with the cscenvrestore command, the HCSC-Manager definition file that exists in the restoration destination is considered as valid and the HCSC-Manager definition file included in the environment backup is restored with an optional name (cscmng_backup.properties). Use cscmng_backup.properties for reference. Also, if this file is not required, it may be deleted.

(c) Automatic backup during recovery

A backup of the environment prior to recovery is automatically performed before recovering from operating environment backup file using the cscenvrestore command. When the environment is recovered from a wrong operating environment backup file, you can use the automatic backup file during recovery and can rollback to

environment prior to recovery.The backup file during recovery is output in the following directory with the file name cscenvrestore_1.zip:

```
<Installation directory of Service Platform>\csc\spool\manager
```

You can change the output destination directory of backup file by the cscmng.envbackup.dir parameter or the cscmng.envbackup.dir.envrestore parameter of the HCSC-Manager definition file. When an old backup file exists in the output destination directory, old file is deleted after successful recovery.

You can set whether to perform automatic backup during recovery, in the cscmng.envbackup.autoget parameter or the cscmng.envbackup.autoget.off parameter of the HCSC-Manager definition file.

For details about the HCSC-Manager definition file, see "HCSC-Manager definition file" in "Service Platform Reference Guide".

7.9.4 How to restore when deadlock occurs

Restore HCSC server by following methods, when a deadlock occurs in a process on HCSC server.

(1) When unable to respond to service component invocation request sent to HCSC server

Following are the steps to investigate when there is no response to the service component invocation requests that are sent to HCSC server:

1. Check the thread information using the cjlistthread command.
2. Use the cjstopthread thread and delete the invalid threads.
3. When unable to delete the threads, specify the -force option of the cscsvstop command and stop the HCSC server forcefully.

   Please note that operations cannot be performed from the operating environment screen of HCSC-Manager.
4. Force stop the HCSC server and when the stop process is complete, use the cscsvstart command to restart HCSC server.

For details about how to use the cjstopthread command, see "cjstopthread (deleting thread) " in "Application Server Command Reference Guide".

For details about how to use cjlistthread command, see "cjlistthread (displaying thread information) " in "Application Server Command Reference Guide".

For details about status of thread and how to check the execution status, see "5.3.11 Checking the execution status of J2EE application" in "Application Server Operation, Monitoring, and Linkage Guide".

For details about how to use the cscsvstop command, see "cscsvstop (stopping HCSC server) " in "Service Platform Reference Guide".

For details about how to use the cscsvstart command, see "cscsvstart (starting HCSC server) " in "Service Platform Reference Guide".

(2) When unable to stop HCSC component or standard reception

Following are the investigation steps to be taken when HCSC component or standard reception cannot be stopped:

1. When unable to delete the thread, specify the -force option of the cscsvstop command and force stop HCSC server.

   Note that operation cannot be performed from the operating environment screen of HCSC-Manager.
2. After forcefully stopping the HCSC server, use the cscsvstart command to restart HCSC server.
3. Use the cscstatus command and check the status of HCSC component and standard reception.

   If the status is stop failed (stopfailed), try to stop HCSC component by entering the csccompostop command for HCSC components. For standard reception, specify -stopfg force in the cscrcptnstop command and try to forcefully stop standard reception.

   When the status becomes inactive (inactive), recover by entering the respective start commands.

For details about how to use all commands, see the corresponding commands under "5. Commands (Operating environment and execution environment) " in "Service Platform Reference Guide".

7.10 Error analysis using message tracking

In preparation for error in Cosminexus Service Platform, acquire the information required for troubleshooting in logs and traces. This section describes about message tracking for analyzing error using performance analysis trace file from logs and traces. A *message tracking* is an error analysis tool that specifies the place where error occurred and supports the error classification and error investigations.

For details about the performance analysis trace file, see *7.4.3 Performance Analysis Trace*.

7.10.1 Examples applicable for message tracking functionality

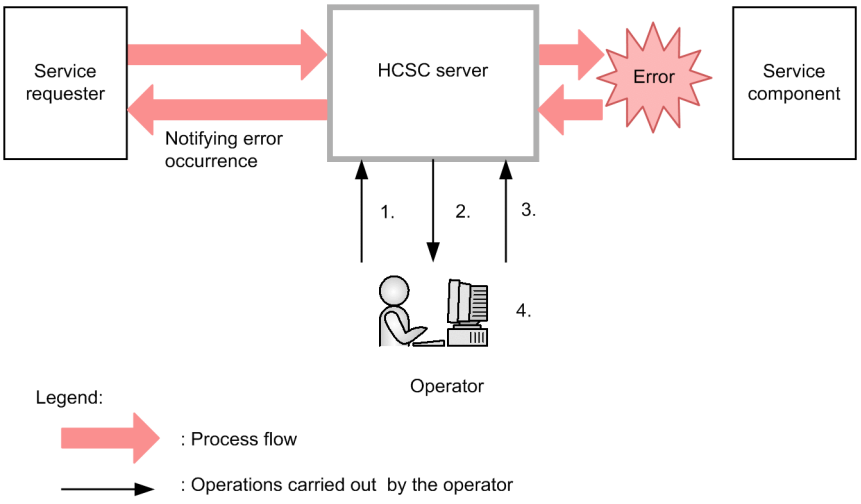
You can use message tracking anywhere if there is a performance analysis trace file when error occurs and if the machine has any of the Service Architect, or Service Platform installed. If there is a performance analysis trace file when error occurs, the error can be analyzed not only on the machine on which HCSC server is running where the error occurred but also from any other remote environment where the HCSC server on which error occurred is not running.

Usage examples of message ranking are as follows:

(1) When error occurred in service component connection

When an error occurred while connecting to service component, analyze the performance analysis trace file and classify the places where error occurred and the reason for error. The following figure shows the flow of error analysis when error occurred while connecting to service component:

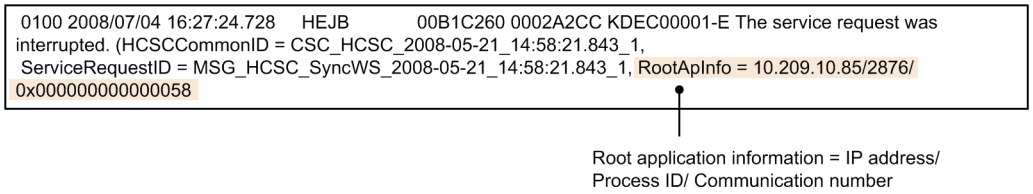
Figure 7–114: Flow of error analysis when error occurred while connecting to service component



1. Access the machine on which HCSC server is running and acquire the performance analysis trace file.
2. Confirm the error information of Cosminexus J2EE server operation log and acquire the following information from error messages output to log:
   - Time when error occurred
   - Root application information
   - Message common ID

   The character string output after "RootApInfo =" is the root application information. Root application information is output to the "IP address/ process ID/ communication number" format.

   The output format of Cosminexus J2EE server operation log is as follows:



3. Start message tracking.

   Sort out the performance analysis trace files read when error occurred and start message tracking. For starting message tracking, see *7.10.2 Starting message tracking*.

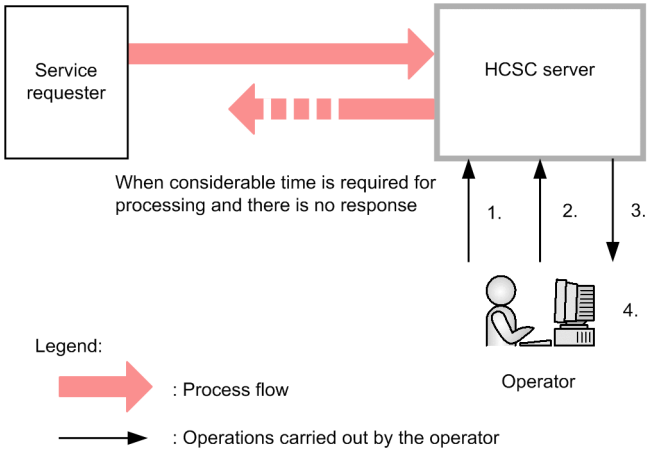
4. Display the performance analysis trace matching the root application information and analyze the error.

   For details about displaying the performance analysis trace matching the root application information, see *7.10.3 Displaying performance analysis trace*.

(2) For investigating errors in the entire system

When the requests are delayed due to hang-up, slowdown, or timeout of process, confirm the information about delayed requests from root application information of performance analysis trace file. Specify the places where error occurred from information about the delayed requests and investigate the errors in the entire system. The following figure shows the error analysis flow when investigating errors in the entire system:

Figure 7–115: Error analysis flow when investigating errors in the entire system



1. Access the machine on which HCSC server is running where the error occurred and acquire the performance analysis trace file.
2. Start message tracking.

   For details about starting the message tracking, see *7.10.2 Starting message tracking*.

3. Display the root application information list of performance analysis trace file and confirm the information about requests that are delayed.

   For details about displaying the root application information list of performance analysis trace file, see *7.10.4 List display of root application information*.

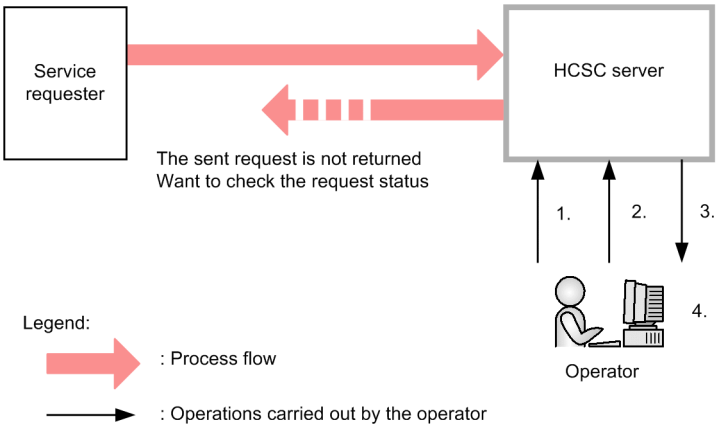
4. Display the performance analysis trace matching the root application information confirmed in 3. and specify the delay places.

(3) For confirming the status of sent requests

When the sent requests are not returned or to confirm the progress status of requests, sort out the performance analysis traces to be analyzed in request sending time and confirm the status of the sent requests.

The following figure shows the error analysis flow when confirming the status of sent requests:

Figure 7–116: Error analysis flow when confirming the sent requests



1. Access the machine on which HCSC server is running where the error occurred and acquire the performance analysis trace file.
2. Start the message tracking.
   For details about starting the message tracking, see *7.10.2 Starting message tracking*.
3. Sort the performance analysis trace to be analyzed in request sending time.
   For details about sorting performance analysis trace to be analyzed, see *7.10.5 Sorting performance analysis trace*.
4. Analyze the sorted performance analysis trace and confirm the status of send requests.

7.10.2 Starting message tracking

This section describes the prerequisites and how to start the message tracking.

(1) Prerequisites

Acquire the performance analysis trace file beforehand for using message tracking. For details about how to acquire the performance analysis trace file, see *7. Analyzing the Performance of a System Using Performance Analysis Trace* in the manual *Cosminexus Application Server Function Guide - Maintenance, Migration, and Compatibility*.

(2) How to start

Start the message tracking by `cscmsgtk` command.

Read the performance analysis trace file and start message tracking by `cscmsgtk` command. After starting the message tracking, an interactive protocol (Here onwards, called as *Message tracking protocol*) is displayed exclusively for message tracking. Commands are executed by message tracking protocol and errors are analyzed.

For details about the `cscmsgtk` command and commands executed by message tracking protocol, see *cscmsgtk (Starting the message tracking functionality)* in the manual *Cosminexus Service Platform Reference*.

Few minutes might be required for starting message tracking due to machine performance and size of performance analysis trace files read while starting the message tracking.

There is normal start and range specified start in message tacking and the range for reading performance analysis trace file during startup differ accordingly. The description of normal start and range specified start is as follows:

(a) Normal start

All the performance analysis traces are read in normal start.

The execution format of `cscmsgtk` command when starting by normal startup is as follows:

```
cscmsgtk -prf performance-analysis-trace-file-name
```

Please note the file size as all the performance analysis traces are read at once in normal start. The standard for file size read once is approximately 140 megabytes. When the "KEOS52044-E A memory shortage occurred." occurs, start as a range specified start and adjust the read file size.

(b) Range specified start

In range specified start, specify the range and sort out the performance analysis traces to be read.

The execution format of the `cscmsgtk` command when starting by range specified start is as follows:

```
cscmsgtk -prf performance-analysis-trace-file-name -date start-reading-week, date-and-
time, reading-completion-week, date-and-time
```

The read range is output as follows when started as range specified start:

```
start-reading-week, date-and-time - reading-completion-week, date-and-time
cscmsgtk
```

Start reading week, date and time and reading completion week, date and time is displayed in (yyyy: Year, MM: Month, dd: Date, hh:Hours, mm: Minutes, ss: Seconds, SSS: Milliseconds) format of `yyyy/MM/dd hh:mm:ss.SSS`.

7.10.3 Displaying performance analysis trace

Display the performance trace that matches with the root application information acquired from the list display of J2EE operation log and root application information. For details on the list display of root application information, see "*7.10.4 List display of root application information*".

(1) Displaying performance analysis trace that matches with root application information

Enter the root application information in message ranking prompt. On entering the root application information, from among the performance analysis traces that were read when message tracking started, the performance analysis trace information that matches with the entered root application information, is output chronologically. You can check places where response takes time or check traces for which the return code is in error, from the performance analysis trace information that is output.

(a) Output format

Execute prf command in message ranking prompt. For details on prf command, see fault analysis command in "cscmsgtk (Starting message tracking function) " in "Service Platform Reference Guide".

The execution format of prf command is as follows:

```
prf <IP address of root application information>/<Process ID of root application
information>/<Communication number of root application information>
```

(b) Output format

The output format is as follows:

```
1  yyyy/MM/dd hh:mm:ss.SSS
2  No. interval(msec) event rc thread(hashcode) interface operation
3  No. + Time elapsed from the trace output before the last event ID return code thread ID
4  interface name operation information
5              Functionality layer: Trace collection point (corresponding event ID)
   Delay level
```

The lines 3 to 5 output the number if traces for performance analysis.

Note that when the output mode is detailed output mode, the performance analysis trace which is collected from other than Service Platform is also output. For details on the output mode, see the output mode switching command in "cscmsgtk (Starting message tracking function) " in "Service Platform Reference Guide".

1st Line: Start output Date and time

The date and time when performance analysis trace output started, is output in "yyyy/MM/dd hh:mm:ss.SSS" format.

- yyyy: Year
- MM: Month
- dd: Day
- hh: Hour
- mm: Minutes
- ss: Seconds
- SSS" Milliseconds

2nd Line: Column

The columns corresponding to performance analysis trace are output. Contents same as the output format are output.

3rd Line: Contents of Performance analysis trace

Outputs the contents of performance analysis trace corresponding to the columns.

Display item	Corresponding column	Description
No.	No.	Indicates a serial number.
Time elapsed from the trace output before the last	interval(msec)	Indicates the elapsed time (Milliseconds) from the performance analysis trace output before the earlier trace. Outputs single byte numeric characters 6 digits (Approximately 16 minutes). When the value exceeds this time, the "999999" is output.
Event ID	event	Indicates the Event ID for trace collection point.
Return code	rc	Indicates return code (hexadecimal). One of the following is displayed: • 0: Normal • Other than 0: Abnormal
Thread ID	thread(hashcode)	Indicates the thread ID of threads in process that has collected trace information, and hash value of threads. • Thread ID Lower case hexadecimals with "0x" added. • Hash value Lower case hexadecimals with "0x" added. If the value is less than 10 digits, digit alignment is performed to 10 digits. If the value is 10 digits or more, all digits are output. Note that if hexadecimal conversion fails, "???????? (????????)" is output. Also, the thread hash value might not be output for the trace information acquired using CTM and redirector. In such cases, only the thread ID is output.
Interface name	interface	Indicates the interface name for each collection point.
Operation information	operation	Indicates the operation information related to collection point.

4th Line: Point name of performance analysis trace

The point name of performance analysis trace is output. "-" is output when performance analysis trace is collected from trace points other than Service Platform.

Display item	Description
Functionality layer	Indicates the layer of functionality that outputs performance analysis trace. One of the following is output: • HCSC (MSG): Messaging infrastructure • HCSC (BP): Business process infrastructure

Display item	Description
Functionality layer	• HCSC (DT): Data transformation infrastructure • HCSC (FTR): FTP reception • HCSC (HTR): HTTP reception • HCSC (MQR): Message Queue reception • HCSC (DBA): DB adapter • HCSC (FFA): File adapter • HCSC (OAA): Object Access adapter • HCSC (MQA): Message Queue adapter • HCSC (FTP): FTP adapter • HCSC (FTI): FTP inbound adapter • HCSC (FOA): File operations adapter • HCSC (MA): Mail adapter • HCSC (HTA): HTTP adapter
Trace collection point	Indicates the point that outputs performance analysis trace in each layer.
Corresponding event ID	Indicates the Event ID corresponding to acquired point. Outputs *-corresponding-event-ID* when the trace is acquired at starting point (inlet), and outputs *corresponding-event-ID-* when the trace is acquired at end point. (Outlet). Not output when there is no event ID.

5th Line: Delay level

The delay level in trace is output.

Display items	Description
No line	Indicates delay level where elapsed milliseconds are within 1 second.
@@ (1sec-10sec)	Indicates delay level where elapsed milliseconds are greater than 1 second.
@@ @@ (10sec-100sec)	Indicates delay level where elapsed milliseconds are greater than 10 seconds.
@@ @@ @@ (100sec more...)	Indicates delay level where elapsed milliseconds are greater than 100 seconds.

(c) Output example

The example of output is as follows:

```
yyyy/MM/dd hh:mm:ss.SSS
No. interval(msec) event rc thread(hashcode) interface operation
007 +000000 0x9808 0  0xb3c(0x0127f4f9) jp.co.Hitachi.so*eliveryWSUserDef onMessage
        HCSC (MSG): Entry to user-defined reception (-0x9809)
031 +000097 0x9840 0 0xb3c(0x0127f4f9) jp.co.Hitachi.so*ageDeliererImpl execAdapter
        HCSC (MSG): Invoking point of business process service (-0x9841)
            :
            :
117 +001859 0x9810 0 0xb3c(0x0127f4f9) jp.co.Hitachi.so*MsgSOAPConverter invoke
        HCSC(MSG): Invoking point of SOAP adapter service component (-0x9811)
@@ (1sec-10sec)
121 +001859 0x9811 0x1 0xb3c(0x0127f4f9) jp.co.Hitachi.so*MsgSOAPConverter invoke
        HCSC(MSG): Invoking point of SOAP adapter service component (0x9810-)
```

Delay Error

In the output example, there is a delay between the trace serial number 117 and trace serial number 121 and there is an error in return code of trace serial number 121.

(2) Displaying detailed information of performance analysis trace

Identify the performance analysis trace, whose information you want to check, from the return code or delay level displayed in "*7.10.3(1) Displaying performance analysis trace that matches with root application information*", and acquire the serial numbers of those performance analysis trace. If you enter the acquired serial number in continuation with the root application information, the detail information of that performance analysis trace is output. Outputs information such as message common ID, request ID, service component name and information useful for error analysis is acquired.

(a) Input format

Execute the prf command in message ranking prompt. Specify the serial number in continuation with root application information, for displaying detailed information of performance analysis trace. For details on the prf command, see fault analysis command in cscmsgtk (Starting message tracking function) " in "Service Platform Reference Guide".

The execution format of prf command is as follows:

```
prf <IP address of root application information>/<Process ID of root application
information>/<Communication number of root application information > serial number
```

(b) Output format

The contents that are output to the ASCII column of performance analysis trace are output. Nothing is output when nothing is setup in the ASCII column.

(c) Output example

Output example is as follows:

- **When detailed information of trace serial number 117 is output**

```
cscmsgtk>prf 10.209.10.85/2876/0x0000000000000586 117
CSC_HCSC_2008-06-09_10:08:14.575_1      MSG_HCSC_SyncBP_2008-06-09_10:08:18.54
4_2 Service Name=WebAdp2, Client ID=null, Adapter Name=2, Address=http://10.208.
177.186/WebApp1/services/EchoWebService1
```

Error in the address

- **When detailed information of trace serial number 121 is output**

```
cscmsgtk>prf 10.209.10.85/2876/0x0000000000000586 121
CSC_HCSC_2008-06-09_10:08:14.575_1      MSG_HCSC_SyncBP_2008-06-09_10:08:18.54
4_2 Service Name=WebAdp2, Client ID=null, Adapter Name=2
```

7.10.4 List display of root application information

You display the root application information list of read performance analysis trace files in the starting order to output performance analysis trace. The number of display cases, display contents and order can be specified.

(1) Input format

Execute the `ls` command in the message ranking prompt. For details about the command, see *cscmsgtk (Starting the message tracking functionality)* in the manual *Cosminexus Service Platform Reference*.

When the how many to display is specified

Displays root application information for specified number of cases. The output order differs as per the option specification. Displays specified number of cases from new information onwards.

The execution format is shown as below:

```
ls number-of-cases-displayed
```

When displaying root application information where error occurred

Execute by specifying the `-e` option. Only the root application information where error occurred is displayed.

The execution format is shown as below:

```
ls -e
```

The trace of error places is not output even after displaying the trace by *7.10.3 Displaying performance analysis trace* methods when the places where error occurred are other than trace points of Cosminexus Service Platform. Change the output mode to detail output mode for confirming the errors occurred with other than Cosminexus Service Platform and output the entire performance analysis trace. For details about the output mode, see *cscmsgtk (Starting the message tracking functionality)* in the manual *Cosminexus Service Platform Reference*.

When displaying root application information in ascending order of elapse time

Execute by specifying the `-t` option. Displays the root application information in the ascending order of elapse time from the trace output first to the last trace in a series of performance analysis trace indicating root application information.

The execution format is shown as below:

```
ls -t
```

(2) Output format

The output format is shown below:

```
1  startDate startTime RootAPInfo processingTime(msec)
2  date-on-which-trace- was-output-first first-trace-output-time root-application-
   information elapse-time
```

The root application information part is output on 2nd line.

1st line: Column

Outputs the column corresponding to performance analysis trace. Outputs the contents same as the output format.

2nd line: Contents of root application information

Outputs the contents of root application information corresponding to the column.

Display items	Corresponding columns	Description
Date on which trace was output first	`startDate`	Indicates the day on which performance analysis trace was output first.
First trace output time	`startTime`	Indicates the time on which performance analysis trace was output for the first time.
Root application information	`RootAPInfo`	Indicates root application information.
Elapse time	`processingTime(msec)`	Indicates the elapse time (milliseconds) from the trace output first to the last trace in a series of performance analysis trace indicating root application information.

(3) Output example

Output examples are shown below:

- **When the how many to display is specified**

```
cscmsgtk>ls 3
startDate startTime RootAPInfo processingTime(msec)
2008/06/09 10:02:20.000 10.209.10.85/5624/0x0000000000000585 547
2008/06/09 10:08:13.000 10.209.10.85/5624/0x0000000000000586 28156
2008/06/09 10:27:33.000 10.209.10.85/5624/0x000000000000058f 21687
```

When "3" is specified in displayed number of cases, displays 3 cases in ascending order of start output week, date and time from the new information of performance analysis trace start output week, date and time.

- **When displaying root application information where error occurred**

```
cscmsgtk>ls -e
startDate startTime RootAPInfoid processingTime(msec)
2008/06/09 15:00:27.000 10.209.10.85/5624/0x000000000000052b 20093
2008/06/09 15:11:48.000 10.209.10.85/5624/0x0000000000000559 2231
2008/06/09 15:25:11.000 10.209.10.85/5624/0x000000000000058f 8140
           :
```

- **When displaying root application information with longer elapse time**

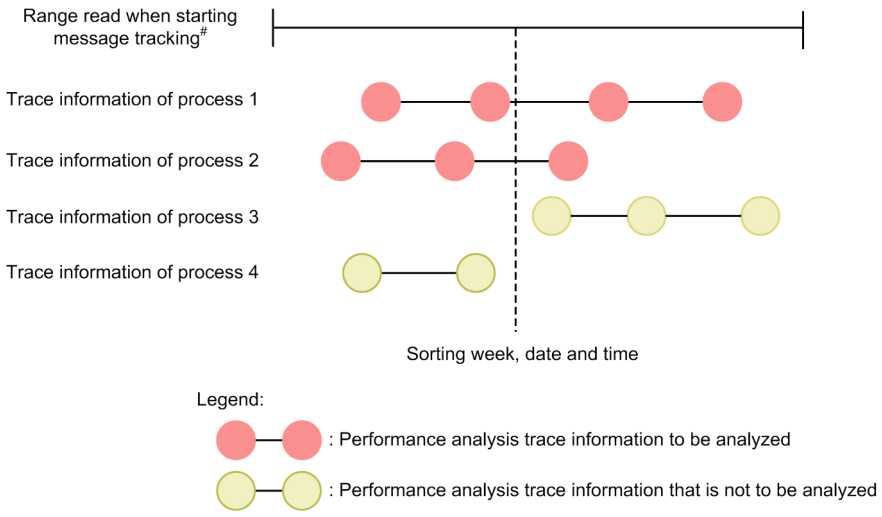
```
cscmsgtk>ls -t
startDate startTime RootAPInfo processingTime(msec)
2008/06/09 10:01:59.000 10.209.10.85/5624/0x000000000000037d 3766
2008/06/09 10:27:48.000 10.209.10.85/5624/0x000000000000058f 21687
2008/06/09 10:08:27.000 10.209.10.85/5624/0x0000000000000586 28156
           :
```

7.10.5 Sorting performance analysis trace

The trace to be analyzed can be sorted out from the trace of processes executed on the specified week, date and time by specifying week, date and time in the message tracking prompt.

The following figure shows the trace to be analyzed that are acquired by sorting the performance analysis trace:

Figure 7–117: Traces to be analyzed by sorting performance analysis trace



Note#:

The performance analysis trace can be sorted in both the normal start and range specified start. For details about starting the message tracking, see *7.10.2 Starting message tracking*.

Execute the `focus` command at message tracking prompt for sorting performance analysis trace. For details about the `focus` command, see *cscmsgtk (Starting the message tracking functionality)* in the manual *Cosminexus Service Platform Reference*.

Important note

Display warning message when week, date and time for which there are no traces to be analyzed is specified. In such cases, omit the sorted week, date and time and execute the `focus` command and restore the traces to be analyzed to startup status.

7.10.6 Displaying performance analysis trace collection points

Display performance analysis trace collection points. If you display trace collection points by specifying event ID, all the trace collection points of Service Platform may be displayed.

(1) Input format

Execute id command using the message tracking prompt. For details on id command, see the trace collection points display command "cscmsgtk (Starting message tracking function) " in "Service Platform Reference Guide".

- **To display trace collection point by specifying event ID**

  The trace collection points for the specified event ID are displayed.

  The execution format is as follows:

```
id <Event ID>
```

  If you specify any event ID other than the ones in Service Platform or any event ID that does not exist, an error will occur.

- **To display all the trace collection points of Service Platform**

  All the trace collection points of Service Platform are displayed.

  The execution format is as follows:

```
id list
```

(2) Output format

The output format is as follows:

- **When trace collection points are displayed by specifying event ID**

```
Functionality layer: Trace collection point (Corresponding event ID)
```

- **When all the trace collection points of Service Platform are displayed**

```
Event ID=Functionality layer: Trace collection point (Corresponding event ID)
```

  The number of trace collection points is output.

The following table lists and describes the display items:

Display items	Description
Event ID	Indicates the event IDs showing the trace collection points.
Functionality layer	Indicates the layer of functionality that outputs the performance analysis trace. One of the following values is output: • HCSC (MSG): Messaging infrastructure • HCSC (BP): Business process infrastructure • HCSC (DT): Data transformation infrastructure • HCSC (FTR): FTP reception • HCSC (HTR): HTTP reception • HCSC (MQR): Message Queue reception • HCSC (DBA): DB adapter • HCSC (FFA): File adapter • HCSC (OAA): Object Access adapter • HCSC (MQA): Message Queue adapter • HCSC (FTP): FTP adapter • HCSC (FTI): FTP inbound adapter

Display items	Description
Functionality layer	• HCSC (FOA): File operations adapter • HCSC (MA): Mail adapter • HCSC (HTA): HTTP adapter
Trace collection point	Indicates the points at which performance analysis trace is output in each functionality layer.
Corresponding event ID	Indicates the event ID corresponding to the collection point. If the trace was collected at the starting point (entrance), "*−corresponding-event-ID*" is output and if the trace was collected at the ending point (exit), "*corresponding-event-ID−*" is output. If the trace is not collected, the event ID is not output.

(3) Output example

The examples of output are as follows:

- **When trace collection points are displayed by specifying event ID**

```
cscmsgtk>id 0x9808
HCSC(MSG): Entry of user-defined reception (-0x9801)
```

- **When all the trace collection points of Service Platform are displayed**

```
cscmsgtk>id list
0x9800=HCSC(MSG):Entry of standard reception (Web service) (-0x9801)
0x9801=HCSC(MSG):Exit of standard reception (Web service)(0x9800-)
0x9802=HCSC(MSG):Entry of standard reception (SessionBean)(-0x9803)
```

7.11 Selecting the errors to be acquired when an exception occurs

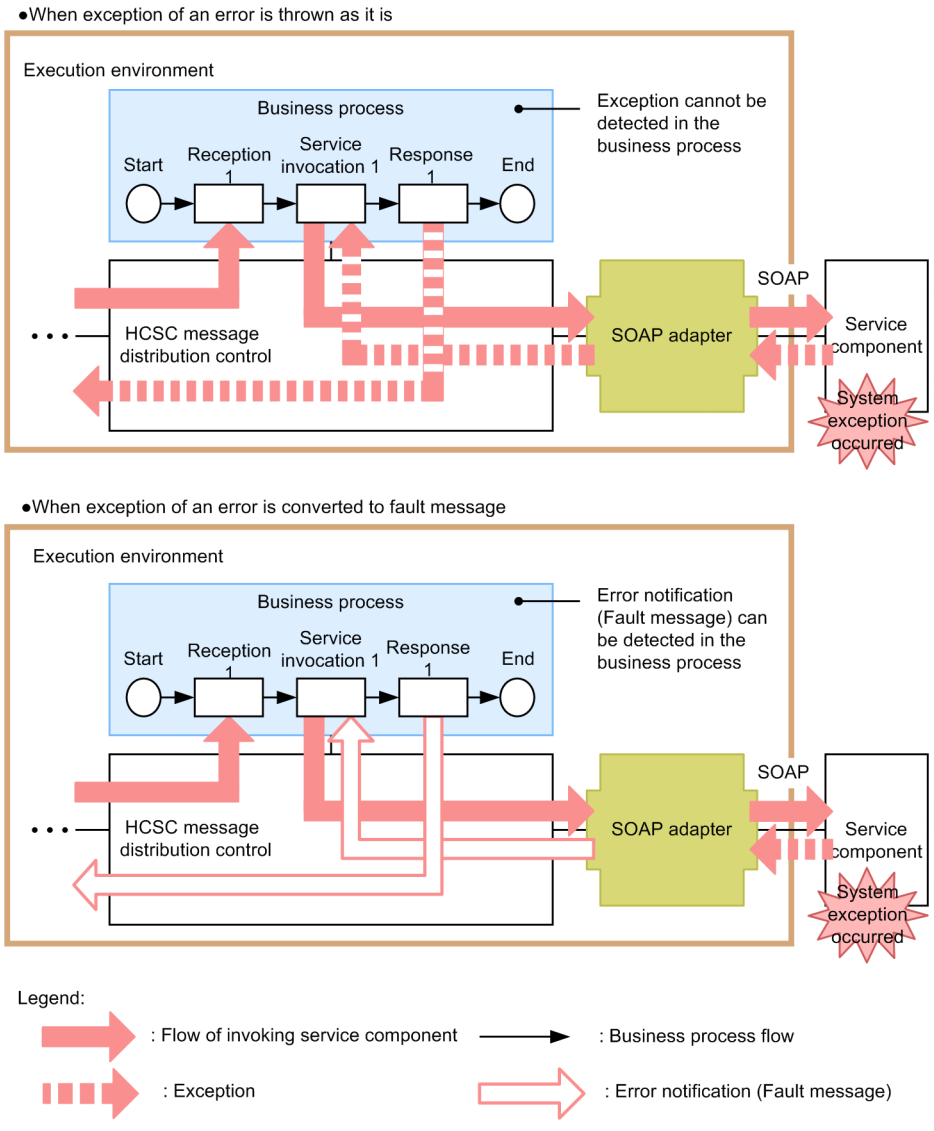
You can choose to throw the error exception or to convert it into a fault message using the service adapter, when the service components (Web services) are invoked from the service adapter.

7.11.1 Difference in processing when the exception is thrown and when the exception is converted into a fault message

If you convert the error exception into a fault message using the service adapter, you can catch the exception as an error in the business process.

The following figure shows the difference in the processing when the exception is thrown and when the exception is converted into a fault message:

Figure 7–118: Figure Difference in processing when the exception is thrown and when the exception is converted into a fault message



Note that for catching a fault message converted with a service adapter using a business process, you must deploy the activities for performing fault processing. For details on the fault processing definition, see "5.4.3 Defining Fault Handling" in "Service Platform Basic Development Guide".

7.11.2 Settings for converting an exception into a fault message

When defining the adapter on the Define Service Adapter screen, specify whether or not to convert an error exception into a fault message. For details about how to define the adapters, see *3. Defining Adapters* in the manual *Cosminexus Service Platform Development Guide*, and for details about the Define Service Adapter screen, see *1.2.2 Window for defining service adapters* in the manual *Cosminexus Service Platform Reference*.

7.11.3 Schema file defining the fault messages

This subsection describes the schema file that defines the fault messages, when you choose the settings for converting the error exception into a fault message.

(1) File storage location

The schema file defining the fault messages is stored in the following location:

<Service Platform installation directory>\CSC\system\msg\cscfault.xsd

(2) Format

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
DO NOT EDIT THIS FILE.
-->
<xs:schema elementFormDefault="qualified" targetNamespace="http://
www.msg.csc.soft.Hitachi.co.jp/cscfault" xmlns:cscft="http://www.msg.csc.soft.Hitachi.co.jp/
cscfault" xmlns:xs="http://www.w3.org/2001/XMLSchema">
 <xs:element name="fault">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="exception-name" type="xs:string" />
    <xs:element name="exception-message" type="xs:string" />
    <xs:element name="stacktrace" type="xs:string" minOccurs="0" />
    <xs:element name="details" type="xs:string" minOccurs="0" />
    <xs:element name="other" type="xs:anyType" minOccurs="0" />
   </xs:sequence>
  </xs:complexType>
 </xs:element>
</xs:schema>
```

(3) Precautions

Do not edit the schema file. If the schema file is edited, the settings for converting the error exception into a fault message will not be applied.

7.12 Failure analysis using faults

You can identify the location of failure in business process and the cause of failure, using faults.

For details about the conditions for sending fault messages, see "4.7 Legend fault which converts system exception into fault" in "Service Platform Overview".

7.12.1 Schema file for defining fault messages

This sub-section describes the schema file that defines general fault messages.

The schema file defines exception information, information to identify the activity in business process in which failure has occurred, and the item (root application information) that is to be used to provide message (KDEC20087-W), which is output in message log for identifying the failure location.

(1) File storage location

The schema file that defines general fault messages is stored in the following location:

```
<Installation directory of Service Platform>CSC\schema\fault\generic_fault.xsd
```

(2) Format

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema elementFormDefault="qualified" targetNamespace="http://
www.msg.csc.soft.Hitachi.co.jp/cscGenericFault" xmlns:xsd="http://www.w3.org/2001/
XMLSchema">
  <xsd:element name="fault">
    <xsd:complexType>
      <xsd:sequence>
        <xsd:element name="exception-name"       type="xsd:string"/>
        <xsd:element name="exception-message"    type="xsd:string"/>
        <xsd:element name="scope-name"           type="xsd:string"/>
        <xsd:element name="activity-name"        type="xsd:string"/>
        <xsd:element name="activity-type"        type="xsd:string"/>
        <xsd:element name="process-instance-id"  type="xsd:string"/>
        <xsd:element name="root-ap-info"         type="xsd:string"/>
        <xsd:element name="extensions" minOccurs="0">
          <xsd:complexType>
            <xsd:sequence>
              <xsd:element name="extension" maxOccurs="unbounded">
                <xsd:complexType>
                  <xsd:simpleContent>
                    <xsd:extension base="xsd:string">
                      <xsd:attribute name="name" type="xsd:string" use="optional"/>
                    </xsd:extension>
                  </xsd:simpleContent>
                </xsd:complexType>
              </xsd:element>
            </xsd:sequence>
          </xsd:complexType>
        </xsd:element>
      </xsd:sequence>
    </xsd:complexType>
  </xsd:element>
</xsd:schema>
```

The settings for general fault messages are as follows:

Tag	Description
exception-name	Used to set exception name. Set the values for Exception.getClass().getName().
exception-message	Set exception information. Set by connecting the string returned by Exception.toString() with a semicolon.
scope-name	Set the scope name to which the activity in which fault has occurred belongs.
activity-name	Set the activity name in which fault has occurred.

Tag	Description
activity-type	Set the type name of activity in which fault has occurred. • Data transformation activity: convert • Assign activity: assign • Switch activity: switch • Validate activity: validate
process-instance-id	Set process instance identifier.
root-ap-info	Set root application information.
Extensions#	Extension area to output specialized information in each activity.

Note #

The format of extension element is as follows:

```
<extensions>
  <extension name="(extension information name)">(extension information contents)</
extension>
</extensions>
```

Set the following for the variable item in extension element.

Activity name	(Extension information name)	(Extension information contents)
Validate activity	variable-name	Variable name of validation error

7.12.2 Settings to output user message trace

You must change as per the underlined part as follows, to output fault messages to user message trace.

Specification example

```
telegramtrace=ON
telegramtrace-trigger=SYSERR, FAULT
telegramtrace-filesize=<user message trace file size (Unit: bytes)>
telegramtrace-filenum=<number of user message traces>
telegramtrace-filepath=<user message trace output destination path>
```

For details about the settings, see "HCSC server runtime definition file" in "Service Platform Reference Guide".

7.13 Operation when OutOfMemoryError occurs

This sub-section describes how to check the occurrence of OutOfMemoryError and the effects of the same.

<INDEXWORD PRONOUNCE="functiontosuppresseffectonbusiness" INDEXITEM="function to suppress effect on business">Function to supress the effect on business</INDEXWORD>

When the memory becomes insufficient due to reasons like the heap size of JavaVM has exceeded upper limit, the "java.lang.OutOfMemoryError" message is displayed. Set the following function to minimize the impact of the OutOfMemoryError on business.

- Force quit function when OutOfMemory occurs

  This is the function to forcefully end J2EE server when OutOfMemoryError occurs. Setting this function forcefully ends the J2EE server and performs automatic restart to enable normal operation. Thus you can control the impact of OutOfMemoryError occurrence on the business which the OutOfMemory has not occurred.

- OutOfMemory handling function

  This function is for continuing the execution of J2EE server, even when you are using the force quit function when OutOfMemory occurs. By setting this function, only the business, with an insufficient memory is stopped. As a result, other businesses without the OutOfMemoryError occurrence are continued.

  Important note

  In spite of setting the OutOfMemory handling function, if the OutOfMemoryError error occurs while executing the businesses which use the following components, the J2EE server system crashes and all the processes are interrupted. Since you cannot cancel only the business with insufficient memory, you must be very careful.

  - Standard reception (MDB (WS-R))
  - Standard reception (MDB (DB queue))
  - MDB (WS-R) adapter
  - MDB (DB queue) adapter
  - Asynchronous business process

<INDEXWORD PRONOUNCE="pointstobeconsideredduringuocexecution" INDEXITEM="points to be considered during UOC execution">Points to be considered during UOC execution</INDEXWORD>

The resources which are reserved during the execution of UOC are not released even after the process ends. The resulting increase in the load of the entire system makes Java heap insufficient which may lead to the occurrence of OutOfMemoryError.

The following functions use UOC and executing these functions, may lead to the occurrence of the OutOfMemoryError. To prepare for OutOfMemoryError, you must implement processes such as process to release resources appropriately and error processing such as rollback at the time of creating UOC.

- Invoke Java activity
- User-defined function
- Character code conversion UOC
- Component-common UOC
- Custom reception
- General custom adapter

Appendixes

A. How to Change the Service Coordinator Administrator

In UNIX, if you have changed the Component Container administrator using the `cjenvsetup` command (sets up a Component Container administrator), you must change the Service Coordinator.

You change the Service Coordinator administrator after implementing the following operations:

- Changing Component Container administrator (`cjenvsetup` command)
- Installing Service Coordinator
- Upgrading versions of execution environment (`cscenvupdate` command)
- `cscsvsetup` (sets up an HCSC server)

This appendix describes how to change the Service Coordinator administrator and notes. user1 and group1 indicate the owner and group associated with the administrator, respectively.

A.1 Change procedure

(1) Changing the file attributes under /opt/Cosminexus/CSC directory

Change the file attributes under /opt/Cosminexus/CSC directory, to administrator owner and group.

(Example)

chown -R user1 /opt/Cosminexus/CSC
chgrp -R group1 /opt/Cosminexus/CSC

(2) Changing the file attributes under repository root

See /opt/Cosminexus/CSC/config/manager/cscmng.properties and change the file attributes as follows:

If a directory other than /opt/Cosminexus/CSC/repository is specified in repository root (cscmng.repository.root)

Change the file attributes under repository root to administrator owner and group.

(Example) When repository root is /home/user1/repository

chown -R user1 /home/user1/repository
chgrp -R group1 /home/user1/repository

(3) Changing the file attributes under log directory

See /opt/Cosminexus/CSC/config/manager/cscmng.properties and, change the file attributes as follows:

If a directory other than /opt/Cosminexus/CSC/log/manager is specified in log directory (cscmng.log.dir)

Change file attributes under log directory to administrator owner and group.

(Example) When log directory is /home/user1/log

chown -R user1 /home/user1/log
chgrp -R group1 /home/user1/log

(4) Changing the file attributes under response message output directory

See /opt/Cosminexus/CSC/config/manager/cscmng.properties and, change the file attributes as follows:

If a value is specified in response message output directory (cscmng.pireexec.response.dir)

Change file attributes under response message output directory to administrator owner and group.

(Example) When /home/user1/response is specified in response message output directory

chown -R user1 /home/user1/response
chgrp -R group1 /home/user1/response

(5) Changing the file attributes under System Administrator information directory

See HCSC server setup information with the command cscutil and, change the file attributes as follows:

If hcscserver-data-filepath property is specified

Change the file attributes under System Administrator information directory to administrator owner and group.

(Example) When /home/user1/cscsys is specified in System Administrator information directory

```
chown -R user1 /home/user1/cscsys
chgrp -R group1 /home/user1/cscsys
```

(6) Changing file attributes of SQL script file

See HCSC server setup information with the command cscutil and, change the file attributes as follows:

If sql-scriptfilename property is specified

Change SQL script file attributes to administrator owner and group.

(Example) When /home/user1/sqlsetup is specified in SQL script file

```
chown user1 /home/user1/sqlsetup
chgrp group1 /home/user1/sqlsetup
```

(7) Changing the file attributes of SOAP Fault action definition file

See HCSC server runtime information with the command cscsvconfig -operation get and, change the file attributes as follows:

If soapfault-targetnamespace-filepath property is specified

Change the SOAP Fault action definition file attributes to administrator owner and group.

(Example) When /home/user1/soapfaultname is specified in SOAP Fault action definition file

```
chown user1 /home/user1/soapfaultname
chgrp group1 /home/user1/soapfaultname
```

(8) Changing the file attributes of the user message trace

See HCSC server runtime information with the command cscsvconfig -operation get and, change the file attributes as follows:

If telegramtrace-filepath property is specified

Change the file attributes under user message trace output destination directory, to administrator owner and group.

(Example) When /home/user1/telegramtracefile is specified in user message trace output destination path

```
chown -R user1 /home/user1/telegramtracefile
chgrp -R group1 /home/user1/telegramtracefile
```

(9) Changing the file attributes under method trace output destination directory

See HCSC server runtime information with the command cscsvconfig -operation get and, change the file attributes as follows:

If methodtrace-filepath property is specified

Change the file attributes under method trace output destination directory to administrator owner and group.

(Example) When /home/user1/methodtracefile is specified in method trace output destination path

```
chown -R user1 /home/user1/methodtracefile
chgrp -R group1 /home/user1/methodtracefile
```

(10) Changing the file attributes under request trace output destination directory

See HCSC server runtime information with the command cscsvconfig -operation get, and, change the file attributes as follows:

If requesttrace-filepath property is specified

Change the file attributes under request trace output destination directory to administrator owner and group.

(Example) When /home/user1/requesttracefile is specified in request trace output destination path

```
chown -R user1 /home/user1/requesttracefile
chgrp -R group1 /home/user1/requesttracefile
```

(11) Changing the file attributes under work folder root

See HCSC server runtime information with the command, cscsvconfig -operation get, and, change the file attributes as follows:

If work-folder property is specified

Change the file attributes under work folder root to administrator owner and group.

(Example) If /home/user1/workfolder is specified in the absolute path of work folder root

```
chown -R user1 /home/user1/workfolder
chgrp -R group1 /home/user1/workfolder
```

(12) Changing the file attributes under common folder

See HCSC server runtime information with the command, cscsvconfig -operation get and, change the file attributes as follows:

common-folder-<common folder definition name> property is specified

Change the file attributes under common folder defined in common folder definition name to administrator owner and group.

(Example) When /home/user1/commonfolder is specified in the absolute path of common folder

```
chown -R user1 /home/user1/commonfolder
chgrp -R group1 /home/user1/commonfolder
```

(13) Changing file attributes under the directory specified in environment variable CSCMNG_HOME

If multiple environments are created (environment variable CSCMNG_HOME is specified) on 1 machine, change the file attributes under the directory specified in CSCMNG_HOME, to administrator owner and group.

(Example) If /home/user1/cscmng1 is specified in environment variable CSCMNG_HOME

```
chown -R user1 /home/user1/cscmng1
chgrp -R group1 /home/user1/cscmng1
```

(14) Changing the file attributes under the directory specified in environment variable CSCFTP_CMD_LOG

If output destination of log at the time of executing operating command is specified (environment variable CSCFTP_CMD_LOG is specified), change the file attributes under the directory specified in CSCFTP_CMD_LOG, to administrator owner and group.

(Example) If /home/user1/ftpcmdlog1 is specified in environment variable CSCFTP_CMD_LOG

```
chown -R user1 /home/user1/ftpcmdlog1
chgrp -R group1 /home/user1/ftpcmdlog1
```

A.2 Notes

- Make sure that the Service Coordinator administrator is the same as the Component Container administrator.
- Do not create any file under the specified repository root (`cscmng.repository.root`), log directory (`cscmng.log.dir`), or the response message output directory (`cscmng.pireexec.response.dir`). Also, do not set a directory that already contains files (such as `/opt` or `/usr`).
- Do not change the administrator while a command provided by Component Container, Manager, or Service Coordinator is running. If an attempt to do this is made, operations are not guaranteed.
- If a command is executed by a different administrator or in an invalid environment, the following messages may be displayed:
  - Because the user *name-of-user-executing-the-command* and file owner of `/opt/Cosminexus/CSC` *directory-owner-user-name* is different, the command cannot be executed.
  - Cannot get owner name of `/opt/Cosminexus/CSC`
  - Cannot get user name (failed:`/usr/bin/id -un`)
  - Cannot get owner id (failed:`/usr/bin/id` *directory-owner-user-name* `-u`)
  - Cannot get user id (failed:`/usr/bin/id -u`)

B. Operations that can be Performed Using Screens and Commands

The operations that can be performed on the service platform during system setup and system operation are different. The following table shows the operations that can be performed using a screen or command:

Table B–1: Table Operations that can be performed using a screen or command

Environment	Classification		Contents	Screen	Command	Command name
	Functional classification	Target				
Operating environment	Management	User	Change login information	N	Y	cscpasswd
		Repository	Import repository	N	Y	cscrepctl
			Export repository	N	Y	cscrepctl
			Display repository information	N	Y	cscrepls
			Manage difference information of repository	N	Y	cscrepdiff
		Service information	Display information	N	Y	cscsvcls
			Manage information	N	Y	cscsvcctl
			Acquiring, setting up and deleting definition information of custom reception or the following service adapters: • DB adapter • TP1 adapter • File adapter • Object Access adapter • Message Queue adapter • FTP adapter • File operations adapter • Mail adapter • HTTP adapter • Custom adapter	N	Y	csccmctl
		Environment information	Acquiring a backup of the environment	N	Y	cscenvbackup
			Restoring the environment	N	Y	cscenvrestore
	Setup	HCSC server	Setting up the HCSC server	N	Y	cscsvsetup
			Unsetup HCSC server	N	Y	cscsvunsetup
		HCSC component	Deploying HCSC components	N	Y	csccompodeploy

Environment	Classification		Contents	Screen	Command	Command name
	Functional classification	Target				
Operating environment	Setup	HCSC component	Deleting HCSC component	N	Y	csccompoundeploy
		Easy Setup	Easy setup of production environment	N	Y	cscsetup
	Operation	HCSC server	Starting HCSC server	Y	Y	cscsvstart
			Stopping HCSC server	Y	Y	cscsvstop
			Specifying and acquire HCSC server runtime definition information	Y	Y	cscsvconfig
			Checking the running status of HCSC server	Y	Y	cscstatus
			Checking HCSC server setup information	N	Y	cscutil
			Checking HCSC server runtime information	N	Y	cscutil
			Displaying HCSC server resource running information	Y	Y	cscresinfo
		Standard reception and user-defined reception	Starting standard reception or user-defined reception	Y	Y	cscrcptnstart
			Stopping standard reception or user-defined reception	Y	Y	cscrcptnstop
			Checking running status of standard reception or user-defined reception	Y	Y	cscstatus
		HCSC component	Starting HCSC component	Y	Y	csccompostart
			Stopping HCSC component	Y	Y	csccompostop
			Pre-caching format definition and data conversion definition	N	Y	cscprecache
			Checking HCSC component runtime information	Y	Y	csccompoconfig
			Checking running status of HCSC component	Y	Y	cscstatus
		Process instance	Search process instance execution log	Y	Y	cscpiselect

Environment	Classification		Contents	Screen	Command	Command name
	Functional classification	Target				
Operating environment	Operation	Process instance	Acquiring correlation set information from process instance execution log	Y	Y	cscpiselect
			Acquiring variable information from process instance execution log	Y	Y	cscpiselect
			Acquiring activity information from process instance execution log	Y	Y	cscpiselect
			Deleting process instance execution log	Y	Y	cscpidelete
			Deleting process instance execution log in batches	Y	Y	cscpidelete
			Re-executing process instance	Y	Y	cscpireexec
			Executing process instance in batches	Y	Y	cscpireexec
		Application	Running applications	N	Y	cscapputil
	Tool	HCSC server	Upgrading the version of HCSC server	N	Y	cscenvupdate
		Message tracking	Starting message tracking	N	Y	cscmsgtk
		Repository	Updating repository	N	Y	cscrepupdate

Legend:

Y: Can be performed.

N: Cannot be performed.

C. Database Table Information

C.1 Table information about process instance execution log management

(1) Table information

The following tables are required for every HCSC cluster.

- Basic information table
- Variable information table
- Message log related information table

(a) Basic information table

The basic information table stores the basic elements (instances) of business process execution.

- **CSCBP_<cluster name>_PROCESS table**

  The contents of CSCBP_<cluster name>_PROCESS table are as follows:

No.	Column name	Description	HiRDB type	ORACLE type	Existence of index	NULL value	Update	Default value
1	ProcessID	Process instance identifier	MVARCHAR(240)	VARCHAR2(240)	Yes	Not possible	Not possible	Not possible
2	ProcessDefinitionName	BP definition name	MVARCHAR(64)	VARCHAR2(64)	Yes	Not possible	Not possible	Not possible
3	ProcessDefinitionVersion	BP definition version	SMALLINT	NUMBER(5)	No	Not possible	Not possible	Not possible
4	State	Process instance status	VARCHAR(20)	VARCHAR2(20)	Yes	Not possible	Yes	Not possible
5	ChangeCount#1	Number of data updates	INTEGER#2	NUMBER(10)#3	No	Not possible	Possible	Not possible
6	StartTime	Process instance Start time (GMT)	TIMESTAMP(0)	TIMESTAMP(0)	Yes	Possible	Possible	NULL
7	EndTime	Process instance end time (GMT)	TIMESTAMP(0)	TIMESTAMP(0)	Yes	Possible	Possible	NULL
8	CSCServerName	Last executed HCSC server name	VARCHAR(8)	VARCHAR2(8)	Yes	Possible	Possible	NULL
9	SplitKey#4	Split key (GMT)	CHAR(2)	CHAR(2)	Yes	Not possible	Not possible	Not possible

Note#1

There is no need to know the value because this item is used for internal management during execution.

Note#2

"SMALLINT" in versions prior to the version 08-10.

Also, if overwrite installation is performed from a version prior to the version 08-10, the type is "SMALLINT", since the area does not change.

Note#3

"NUMBER(5)" in versions prior to the version 08-10.

Also, if overwrite installation is performed from a version prior to the version 08-10, the type is "NUMBER(5)", since the area does not change.

Note#4

This column is included in SQL script file if you set up by specifying a value other than "NONE" in the db-tbl-split-key of HCSC server setup definition file. For details on db-tbl-split-key, see "HCSC server setup definition file" in "Service Platform Reference Guide".

- **CSCBP_<cluster name>_ACTIVITY table**

The contents of CSCBP_<cluster name>_ACTIVITY table are as follows:

No.	Column name	Description	HiRDB type	ORACLE Type	Index	NULL	Update	Default value
1	ProcessID	Process instance identifier	MVARCHAR(240)	VARCHAR2(240)	Yes	Not possible	Not possible	Not possible
2	ActivityNumber	Number to identify activity instance. Unique in process instance.	INTEGER#2	NUMBER(10)#3	No	Not possible	Not possible	Not possible
3	ActivityDefinitionName	Activity definition name	MVARCHAR(64)	VARCHAR2(64)	No	Not possible	Not possible	Not possible
4	ActivityKind	Activity type	VARCHAR(16)	VARCHAR2(16)	No	Not possible	Not possible	Not possible
5	ParentNumber#1	New activity instance identifier	INTEGER#2	NUMBER(10)#3	No	Not possible	Not possible	Not possible
6	ScopeNumber	Identification number of the associated scope instance	INTEGER#2	NUMBER(10)#3	No	Not possible	Not possible	Not possible
7	RepeatNumber#1	Identification number of the associated repeat process	INTEGER#2	NUMBER(10)#3	No	Not possible	Not possible	Not possible
8	State	Activity instance status	VARCHAR(20)	VARCHAR2(20)	No	Not possible	Possible	Not possible
9	FirstChildNumber#1	Smallest identification number of child activity instance	INTEGER#2	NUMBER(10)#3	No	Not possible	Possible	Not possible
10	LastChildNumber#1	Largest identification number of child activity instance	INTEGER#2	NUMBER(10)#3	No	Not possible	Possible	Not possible
11	StartTime	Activity instance start time (GMT)	TIMESTAMP(0)	TIMESTAMP(0)	No	Possible	Possible	NULL
12	EndTime	Activity instance end time (GMT)	TIMESTAMP(0)	TIMESTAMP(0)	No	Possible	Possible	NULL
13	WaitTime	Wait cancellation time of Activity (GMT)	TIMESTAMP(0)	TIMESTAMP(0)	No	Possible	Possible	NULL
14	SplitKey#4	Split key (GMT)	CHAR(2)	CHAR(2)	Yes	Not possible	Not possible	Not possible

#1

There is no need to know the value because this item is used for internal management during execution.

#2

"SMALLINT" in versions prior to the version 08-10.

Also, if overwrite installation is performed from a version prior to the version 08-10, the type is "SMALLINT", since the area does not change.

#3

"NUMBER(5)" in versions prior to the version 08-10.

Also, if overwrite installation is performed from a version prior to the version 08-10, the type is "NUMBER(5)", since the area does not change.

#4

This column is included in SQL script file, if you set up by specifying a value other than "NONE" in the db-tbl-split-key of HCSC server setup definition file. For details on db-tbl-split-key, see "HCSC server setup definition file" in "Service Platform Reference Guide".

- **CSCBP_<cluster name>_LINK table**

The contents of CSCBP_<cluster name>_LINK table are as follows:

No.	Column name	Description	HiRDB type	ORACLE type	Index	NULL	Update	Default value
1	ProcessID	Process instance identifier	MVARCHAR(240)	VARCHAR2(240)	Yes	Not possible	Not possible	Not possible
2	LinkDefinitionName	Link definition name	MVARCHAR(64)	VARCHAR2(64)	Yes	Not possible	Not possible	Not possible
3	RepeatNumber#1	Identification number of the associated repeat process	INTEGER#2	NUMBER(10) #3	Yes	Not possible	Not possible	Not possible
4	State	Link status (true or false)	CHAR(1)	CHAR(1)	No	Not possible	Not possible	Not possible
5	SplitKey#4	Split key (GMT)	CHAR(2)	CHAR(2)	Yes	Not possible	Not possible	Not possible

Note#1

There is no need to know the value, since this item is used for internal management during execution.

Note#2

"SMALLINT" in versions prior to the version 08-10.

Also, if overwrite installation is performed from a version prior to the version 08-10, the type is "SMALLINT", since the area does not change.

Note#3

"NUMBER(5)" in versions prior to the version 08-10.

Also, if overwrite installation is performed from a version prior to the version 08-10, the type is "NUMBER(5)", since the area does not change.

Note#4

This column is included in SQL script file, if you set up by specifying a value other than "NONE" in the db-tbl-split-key of HCSC server setup definition file. For details on db-tbl-split-key, see "HCSC server setup definition file" in "Service Platform Reference Guide".

- **CSCBP_<cluster name>_CORRELATIONSET table**

The contents of CSCBP_<cluster name>_CORRELATIONSET table are as follows:

No.	Column name	Description	HiRDB type	ORACLE type	Index	NULL	Update	Default value
1	ProcessID	Process instance identifier	MVARCHAR(240)	VARCHAR2(240)	Yes	Not possible	Not possible	Not possible
2	ProcessDefinitionName	BP definition name	MVARCHAR(64)	VARCHAR2(64)	Yes	Not possible	Not possible	Not possible

No.	Column name	Description	HiRDB type	ORACLE type	Index	NULL	Update	Default value
3	ProcessDefinitionVersion	BP definition version	SMALLINT	NUMBER(5)	No	Not possible	Not possible	Not possible
4	ScopeDefinitionName	Scope definition name	MVARCHAR(64)	VARCHAR2(64)	Yes	Not possible	Not possible	Not possible
5	ScopeNumber	Scope instance identification number	INTEGER#1	NUMBER(10)#2	Yes	Not possible	Not possible	Not possible
6	CorrelationSetName	Correlation set definition name	MVARCHAR(64)	VARCHAR2(64)	Yes	Not possible	Not possible	Not possible
7	CorrelationSetValue	Correlation set value. Stringizing and linking of this value is done and then it is stored.	MVARCHAR(512)	VARCHAR2(512)	Yes	Not possible	Not possible	Not possible
8	State	Validity of correlation set (true or false)	CHAR(1)	CHAR(1)	No	Not possible	Possible	Not possible
9	SplitKey#3	Split key (GMT)	CHAR(2)	CHAR(2)	Yes	Not possible	Not possible	Not possible

Note#1

"SMALLINT" in versions prior to the version 08-10.

Also, if overwrite installation is performed from a version prior to the version 08-10, the type is "SMALLINT", since the area does not change.

Note#2

"NUMBER(5)" in versions prior to the version 08-10.

Also, if overwrite installation is performed from a version prior to the version 08-10, the type is "NUMBER(5)", since the area does not change.

Note#3

This column is included in SQL script file, if you set up by specifying a value other than "NONE" in the db-tbl-split-key of HCSC server setup definition file. For details on db-tbl-split-key, see "HCSC server setup definition file" in "Service Platform Reference Guide".

(b) Variable information table

The variable information table stores the values of user-defined variables while business processes are being executed.

- **CSCBP_<cluster name>_STR_VARIABLE table**

  The contents of the CSCBP_<cluster name>_STR_VARIABLE table are as follows:

No.	Column name	Description	HiRDB type	ORACLE type	Index	NULL	Update	Default value
1	ProcessID	Process instance identifier	MVARCHAR(240)	VARCHAR2(240)	Yes	Not possible	Not possible	Not possible
2	ScopeNumber	Scope instance identification number	INTEGER#1	NUMBER(10)#2	Yes	Not possible	Not possible	Not possible
3	VariableName	Variable definition name	MVARCHAR(64)	VARCHAR2(64)	Yes	Not possible	Not possible	Not possible
4	VariableValue	Variable value	MVARCHAR(4000)	VARCHAR2(4000)	No	Possible#3	Possible	Not possible
5	SplitKey#4	Split key (GMT)	CHAR(2)	CHAR(2)	Yes	Not possible	Not possible	Not possible

Note#1

"SMALLINT" in versions prior to the version 08-10.

Also, if overwrite installation is performed from a version prior to the version 08-10, the type is "SMALLINT", since the area does not change.

Note#2

"NUMBER(5)" in versions prior to the version 08-10.

Also, if overwrite installation is performed from a version prior to the version 08-10, the type is "NUMBER(5)", since the area does not change.

Note#3

In HiRDB, the null value cannot be specified, but in Oracle, the null value can be specified.

Note#4

This column is included in SQL script file, if you set up by specifying a value other than "NONE" in the db-tbl-split-key of HCSC server setup definition file. For details on db-tbl-split-key, see "HCSC server setup definition file" in "Service Platform Reference Guide".

- **CSCBP_<cluster name>_NUM_VARIABLE table**

The contents of the CSCBP_<cluster name>_NUM_VARIABLE table are as follows:

No.	Column name	Description	HiRDB type	ORACLE type	Index	NULL	Update	Default value
1	ProcessID	Process instance identifier	MVARCHAR(240)	VARCHAR2(240)	Yes	Not possible	Not possible	Not possible
2	ScopeNumber	Scope instance identification number	INTEGER#1	NUMBER(10)#2	Yes	Not possible	Not possible	Not possible
3	VariableName	Variable definition name	MVARCHAR(64)	VARCHAR2(64)	Yes	Not possible	Not possible	Not possible
4	VariableValue	Variable value	DOUBLE PRECISION	NUMBER	No	Not possible	Possible	Not possible
5	SplitKey#3	Split key (GMT)	CHAR(2)	CHAR(2)	Yes	Not possible	Not possible	Not possible

Note#1

"SMALLINT" in versions prior to the version 08-10.

Also, if overwrite installation is performed from a version prior to the version 08-10, the type is "SMALLINT", since the area does not change.

Note#2

"NUMBER(5)" in versions prior to the version 08-10.

Also, if overwrite installation is performed from a version prior to the version 08-10, the type is "NUMBER(5)", since the area does not change.

Note#3

This column is included in SQL script file, if you set up by specifying a value other than "NONE" in the db-tbl-split-key of HCSC server setup definition file. For details on db-tbl-split-key, see "HCSC server setup definition file" in "Service Platform Reference Guide".

- **CSCBP_<cluster name>_BOOL_VARIABLE table**

The contents of the CSCBP_<cluster name>_BOOL_VARIABLE table are as follows:

No.	Column name	Description	HiRDB type	ORACLE type	Index	NULL	Update	Default value
1	ProcessID	Process instance identifier	MVARCHAR(240)	VARCHAR2(240)	Yes	Not possible	Not possible	Not possible
2	ScopeNumber	Scope instance identification number	INTEGER#1	NUMBER(10)#2	Yes	Not possible	Not possible	Not possible
3	VariableName	Variable definition name	MVARCHAR(64)	VARCHAR2(64)	Yes	Not possible	Not possible	Not possible

No.	Column name	Description	HiRDB type	ORACLE type	Index	NULL	Update	Default value
4	VariableValue	Variable value	CHAR(1)	CHAR(1)	No	Not possible	Possible	Not possible
5	SplitKey#3	Split key (GMT)	CHAR(2)	CHAR(2)	Yes	Not possible	Not possible	Not possible

Note#1

"SMALLINT" in versions prior to the version 08-10.

Also, if overwrite installation is performed from a version prior to the version 08-10, the type is "SMALLINT" because the area does not change.

Note#2

"NUMBER(5)" in versions prior to the version 08-10.

Also, if overwrite installation is performed from a version prior to the version 08-10, the type is "NUMBER(5)", since the area does not change.

Note#3

This column is included in SQL script file, if you set up by specifying a value other than "NONE" in the db-tbl-split-key of HCSC server setup definition file. For details on db-tbl-split-key, see "HCSC server setup definition file" in "Service Platform Reference Guide".

- **CSCBP_<cluster name>_MSG_VARIABLE table**

The contents of the CSCBP_<cluster name>_MSG_VARIABLE table are as follows:

No.	Column name	Description	HiRDB type	ORACLE type	Index	NULL	Update	Default value
1	ProcessID	Process instance identifier	MVARCHAR(240)	VARCHAR2(240)	Yes	Not possible	Not possible	Not possible
2	ScopeNumber	Identification number of a scope instance	INTEGER#1	NUMBER(10) #2	Yes	Not possible	Not possible	Not possible
3	VariableName	Variable definition Name	MVARCHAR(64)	VARCHAR2(64)	Yes	Not possible	Not possible	Not possible
4	VariableValue	Variable Value	BINARY(2147483639)	BLOB	No	Possible #3	Possible	Not possible
5	SplitKey#4	Split key (GMT)	CHAR(2)	CHAR(2)	Yes	Not possible	Not possible	Not possible

Note#1

"SMALLINT" in versions prior to the version 08-10.

Also, if overwrite installation is performed from a version prior to the version 08-10, the type is "SMALLINT", since the area does not change.

Note#2

"NUMBER(5)" in versions prior to the version 08-10.

Also, if overwrite installation is performed from a version prior to the version 08-10, the type is "NUMBER(5)", since the area does not change.

Note#3

In HiRDB, the null value cannot be specified. However, the null value can be specified in Oracle.

Note#4

This column is included in SQL script file, if you set up by specifying a value other than "NONE" in the db-tbl-split-key of HCSC server setup definition file. For details on db-tbl-split-key, see "HCSC server setup definition file" in "Service Platform Reference Guide".

(c) Message log related information table

The message log related information table stores the message log related data.

- **CSCBP_<cluster name>_MSG_RELATION table**

The contents of the CSCBP_<cluster name>_MSG_RELATION table are as follows:

No.	Column name	Description	HiRDB type	ORACLE type	Index	NULL	Update	Default value
1	MessageID#1	Message common ID	VARCHAR(75)	VARCHAR2(75)	Yes	Not possible	Not possible	Not possible
2	ProcessID#1	Process instance identifier	MVARCHAR(240)	VARCHAR2(240)	Yes	Not possible	Not possible	Not possible
3	ActivityNumber#1	Identification number of an activity instance	INTEGER#2	NUMBER(10)#3	Yes	Not possible	Not possible	Not possible
4	SendOrReceive#1	Send/receive flag for the message	CHAR(1)	CHAR(1)	Yes	Not possible	Not possible	Not possible
5	AsynchronousMessagingID#1	Asynchronous messaging ID that uses Reliable Messaging	VARCHAR(255)	VARCHAR2(255)	Yes	Possible	Not possible	NULL
6	SplitKey#4	Split key (GMT)	CHAR(2)	CHAR(2)	Yes	Not possible	Not possible	Not possible

Note#1

There is no need to know the value, since this item is used for internal management during execution.

Note#2

"SMALLINT" in versions prior to the version 08-10.

Also, if overwrite installation is performed from a version prior to the version 08-10, the type is "SMALLINT", since the area does not change.

Note#3

"NUMBER(5)" in versions prior to the version 08-10.

Also, if overwrite installation is performed from a version prior to the version 08-10, the type is "NUMBER(5)", since the area does not change.

Note#4

This column is included in SQL script file, if you set up by specifying a value other than "NONE" in the db-tbl-split-key of HCSC server setup definition file. For details on db-tbl-split-key, see "HCSC server setup definition file" in "Service Platform Reference Guide".

(2) Status information

This subsection describes the values that are stored in the table and the actual values (character strings).

(a) HCSC cluster name

Specify a name consisting of a maximum of 8 alphanumeric characters.

(b) Process instance identifier

This is an identifier used to uniquely identify each process instance.

(c) Process instance status

No.	Name	Description	Value in database
1	Unexecuted	The process instance is not executed and might be executed in the future.	Unexecution
2	Executing	The process instance is executing.	Executing
3	Error	An exception occurred in the invoke service activity or scope activity, and the process instance was interrupted with an error.	Error

No.	Name	Description	Value in database
4	Completed	The global scope of the process is completed and the process instance is completed.	Completed
5	Terminated with fault	A fault occurred and could not be detected by the global scope, resulting in termination of the process instance with a fault.	Faulted
6	Forced termination	The process instance was forcibly terminated in the end activity.	Terminated

(d) Activity type

No.	Name	Description	Value in database
1	receive	Indicates a receive activity.	RECEIVE
2	reply	Indicates a reply activity.	REPLY
3	invoke	Indicates an invoke service activity.	INVOKE
4	assign	Indicates an assign activity.	ASSIGN
5	scope	Indicates a scope activity.	SCOPE
6	sequence	Indicates activities to be executed in the defined order.	SEQUENCE
7	flow	Indicates a flow activity.	FLOW
8	switch	Indicates a switch activity.	SWITCH
9	while	Indicates a while activity.	WHILE
10	java	Indicates an invoke Java activity.	JAVA
11	wait	Indicates a standby activity.	WAIT
12	empty	Indicates an empty activity.	EMPTY
13	throw	Indicates a throw activity.	THROW
14	validate	Indicates a validation activity.	VALIDATE

(e) Activity instance status

No.	Name	Description	Value in database
1	Unexecuted	The activity instance is not executed and might be executed in the future.	Unexecution
2	Unomitted	The activity instance is not executed and its execution might be omitted in the future.	Unomission
3	Executing	The activity instance is executing.	Executing
4	Executing (Wait)	Roll back is executed and the scope activity instance might be re-executed in future.	Executingwait
5	Waiting	The receive activity instance is ready to receive.	Awaiting
6	Faulting	The scope activity instance is executing an activity that was detected during fault processing.	Faulting
7	Error	An exception (error) occurred in the invoke service activity or the scope activity, and the activity instance was interrupted with an error.	Error
8	Completed	The activity instance was executed normally and then terminated.	Completed
9	Completed (Wait)	The scope activity or reply activity instance was executed normally and might be re-executed in future.	Completedwait

No.	Name	Description	Value in database
10	Cancelled	A fault occurred and execution of the activity instance was cancelled.	Canceled
11	Terminated with fault	A fault occurred during execution of the activity instance, and the activity instance was terminated.	Faulted
12	Execution omitted	Execution of the activity instance was omitted and terminated.	Omitted

(f) Link status

No.	Name	Description	Value in database
1	True	Indicates true active status.	1
2	False	Indicates false active status.	0

(g) Correlation set status

No.	Name	Description	Value in database
1	Valid	Indicates valid status.	1
2	Invalid	Indicates invalid status.	0

(h) Value of Boolean variable

No.	Name	Description	Value in database
1	True	Indicates true.	1
2	False	Indicates false.	0

(i) Send/receive flag for the message

No.	Name	Description	Value in database
1	receive reception	Flag indicating that the message was received by a receive activity.	R
2	invoke transmission	Flag indicating that the message was sent by an invoke service activity.	O

(j) Identification number of the dependent repetition process (RepeatNumber)

- Sets the local activity instance identification number, when parent activity definition is a repetition process.
- Sets the parent activity instance repetition process identification number, when parent activity definition is not a repetition process.

(k) Smallest and largest identification numbers of child activity instances (FirstChildNumber/LastChildNumber)

- Default value indicates local activity instance identification number.
- When child activity instances are created, sets the smallest or largest identification number for them.

(3) Index information

The following table describes the information of index to be given in respective tables:

- **Index for the CSCBP_<cluster name>_PROCESS table**

No.	Index name	UNIQUE attribute	Order in index	Column name
1	CSCBP_<cluster name>_PROCESS_IDX1	Yes	1	ProcessID
			2	SplitKey#
2	CSCBP_<cluster name >_PROCESS_IDX2	No	1	ProcessDefinitionName
			2	State
			3	StartTime
3	CSCBP_<cluster name >_PROCESS_IDX3	No	1	ProcessDefinitionName
			2	State
			3	EndTime
4	CSCBP_<cluster name >_PROCESS_IDX4	No	1	CSCServerName
			2	ProcessDefinitionName
			3	State

Note#

This column is included in SQL script, if you split the range as per the date data (set up by specifying a value other than "NONE" for db-tbl-split-key in HCSC server setup definition file). For details on db-tbl-split-key, see "HCSC server setup definition file" in "Service Platform Reference Guide".

- **Index for the CSCBP_<cluster name>_ACTIVITY table**

No.	Index name	UNIQUE attribute	Order in index	Column name
1	CSCBP_<cluster name>_ACTIVITY_IDX	Yes	1	ProcessID
			2	ActivityNumber
			3	SplitKey#

Note#

This column is included in SQL script, if you split the range as per the date data (set up by specifying a value other than "NONE" for db-tbl-split-key in HCSC server setup definition file). For details on db-tbl-split-key, see "HCSC server setup definition file" in "Service Platform Reference Guide".

- **Index for the CSCBP_<cluster name>_LINK table**

No.	Index name	UNIQUE attribute	Order in index	Column name
1	CSCBP_< luster name >_LINK_IDX	Yes	1	ProcessID
			2	LinkDefinitionName
			3	RepeatNumber
			4	SplitKey#

Note#

This column is included in SQL script, if you split the range as per the date data (set up by specifying a value other than "NONE" for db-tbl-split-key in HCSC server setup definition file). For details on db-tbl-split-key, see "HCSC server setup definition file" in "Service Platform Reference Guide".

- **Index for the SCBP_<cluster name>_CORRELATIONSET table**

No.	Index name	UNIQUE attribute	Order in index	Column name
1	CSCBP_<cluster name>_CORREL_IDX1	Yes	1	ProcessID
			2	ScopeNumber
			3	CorrelationSetName
			4	SplitKey#2
2	CSCBP_<cluster name>_CORREL_IDX2	Yes	1	ProcessDefinitionName
			2	ScopeDefinitionName
			3	CorrelationSetName
			4	CorrelationSetValue
			5	ProcessID#1
			6	SplitKey#2

Note#1

This column is to be included in SQL script file, when performing hash partitioning as per ProcessID.

Note#2

This column is included in SQL script, if you split the range as per the date data (set up by specifying a value other than "NONE" for db-tbl-split-key in HCSC server setup definition file). For details on db-tbl-split-key, see "HCSC server setup definition file" in "Service Platform Reference Guide".

- **Index for the CSCBP_<cluster name>_STR_VARIABLE table**

No.	Index name	UNIQUE attribute	Order in index	Column name
1	CSCBP_<cluster name>_STR_VAR_IDX	Yes	1	ProcessID
			2	ScopeNumber
			3	VariableName
			4	SplitKey#

#

This column is included in SQL script, if you split the range as per the date data (set up by specifying a value other than "NONE" for db-tbl-split-key in HCSC server setup definition file). For details on db-tbl-split-key, see "HCSC server setup definition file" in "Service Platform Reference Guide".

- **Index for the CSCBP_<cluster name>_NUM_VARIABLE table**

No.	Index name	UNIQUE attribute	Order in index	Column name
1	CSCBP_<cluster name>_NUM_VAR_IDX	Yes	1	ProcessID
			2	ScopeNumber
			3	VariableName
			4	SplitKey#

Note#

This column is included in SQL script, if you split the range as per the date data (set up by specifying a value other than "NONE" for db-tbl-split-key in HCSC server setup definition file). For details on db-tbl-split-key, see "HCSC server setup definition file" in "Service Platform Reference Guide".

- **Index for the CSCBP_<cluster name>_BOOL_VARIABLE table**

No.	Index name	UNIQUE attribute	Order in index	Column name
1	CSCBP_<cluster name>_BOOL_VAR_IDX	Yes	1	ProcessID
			2	ScopeNumber
			3	VariableName
			4	SplitKey#

Note#

This column is included in SQL script, if you split the range as per the date data (set up by specifying a value other than "NONE" for db-tbl-split-key in HCSC server setup definition file). For details on db-tbl-split-key, see "HCSC server setup definition file" in "Service Platform Reference Guide".

- **Index for the CSCBP_<cluster name>_MSG_VARIABLE table**

No.	Index name	UNIQUE attribute	Order in index	Column name
1	CSCBP_<cluster name>_MSG_VAR_IDX	Yes	1	ProcessID
			2	ScopeNumber
			3	VariableName
			4	SplitKey#

Note#

This column is included in SQL script, if you split the range as per the date data (set up by specifying a value other than "NONE" for db-tbl-split-key in HCSC server setup definition file). For details on db-tbl-split-key, see "HCSC server setup definition fil" in "Service Platform Reference Guide".

- **Index for the CSCBP_<cluster name>_MSG_RELATION table**

No.	Index name	UNIQUE attribute	Order in index	Column name
1	CSCBP_<cluster name>_MSG_REL_IDX1	None	1	MessageID
2	CSCBP_<cluster name >_MSG_REL_IDX2	Yes	1	ProcessID
			2	ActivityNumber
			3	SendOrReceive
			4	SplitKey#
3	CSCBP_<cluster name >_MSG_REL_IDX3	None	1	AsynchronousMessagingID

Note#

This column is included in SQL script, if you split the range as per the date data (set up by specifying a value other than "NONE" for db-tbl-split-key in HCSC server setup definition file). For details on db-tbl-split-key, see "HCSC server setup definition file" in "Service Platform Reference Guide".

(4) View table information

The following table describes information of the View table:

- **CSCBP_<cluster name>_V_ACTIVITY view table**

No.	Column name	Reference table	Reference column
1	ProcessID	ACTIVITY	ProcessID

No.	Column name	Reference table	Reference column
2	ActivityNumber	ACTIVITY	ActivityNumber
3	ProcessDefinitionName	PROCESS	ProcessDefinitionName
4	ProcessDefinitionVersion	PROCESS	ProcessDefinitionVersion
5	ActivityDefinitionName	ACTIVITY	ActivityDefinitionName
6	ActivityKind	ACTIVITY	ActivityKind
7	ParentNumber#1	ACTIVITY	ParentNumber
8	ScopeNumber	ACTIVITY	ScopeNumber
9	RepeatNumber#1	ACTIVITY	RepeatNumber
10	State	ACTIVITY	State
11	FirstChildNumber#1	ACTIVITY	FirstChildNumber
12	LastChildNumber#1	ACTIVITY	LastChildNumber
13	StartTime	ACTIVITY	StartTime
14	EndTime	ACTIVITY	EndTime
15	WaitTime	ACTIVITY	WaitTime
16	CSCServerName	PROCESS	CSCServerName
17	SplitKey#2	PROCESS	SplitKey

Note#1

There is no need to know the value, since this item is used for internal management during execution.

Note#2

This column is included in view only when you specify activity in the -table option of the cscpiselect command and specify SplitKey column in the -where or -wherefile option.

- **CSCBP_<cluster name>_V_LINK view table**

No.	Column name	Reference table	Reference column
1	ProcessID	LINK	ProcessID
2	ProcessDefinitionName	PROCESS	ProcessDefinitionName
3	ProcessDefinitionVersion	PROCESS	ProcessDefinitionVersion
4	LinkDefinitionName	LINK	LinkDefinitionName
5	RepeatNumber#1	LINK	RepeatNumber
6	State	LINK	State
7	SplitKey#2	PROCESS	SplitKey

Note#1

There is no need to know the value, since this item is used for internal management during execution.

Note#2

This column is included in view only when you specify link in the -table option of the cscpiselect command and specify SplitKey column in the -where or -wherefile option.

- **CSCBP_<cluster name>_V_STR_VARIABLE view table**

No.	Column name	Reference table	Reference column
1	ProcessID	STR_VARIABLE	ProcessID

No.	Column name	Reference table	Reference column
2	ProcessDefinitionName	PROCESS	ProcessDefinitionName
3	ProcessDefinitionVersion	PROCESS	ProcessDefinitionVersion
4	ScopeDefinitionName	ACTIVITY	ActivityDefinitionName
5	ScopeNumber	STR_VARIABLE	ScopeNumber
6	VariableName	STR_VARIABLE	VariableName
7	VariableValue	STR_VARIABLE	VariableValue
8	SplitKey#	PROCESS	SplitKey

Note#

This column is included in view only when you specify string in the -table option of the cscpiselect command and specify SplitKey column in the -where or -wherefile option.

- **CSCBP_<cluster name>_V_NUM_VARIABLE view table**

No.	Column name	Reference table	Reference column
1	ProcessID	NUM_VARIABLE	ProcessID
2	ProcessDefinitionName	PROCESS	ProcessDefinitionName
3	ProcessDefinitionVersion	PROCESS	ProcessDefinitionVersion
4	ScopeDefinitionName	ACTIVITY	ActivityDefinitionName
5	ScopeNumber	NUM_VARIABLE	ScopeNumber
6	VariableName	NUM_VARIABLE	VariableName
7	VariableValue	NUM_VARIABLE	VariableValue
8	SplitKey#	PROCESS	SplitKey

Note#

This column is included in view only when you specify numeric in the -table option of the cscpiselect command and specify SplitKey column in the -where or -wherefile option.

- **CSCBP_<cluster name>_V_BOOL_VARIABLE view table**

No.	Column name	Reference table	Reference column
1	ProcessID	BOOL_VARIABLE	ProcessID
2	ProcessDefinitionName	PROCESS	ProcessDefinitionName
3	ProcessDefinitionVersion	PROCESS	ProcessDefinitionVersion
4	ScopeDefinitionName	ACTIVITY	ActivityDefinitionName
5	ScopeNumber	BOOL_VARIABLE	ScopeNumber
6	VariableName	BOOL_VARIABLE	VariableName
7	VariableValue	BOOL_VARIABLE	VariableValue
8	SplitKey#	PROCESS	SplitKey

Note#

This column is included in view only when you specify boolean in the -table option of the cscpiselect command and specify SplitKey column in the -where or -wherefile option.

- **CSCBP_<cluster name>_V_MSG_VARIABLE view table**

No.	Column name	Reference table	Reference column
1	ProcessID	MSG_VARIABLE	ProcessID
2	ProcessDefinitionName	PROCESS	ProcessDefinitionName
3	ProcessDefinitionVersion	PROCESS	ProcessDefinitionVersion
4	ScopeDefinitionName	ACTIVITY	ActivityDefinitionName
5	ScopeNumber	MSG_VARIABLE	ScopeNumber
6	VariableName	MSG_VARIABLE	VariableName
7	VariableValue	MSG_VARIABLE	VariableValue
8	SplitKey#	PROCESS	SplitKey

Note#

This column is included in view only when you specify message in the -table option of the cscpiselect command and specify SplitKey column in the -where or -wherefile option.

C.2 Table Information About Message Execution Log Management

(1) Table information

The following table is required for each cluster:

- Execution log information table

(a) Execution log information table

- CSCMSG_Ccluster-name_EXECHISTORY table

No.	Column name	Description	HiRDB type	ORACLE type	Use of index	Null value	UNIQUE attribute
1	MESSAGE_ID	Unique identifier assigned to each message • CSC + *HCSC-server-name* + *current-time-(milliseconds)* + *serial-number*	VARCHAR(75)	VARCHAR2(75)	Yes	Yes	None
2	MESSAGE_ID_CSC_MSG	Unique identifier used to identify a message for the messaging infrastructure at the HCSC server • MSG + *HCSC-server-name* + *acceptance-type* + *current-time-(milliseconds)* + *serial-number*	VARCHAR(84)	VARCHAR2(84)	None	Yes	None
3	REQUEST_CSC_SERVER_NAME	Name of the HCSC server that accepted the request	VARCHAR(8)	VARCHAR2(8)	None	Yes	None
4	HISTORY_KIND_DIRECTION	Direction of execution log collection	VARCHAR(26)	VARCHAR2(26)	None	Yes	None

No.	Column name	Description	HiRDB type	ORACLE type	Use of index	Null value	UNIQUE attribute
4	HISTORY_KIND_DIRECTION	Service Request Direction/Service Response Direction/ Service Error/Service Fault	VARCHAR(26)	VARCHAR2(26)	None	Yes	None
5	TIME_STAMP	Execution log collection time stamp (milliseconds)	TIMESTAMP(4)	NUMBER(20.0)	None	Yes	None
6	REQUEST_SYNCHRONOUS_KIND	Requester's protocol WebService/ SessionBean/ MDB_WSR/ MDB_DBQ	VARCHAR(16)	VARCHAR2(16)	None	Yes	None
7	SERVICE_REQUEST_TYPE	Type of service requester • ClientProgram (client program) • BusinessProcess (business process)	VARCHAR(24)	VARCHAR2(24)	None	Yes	None
8	REQUEST_USER_TEL_TYPE	Type of request user message XML/BINARY/ANY	VARCHAR(8)	VARCHAR2(8)	None	Yes	None
9	RESPONSE_USER_TEL_TYPE	Type of reply user message XML/BINARY/ANY	VARCHAR(8)	VARCHAR2(8)	None	Yes	None
10	SERVICE_NAME	Input service name from requester (request target service module)	MVARCHAR(64)	NVARCHAR2(64)	None	Yes	None
11	CLIENT_ID	Correlation identifier used to identify the message specified by the client program	VARCHAR(255)	VARCHAR2(255)	Yes	Yes	None
12	SERVICE_OPERATION_NAME	Operation of service modules required in the case of Synchronous (Web Services) Operation of WSDL <wsdl:operation>	MVARCHAR(255)	NVARCHAR2(255)	None	Yes	None
13	REPLY_TO_QUEUE_NAME	Name of queue for receiving response for asynchronous service (MDB (WS-R), MDB (database queue))	VARCHAR(30)	VARCHAR2(30)	None	Yes	None
14	ADAPTER_NAME	Service ID of service adapter or business process	VARCHAR(8)	VARCHAR2(8)	None	Yes	None
15	ADAPTER_SERVICE_NAME	Service name • Service name of service adapter	MVARCHAR(64)	NVARCHAR2(64)	None	Yes	None

No.	Column name	Description	HiRDB type	ORACLE type	Use of index	Null value	UNIQUE attribute
15	ADAPTER_SERVICE_NAME	• Service name of business process • Service group name	MVARCHAR(64)	NVARCHAR2(64)	None	Yes	None
16	ADAPTER_CLUSTER_NAME	Information about the cluster to which the adapter belongs	VARCHAR(8)	VARCHAR2(8)	None	Yes	None
17	ADAPTER_KIND	Type of service modules for adapter ServiceAdapter/ BusinessProcess/ ServiceGroup	VARCHAR(32)	VARCHAR2(32)	None	Yes	None
18	ADAPTER_SYNCHRONOUS_KIND	Service module protocol at the adapter target WebService/ SessionBean/ MDB_WSR/ MDB_DBQ/Custom	VARCHAR(16)	VARCHAR2(16)	None	Yes	None
19	INTERLOCK_CSC_PROTOCOL	Protocol used for transfer to the linked HCSC server WebService/ SessionBean/ MDB_WSR	VARCHAR(32)	VARCHAR2(32)	None	Yes	None
20	MESSAGE_ID_CSC_BP_ACTIVITY	Business process activity number (number used to identify a business process activity instance) No value: -1	INTEGER#1	NUMBER(10,0)#2	None	Yes	None
21	MESSAGE_ID_CSC_BP_PROCESS	Process ID of business process	MVARCHAR(240)	NVARCHAR2(240)	None	Yes	None
22	CSC_BP_REQUEST_TYPE	Type of requests for business processes • `REPLY_AFTER`: Request for continuous execution after `reply` • `RECOVER`: Request for process re-execution • `WAIT_AFTER`: Request for process execution after wait	VARCHAR(32)	VARCHAR2(32)	None	Yes	None
23	JMS_HEADER_JMS_MESSAGE_ID	JMS header • JMSMessageID	VARCHAR(255)	VARCHAR2(255)	None	Yes	None
24	JMS_HEADER_JMS_CORRELATION_ID	JMS header	VARCHAR(255)	VARCHAR2(255)	None	Yes	None

No.	Column name	Description	HiRDB type	ORACLE type	Use of index	Null value	UNIQUE attribute
24	JMS_HEADER_JMS_CORRELATION_ID	• JMSCorrelationID	VARCHAR(255)	VARCHAR2(255)	None	Yes	None
25	ROUTE_HISTORY	Information passed as route history (Displaying with a character string to which *HCSC-server-name* or *service-ID* is attached by '->')	VARCHAR(255)	VARCHAR2(255)	None	Yes	None
26	ERROR_CODE	Error (Fault) information from a service module, business process, or custom adapter	MVARCHAR(4000)	NVARCHAR2(1333)	None	Yes	None
27	USER_TEL_ORG_BINARY	User message	BINARY(2147483639)	LONG RAW	None	Yes	None
28	OPTION1	Reserve 1	BINARY(2000)	RAW(2000)	None	Yes	None
29	OPTION2	Reserve 2	BINARY(2000)	RAW(2000)	None	Yes	None
30	OPTION3	Reserve 3	BINARY(2000)	RAW(2000)	None	Yes	None

#1

"SMALLINT" in versions prior to the version 08-10.

Also, if overwrite installation is performed from a version prior to the version 08-10, the type is "SMALLINT" because the area does not change.

#2

"NUMBER(5)" in versions prior to the version 08-10.

Also, if overwrite installation is performed from a version prior to the version 08-10, the type is "NUMBER(5)" because the area does not change.

(2) Index information

The following lists and describes the information about the index that is assigned to the table

- **Index for the CSCMSG_Ccluster-name_EXECHISTORY table**

No.	Index name	UNIQUE attribute	Order in index	Column name
1	CSCMSG_<individualname>_EXECHISTORY_I	None	1	MESSAGE_ID
2			2	CLIENT_ID

Note:

The execution log information of messages in the HCSC server is collected. Additionally, the number of records added is as many as the number of service module calls.

C.3 Table information about execution environment setup

(1) Table information

The following tables are required for each HCSC server or cluster.

- HCSC basic information table
- HCSC linkage directory information table

- Location directory information table
- Routing rule directory information table
- Data transformation definition directory information table
- Cluster basic information management table
- Asynchronous adapter service ID management table

(a) HCSC basic information table

- **CSCMSG_S<HCSC server name>_CSC_PERSIST table**

  The contents of the CSCMSG_S<HCSC server name>_CSC_PERSIST table are as follows:

No.	Column name	Description	HiRDB type	ORACLE type	Existence of index	NULL	UNIQUE attribute
1	CSC_SERVER_NAME	Name of local HCSC server	VARCHAR(8)	VARCHAR2(8)	No	Not possible	No
2	CSC_SERVER_STATUS	Status of the HCSC server (unused) • 1: Starting • 2: Active • 3: Start failed • 4: Inactive • 5: Stopping • 6: Stop failed	INTEGER	NUMBER(10,0)	No	Not possible	No
3	CSC_REQUEST_STATUS	Status of synchronous reception • 1: Starting • 2: Active • 3: Start failed • 4: Inactive • 5: Stopping • 6: Stop failed	INTEGER	NUMBER(10,0)	No	Not possible	No
4	CSC_CONNECT_STATUS	Status of linkage reception • 1: Starting • 2: Active • 3: Start failed • 4: Inactive • 5: Stopping • 6: Stop failed	INTEGER	NUMBER(10,0)	No	Not possible	No
5	CSC_TABLE_VERSION	Table version number for entire HCSC	INTEGER	NUMBER(10,0)	No	Not possible	No
6	CSC_TABLE_REVISION	Table revision number for entire HCSC	INTEGER	NUMBER(10,0)	No	Not possible	No
7	OPTION1	Reserve 1	BINARY(2000)	RAW(2000)	No	Possible	No
8	OPTION2	Reserve 2	BINARY(2000)	RAW(2000)	No	Possible	No
9	OPTION3	Reserve 3	BINARY(2000)	RAW(2000)	No	Possible	No

Note:
By default, INDEX is not used.

(b) HCSC linkage directory information table

- **CSCMSG_C<cluster name>_CSC_CONNECT table**

The contents of the CSCMSG_C<cluster name>_CSC_CONNECT table are as follows:

No.	Column name	Description	HiRDB type	ORACLE type	Existence of index	NULL	UNIQUE attribute
1	CONNECT_CLUSTER_NAME#	Linked cluster name	VARCHAR(8)	VARCHAR2(8)	No	Not possible	Yes
2	CONNECT_VERSION	Request source HCSC server version number	INTEGER	NUMBER(10,0)	No	Not possible	No
3	CONNECT_REVISION	Request source HCSC server revision number	INTEGER	NUMBER(10,0)	No	Not possible	No
4	CONNECT_ID	Linkage start timestamp for linkage at the request source HCSC server	TIMESTAMP(4)	NUMBER(20,0)	No	Not possible	No
5	CONNECT_STATUS	Status of linkage with HCSC server • 1: OFFLINE (Not linked) • 2: ONLINE (Linked)	INTEGER	NUMBER(10,0)	No	Not possible	No
6	CONNECT_OPTION	Synchronization type (Which of the following is used for synchronous interface) • SOAP • EJB	VARCHAR(16)	VARCHAR2(16)	No	Possible	No
7	CONNECT_WEB_URL	URL of Web Services for SOAP transfer	VARCHAR(2086)	VARCHAR2(2086)	No	Possible	No
8	CONNECT_WEB_USER_ID	User ID for SOAP transfer	VARCHAR(256)	VARCHAR2(256)	No	Possible	No
9	CONNECT_WEB_PASSWORD	Password for SOAP transfer	VARCHAR(256)	VARCHAR2(256)	No	Possible	No
10	CONNECT_J2EE_NAME	Name of the J2EE server used for invoking EJB used for transfer	VARCHAR(255)	VARCHAR2(255)	No	Possible	No
11	CONNECT_NAMING_HOST	Host name of Naming Service used for invoking EJB used for transfer	VARCHAR(255)	VARCHAR2(255)	No	Possible	No
12	CONNECT_NAMING_PORT	Port number of Naming Service used for invoking EJB used for transfer	VARCHAR(5)	VARCHAR2(5)	No	Possible	No
13	OPTION1	Reserve 1	BINARY(2000)	RAW(2000)	No	Possible	No
14	OPTION2	Reserve 2	BINARY(2000)	RAW(2000)	No	Possible	No

No.	Column name	Description	HiRDB type	ORACLE type	Existence of index	NULL	UNIQUE attribute
15	OPTION3	Reserve 3	BINARY(2000)	RAW(2000)	No	Possible	No

Note#

CONNECT_CLUSTER_NAME is defined by UNIQUE CLUSTER KEY (indexes are created automatically).

(c) Location directory information table

- **CSCMSG_S<HCSC server name>_LC_DIRECTORY table**

The contents of the CSCMSG_S<HCSC server name>_LC_DIRECTORY table are as follows:

No.	Column name	Description	HiRDB type	ORACLE type	Existence of index	NULL	UNIQUE attribute
1	SERVICE_NAME#	Service name (Target service component) • Service name of service adapter • Service name of business process • Service group name	MVARCHAR(64)	NVARCHAR2(64)	No	Not possible	Yes
2	ADAPTER_NAME	Service ID of service adapter or Service ID of business process	VARCHAR(8)	VARCHAR2(8)	No	Possible	No
3	SERVICE_KIND	Type of service component • Single service component • Business process • Service group • User-defined reception	INTEGER	NUMBER(10,0)	No	Not possible	No
4	SERVICE_PROTOCOL_KIND	Type of service adapter • 1: MDB_WSR (Asynchronous) • 2: MDB_DBQ (Asynchronous) • 3: SessionBean (Synchronous) • 4: WebService (Synchronous) • 5: Custom (Other than 1~4 given above)	INTEGER	NUMBER(10,0)	No	Not possible	No
5	SERVICE_STATUS	Status of HCSC component or service group • 1: Active ACTIVE • 2: Inactive INACTIVE	INTEGER	NUMBER(10,0)	No	Not possible	No

No.	Column name	Description	HiRDB type	ORACLE type	Existence of index	NULL	UNIQUE attribute
5	SERVICE_STATUS	• 3: Stop failed STOP_FAILED • 4: Stopping STOPPING • 5: Start failed START_FAILED • 6: Starting STARTING • 7: Deleting DELETING	INTEGER	NUMBER(10,0)	No	Not possible	No
6	ADAPTER_ENTRY_TIME	Time at which the adapter definition was added	TIMESTAMP(4)	NUMBER(20,0)	No	Not possible	No
7	LC_VERSION	Location directory version number	INTEGER	NUMBER(10,0)	No	Not possible	No
8	LC_REVISION	Location directory revision number	INTEGER	NUMBER(10,0)	No	Not possible	No
9	ADAPTER_LOCAL_CALL	Value specified for parameter (local-call) in adapter definition file	INTEGER	NUMBER(10,0)	No	Not possible	No
10	ADAPTER_MODIFIED_TIME	Service adapter or business process update time	TIMESTAMP(4)	NUMBER(20,0)	No	Not possible	No
11	OPTION1	Reception-related information of a user-specified interface	BINARY(2000)	RAW(2000)	No	Possible	No
12	OPTION2	Reserve 2	BINARY(2000)	RAW(2000)	No	Possible	No
13	OPTION3	Reserve 3	BINARY(2000)	RAW(2000)	No	Possible	No

Note#

SERVICE_NAME is defined by UNIQUE CLUSTER KEY (indexes are created automatically).

- **CSCMSG_S<HCSC server name>_LC_BPFORMAT table**

  The contents of the CSCMSG_S<HCSC server name>_LC_BPFORMAT table are as follows:

No.	Column name	Description	HiRDB type	ORACLE type	Existence of index	NULL	UNIQUE attribute
1	SERVICE_NAME	Service name (target service component) • Service name of business process	MVARCHAR(64)	NVARCHAR2(64)	No	Not possible	No
2	OPERATION_NAME	Operation name of service definition file	MVARCHAR(255)	NVARCHAR2(255)	No	Not possible	No
3	REQ_FORMAT_ID	Request format ID of service definition file	VARCHAR(1024)	VARCHAR2(1024)	No	Possible	No
4	RES_FORMAT_ID	Response format ID of service definition file	VARCHAR(1024)	VARCHAR2(1024)	No	Possible	No
5	OPTION1	Reserve 1	BINARY(2000)	RAW(2000)	No	Possible	No

No.	Column name	Description	HiRDB type	ORACLE type	Existence of index	NULL	UNIQUE attribute
6	OPTION2	Reserve 2	BINARY(2000)	RAW(2000)	No	Possible	No
7	OPTION3	Reserve 3	BINARY(2000)	RAW(2000)	No	Possible	No

Note:
By default, INDEX is not used.

(d) Routing rule directory information table

- **CSCMSG_S<HCSC server name>_RT_RULE table**

The contents of the CSCMSG_S<HCSC server name>_RT_RULE table are as follows:

No.	Column name	Description	HiRDB type	ORACLE type	Existence of index	NULL	UNIQUE attribute
1	SERVICE_GROUP_NAME#	Service group name	MVARCHAR(64)	NVARCHAR2(64)	No	Not possible	Yes
2	RULES	Byte string of XML routing definition	BINARY(2147483639)	LONG RAW	No	Possible	No
3	OPTION1	Reserve 1	BINARY(2000)	RAW(2000)	No	Possible	No
4	OPTION2	Reserve 2	BINARY(2000)	RAW(2000)	No	Possible	No
5	OPTION3	Reserve 3	BINARY(2000)	RAW(2000)	No	Possible	No

Note#
SERVICE_NAME is defined by UNIQUE CLUSTER KEY (indexes are created automatically).

(e) Data transformation definition directory information table

- **CSCMSG_S<HCSC server name>_CV_MAPPING table**

The contents of the CSCMSG_S<HCSC server name>_CV_MAPPING table are as follows:

No.	Column name	Description	HiRDB type	ORACLE type	Existence of index	NULL	UNIQUE attribute
1	BEF_FORMAT_ID	Message format ID (For conversion source)	VARCHAR(1024)	VARCHAR2(1024)	No	Possible	No
2	AFT_FORMAT_ID	Message format ID (For conversion destination)	VARCHAR(1024)	VARCHAR2(1024)	No	Possible	No
3	ENTRY_TIME	Time at which the data transformation definition was added	TIMESTAMP(4)	NUMBER(20,0)	No	Possible	No
4	ROOT_FILE	Flag indicating whether or not this is the root • 0: false • 1: true	INTEGER	NUMBER(10,0)	No	Possible	No
5	DEFINITION_NAME	Name of data transformation definition file	MVARCHAR(255)	NVARCHAR2(255)	No	Possible	No

No.	Column name	Description	HiRDB type	ORACLE type	Existence of index	NULL	UNIQUE attribute
6	TRANSFORM_DEFINITION	Data transformation definition	BINARY(2147483639)	LONG RAW	No	Possible	No
7	OPTION1	Reserve 1	BINARY(2000)	RAW(2000)	No	Possible	No
8	OPTION2	Reserve 2	BINARY(2000)	RAW(2000)	No	Possible	No
9	OPTION3	Reserve 3	BINARY(2000)	RAW(2000)	No	Possible	No

Note:
By default, INDEX is not used.

- **CSCMSG_S<HCSC server name>_CV_FORMAT table**

The contents of the CSCMSG_S<HCSC server name>_CV_FORMAT table are as follows:

No.	Column name	Description	HiRDB type	ORACLE type	Existence of index	NULL	UNIQUE attribute
1	FORMAT_ID	Message format ID • For conversion source • For conversion target	VARCHAR(1024)	VARCHAR2(1024)	No	Possible	No
2	FORMAT_TYPE	Type of message format • 1: XML • 2: BINARY	INTEGER	NUMBER(10,0)	No	Possible	No
3	ENTRY_TIME	Time when message format definition was added	TIMESTAMP(4)	NUMBER(20,0)	No	Possible	No
4	ROOT_FILE	Flag indicating whether or not this is the root • 0: false • 1: true	INTEGER	NUMBER(10,0)	No	Possible	No
5	DEFINITION_NAME	Format definition file name	MVARCHAR(255)	NVARCHAR2(255)	No	Possible	No
6	FORMAT_DEFINITION	Message format definition (Data definition)	BINARY(2147483639)	LONG RAW	No	Possible	No
7	OPTION1	Reserve 1	BINARY(2000)	RAW(2000)	No	Possible	No
8	OPTION2	Reserve 2	BINARY(2000)	RAW(2000)	No	Possible	No
9	OPTION3	Reserve 3	BINARY(2000)	RAW(2000)	No	Possible	No

Note:
By default, INDEX is not used.

(f) Cluster basic information management table

- **CSCMSG_C<cluster name>_CLUSTER table**

The contents of the CSCMSG_C<cluster name>_CLUSTER table are as follows:

No.	Column name	Description	HiRDB type	ORACLE type	Existence of index	NULL	UNIQUE attribute
1	CSC_SERVER_NAME[#1]	Name of the HCSC server that was set up	VARCHAR(8)	VARCHAR2(8)	No	Not possible	No
2	CLUSTER_TYPE	Cluster type of the HCSC server that was set up	VARCHAR(2)	VARCHAR2(2)	No	Not possible	No
3	J2EE_NAME	Name of the J2EE server on which HCSC server is set up	VARCHAR(255)	VARCHAR2(255)	No	Not possible	No
4	SOAP_RCP	If standard reception (Web service) is set up or not: • 0: Not set up • 1: Set up	INTEGER	NUMBER(1)	No	Not possible	No
5	EJB_RCP	If standard reception (SessionBean) is set up or not: • 0: Not set up • 1: Set up	INTEGER	NUMBER(1)	No	Not possible	No
6	WSR_RCP	If standard reception (MDB (WS-R)) is set up or not: • 0: Not set up • 1: Set up	INTEGER	NUMBER(1)	No	Not possible	No
7	DBQ_RCP	If standard reception (MDB (DB queue)) is set up or not: • 0: Not set up • 1: Set up	INTEGER	NUMBER(1)	No	Not possible	No
8	RM_SYSNAME	RM system name specified at the time of setting up HCSC server If the RM system name is not specified, "" is specified.	VARCHAR(3)	VARCHAR2(3)	No	Not possible	No
9	CLUSTER_PROPS	Retain information in extension column in the format of "Key name=value"[#2]	VARCHAR(4000)	VARCHAR2(4000)	No	Not possible	No

Note:
By default, INDEX is not used.

Note#1
PRIMARY KEY of this table.

Note#2
The information that can be stored in CLUSTER_PROPS in the following manner:

Key name	Key description	Key value description
db-tbl-split-key	Type of key used for split range	NONE Split range is not used. MONTH Uses "Month" for split key
db-tbl-split-corcheck-use	Whether the check for correlation set duplication is to be enhanced	ON Correlation set duplication check is enhanced. OFF Correlation set duplication set is not enhanced.

(g) Asynchronous adapter service ID management table

- **CSCMSG_C<cluster name>_HA_ASYNC_ADP table**

  The contents of the CSCMSG_C<cluster name>_HA_ASYNC_ADP table are as follows:

No.	Column name	Description	HiRDB type	ORACLE type	Existence of Index	NULL	UNIQUE attribute
1	CSC_SERVER_NAME#	Name of HCSC server on which a component is deployed	VARCHAR(8)	VARCHAR2(8)	No	Not possible	No
2	ADAPTER_ID#	Service ID of service adapter	VARCHAR(8)	VARCHAR2(8)	No	Not possible	No

Note:
By default, INDEX is not used.

Note#
PRIMARY KEY of this table.

C.4 Precautions to be taken when user creates his own table or index

When creating your own table or index on a database similar to HCSC, do not use any name that starts with "CSC +aphanumerics+underscore" (for example, "CSCMSG_" or "CSCBP_"). If you use such names, then it will result in duplication with the names that HCSC will use in later versions.

D. Setting up the SQL Script File

The SQL script file is used to customize the tables that are used with the messaging infrastructure or business process infrastructure in the following cases.

- When setting up RD area or table area (table space) in detail:
  In HCSC server setup definition file, you can specify only the standard storage area.. To specify a more detailed storage area, you must use SQL script file. Specific example is as follows:
  - Location directory information table and data transformation directory information table is a collective name for multiple tables. However, even if you use location-tbl-area property or cv-tbl-area property, you can set up only 1 RD area or table area (table space) for multiple tables.
  - You cannot set RD area or table area (table space) for PRIMARY KEY and CLUSTER KEY.
  - You can set only 1 RD area or table area (table space) for 1 table. (Split definition is not possible.)
- When you want to improve search performance:
  For the functions that are frequently used, indexes are set for columns according to the operations that are performed. For example, when the execution log information is displayed, an index can be set for the information that is used as the key values

D.1 Types and storage destinations of SQL script files

You can create an SQL script file using the sample file stored in the following directory:

```
<Service platform installation directory>\CSC\sql
```

This directory contains the following files and, the files to be used differ depending on the type of database and usage.

Table D–1: Table Types of SQL script files

Database type	Classification	File name	Description
HiRDB	For creating a table	CreateTables_HiRDB.sql	Used to set up a stand-alone HCSC server or the first HCSC server in a cluster configuration.
		CreateTables_HiRDB_for_Matrix.sql	Used to set up a stand-alone HCSC server or the first HCSC server in a cluster configuration, when HiRDB matrix splitting is used.
		CreateTables_HiRDB_for_Range.sql	Used to set up a stand-alone HCSC server or the first HCSC server in a cluster configuration when HiRDB range splitting is used.
		CreateCSCIndividualTables_HiRDB.sql	Used to set up the second HCSC server in a cluster configuration.
	For deleting a table	DeleteTables_HiRDB.sql	Used to cancel the setup of a stand-alone HCSC server or the first HCSC server in a cluster configuration.
		DeleteCSCIndividualTables_HiRDB.sql	Used to cancel setup of the second HCSC server in a cluster configuration.
Oracle 11g	For creating a table	CreateTables_Oracle.sql	Used to set up a stand-alone HCSC server or the first HCSC server in a cluster configuration.
		CreateCSCIndividualTables_Oracle.sql	Used to set up the second HCSC server in a cluster configuration.

Database type	Classification	File name	Description
Oracle 11g	For deleting a table	DeleteTables_Oracle.sql	Used to cancel setup of a stand-alone HCSC server or the first HCSC server in a cluster configuration.
		DeleteCSCIndividualTables_Oracle.sql	Used to cancel setup of the second HCSC server in a cluster configuration.

D.2 Method of setting SQL script file

When setting up SQL script file, you must rename tables and RD Areas or table areas.

(1) Renaming tables

Change the following part of each table in SQL script file.

- <individualname>: Cluster name or HCSC server name

The following table describes the renaming rules for each table.

Table D–2: Table **Rules for renaming tables**

Table name of index name before replacement	Replacement method	Example
CSCMSG_<individualname>_CSC_CONNECT CSCMSG_<individualname>_EXECHISTORY CSCMSG_<individualname>_EXECHISTORY_I CSCMSG_<individualname>_CLUSTER CSCMSG_<individualname>_HA_ASYNC_ADP	C<cluster name>	• When the cluster name is "Cluster"SCMSG_CCluster_CSC_CONNECT
CSCMSG_<individualname>_CSC_PERSIST CSCMSG_<individualname>_LC_DIRECTORY CSCMSG_<individualname>_LC_BPFORMAT CSCMSG_<individualname>_RT_RULE CSCMSG_<individualname>_CV_MAPPING CSCMSG_<individualname>_CV_FORMAT	S<HCSC server name>	• When HCSC server name is "HCSC" CSCMSG_SHCSC_CSC_PERSIST
CSCBP_<individualname>_PROCESS CSCBP_<individualname>_ACTIVITY CSCBP_<individualname>_LINK CSCBP_<individualname>_CORRELATIONSET CSCBP_<individualname>_STR_VARIABLE CSCBP_<individualname>_NUM_VARIABLE CSCBP_<individualname>_BOOL_VARIABLE CSCBP_<individualname>_MSG_VARIABLE CSCBP_<individualname>_MSG_RELATION CSCBP_<individualname>_PROCESS_IDX1 CSCBP_<individualname>_PROCESS_IDX2 CSCBP_<individualname>_PROCESS_IDX3 CSCBP_<individualname>_PROCESS_IDX4 CSCBP_<individualname>_ACTIVITY_IDX CSCBP_<individualname>_LINK_IDX CSCBP_<individualname>_CORREL_IDX1 CSCBP_<individualname>_CORREL_IDX2	<cluster name>	• When cluster name is "Cluster" CSCBP_Cluster_PROCESS

Table name of index name before replacement	Replacement method	Example
CSCBP_<individualname>_STR_VAR_IDX CSCBP_<individualname>_NUM_VAR_IDX CSCBP_<individualname>_BOOL_VAR_IDX CSCBP_<individualname>_MSG_VAR_IDX CSCBP_<individualname>_MSG_REL_IDX1 CSCBP_<individualname>_MSG_REL_IDX2 CSCBP_<individualname>_MSG_REL_IDX3 CSCBP_<individualname>_V_ACTIVITY CSCBP_<individualname>_V_LINK CSCBP_<individualname>_V_STR_VARIABLE CSCBP_<individualname>_V_NUM_VARIABLE CSCBP_<individualname>_V_BOOL_VARIABLE CSCBP_<individualname>_V_MSG_VARIABLE	<cluster name>	• When cluster name is "Cluster" CSCBP_Cluster_PROCESS

(2) Renaming RD Areas or table areas

Rename RD Areas or table areas for each database as follows:

(a) For HiRDB

Rewrite the following part of each table in SQL script file. If RD Area is not specified, delete "IN <RDDATA>" or "IN <RDINDX>".

- IN <RDDATA>: Specifies the name of the RD Area that stores each table.
- IN <RDINDX>: Specifies the name of the RD Area that stores each index.

Further, if SQL script file "CreateTables_HiRDB_for_Range.sql" or "CreateTables_HiRDB_for_Matrix.sql" is used, rewrite the following part.

- <RDDATA*n*>: Specifies the name of the RD Area that stores *n Month (n:* 01~12) data.
- <RDINDX*n*>: Specifies the name of the RD Area that stores *n Month (n:* 01~12) index.

By dividing RD Area specification in January~December, you can assign RD Area cyclically in 1 year unit (12 months). Also, you can conserve the required RD area, by specifying same RD Area in multiple months.

(Example 1)

The example shows the following contents defined in SQL script file "CreateTables_HiRDB_for_Range.sql".

Unit of data to be handled: 1 month

Cyclic assignment period: 3 months

- Table definition example

```
IN
  ((RDDATA1)'01', /* RD Area that stores data for January */
   (RDDATA2)'02', /* RD Area that stores data for February */
   (RDDATA3)'03', /* RD Area that stores data for March */
   (RDDATA1)'04', /* RD Area that stores data for April */
   (RDDATA2)'05', /* RD Area that stores data for May */
   (RDDATA3)'06', /* RD Area that stores data for June */
   (RDDATA1)'07', /* RD Area that stores data for July */
   (RDDATA2)'08', /* RD Area that stores data for August */
   (RDDATA3)'09', /* RD Area that stores data for September */
   (RDDATA1)'10', /* RD Area that stores data for October */
   (RDDATA2)'11', /* RD Area that stores data for November */
   (RDDATA3));    /* RD Area that stores data for December */
```

- Index definition example

```
IN
  ((RDINDEX1), /* RD Area that stores index for January */
   (RDINDEX2), /* RD Area that stores index for February */
   (RDINDEX3), /* RD Area that stores index for March */
   (RDINDEX1), /* RD Area that stores index for April */
   (RDINDEX2), /* RD Area that stores index for May */
   (RDINDEX3), /* RD Area that stores index for June */
   (RDINDEX1), /* RD Area that stores index for July */
   (RDINDEX2), /* RD Area that stores index for August */
   (RDINDEX3), /* RD Area that stores index for September */
   (RDINDEX1), /* RD Area that stores index for October */
   (RDINDEX2), /* RD Area that stores index for November */
   (RDINDEX3));/* RD Area that stores index for December */
```

(Example 2)

The example shows the following contents defined in SQL script file "CreateTables_HiRDB_for_Matrix.sql.

Unit of data to be handled: 1 month

Cyclic assignment period: 3 months

Backend servers: 3

- Table definition example

```
IN
  ((BES1RDDATA1,BES2RDDATA1,BES3RDDATA1), /* RD Area that stores data for January */
   (BES1RDDATA2,BES2RDDATA2,BES3RDDATA2), /* RD Area that stores data for February */
   (BES1RDDATA3,BES2RDDATA3,BES3RDDATA3), /* RD Area that stores data for March */
   (BES1RDDATA1,BES2RDDATA1,BES3RDDATA1), /* RD Area that stores data for April */
   (BES1RDDATA2,BES2RDDATA2,BES3RDDATA2), /* RD Area that stores data for May */
   (BES1RDDATA3,BES2RDDATA3,BES3RDDATA3), /* RD Area that stores data for June */
   (BES1RDDATA1,BES2RDDATA1,BES3RDDATA1), /* RD Area that stores data for July */
   (BES1RDDATA2,BES2RDDATA2,BES3RDDATA2), /* RD Area that stores data for August */
   (BES1RDDATA3,BES2RDDATA3,BES3RDDATA3), /* RD Area that stores data for September */
   (BES1RDDATA1,BES2RDDATA1,BES3RDDATA1), /* RD Area that stores data for October */
   (BES1RDDATA2,BES2RDDATA2,BES3RDDATA2), /* RD Area that stores data for November */
   (BES1RDDATA3,BES2RDDATA3,BES3RDDATA3));/* RD Area that stores data for December */
```

- Index definition example

```
IN
  ((BES1RDINDEX1,BES2RDINDEX1,BES3RDINDEX1), /* RD Area that stores index for January */
   (BES1RDINDEX2,BES2RDINDEX2,BES3RDINDEX2), /* RD Area that stores index for February */
   (BES1RDINDEX3,BES2RDINDEX3,BES3RDINDEX3), /* RD Area that stores index for March */
   (BES1RDINDEX1,BES2RDINDEX1,BES3RDINDEX1), /* RD Area that stores index for April */
   (BES1RDINDEX2,BES2RDINDEX2,BES3RDINDEX2), /* RD Area that stores index for May */
   (BES1RDINDEX3,BES2RDINDEX3,BES3RDINDEX3), /* RD Area that stores index for June */
   (BES1RDINDEX1,BES2RDINDEX1,BES3RDINDEX1), /* RD Area that stores index for July */
   (BES1RDINDEX2,BES2RDINDEX2,BES3RDINDEX2), /* RD Area that stores index for August */
   (BES1RDINDEX3,BES2RDINDEX3,BES3RDINDEX3), /* RD Area that stores index for September */
   (BES1RDINDEX1,BES2RDINDEX1,BES3RDINDEX1), /* RD Area that stores index for October */
   (BES1RDINDEX2,BES2RDINDEX2,BES3RDINDEX2), /* RD Area that stores index for November */
   (BES1RDINDEX3,BES2RDINDEX3,BES3RDINDEX3));/* RD Area that stores index for December */
```

Additionally, to use the table split functionality (range split or matrix split) and specify SplitKey as search condition in -where option or -wherefile option of cscpiselect command, you must change CREATE VIEW of SQL script file. For the relationship between commands and view table, see "cscpiselect (Search process instance)" in "Service Platform Reference Guide". If you do not specify SplitKey in the search conditions of cscpiselect command, we recommend that you do not change CREATE VIEW, to avoid any adverse effect on the process performance.

(Example 3)

The definition example of CSCBP_<individualname>_V_ACTIVITY view table is as follows:

```
CREATE VIEW CSCBP_<individualname>_V_ACTIVITY
(
    ProcessID,
    ActivityNumber,
    ProcessDefinitionName,
    ProcessDefinitionVersion,
    ActivityDefinitionName,
    ActivityKind,
    ParentNumber,
    ScopeNumber,
    RepeatNumber,
    State,
    FirstChildNumber,
    LastChildNumber,
```

```
    StartTime,
    EndTime,
    WaitTime,
    CSCServerName,
    SplitKey                                        ・ #1
) AS SELECT a.ProcessID,
            a.ActivityNumber,
            p.ProcessDefinitionName,
            p.ProcessDefinitionVersion,
            a.ActivityDefinitionName,
            a.ActivityKind,
            a.ParentNumber,
            a.ScopeNumber,
            a.RepeatNumber,
            a.State,
            a.FirstChildNumber,
            a.LastChildNumber,
            a.StartTime,
            a.EndTime,
            a.WaitTime,
            p.CSCServerName,
            p.SplitKey                                ・ #2
     FROM CSCBP_<individualname>_ACTIVITY a, CSCBP_<individualname>_PROCESS p
     WHERE a.ProcessID = p.ProcessID;
```

Note#1

Add the SplitKey column at the end of the configuration string in accordance with the contents in "*Appendix C.1(4) View table information*".

Note#2

Specify the column name of reference table in accordance with the contents in "*Appendix C.1(4) View table information*".

(b) For Oracle

Rewrite the following part of each table or index in SQL script file. If table area is not specified, delete "TABLESPACE <EXAMPLE>".

- TABLESPACE <EXAMPLE>

  Specifies the table area to be used (table space) or table area to store the message variable value (BLOB) from the message variable table.

D.3 Points to be considered when setting up SQL script file

Following are the points to be considered when setting up SQL script file. If the following points are violated, operation is not guaranteed.

- You cannot change column names, data type and constraint keys of all tables, as shown below. You cannot change the order of columns.

  (Example)

  Column name: CSC_SERVER_NAME, CSC_SERVER_STATUS, etc.

  Data type: VARCHAR2(8), NUMBER(10,0), etc.

  Constraint key: NOT NULL specification, UNIQUE specification, etc.
- You cannot change the order of table or index creation.
- You cannot delete the indexes, view table and tables defined in template. If you delete or if you wrongly replace <individualname>, error occurs at the time of setting up HCSC server.
- You can add column in view table only when you use the horizontal split function. Also, make sure that the definition contents of the column to be added match with "*Appendix C.1 Table information about process instance execution log management*.
- The contents mentioned between "/*" and "*/" are considered as comments and are deleted at the time of issuing SQL.
- You cannot use simple comment (comment starting with "--". If you use such comments, normal operation is not guaranteed.
- You cannot use quotation marks (" and '). If you use quotation marks, operation is not guaranteed.

E. Statistical Information of Resource Statistics for HCSC Server

You can reference HCSC server resource statistics as statistical information. To reference statistical information, use the statistics files output on Service Platform.

A statistics file is a file in which statistics information within the J2EE servers and SFO servers is regularly output. HCSC server resource running information is also recorded in this file. For details about statistics files, see *3.3 Statistics File Output Functionality* in the *uCosminexus Application Server Operation, Monitoring, and Linkage Guide*.

E.1 Statistics file output

(1) Output destination of statistics file

The statistics file will be created in the following folders in case of default settings.

For Windows

<Work directory>#\ejb\<J2EE server name>\stats

- Default value of <Work directory>
  <Service Platform installation directory>\CC\server\public

For UNIX

<Work directory>#/ejb/<J2EE server name>/stats

- Default value of <Work directory>
  /opt/Cosminexus/CC/server/public

Note#

You can check the <Work directory> using one of the following methods:

When checking from the operating environment portal

You can check the Work directory in the [J2EE container settings] screen. For details, see 10.9.2 Setting up J2EE container in "Application Server Management Portal Operation Guide".

When checking from the Easy Setup definition file

You can check the Work directory in the ejb.public.directory parameter, specified within the <configuration> tag of the logical J2EE server (j2ee-server) in Easy Setup definition file. For details, see 4.6 Easy Setup definition file in "Application Server Definition Reference Guide".

(2) Statistics file for resources of HCSC server

The following table describes statistics file, header file and ObjectName identification value for resources of HCSC server.

Table E–1: Table Statistics file for resources of HCSC server

Resource name	Statistics file	Header file	ObjectName identification value#
JavaVM	HJVMStats_<YYYYMMDDhhmm><TZ>.csv	HJVMStats.txt	-
DB connection	HJCAConnectionPoolStats_<YYYYMMDDhhmm><TZ>.csv	HJCAConnectionPoolStats.txt	J2EEServer=<J2EE server name> ResourceAdapter=<Resource adapter display name>
Standard reception (Web service SOAP1.1)	HWebModuleStats_<YYYYMMDDhhmm><TZ>.csv	HWebModuleStats.txt	• In SOAP1.1 mode J2EEApplication=CSCMsgSyncServiceDeliveryWS

Resource name	Statistics file	Header file	ObjectName identification value#
Standard reception (Web service SOAP1.1)	HWebModuleStats_<YYYYMMDDhhmm><TZ>.csv	HWebModuleStats.txt	name=CSCMsgSyncServiceDeliveryWS • In SOAP1.1/1.2 combined mode J2EEApplication=CSCMsgSyncServiceDeliveryWS name=CSCMsgSyncServiceDeliverySOAP11
Standard reception (Web service SOAP1.2)	HWebModuleStats_<YYYYMMDDhhmm><TZ>.csv	HWebModuleStats.txt	J2EEApplication=CSCMsgSyncServiceDeliveryWS name=CSCMsgSyncServiceDeliverySOAP12
User-defined reception	HWebModuleStats_<YYYYMMDDhhmm><TZ>.csv	HWebModuleStats.txt	J2EEApplication=<Reception ID of user-defined reception>
Service adapter	HStatelessSessionBeanStats_<YYYYMMDDhhmm><TZ>.csv	HStatelessSessionBeanStats.txt	J2EEApplication=<Service ID>
Business process	HStatelessSessionBeanStats_<YYYYMMDDhhmm><TZ>.csv	HStatelessSessionBeanStats.txt	J2EEApplication=<Service ID> name=CSCBPMessageReceiverEJB

Legend:

-: There is no identification value.

Note#

When there are two identification values, consider any one of the values.

(3) Statistics file output settings

As per the default settings, the statistics file is output.

See the following manual to change the statistics file output destination directory and to change the settings for whether to output statistics file.

When changing from operating environment portal

See "10.9.17 Setting up statistics monitoring (J2EE server)" in "Application Server Management Portal Operation Guide".

When using Smart Composer functionality to change

See "3.3 Output function of statistics file "and "3.4 Event occurrence functionality" in "Application Server Operation, Monitoring, and Linkage Guide.

E.2 Viewing statistics

The steps to reference statistics information are as follows:

1. Determine the resource for which, you want to see the statistics information, from the following:
   - JavaVM
   - DB connection
   - Standard reception (Web service)
   - User-defined reception
   - Service adapter
   - Business process
2. Copy the statistics file and header file (for the target resource) from the statistics file output directory to any directory you like.

   For details about the statistics file output directory, and about the statistics file and header file for each resource, see *E.1 Statistics file output*.

3. Edit the statistics file and the header file copied in the step (2) into one file, and reference these files in an application program like Excel.
4. Search the resource for which statistics information is to be referenced, from ObjectName identification value.

   If you are using Excel, set a filter in the header of the file edited into 1 file and, select the resource whose statistics information you want to reference from ObjectName identification value.

   For ObjectName identification value corresponding to resources, see "*Appendix E.1 Statistics file output*".
5. Specify the type of statistics for the resource that you searched in Step 4.

   Specify the type of statistics for resource from the item name of header file. For type of statistics for resource and their corresponding header file item name, see "*Appendix E.3 Types of statistics for resources*".

E.3 Types of statistics for resources

The types of statistics for resources differ depending on the resource. The following table describes the types of the statistics for resources, and the corresponding header file item names:

Table E–2: Table Types of statistics for resources and corresponding header file item names

Resource name	Type of statistics for resources		Header file item name
JavaVM	Heap size	Upper limit value	HeapSize.UpperBound
		Maximum value	HeapSize.HighWaterMark
DB connection	Connection count	Upper limit value	PoolSize.UpperBound
		Maximum value	PoolSize.HighWaterMark
Standard reception (Web service SOAP1.1) Standard reception (Web service SOAP1.2) User-defined reception	Queue waiting count	Upper limit value	WaitingRequestCount.UpperBound
		Maximum value	WaitingRequestCount.HighWaterMark
	Execution count	Upper limit value	ActiveThreadCount.UpperBound
		Maximum value	ActiveThreadCount.HighWaterMark
Service adapter Business process	Execution count	Upper limit value	ActivePooledInstanceCount.UpperBound
		Maximum value	ActivePooledInstanceCount.HighWaterMark

F. Messages that Notify JP1 Event

When the JP1 linkage facility is used, error message that occur on Service Platform are notified to JP1 as JP1 events. You can edit the message mapping file to change the existence of JP1 event notifications. For details on editing the message mapping files, see *2.8.5 Editing message mapping files*".

The following is a list of message IDs output on service platform and the default settings for JP1 event notification:

(1) Messages from KDEC00001 to KDEC19999 (Messaging infrastructure related messages)

Message ID	Existence of JP1 event notification
KDEC00001	Y
KDEC00002	Y
KDEC00003	Y
KDEC00005	A
KDEC00010	A
KDEC00011	A
KDEC00012	A
KDEC00013	A
KDEC00014	A
KDEC00016	A
KDEC00018	A
KDEC00019	A
KDEC00020	A
KDEC00021	A
KDEC00022	A
KDEC00023	A
KDEC00024	A
KDEC00025	A
KDEC00026	A
KDEC00027	A
KDEC00028	A
KDEC00029	A
KDEC00030	A
KDEC00031	A
KDEC00032	A
KDEC00033	A
KDEC00034	A
KDEC00035	A
KDEC00036	A

Message ID	Existence of JP1 event notification
KDEC00037	Y
KDEC00038	Y
KDEC00039	A
KDEC00040	A
KDEC00041	A
KDEC00042	A
KDEC00043	A
KDEC00044	A
KDEC00045	A
KDEC00046	A
KDEC00047	N
KDEC00048	N
KDEC00049	A
KDEC00351	N
KDEC00361	Y
KDEC00362	Y
KDEC00363	Y
KDEC00364	Y
KDEC00365	Y
KDEC00366	Y
KDEC00371	N
KDEC00372	N
KDEC00381	N
KDEC00382	Y
KDEC00383	Y
KDEC00384	Y
KDEC00385	Y
KDEC00386	Y
KDEC00387	Y
KDEC00388	N
KDEC00391	Y
KDEC00392	Y
KDEC00393	Y
KDEC00394	Y
KDEC00395	Y
KDEC00396	Y

Message ID	Existence of JP1 event notification
KDEC00397	Y
KDEC00398	N
KDEC00399	Y
KDEC00400	Y
KDEC00401	Y
KDEC00402	Y
KDEC00403	Y
KDEC00404	N
KDEC00405	N
KDEC00406	Y
KDEC00407	Y
KDEC00408	N
KDEC00409	N
KDEC00410	N
KDEC00411	Y
KDEC00412	Y
KDEC00413	Y
KDEC00421	N
KDEC00423	Y
KDEC00424	Y
KDEC00425	Y
KDEC00426	Y
KDEC00501	A
KDEC00502	A
KDEC00503	A
KDEC00504	A
KDEC00505	A
KDEC00506	A
KDEC00508	A
KDEC00509	N
KDEC00510	N
KDEC00511	N
KDEC00512	A
KDEC00513	A
KDEC00514	A
KDEC00515	A

Message ID	Existence of JP1 event notification
KDEC00516	A
KDEC00517	A
KDEC00518	A
KDEC00519	A
KDEC00520	A
KDEC00521	A
KDEC00522	A
KDEC00523	A
KDEC00524	A
KDEC00525	A
KDEC00526	A
KDEC00527	A
KDEC00528	A
KDEC01001	A
KDEC01002	A
KDEC01003	A
KDEC01004	A
KDEC01005	A
KDEC01006	A
KDEC01007	A
KDEC01008	A
KDEC01009	A
KDEC01011	A
KDEC01012	N
KDEC01013	A
KDEC01015	A
KDEC01016	A
KDEC01017	A
KDEC01018	A
KDEC01019	A
KDEC01020	A
KDEC01021	A
KDEC01022	A
KDEC01023	A
KDEC01024	A
KDEC01025	A

Message ID	Existence of JP1 event notification
KDEC01026	A
KDEC01501	A
KDEC01502	A
KDEC01503	A
KDEC01504	A
KDEC01505	A
KDEC01506	A
KDEC01507	A
KDEC01508	A
KDEC01509	A
KDEC01510	A
KDEC01511	A
KDEC01512	A
KDEC01513	A
KDEC01514	A
KDEC01515	A
KDEC01516	A
KDEC01517	A
KDEC01518	A
KDEC01519	A
KDEC01520	A
KDEC01521	A
KDEC01522	A
KDEC02001	A
KDEC02002	A
KDEC02003	A
KDEC02004	A
KDEC02005	A
KDEC02501	Y
KDEC02502	Y
KDEC02503	Y
KDEC02504	Y
KDEC02511	A
KDEC02512	A
KDEC02513	A
KDEC02514	A

Message ID	Existence of JP1 event notification
KDEC02515	A
KDEC02516	A
KDEC02517	A
KDEC02518	A
KDEC02519	A
KDEC02520	A
KDEC02521	A
KDEC02523	A
KDEC02524	A
KDEC02525	A
KDEC03001	A
KDEC03002	A
KDEC03003	A
KDEC03005	A
KDEC03006	A
KDEC03007	A
KDEC03011	A
KDEC03012	A
KDEC03013	A
KDEC03014	A
KDEC03015	A
KDEC03016	A
KDEC03017	A
KDEC03018	A
KDEC03019	A
KDEC03020	A
KDEC03021	A
KDEC03022	A
KDEC03023	A
KDEC03024	A
KDEC03025	A
KDEC03026	A
KDEC03027	A
KDEC03028	A
KDEC03029	A
KDEC03030	A

Message ID	Existence of JP1 event notification
KDEC03031	A
KDEC03032	A
KDEC04501	Y
KDEC04502	Y
KDEC04503	Y
KDEC04504	Y
KDEC04505	Y
KDEC04506	Y
KDEC04510	Y
KDEC04511	Y
KDEC04512	Y
KDEC04513	Y
KDEC04514	Y
KDEC04515	Y
KDEC04516	Y
KDEC04517	Y
KDEC04518	Y
KDEC04519	Y
KDEC04520	A
KDEC04601	N
KDEC04602	N
KDEC04603	N
KDEC04604	N
KDEC04605	N
KDEC04609	Y
KDEC05001	A
KDEC05002	A
KDEC05003	A
KDEC05004	A
KDEC05005	A
KDEC05006	A
KDEC05008	A
KDEC05009	A
KDEC05010	A
KDEC05011	A
KDEC05012	A

Message ID	Existence of JP1 event notification
KDEC05013	A
KDEC05014	A
KDEC05015	N
KDEC05016	N
KDEC05101	A
KDEC05102	A
KDEC05103	A
KDEC05104	A
KDEC05105	A
KDEC05106	A
KDEC05107	A
KDEC05108	A
KDEC05201	A
KDEC05202	A
KDEC05203	A
KDEC05204	A
KDEC05205	A
KDEC05206	A
KDEC05207	A
KDEC05208	A
KDEC05209	A
KDEC05210	A
KDEC05211	A
KDEC05212	A
KDEC05301	N
KDEC05302	N
KDEC05303	N
KDEC05304	N
KDEC05305	N
KDEC05306	N
KDEC05307	N
KDEC05308	N
KDEC05309	N
KDEC05310	N
KDEC05311	N
KDEC05312	N

Message ID	Existence of JP1 event notification
KDEC05313	N
KDEC05314	N
KDEC05315	N
KDEC05501	A
KDEC05502	A
KDEC05503	A
KDEC05504	A
KDEC05505	A
KDEC05506	A
KDEC06001	A
KDEC06002	A
KDEC06003	A
KDEC06004	A
KDEC06005	A
KDEC06006	A
KDEC06007	A
KDEC06008	A
KDEC06009	A
KDEC06010	A
KDEC06011	A
KDEC06012	A
KDEC06013	A
KDEC06014	A
KDEC06501	A
KDEC06502	A
KDEC06504	A
KDEC06505	A
KDEC06506	A
KDEC06507	A
KDEC06509	A
KDEC06510	A
KDEC06511	A
KDEC06512	A
KDEC06513	A
KDEC06601	A
KDEC06602	A

Message ID	Existence of JP1 event notification
KDEC06603	A
KDEC06604	A
KDEC06605	A
KDEC06606	A
KDEC06607	A
KDEC06608	A
KDEC06609	A
KDEC06610	A
KDEC06611	A
KDEC07001	Y
KDEC07002	Y
KDEC07003	Y
KDEC07004	N
KDEC07005	N
KDEC07006	Y
KDEC07007	Y
KDEC07008	Y
KDEC07501	N
KDEC07506	N
KDEC07507	N
KDEC07508	N
KDEC07509	N
KDEC07510	N
KDEC07511	N
KDEC07512	N
KDEC07513	N
KDEC07514	N
KDEC07515	N
KDEC07516	N
KDEC07517	N
KDEC07520	N
KDEC07521	N
KDEC07522	N
KDEC07523	N
KDEC07524	N
KDEC07525	N

Message ID	Existence of JP1 event notification
KDEC07526	N
KDEC07527	N
KDEC07528	N
KDEC07529	N
KDEC07530	N
KDEC07531	N
KDEC07532	N
KDEC07533	N
KDEC07539	N
KDEC07540	N
KDEC07541	N
KDEC07542	N
KDEC07543	N
KDEC07544	N
KDEC07545	N
KDEC07546	N
KDEC07548	N
KDEC07549	N
KDEC07550	N
KDEC07551	N
KDEC07552	N
KDEC07553	N
KDEC07554	N
KDEC07555	N
KDEC07556	N
KDEC07557	N
KDEC07558	N
KDEC07559	N
KDEC07560	N
KDEC07563	N
KDEC07564	N
KDEC07565	N
KDEC07567	N
KDEC07568	N
KDEC07569	N
KDEC07570	N

Message ID	Existence of JP1 event notification
KDEC07571	N
KDEC07572	N
KDEC07573	N
KDEC07574	N
KDEC07575	N
KDEC07576	N
KDEC07577	N
KDEC07578	N
KDEC07579	N
KDEC07580	N
KDEC07581	N
KDEC07585	N
KDEC07586	N
KDEC07587	N
KDEC07588	N
KDEC07589	N
KDEC07590	N
KDEC07591	N
KDEC07592	N
KDEC07593	N
KDEC07594	N
KDEC07595	N
KDEC07596	N
KDEC10001	N
KDEC10002	N
KDEC10003	N
KDEC10004	N
KDEC10005	N
KDEC10006	N
KDEC10007	N
KDEC10008	N
KDEC10009	N
KDEC10010	N
KDEC10011	N
KDEC10012	N
KDEC10013	N

Message ID	Existence of JP1 event notification
KDEC10014	N
KDEC10015	N
KDEC10016	N
KDEC10017	N
KDEC10020	N
KDEC10021	N
KDEC10022	N
KDEC10023	N
KDEC10024	N
KDEC10025	N
KDEC10026	N
KDEC10027	N
KDEC10028	N
KDEC10029	N
KDEC10030	N
KDEC10031	N
KDEC10033	N
KDEC10034	N
KDEC10035	N
KDEC10036	N
KDEC10037	N
KDEC10038	N
KDEC10039	N
KDEC10040	N
KDEC10041	N
KDEC10042	N
KDEC10043	N
KDEC10044	N
KDEC10045	N
KDEC10046	N
KDEC10047	N
KDEC10048	N
KDEC10049	N
KDEC10050	N
KDEC10051	N
KDEC10052	N

Message ID	Existence of JP1 event notification
KDEC10053	N
KDEC10054	N
KDEC10055	N
KDEC10056	N
KDEC10057	N
KDEC10058	N
KDEC10059	N
KDEC10060	N
KDEC10061	N
KDEC10062	N
KDEC10063	N
KDEC10064	N
KDEC10065	N
KDEC10066	N
KDEC10067	N
KDEC10068	N
KDEC10069	N
KDEC10070	N
KDEC10071	N
KDEC10072	N
KDEC10073	N
KDEC10074	N
KDEC10075	N
KDEC10076	N
KDEC10077	N
KDEC10078	N
KDEC10079	N
KDEC10080	N
KDEC10081	N
KDEC10082	N
KDEC10083	N
KDEC10084	N
KDEC10085	N
KDEC10086	N
KDEC10087	N
KDEC10088	N

Message ID	Existence of JP1 event notification
KDEC10089	N
KDEC10090	N
KDEC10091	N
KDEC10092	N
KDEC10093	N
KDEC10094	N
KDEC10095	N
KDEC10096	N
KDEC10097	N
KDEC10098	N
KDEC10099	N
KDEC10100	N
KDEC10101	N
KDEC10102	N
KDEC10400	N
KDEC10401	N
KDEC10403	N
KDEC10407	N
KDEC10408	N
KDEC10409	N
KDEC10410	N
KDEC10411	N
KDEC10501	N
KDEC10502	N
KDEC11001	N
KDEC11002	N
KDEC11003	N
KDEC11101	Y
KDEC19901	Y
KDEC19902	Y
KDEC19903	Y

Legend:

Y: Notifies JP1 event.

A: Defined with comments. If you want to notify JP1 event, remove the comment.

N: Does not notify JP1 event.

(2) Messages from KDEC20000 to KDEC39999 (Business process infrastructure related messages)

Message ID	Existence of JP1 event notification
KDEC20000	Y
KDEC20001	Y
KDEC20002	A
KDEC20003	A
KDEC20004	Y
KDEC20005	Y
KDEC20006	N
KDEC20007	A
KDEC20008	A
KDEC20009	Y
KDEC20010	Y
KDEC20012	Y
KDEC20013	N
KDEC20014	Y
KDEC20015	Y
KDEC20016	A
KDEC20017	A
KDEC20018	A
KDEC20023	N
KDEC20024	A
KDEC20025	A
KDEC20026	A
KDEC20027	Y
KDEC20028	A
KDEC20029	Y
KDEC20030	A
KDEC20031	A
KDEC20032	A
KDEC20033	Y
KDEC20034	A
KDEC20035	Y
KDEC20036	N
KDEC20037	A
KDEC20038	N

Message ID	Existence of JP1 event notification
KDEC20039	A
KDEC20040	A
KDEC20041	A
KDEC20042	A
KDEC20043	A
KDEC20044	A
KDEC20045	A
KDEC20046	Y
KDEC20047	Y
KDEC20048	Y
KDEC20049	Y
KDEC20051	A
KDEC20052	A
KDEC20053	A
KDEC20054	A
KDEC20055	A
KDEC20056	A
KDEC20057	A
KDEC20058	Y
KDEC20059	Y
KDEC20060	A
KDEC20061	A
KDEC20062	A
KDEC20063	A
KDEC20065	A
KDEC20066	A
KDEC20067	A
KDEC20068	Y
KDEC20069	N
KDEC20070	Y
KDEC20071	A
KDEC20072	A
KDEC20073	A
KDEC20074	A
KDEC20075	A
KDEC20076	A

Message ID	Existence of JP1 event notification
KDEC20077	A
KDEC20078	N
KDEC20079	Y
KDEC20080	Y
KDEC20081	A
KDEC20082	A
KDEC20083	A
KDEC20084	A
KDEC20085	N
KDEC20086	A
KDEC20087	N
KDEC20088	Y
KDEC20090	N
KDEC20091	A
KDEC20092	N
KDEC30000	N
KDEC30001	N
KDEC30002	N
KDEC30003	N
KDEC30004	N
KDEC30005	N
KDEC30006	N
KDEC30007	N
KDEC30008	N
KDEC35000	N
KDEC35001	N
KDEC35002	N
KDEC35003	N
KDEC35004	N
KDEC35005	N
KDEC35006	N
KDEC35007	N
KDEC35008	N
KDEC35009	N
KDEC35011	N
KDEC35012	N

Message ID	Existence of JP1 event notification
KDEC35013	N
KDEC35014	N
KDEC35015	A
KDEC35016	A

Legend:

Y: Notifies JP1 event.

A: Defines with comments. If you want to notify JP1 event, remove the comment.

N: Does not notify JP1 event.

(3) Messages from KDEC40000 to KDEC59999 (Data transformation infrastructure related messages)

All messages from KDEC40000 to KDEC59999 notify JP1 event.

(4) Messages from KDEC60000 to KDEC79999 (DB adapter related messages)

Message ID	Existence of JP1 event notification
KDEC60000	Y
KDEC60001	Y
KDEC60002	A
KDEC60003	A
KDEC62000	A
KDEC62001	A
KDEC63000	Y
KDEC63001	Y
KDEC63002	Y
KDEC63003	A
KDEC64000	Y
KDEC64001	Y
KDEC64002	Y
KDEC64003	Y
KDEC64004	Y
KDEC64005	Y
KDEC64006	Y
KDEC64007	Y
KDEC64008	Y
KDEC64009	Y
KDEC64010	Y
KDEC64011	Y

Message ID	Existence of JP1 event notification
KDEC64012	Y
KDEC66000	Y
KDEC66001	A
KDEC66002	Y
KDEC66003	Y
KDEC66004	Y
KDEC66005	Y
KDEC66006	Y
KDEC66007	Y
KDEC68000	N
KDEC68001	N
KDEC68002	N
KDEC68003	N
KDEC68004	N
KDEC68005	N
KDEC68006	N
KDEC68007	N
KDEC68008	N
KDEC68009	N
KDEC68010	N
KDEC68011	N
KDEC68020	N
KDEC68021	N
KDEC68022	N
KDEC68023	N
KDEC68024	N
KDEC68025	N
KDEC68026	N
KDEC68027	N
KDEC68028	N
KDEC68029	N
KDEC68030	N
KDEC68031	N
KDEC68032	N
KDEC68099	N
KDEC70002	Y

Message ID	Existence of JP1 event notification
KDEC70003	A
KDEC70004	A
KDEC70005	A
KDEC70006	A
KDEC79000	Y

Legend:

Y: Notifies JP1 event.

A: Defined with comments. If you want to notify JP1 event, remove the comment.

N: Does not notify JP1 event.

(5) Messages from KDEC80000 to KDEC80399 (File operations adapter related messages)

Message ID	Existence of JP1 event notification
KDEC80000	Y
KDEC80001	Y
KDEC80002	Y
KDEC80003	Y
KDEC80004	Y
KDEC80005	Y
KDEC80006	Y
KDEC80007	Y
KDEC80008	Y
KDEC80009	Y
KDEC80010	Y
KDEC80011	Y
KDEC80012	Y
KDEC80013	Y
KDEC80014	Y
KDEC80015	N
KDEC80016	N
KDEC80017	N
KDEC80018	Y
KDEC80019	Y
KDEC80020	Y
KDEC80021	Y
KDEC80022	Y
KDEC80023	Y
KDEC80024	N

Message ID	Existence of JP1 event notification
KDEC80025	N
KDEC80026	N
KDEC80027	Y
KDEC80028	Y
KDEC80029	Y
KDEC80030	N
KDEC80031	Y
KDEC80032	Y
KDEC80033	Y
KDEC80034	Y
KDEC80035	Y
KDEC80036	N
KDEC80037	Y
KDEC80038	Y
KDEC80039	Y
KDEC80040	N
KDEC80041	Y
KDEC80043	Y
KDEC80044	Y
KDEC80045	N
KDEC80046	Y
KDEC80047	Y
KDEC80049	Y
KDEC80050	Y
KDEC80051	Y
KDEC80052	Y
KDEC80053	Y
KDEC80054	Y
KDEC80055	Y
KDEC80056	Y
KDEC80057	Y
KDEC80058	Y
KDEC80059	Y
KDEC80060	Y
KDEC80061	Y
KDEC80062	Y

Message ID	Existence of JP1 event notification
KDEC80081	Y
KDEC80082	N
KDEC80083	Y
KDEC80084	Y
KDEC80085	N
KDEC80101	Y
KDEC80102	Y
KDEC80103	N
KDEC80104	Y
KDEC80105	Y
KDEC80106	Y
KDEC80107	Y
KDEC80121	Y
KDEC80122	Y
KDEC80123	Y
KDEC80125	Y
KDEC80126	Y
KDEC80127	Y
KDEC80128	Y
KDEC80129	Y
KDEC80130	N

Legend:
Y: Notifies JP1 event.
N: Does not notify JP1 event.

(6) Messages from KDEC80400 to KDEC80499 (HTTP reception related messages)

Message ID	Existence of JP1 event notification
KDEC80421	Y
KDEC80422	Y
KDEC80423	Y
KDEC80424	Y
KDEC80425	N
KDEC80426	N
KDEC80427	Y
KDEC80428	Y
KDEC80429	Y

Message ID	Existence of JP1 event notification
KDEC80430	N
KDEC80431	Y
KDEC80432	N
KDEC80435	Y
KDEC80436	Y
KDEC80438	Y
KDEC80439	Y
KDEC80440	Y
KDEC80441	Y
KDEC80442	Y
KDEC80443	Y
KDEC80444	Y
KDEC80445	Y
KDEC80450	Y
KDEC80452	Y
KDEC80453	Y
KDEC80454	Y
KDEC80455	Y
KDEC80457	Y
KDEC80458	Y
KDEC80459	N

Legend:
Y: Notifies JP1 event.
N: Does not notify JP1 event.

(7) Messages from KDEC80500 to KDEC80999 (Mail adapter related messages)

Message ID	Existence of JP1 event notification
KDEC80500	N
KDEC80501	Y
KDEC80502	Y
KDEC80522	Y
KDEC80523	Y
KDEC80524	N
KDEC80525	Y
KDEC80535	Y
KDEC80536	Y

Message ID	Existence of JP1 event notification
KDEC80537	Y
KDEC80540	N
KDEC80544	Y
KDEC80545	Y
KDEC80546	Y
KDEC80548	Y
KDEC80621	Y
KDEC80622	Y
KDEC80623	N
KDEC80624	N
KDEC80625	Y
KDEC80626	N
KDEC80627	N
KDEC80628	Y
KDEC80651	N
KDEC80672	N
KDEC80673	N
KDEC80701	Y
KDEC80702	Y
KDEC80703	Y
KDEC80704	Y
KDEC80705	Y
KDEC80706	Y
KDEC80707	Y
KDEC80708	Y
KDEC80709	Y
KDEC80710	Y
KDEC80711	Y
KDEC80712	Y
KDEC80720	Y
KDEC80721	Y
KDEC80726	N
KDEC80730	N
KDEC80731	Y
KDEC80733	Y
KDEC80734	Y

Message ID	Existence of JP1 event notification
KDEC80735	Y
KDEC80736	Y
KDEC80801	Y
KDEC80802	Y
KDEC80806	N
KDEC80807	N
KDEC80809	Y
KDEC80810	Y
KDEC80812	Y
KDEC80813	Y
KDEC80814	Y
KDEC80815	Y
KDEC80816	Y
KDEC80817	Y
KDEC80851	N
KDEC80852	N
KDEC80853	N
KDEC80854	N
KDEC80855	N
KDEC80856	N
KDEC80857	N
KDEC80858	N
KDEC80859	N
KDEC80860	N
KDEC80861	N
KDEC80862	N
KDEC80863	Y
KDEC80864	Y
KDEC80865	N
KDEC80866	Y
KDEC80867	Y
KDEC80868	Y
KDEC80869	Y
KDEC80870	Y
KDEC80871	Y
KDEC80873	Y

Message ID	Existence of JP1 event notification
KDEC80874	Y
KDEC80875	Y
KDEC80876	Y
KDEC80877	Y
KDEC80878	N
KDEC80879	Y
KDEC80882	Y
KDEC80883	Y
KDEC80884	N
KDEC80886	N
KDEC80887	N
KDEC80888	N
KDEC80889	N
KDEC80902	N

Legend:
Y: Notifies JP1 event.
N: Does not notify JP1 event.

(8) Messages from KDEC81000 to KDEC81499 (HTTP adapter related messages)

Message ID	Existence of JP1 event notification
KDEC81000	Y
KDEC81001	Y
KDEC81002	Y
KDEC81003	Y
KDEC81004	Y
KDEC81005	Y
KDEC81006	Y
KDEC81007	Y
KDEC81008	Y
KDEC81051	Y
KDEC81052	Y
KDEC81053	Y
KDEC81054	Y
KDEC81055	Y
KDEC81056	A
KDEC81057	Y

Message ID	Existence of JP1 event notification
KDEC81058	Y
KDEC81059	Y
KDEC81060	Y
KDEC81061	Y
KDEC81064	A
KDEC81065	A
KDEC81066	Y
KDEC81069	Y
KDEC81070	Y
KDEC81071	A
KDEC81101	Y
KDEC81102	Y
KDEC81103	A
KDEC81104	A
KDEC81401	Y
KDEC81402	Y
KDEC81403	A
KDEC81404	Y
KDEC81450	N
KDEC81451	N
KDEC81452	N
KDEC81453	N
KDEC81454	A
KDEC81499	Y

Legend:

Y: Notifies JP1 event.

A: Defined with comments. If you want to notify JP1 event, remove the comment.

N: Does not notify JP1 event.

(9) Messages from KDEE10000 to KDEE13999 (TP1 adapter related messages)

Message ID	Existence of JP1 event notification
KDEE10000	N
KDEE10001	Y
KDEE10002	Y
KDEE10003	Y
KDEE10004	Y
KDEE10005	Y

Message ID	Existence of JP1 event notification
KDEE10006	Y
KDEE10007	Y
KDEE10008	Y
KDEE10009	Y
KDEE10010	Y
KDEE10011	Y
KDEE10013	Y
KDEE10014	Y
KDEE10500	N
KDEE10501	A
KDEE10502	A
KDEE10503	A
KDEE10504	A
KDEE11000	Y
KDEE11001	Y
KDEE11002	Y
KDEE11003	Y
KDEE11004	Y
KDEE11005	Y
KDEE11006	Y
KDEE11007	Y
KDEE11008	Y
KDEE11009	Y
KDEE11010	Y
KDEE11011	Y
KDEE11012	Y
KDEE11013	Y
KDEE11014	Y
KDEE11015	Y
KDEE11016	Y
KDEE11017	Y
KDEE11018	Y
KDEE11019	Y
KDEE11020	A
KDEE11021	Y
KDEE11022	Y

Message ID	Existence of JP1 event notification
KDEE11023	Y
KDEE11024	Y
KDEE11025	Y
KDEE11026	Y
KDEE11027	Y
KDEE11028	Y
KDEE11029	Y
KDEE11030	Y
KDEE11031	Y
KDEE11032	Y
KDEE11033	Y
KDEE11034	Y
KDEE12000	N
KDEE12001	N
KDEE12002	Y
KDEE12003	Y
KDEE12004	Y
KDEE12005	Y
KDEE12006	Y
KDEE12007	Y
KDEE12008	Y
KDEE12009	Y
KDEE12010	Y
KDEE12011	A
KDEE12012	A
KDEE12013	A
KDEE12014	A
KDEE12015	A
KDEE12016	Y
KDEE12017	Y
KDEE12018	Y
KDEE12019	Y
KDEE12020	Y
KDEE12021	A
KDEE13000	Y
KDEE13001	Y

Message ID	Existence of JP1 event notification
KDEE13002	A
KDEE13003	A
KDEE13004	A
KDEE13005	A
KDEE13006	A
KDEE13007	A
KDEE13008	A
KDEE13009	A
KDEE13010	A
KDEE13011	A
KDEE13012	A

Legend:

Y: Notifies JP1 event.

A: Defined with comments. If you want to notify JP1 event, remove the comment.

N: Does not notify JP1 event.

(10) Messages from KDEF10000 to KDEF30999 (Object Access adapter related messages)

All messages from KDEF10000 to KDEF30999 do not notify JP1 event.

(11) Messages from KDEG20000 to KDEG30999 (File adapter related messages)

All messages from KDEG20000 to KDEG30999 do not notify JP1 event.

(12) Messages from KDEH20000 to KDEH30999 (Message Queue adapter related messages)

All messages from KDEH20000 to KDEH30999 do not notify JP1 event.

(13) Messages from KDEK20000 to KDEK30999 (FTP adapter related messages)

Message ID	Existence of JP1 event notification
KDEK20000	N
KDEK20001	Y
KDEK20002	Y
KDEK20201	Y
KDEK20202	Y
KDEK20203	Y
KDEK20204	N
KDEK20205	Y
KDEK20206	Y
KDEK20208	Y

Message ID	Existence of JP1 event notification
KDEK20209	Y
KDEK20210	Y
KDEK20211	N
KDEK20212	Y
KDEK20213	Y
KDEK20215	Y
KDEK20900	Y
KDEK20901	Y
KDEK20902	N
KDEK20903	N
KDEK20904	Y
KDEK20905	N
KDEK20907	Y
KDEK20908	N
KDEK20909	N
KDEK20910	Y
KDEK21000	N
KDEK21001	N
KDEK21900	N
KDEK21901	N
KDEK30000	Y
KDEK30001	Y
KDEK30202	Y
KDEK30203	Y
KDEK30204	Y
KDEK30205	Y
KDEK30206	Y
KDEK30207	Y
KDEK30400	Y
KDEK30401	Y
KDEK30402	Y
KDEK30403	Y
KDEK30404	Y
KDEK30405	Y
KDEK30406	Y
KDEK30407	Y

Message ID	Existence of JP1 event notification
KDEK30408	N
KDEK30409	Y
KDEK30410	N
KDEK30411	Y
KDEK30412	Y
KDEK30413	Y
KDEK30414	Y
KDEK30415	Y
KDEK30416	Y
KDEK30417	Y
KDEK30418	Y
KDEK30419	Y
KDEK30420	Y
KDEK30421	N
KDEK30422	Y
KDEK30423	Y
KDEK30424	Y
KDEK30425	Y
KDEK30426	Y
KDEK30427	Y
KDEK30428	Y
KDEK30432	Y
KDEK30433	Y
KDEK30434	Y
KDEK30435	N
KDEK30501	N
KDEK30502	N
KDEK30503	N
KDEK30511	N
KDEK30512	N
KDEK30513	N
KDEK30514	N
KDEK30515	N
KDEK30516	N
KDEK30531	N
KDEK30532	N

Message ID	Existence of JP1 event notification
KDEK30533	N
KDEK30541	N
KDEK30542	N
KDEK30543	N
KDEK30551	N
KDEK30552	N
KDEK30553	N
KDEK30554	N
KDEK30555	N
KDEK30557	N
KDEK30558	N
KDEK30559	N
KDEK30571	N
KDEK30572	N
KDEK30573	N
KDEK30601	N
KDEK30602	N
KDEK30603	N
KDEK30604	N
KDEK30605	N
KDEK30606	N
KDEK30607	N
KDEK30608	N
KDEK30609	N
KDEK30901	N

Legend:

Y: Notifies JP1 event.

N: Does not notify JP1 event.

(14) Messages from KEOS50000 to KEOS59999 (HCSC-Manager related messages)

All messages from KEOS50000 to KEOS59999 do not notify JP1 event.

G. Migration from an Old Version

If you have a development, operating, and execution environment created by using an old version of Service Platform, you can update them to version 09-51. The repository information (HCSC components and deployment definitions) used with the old version can also be used with the new version by converting the repository information through processing called *migration*.

This manual describes the version update procedure that allows the new version to use the existing repository information as is. Repository migration can be performed in either the development environment or operating environment. If you choose to perform migration and update the version in the operating environment, see *Appendix H. Performing Repository Migration from an Old Version in the Operating Environment*.

If you choose to convert the existing repository information before or after a version update in the development environment, and to use the converted repository information with the new version, see *Appendix A. Migrating from old version* in the *uCosminexus BPM/ESB Service Platform Basic Development Guide*.

! Important note

Make sure that the development, operating, and execution environments have been updated to the same version.

G.1 Versions supporting repository migration

The versions listed below support migration of repository information. If you update the version from one of these versions to 09-51 in each environment, you can continue to use the existing repository information by using migration.

- Service Architect 07-10
- Service Platform 07-10
- Service Architect 07-20
- Service Platform 07-20
- Service Architect 07-50
- Service Platform 07-50
- Service Architect 07-60
- Service Platform 07-60
- Service Architect 08-00
- Service Platform 08-00
- Service Architect 08-10
- Service Platform 08-10
- Service Architect 08-50
- Service Platform 08-50
- Service Architect 08-51
- Service Platform 08-51
- Service Architect 08-53
- Service Platform 08-53
- Service Architect 08-70
- Service Platform 08-70
- Service Architect 09-00
- Service Platform 09-00
- Service Architect 09-50
- Service Platform 09-50

Note that the migration method differs depending on whether the old version is earlier than 07-50.

Migration to 09-51 from a version earlier than 07-50

Uninstall the old version, and then install the new version (09-51) as a new installation. For details about the migration procedure, see *G.2 Migration procedure for a new installation*.

Migration to 09-51 from 07-50 or a later version

You can use one of the following three ways to perform migration:

- Uninstall the old version, and then install the new version (09-51) as a new installation. We recommend that you use this method if the old version has been set up by using HCSC Easy Setup. For details about how to perform migration, see *G.2 Migration procedure for a new installation*.
- Install the new version (09-51) as an update installation. For details about how to perform migration, see *G.3 Migration procedure for an update installation*.
- Install the new version (09-51) as an update installation without fully stopping the system (*rolling update*). If the product is running in a load-balancing cluster configuration, use this method. For details about how to perform migration, see *G.4 Migration procedure for a rolling update*.

The following table lists the product versions and the repository versions that support the product versions.

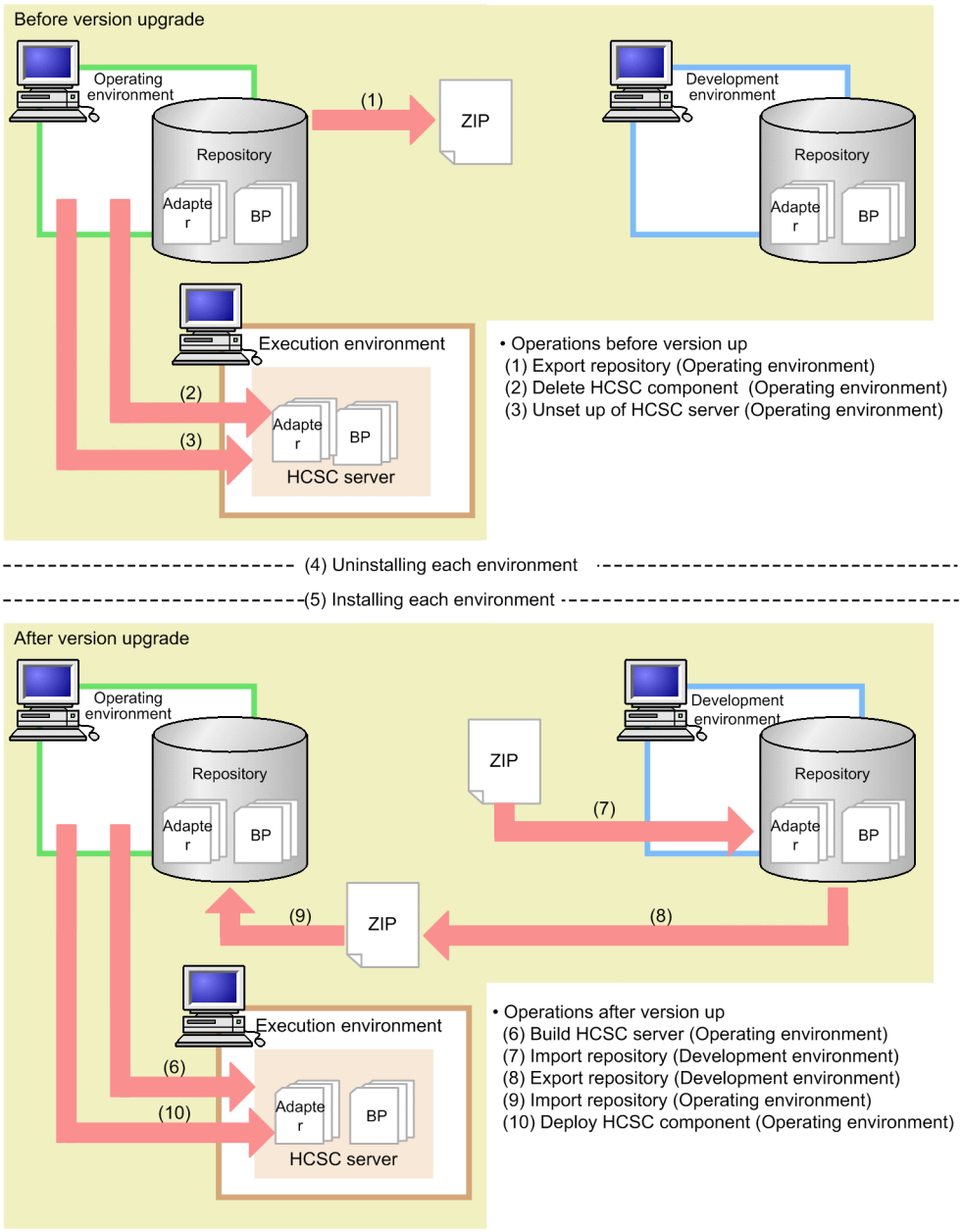
Table G–1: Repository versions supporting product versions

Product version	Repository version
07-50	1.0
07-60	1.1
08-00	1.1
08-10	1.2
08-50	1.3
08-51	1.4
08-53	1.5
08-70	1.6
09-00	1.7
09-50	1.8
09-51	1.9

G.2 Migration procedure for a new installation

Update Service Platform from the old version to the new version (09-51), following the steps in the below figure (*(1) Export the repository (operating environment)* to *(10) Deploy HCSC components (operating environment)*).

Figure G–1: Migration procedure for a new installation



The steps in Figure G-1 (*(1) Export the repository (operating environment)* to *(10) Deploy HCSC components (operating environment)*) are described below.

For details about the commands used in these steps, see *Chapter 5. Commands (Operating and Execution Environments)* in the *uCosminexus Service Platform Reference Guide*. For details about the tasks performed in the development environment, see the manual *uCosminexus BPM/ESB Service Platform Basic Development Guide*.

! Important note

From version 07-60, the development environment and operating environment cannot share the same repository. If the repository is shared by the development and operating environments in the old version, prepare separate repositories in these environments before starting migration. For details about the migration procedure, see *A.3 Migrating procedure when a repository is shared between development environment and operating environment in earlier version* in the *uCosminexus BPM/ESB Service Platform Basic Development Guide*.

(1) Export the repository (operating environment)

Before you update the version, in the operating environment, export the repository as a backup. If there are multiple repositories, export all necessary repositories as backups.

In the operating environment, execute the `cscrepctl` command (with the `-export` option) to export the repository (or repositories).

For details about how to export a repository, see *4.2 Exporting Repository Information*.

(2) Delete HCSC components (operating environment)

Before you update the version, in the execution environment, delete all HCSC components deployed on the HCSC server. If there are multiple HCSC servers, delete all HCSC components from all of the HCSC servers.

In the operating environment, execute the `csccompoundeploy` command as shown below. This command deletes all HCSC components deployed on the specified HCSC server.

```
csccompoundeploy -csc HCSC-server-name -type {adapter|bp} -name service-adapter's-service-ID
```

(3) Perform unsetup of the HCSC servers (operating environment)

Before you update the version, in the execution environment, perform unsetup of all HCSC servers.

In the operating environment, execute the `cscsvunsetup` command to perform unsetup of all HCSC servers. For a test environment in which Service Platform was set up by using HCSC Easy Setup, use HCSC Easy Setup to perform unsetup.

For details about how to perform unsetup of HCSC servers, see *3.3.5 Unsetting up an HCSC server*.

If you have updated a version earlier than 07-50 to 09-50 without performing unsetup, you must delete the HCSC servers manually. You do not need to manually delete the HCSC servers if the update is from 07-50 or later to 09-50.

(4) Uninstall Service Platform in each environment

Uninstall the old version of Service Platform in the development, operating, and execution environments. We recommend that you back up the Service Platform installation directory before uninstalling Service Platform.

(a) Notes on uninstallation

- Before you start uninstallation, terminate all components, such as the J2EE server, Management Server, and PRF, in the execution environment.
- If an embedded database is used, terminate it before you start uninstallation.

(b) Notes applying to an update from a version earlier than 07-50

- Finish unsetup of all HCSC servers before updating the version.
- Before you update the version of the execution environment, use the `cscrepls` command to confirm that no HCSC server information remains. If HCSC server information remains, perform unsetup of those HCSC servers, and then update the version. If you attempt to update the version when HCSC server information remains, the update will not be performed correctly.
- After performing unsetup of HCSC servers, delete the repository root, including the contents.

(c) Notes applying to an update from a version earlier than 09-00

The products listed below come with Service Platform 09-00 or later. If any of the products listed below have already been installed, we recommend that you uninstall them.

- Service Adapter for Flat Files
- Service Adapter Architect for Flat Files
- Service Adapter for FTP
- Service Adapter Architect for FTP

- Service Adapter for Message Queue
- Service Adapter Architect for Message Queue
- Service Adapter for Object Access
- Service Adapter Architect for Object Access
- Service Adapter for TP1
- Service Adapter Architect for TP1
- Code Conversion - Development Kit
- Code Conversion - Server Runtime
- Code Conversion - Runtime
- TP1/Client/J

(d) Note on updating the development environment

In the development environment, delete the HCSCTE project before updating the version, and then re-create the project after updating the version.

(5) Install Service Platform in each environment

Install Service Platform 09-51 to update the version in the development, operating, and execution environments.

(6) Set up an HCSC server (operating environment)

Set up and define the same environment as the previously created HCSC server, based on the following files that were created previously:

- HCSC server configuration definition file
- HCSC server setup definition file
- HCSC server runtime definition file
- User-defined reception runtime definition file

In a test environment, use HCSC Easy Setup to set up an HCSC server.

(7) Import the repository (development environment)

In *(1) Export the repository (operating environment)* above, you exported the repository. Here, import the exported repository in the development environment. Before you import the repository, make sure that **Build Automatically** (in the **Project** menu) is disabled in Eclipse. After the repository has been imported, enable **Build Automatically** again.

When you import the repository that was used in the old version, packaging and deployment definition are automatically performed, and the new version inherits the repository information. Note that packaging and deployment definition are automatically performed for only the service adapters, business processes, and user-defined receptions for which packaging and deployment definition were performed in the old version.

(a) Note applying to update from a version earlier than 07-50

If the following file names are set in a user-defined class of the SessionBean adapter, a warning message appears:

- `csmsvcadpdef.jar`
- `cscmsg_adpejb.jar`

If a warning message appears, in the Service Adapter Settings window, delete that user-defined class, change the file names, and then set the new file names again.

(b) Note applying to update from version 07-60 or later

If the version that you want to update is 07-60 or later, the service adapters and user-defined receptions to be deployed in the execution environment must be imported to the development environment and packaged again. If you do not repackage service adapters, the KDEC03007-E message might not be output. If you do not repackage user-defined

receptions, incorrect characters might be output to the KDEC00001-E message. For details about how to perform packaging, see *7.2 Packaging* in the *uCosminexus BPM/ESB Service Platform Basic Development Guide*.

(c) Note applying to update from a version earlier than 08-10

If the elements (compositors) listed below are defined under the `sequence` or `choice` element in the data transformation definition and the number of occurrences is fixed to 1 for those elements, the node display is changed. As a result, an error message appears, indicating that the XML schema used in the mapping definition file has been changed.

- `sequence`
- `choice`

If this error message appears, restart mapping definition, and then apply the change.

(d) Notes applying to update from a version earlier than 09-50

- If the data transformation definition includes the schema definitions shown below, the namespace is changed. As a result, an error message appears, indicating that the XML schema used in the mapping definition file has been changed.
  1. The schema that defines the target namespace (`targetNamespace`) at the import destination is specified on the transformation source node.
  2. The namespace in 1 is not defined in all namespace declarations (`xmlns[:prefix]`) including the import or include destination.

  If this error message appears, restart mapping definition, and then apply the change.
- Because the default values are used for the minimum and maximum numbers of pooled instances, if the `xml-pooled-instance-minimum` or `xml-pooled-instance-maximum` property is specified in the HCSC server runtime definition file, the specification of these properties might affect performance. To prevent performance from being affected, make sure that the same values are specified for these properties and the corresponding properties in the `usrconf.properties` file (user property file for the J2EE server), as shown below.

Item	Properties in the HCSC server runtime definition file#1	Properties in the usrconf.properties file (user property file for the J2EE server)#2
Min.	`xml-pooled-instance-minimum`	`csc.dt.pool.DocumentBuilder.initialSize`
Max.	`xml-pooled-instance-maximum`	`csc.dt.pool.DocumentBuilder.maxSize`

#1

For details about the HCSC server runtime definition file, see *HCSC server runtime definition file* in the *uCosminexus Service Platform Reference Guide*.

#2

For details about how to specify these properties, see *2.3.10 Using XML parser pool functionality option*.

(e) Note on memory

Import of the repository used in the old version requires a lot of memory. Therefore, use the procedure below to check whether the amount of installed memory is sufficient. If the amount of installed memory is insufficient, increase memory, and then import the repository.

1. From the Eclipse menu, select **Window**, and then **Preferences**.
2. In the tree view at the left of the dialog box that opens, select **General**.
3. Select the **Show heap status** check box at the right of the dialog box.
4. Select the trash can icon in the bottom right of the Eclipse window to run the garbage collector.
5. Check the heap size displayed to the left of the trash can icon.
6. If unused heap space is insufficient, edit the `eclipse.ini` file to increase the memory size (the value of `-Xmx`). For details about how to edit the `eclipse.ini` file, see *2.4.3 Setting up the Eclipse environment* in the *uCosminexus Application Server Application Development Guide*.

(f) Notes on the client definition file

If the SOAP adapter is defined in the development environment, the value of the `c4web.logger.log_file_prefix` property in the client definition file (`c4webcl.properties`) is automatically changed to the service ID. Delete the old client definition file if it is unnecessary. For details, see *3.3.1 Defining SOAP adapters* in the *uCosminexus BPM/ESB Service Platform Reception and Adapter Definition Guide*.

(8) Export the repository (development environment)

Export the repository that was imported in *(7) Import the repository (development environment)*.

(9) Import the repository (operating environment)

Import the repository that was exported in *(8) Export the repository (development environment)*. Note that you cannot import the repository that was used in the old version.

Execute the `cscrepctl` command (with the `-import` option) in the operating environment.

For details about how to import the repository, see *4.3 Importing a repository*.

(10) Deploy HCSC components (operating environment)

After you have imported the repository information in *(9) Import the repository (operating environment)*, deploy the HCSC components included in the repository information on the HCSC server. Make sure that the resulting environment is the same as the environment existing when the repository was exported in *(1) Export the repository (operating environment)*.

Execute the `csccompodeploy` command (with the `-all` option) in the operating environment.

For details about how to deploy HCSC components, see *3.1.8 Deploying a service adapter* and *3.1.13 Deploying a business process*.

After you have deployed the HCSC components, you can perform operations on them as you could before the version was updated.

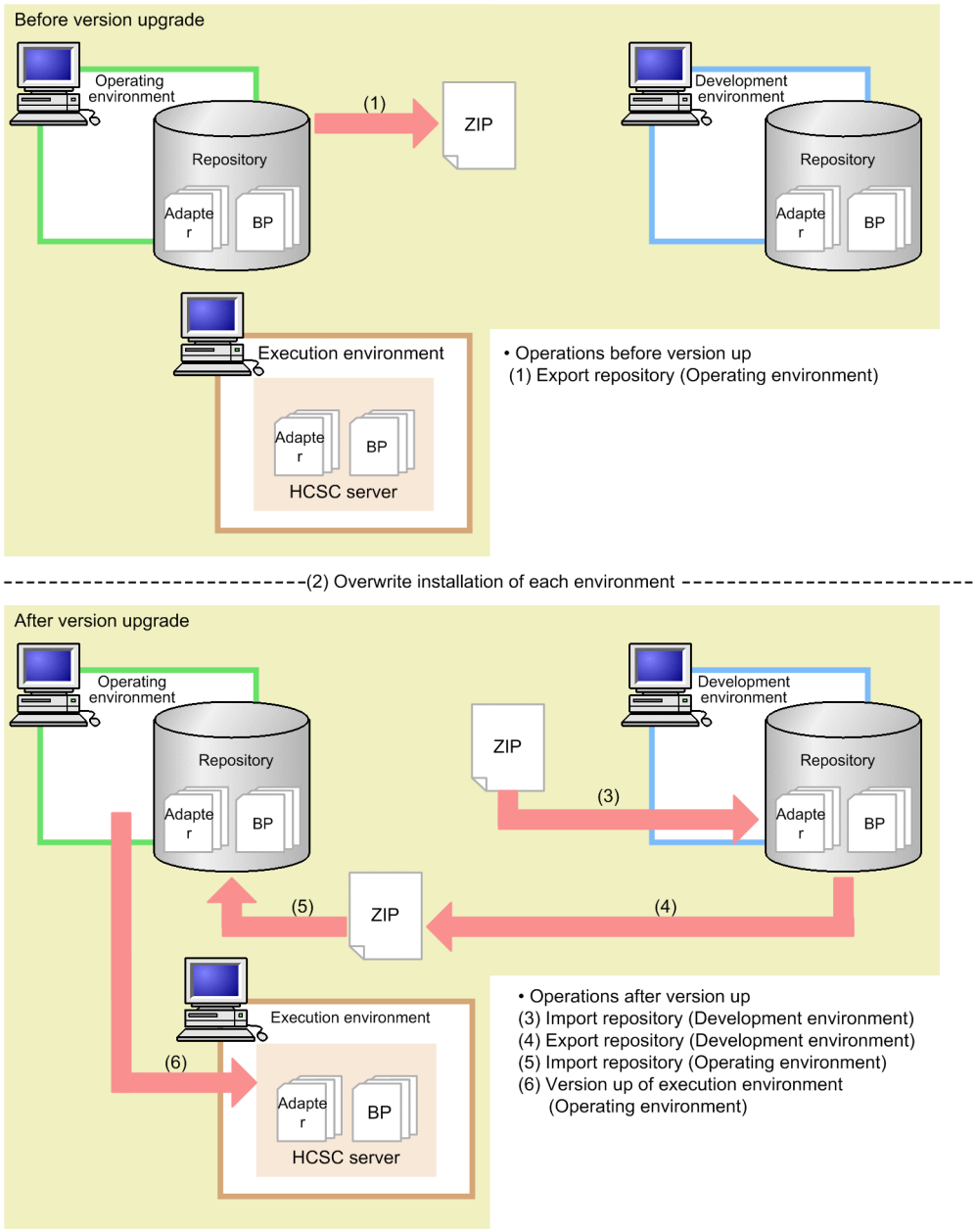
If you choose to convert the existing repository information before or after version update in the development environment, and to use the converted repository information with the new version, see *A.3 Migrating procedure when a repository is shared between development environment and operating environment in earlier version*< in the *uCosminexus BPM/ESB Service Platform Basic Development Guide*.

G.3 Migration procedure for an update installation

Note: Update installation can be used only when the version to be updated is 07-50 or later. To update a version earlier than 07-50, install version 09-51 as a new installation.

Update Service Platform from the old version (07-50 or later) to the new version (09-51), following the steps in the below figure (*(1) Export the repository (operating environment)* to *(10) Update the execution environment (operating environment)*.

Figure G–2: Migration procedure for an update installation



The steps in Figure G-2 (*(1) Export the repository (operating environment)* to *(10) Update the execution environment (operating environment)*) are described below.

For details about the commands used in these steps, see *Chapter 5. Commands (Operating and Execution Environments)* in the *uCosminexus Service Platform Reference Guide*. For details about the tasks performed in the development environment, see the manual *uCosminexus BPM/ESB Service Platform Basic Development Guide*.

Important note

- From version 07-60, the development environment and operating environment cannot share the same repository. If the repository is shared by the development and operating environments in the old version, prepare separate repositories in these environments before starting migration. For details about the migration procedure, see *A.3 Migrating procedure when a repository is shared between development environment and operating environment in earlier version* in the *uCosminexus BPM/ESB Service Platform Basic Development Guide*.
- If you stop the HCSC server and update the version of the execution environment while HCSC components are running, the HCSC components will stop when you restart the HCSC server. Therefore, after you restart the HCSC server, you must also restart the HCSC components.

- Check whether the Service Coordinator administrator has been changed from `root` in a UNIX environment. If so, change the owner of the files in the following directory to the Service Coordinator administrator, and the owner group of those files to the group that the Service Coordinator administrator belongs to:
  `/opt/Cosminexus/CSC`

---

(1) Export the repository (operating environment)

Before you update the version, in the operating environment, export the repository as a backup. If there are multiple repositories, export all necessary repositories as backups.

In the operating environment, execute the `cscrepctl` command (with the `-export` option) to export the repository (or repositories).

For details about how to export a repository, see *4.2 Exporting Repository Information*.

(2) Perform update installation in each environment

Update the version of Service Platform by installing Service Platform 09-51 as an update installation in the development, operating, and execution environments. For a test environment in which Service Platform was set up by using HCSC Easy Setup, use HCSC Easy Setup to perform unsetup before you perform update installation, and perform setup again after update installation.

The following shows the prerequisites for update installation in each environment.

Prerequisites:

- The HCSC server has been set up.
- Service Platform and Reliable Messaging are not running.
- The embedded database (if used) is not running.
- The HCSC server, J2EE server, and HCSC components are not running.

Notes

Notes on update installation:

- Before you start update installation, terminate all components, such as the J2EE server, Management Server, and PRF, in the execution environment.
- If an embedded database is used, terminate it before you start update installation.

Notes on updating the version in the development environment:

In the development environment, delete the HCSCTE project before updating the version, and then re-create the project after updating the version.

Note that update installation overwrites all files other than the files listed below:

- *Service-Platform-installation-directory*`\CSC\config\manager\csccmd.properties`
- *Service-Platform-installation-directory*`\CSC\config\manager\cscmng.properties`
- *Service-Platform-installation-directory*`\CSC\config\msg\cmdconf.bat`
- *Service-Platform-installation-directory*`\CSC\inbound-adapter\ftp\config\command\log4j.xml`
- *Service-Platform-installation-directory*`\CSC\inbound-adapter\ftp\config\FTP_Inbound_Resource_Adapter\serverstatus.properties`
- *Service-Platform-installation-directory*`\CSC\inbound-adapter\ftp\config\FTP_Inbound_Resource_Adapter\users.properties`
- *Service-Platform-installation-directory*`\CSC\system\manager\setup\input.properties`

(3) Change the class path of the J2EE server

If the version to be updated is earlier than 09-00 and the option definition file for the J2EE server (`usrconf.cfg`) contains the entries listed below, delete all of them. When you change the definition, we recommend that you use Smart Composer functionality or management portal.

- add.class.path=*TP1-adapter-installation-directory*\lib\adptp1rt.jar
- add.class.path=*file-adapter-installation-directory*\lib\adpffrt.jar
- add.class.path=*Object-Access-adapter-installation-directory*\lib\adpoart.jar
- add.class.path=*Object-Access-adapter-installation-directory*\usrlib\adpoaow.jar
- add.class.path=*Message-Queue-adapter-installation-directory*\lib\adpmqrt.jar
- add.class.path=*FTP-adapter-installation-directory*\lib\adpftprt.jar
- add.class.path=*FTP-adapter-installation-directory*\lib\ftp_common.jar
- add.class.path=*code-conversion-library-installation-directory*\java\codeconv.jar
- add.class.path=*TP1/Client/J-installation-directory*\LIB\TP1Client.jar

(4) Perform migration of old option adapter definition files

Migration of the option adapters that were used in a version earlier than 09-00 requires the tasks described below.

(a) Migration of the TP1 adapter definition files

Copy the TP1 adapter execution-environment property files. The files to be copied and the copy destination directory are as follows:

Files to be copied: *TP1-adapter-installation-directory*\config*.properties

Copy destination: *Service-Platform-installation-directory*\CSC\custom-adapter\TP1\config\

(b) Migration of the file adapter definition files

Copy the file adapter execution-environment property files. The files to be copied and the copy destination directory are as follows:

Files to be copied: *file-adapter-installation-directory*\config*.properties

Copy destination: *Service-Platform-installation-directory*\CSC\custom-adapter\File\config\

(c) Migration of the Object Access adapter definition files

Copy the Object Access adapter execution-environment property files. The files to be copied and the copy destination directory are as follows:

Files to be copied: *Object-Access-adapter-installation-directory*\config*.properties

Copy destination: *Service-Platform-installation-directory*\CSC\custom-adapter\OA\config\

(d) Migration of the Message Queue adapter definition files

Copy the Message Queue adapter execution-environment property files. The files to be copied and the copy destination directory are as follows:

Files to be copied: *Message-Queue-adapter-installation-directory*\config*.properties

Copy destination: *Service-Platform-installation-directory*\CSC\custom-adapter\MQ\config\

(e) Migration of the FTP adapter definition files

Copy the FTP adapter command definition files and FTP adapter execution-environment property files. The files to be copied and the copy destination directory are as follows:

Files to be copied: *FTP-adapter-installation-directory*\config*.properties

Copy destination: *Service-Platform-installation-directory*\CSC\custom-adapter\FTP\config\

(5) Uninstall products

The products listed below come with Service Platform 09-00 or later. If you update Service Platform from a version earlier than 09-00 and any of these products have already been installed, we recommend that you uninstall them.

- Service Adapter for Flat Files

- Service Adapter Architect for Flat Files
- Service Adapter for FTP
- Service Adapter Architect for FTP
- Service Adapter for Message Queue
- Service Adapter Architect for Message Queue
- Service Adapter for Object Access
- Service Adapter Architect for Object Access
- Service Adapter for TP1
- Service Adapter Architect for TP1
- Code Conversion - Development Kit
- Code Conversion - Server Runtime
- Code Conversion - Runtime
- TP1/Client/J

(6) Import the repository (development environment)

In *(1) Export the repository (operating environment)* above, you exported the repository. Here, import the exported repository in the development environment. When you import the repository that was used in the old version, packaging and deployment definition are automatically performed, and the new version inherits the repository information. Note that packaging and deployment definition are automatically performed for only the service adapters, business processes, and user-defined receptions for which packaging and deployment definition were performed in the old version.

(a) Note applying to update from version 07-60 or later

If the version that you want to update is 07-60 or later, the service adapters and user-defined receptions to be deployed in the execution environment must be imported to the development environment and must be packaged again. If you do not repackage service adapters, the KDEC03007-E message might not be output. If you do not repackage user-defined receptions, incorrect characters might be output to the KDEC00001-E message. For details about how to perform packaging, see *7.2 Packaging* in the *uCosminexus BPM/ESB Service Platform Basic Development Guide*.

(b) Note applying to update from a version earlier than 08-10

If the elements (compositors) listed below are defined under the `sequence` or `choice` element in the data transformation definition and the number of occurrences is fixed to 1 for those elements, the node display is changed. As a result, an error message appears, indicating that the XML schema used in the mapping definition file has been changed.

- `sequence`
- `choice`

If this error message appears, restart mapping definition, and then apply the change.

(c) Notes applying to update from a version earlier than 09-50

- If the data transformation definition includes the schema definitions shown below, the namespace is changed. As a result, an error message appears, indicating that the XML schema used in the mapping definition file has been changed.
  1. The schema that defines the target namespace (`targetNamespace`) at the import destination is specified on the transformation source node.
  2. The namespace in 1 is not defined in all namespace declarations (`xmlns[:prefix]`) including the import or include destination.

  If this error message appears, restart mapping definition, and then apply the change.
- Default values are used for the minimum and maximum numbers of pooled instances. Therefore, if the property `xml-pooled-instance-minimum` or `xml-pooled-instance-maximum` is specified in the HCSC

server runtime definition file, performance might be affected because of the specifications of these properties. To prevent performance from being affected, make sure that the same values are specified for these properties and the corresponding properties in the `usrconf.properties` file (user property file for the J2EE server), as shown below.

Item	Properties in the HCSC server runtime definition file[#1]	Properties in the usrconf.properties file (user property file for the J2EE server)[#2]
Min.	`xml-pooled-instance-minimum`	`csc.dt.pool.DocumentBuilder.initialSize`
Max.	`xml-pooled-instance-maximum`	`csc.dt.pool.DocumentBuilder.maxSize`

#1

For details about the HCSC server runtime definition file, see *HCSC server runtime definition file* in the *uCosminexus Service Platform Reference Guide*.

#2

For details about how to specify these properties, see *2.3.10 Using XML parser pool functionality option*.

(d) Note on memory

Import of the repository used in the old version requires a lot of memory. Therefore, use the procedure below to check whether the amount of installed memory is sufficient. If the amount of installed memory is insufficient, increase memory, and then import the repository.

1. From the Eclipse menu, select **Window**, and then **Preferences**.
2. In the tree view at the left of the dialog box that opens, select **General**.
3. Select the **Show heap status** check box at the right of the dialog box.
4. Select the trash can icon in the bottom right of the Eclipse window to run the garbage collector.
5. Check the heap size displayed to the left of the trash can icon.
6. If unused heap space is insufficient, edit the `eclipse.ini` file to increase the memory size (the value of `-Xmx`). For details about how to edit the `eclipse.ini` file, see *2.4.3 Setting up the Eclipse environment* in the *uCosminexus Application Server Application Development Guide*.

(7) Export the repository (development environment)

Export the repository that was imported in *(6) Import the repository (development environment)*.

(8) Import the repository (operating environment)

Import the repository that was exported in *(7) Export the repository (development environment)*. Note that you cannot import the repository that was used in the old version.

Execute the `cscrepctl` command (with the `-import` option) in the operating environment.

For details about how to import the repository, see *4.3 Importing a repository*.

(9) Update Service Platform and Reliable Messaging (execution environment)

Update Service Platform and Reliable Messaging by using the following procedure, which is also required when the version to be updated is earlier than 09-00:

- Execute the update command (`mngenvupdate`).
- Add properties to `mserver.properties` (Management Server environment configuration file).

  The properties to be added are shown below. If you start Management Server without adding these properties, commands whose names begin with `csc` might fail. For details about how to add properties, see *2.1.6(1) Setting mserver.properties (Management Server environment settings file)*.

  ```
  ejbserver.naming.port
  ejbserver.server.edition.settingforce
  ```

(10) Update the execution environment (operating environment)

Update the version of the execution environment from the operating environment.

(a) Prerequisites

The execution environment can be updated when all of the following conditions are satisfied:

- Management Server is running.
- The embedded database (if used) is running.
- The versions of the repository and installation are the same.
  If the repository version and installation version do not match, update the development environment, and then execute `cscrepctl -import` *repository-ZIP-file* to update the repository.
- (If the FTP inbound adapter is to be used) The resource adapter has already been updated by using the `cjrarupdate` command#.

  #

  For the `cjrarupdate` command, specify the following options and values:

  `-type` option: `rar`

  `-f` option: *Service-Platform-installation-directory*`\CSC\inbound-adapter\ftp\rar\ftp_inbound_adapter.rar`

  For details about the `cjrarupdate` command, see *cjrarupdate (update resource adapter version)* in the *uCosminexus Application Server Command Reference Guide*.

  Note that if you update the FTP inbound adapter from a version earlier than 09-50, the default terminator used for FTP response changes from the OS-dependent line break code to CR-LF. If you do not want to change the terminator, use the `cjgetrarprop` command to obtain the attribute file from the FTP inbound adapter's RAR files, change the definition, and then use the `cjsetrarprop` command to set the attribute file. For details about how to set the attribute file, see *3.2.3(3) Setting up the FTP inbound adapter*.

If the prerequisites listed above are not satisfied, satisfy them in the order in which they are listed.

(b) How to update the version

Execute the `cscenvupdate` command to update the version of the repository and HCSC server.

```
cscenvupdate -csc name-of-the-HCSC-server-to-be-updated
```

If you choose to convert the existing repository information before or after version update in the development environment, and to use the converted repository information with the new version, see *Appendix A. Migrating from old version* in the *uCosminexus BPM/ESB Service Platform Basic Development Guide*.

! Important note

If HTTP reception is used in the old version and the HITACHI Application Integrated Property File has been edited except the following elements, the changes are not applied to the new HITACHI Application Integrated Property File:

- `//hitachi-application-all-property/ejb-jar/hitachi-ejb-jar-property/display-name[.='cscmsg_urecp_custom']/../../hitachi-session-bean-property/display-name[.='CSCMsgCustomServiceDelivery']/../session-runtime/stateless/pooled-instance/minimum`
- `//hitachi-application-all-property/ejb-jar/hitachi-ejb-jar-property/display-name[.='cscmsg_urecp_custom']/../../hitachi-session-bean-property/display-name[.='CSCMsgCustomServiceDelivery']/../session-runtime/stateless/pooled-instance/maximum`
- `//hitachi-application-all-property/ejb-jar/hitachi-ejb-jar-property/display-name[.='cscmsg_urecp_custom']/../../hitachi-session-bean-property/display-name[.='CSCMsgCustomServiceDelivery']/../ejb-transaction-timeout/method/method-name[.='*']/../../transaction-timeout`

Therefore, if necessary, use the `csccompoconfig` command to obtain the HITACHI Application Integrated Property File, edit the contents, and then apply the changes.

For details about how to use the `csccompoconfig` command, see A.6 *csccompoconfig (Defining HCSC components)* in the *uCosminexus Service Platform Reference Guide*.

G.4 Migration procedure for a rolling update

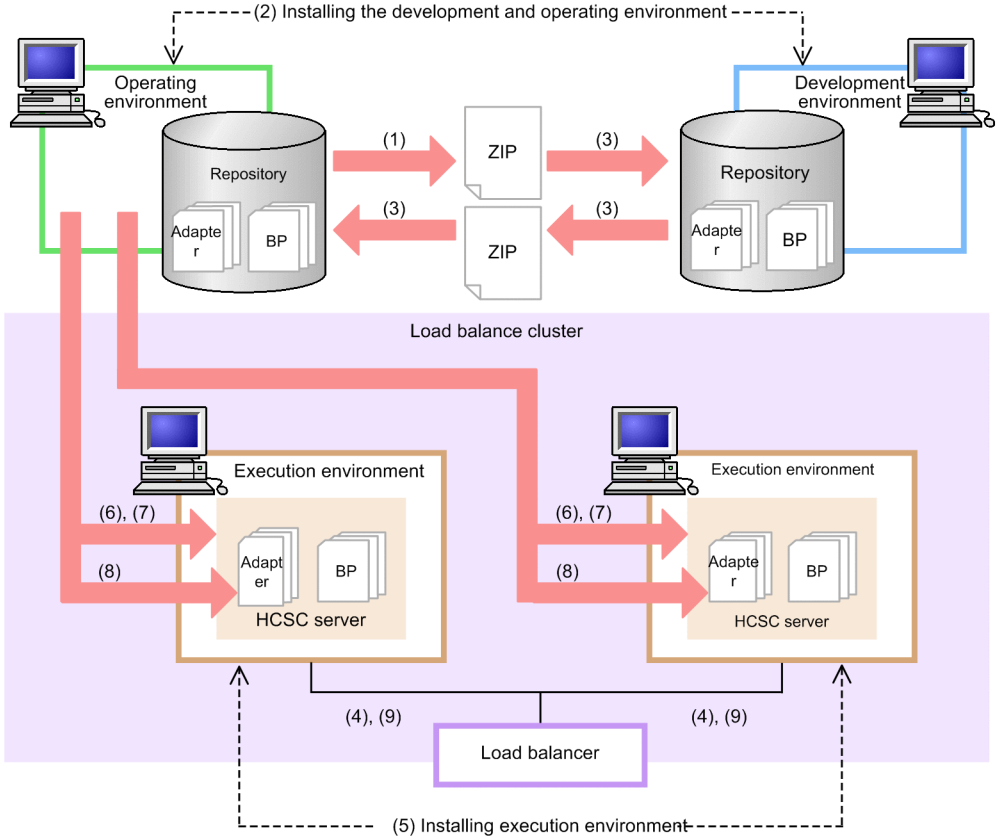
Rolling update is an update installation that is performed without fully stopping the system.

Rolling update can be performed only when the version to be updated is 07-50 or later. If the version to be updated is earlier than 07-50, install version 09-51 as a new installation. For notes on rolling update, see *(15) Notes on rolling update*.

Rolling update requires two or more HCSC servers that make up a load-balancing cluster.

Update Service Platform from the old version (07-50 or later) to the new version (09-51), following the steps in the below figure (*(1) Export the repository (operating environment)* to *(13) Respecify the request transmission control (load balancer) settings*).

Figure G–3: Migration procedure for a rolling update



• Operations before version upgrade
(1) Export repository (Operating environment)

• Version upgrade of development and operating environment
(2) Installing development and operating environment
(3) Import/ Export of repository (Development and operating environment)

• Version upgrade of execution environment
(4) Control sending of requests (Load balancer)
(5) Installing execution environment
(6) Version up of execution environment (Operating environment)
(7) Starting the HCSC server (Operating environment)
(8) Starting the HCSC component (Operating environment)
(9) Cancelling the control on sending requests (Load balancer)

The steps in Figure G-3 (*(1) Export the repository (operating environment)* to *(13) Respecify the request transmission control (load balancer) settings*) are described below. Note that, for the HCSC servers other than the first, you must perform *(14) Perform tasks on the HCSC servers other than the first HCSC server (execution environment)*.

For details about the commands used in these steps, see *Chapter 5. Commands (Operating and Execution Environments)* in the *uCosminexus Service Platform Reference Guide*. For details about the tasks performed in the development environment, see the *uCosminexus BPM/ESB Service Platform Basic Development Guide*.

Important note

- From version 07-60, the development environment and operating environment cannot share the same repository. If the repository is shared by the development and operating environments in the old version, prepare separate repositories in these environments before starting migration. For details about the migration procedure, see *A.3 Migrating procedure when a repository is shared between development environment and operating environment in earlier version* in the *uCosminexus BPM/ESB Service Platform Basic Development Guide*.
- You cannot perform the following operations in the old system until rolling update finishes:
  - Use the `cscsvsetup` command to set up a new HCSC server.
  - Use the `csccompodeploy` command to deploy a new HCSC component.

(1) Export the repository (operating environment)

Before you update the version, in the operating environment, export the repository as a backup. If there are multiple repositories, export all necessary repositories as backups.

In the operating environment, execute the `cscrepctl` command (with the `-export` option) to export the repository (or repositories).

For details about how to export a repository, see *4.2 Exporting Repository Information*.

(2) Install Service Platform in the development and operating environments

In the development and operating environments, install Service Platform 09-51 to update the version.

In the development environment, install Service Platform as a new installation or an update installation. In the operating environment, install Service Platform as an update installation.

To install Service Platform as a new installation:

Perform *(2) Delete HCSC components (operating environment)* to *(6) Set up an HCSC server (operating environment)* in *G.2 Migration procedure for a new installation*.

To install Service Platform as an update installation:

Perform *(2) Perform update installation in each environment* to *(5) Uninstall products* in *G.3 Migration procedure for an update installation*.

The prerequisites for installing Service Platform in the development and operating environments are as follows.

Prerequisites:

- HCSC servers have been set up.
- Service Platform and Reliable Messaging are not running.
- The embedded database (if used) is not running.
- The HCSC server, J2EE server, and HCSC components are not running.

Notes

Note the following points when you perform update installation:

- If the J2EE server, Management Server, PRF, and other components that make up the Service Platform execution environment are running in the environment in which you install Service Platform, stop all of them, and then start update installation.
- If an embedded database is used, stop it, and then start update installation.

(3) Change the class path of the J2EE server (development environment)

If the version to be updated is earlier than 09-00 and the option definition file for the J2EE server (`usrconf.cfg`) contains the entries listed below, delete all of them. When you change the definition, we recommend that you use Smart Composer functionality or management portal.

- `add.class.path=`*TP1-adapter-installation-directory*`\lib\adptp1rt.jar`
- `add.class.path=`*file-adapter-installation-directory*`\lib\adpffrt.jar`
- `add.class.path=`*Object-Access-adapter-installation-directory*`\lib\adpoart.jar`
- `add.class.path=`*Object-Access-adapter-installation-directory*`\usrlib\adpoaow.jar`
- `add.class.path=`*Message-Queue-adapter-installation-directory*`\lib\adpmqrt.jar`
- `add.class.path=`*FTP-adapter-installation-directory*`\lib\adpftprt.jar`
- `add.class.path=`*FTP-adapter-installation-directory*`\lib\ftp_common.jar`
- `add.class.path=`*code-conversion-library-installation-directory*`\java\codeconv.jar`
- `add.class.path=`*TP1/Client/J-installation-directory*`\LIB\TP1Client.jar`

(4) Perform migration of old option adapter definition files (development environment)

Migration of the option adapters that were used in a version earlier than 09-00 requires the tasks described below.

(a) Migration of the TP1 adapter definition files

Copy the TP1 adapter execution-environment property files. The files to be copied and the copy destination directory are as follows:

Files to be copied: *TP1-adapter-installation-directory*`\config\*.properties`

Copy destination: *Service-Platform-installation-directory*`\CSC\custom-adapter\TP1\config\`

(b) Migration of the file adapter definition files

Copy the file adapter execution-environment property files. The files to be copied and the copy destination directory are as follows:

Files to be copied: *file-adapter-installation-directory*`\config\*.properties`

Copy destination: *Service-Platform-installation-directory*`\CSC\custom-adapter\File\config\`

(c) Migration of the Object Access adapter definition files

Copy the Object Access adapter execution-environment property files. The files to be copied and the copy destination directory are as follows:

Files to be copied: *Object-Access-adapter-installation-directory*`\config\*.properties`

Copy destination: *Service-Platform-installation-directory*`\CSC\custom-adapter\OA\config\`

(d) Migration of the Message Queue adapter definition files

Copy the Message Queue adapter execution-environment property files. The files to be copied and the copy destination directory are as follows:

Files to be copied: *Message-Queue-adapter-installation-directory*`\config\*.properties`

Copy destination: *Service-Platform-installation-directory*`\CSC\custom-adapter\MQ\config\`

(e) Migration of the FTP adapter definition files

Copy the FTP adapter command definition files and FTP adapter execution-environment property files. The files to be copied and the copy destination directory are as follows:

Files to be copied: *FTP-adapter-installation-directory*`\config\*.properties`

Copy destination: *Service-Platform-installation-directory*`\CSC\custom-adapter\FTP\config\`

(5) Uninstall products

The products listed below come with Service Platform 09-00 or later. If you update Service Platform from a version earlier than 09-00 and any of these products have already been installed, we recommend that you uninstall them.

- Service Adapter for Flat Files
- Service Adapter Architect for Flat Files
- Service Adapter for FTP
- Service Adapter Architect for FTP
- Service Adapter for Message Queue
- Service Adapter Architect for Message Queue
- Service Adapter for Object Access
- Service Adapter Architect for Object Access
- Service Adapter for TP1
- Service Adapter Architect for TP1
- Code Conversion - Development Kit
- Code Conversion - Server Runtime
- Code Conversion - Runtime
- TP1/Client/J

(6) Import and export the repository (development and operating environments)

In *(1) Export the repository (operating environment)* above, you exported the repository. Here, import the exported repository in the development environment. The new version inherits the repository information from the old version. Then, similarly, import the exported repository in the new operating environment so that the repository information is also inherited in the new operating environment.

The tasks to be performed in import and export of the repository differ depending on how the development environment was installed in *(2) Install Service Platform in the development and operating environments*, as shown below.

If Service Platform is installed as a new installation:

Perform *(7) Import the repository (development environment)* to *(9) Import the repository (operating environment)* in *G.2 Migration procedure for a new installation*.

If Service Platform is installed as an update installation:

Perform *(6) Import the repository (development environment)* to *(8) Import the repository (operating environment)* in *G.3 Migration procedure for an update installation*.

(7) Specify the request transmission control (load balancer) settings

Specify the load balancer settings so that requests are not sent to the HCSC server being updated. Before doing this, make sure that no requests are being sent. How to specify the load balancer settings differs depending on the specifications of the load balancer you are using.

(8) Install Service Platform in the execution environment

In the execution environment, install Service Platform 09-51 to update the version.

In the execution environment, install Service Platform as a new installation or an update installation.

To install Service Platform as a new installation:

Perform *(2) Delete HCSC components (operating environment)* to *(6) Set up an HCSC server (operating environment)* in *G.2 Migration procedure for a new installation*.

To install Service Platform as an update installation:

Perform *(2) Perform update installation in each environment* to *(5) Uninstall products* in *G.3 Migration procedure for an update installation*.

(9) Update Service Platform and Reliable Messaging (execution environment)

Update Service Platform and Reliable Messaging by using the following procedure, which is also required when the version to be updated is earlier than 09-00:

- Execute the update command (`mngenvupdate`).
- Add properties to `mserver.properties` (Management Server environment configuration file).

  The properties to be added are shown below. If you start Management Server without adding these properties, commands whose names begin with `csc` might fail. For details about how to add properties, see *2.1.6(1) Setting mserver.properties (Management Server environment settings file)*.

  ```
  ejbserver.naming.port
  ejbserver.server.edition.settingforce
  ```

(10) Update the execution environment (operating environment)

Update the version of the execution environment from the operating environment.

(a) Prerequisites

The execution environment can be updated when all of the following conditions are satisfied:

- Management Server is running.
- The embedded database (if used) is running.
- The versions of the repository and installation are the same.

  If the repository version and installation version do not match, update the development environment, and then execute `cscrepctl -import` *repository-ZIP-file* to update the repository.

If the prerequisites listed above are not satisfied, satisfy them in the order in which they are listed.

(b) How to update the version

Execute the `cscenvupdate` command to update the version of the repository and HCSC server.

```
cscenvupdate -csc name-of-the-HCSC-server-to-be-updated
```

(11) Start the HCSC server (operating environment)

Start the updated HCSC server.

(12) Start the HCSC components (operating environment)

Start the HCSC components that are deployed on the HCSC server whose version was updated in *(10) Update the execution environment (operating environment)*.

(13) Respecify the request transmission control (load balancer) settings

Respecify the load balancer settings so that requests are sent to the updated HCSC server. How to specify the load balancer settings differs depending on the specifications of the load balancer you are using.

(14) Perform tasks on the HCSC servers other than the first HCSC server (execution environment)

On all HCSC servers that make up the load-balancing cluster, perform *(7) Specify the request transmission control (load balancer) settings* to *(13) Respecify the request transmission control (load balancer) settings*.

If you choose to convert the existing repository information before or after version update in the development environment, and to use the converted repository information with the new version, see *Appendix A. Migrating from old version* in the *uCosminexus BPM/ESB Service Platform Basic Development Guide*.

(15) Notes on rolling update

(a) If the target of rolling update is version 08-70 or earlier

The `cscenvupdate` command might fail when all of the following conditions exist:

- Service Platform has been set up in a configuration that uses HiRDB (as a database) and Reliable Messaging.
- Business processes are used.
- The update being performed is the first update performed in the cluster.
- Rolling update is performed for Service Platform whose version is 08-70 or earlier.

The following describes the countermeasures for operating the system normally under the above conditions, and provides an operation example.

- Countermeasures:
  Perform the following procedure (steps 1 to 4) on all running HCSC servers:
  1. Stop the execution log reference command and system operation GUI.
  2. Specify the request transmission control settings to prevent requests from being sent to the HCSC servers.
  3. Stop HCSC server receptions (standard and user-defined receptions).
  4. Discard the all resource adapter pools (by using the `cjclearpool` command).

  After performing the above procedure, execute the `cscenvupdate` command on one of the updated HCSC servers. You do not need to perform the above procedure on the rest of the updated HCSC servers. Note that after normal termination of the first `cscenvupdate` command is confirmed, the functions stopped in steps 1 to 3 can be restarted regardless of when an operation is performed on the second and following servers.
- Operation example:
  This example assumes that the version is updated under the following conditions:
  - The cluster consists of HCSC servers A, B, and C.
  - While HCSC servers B and C are running, the `cscenvupdate` command is executed on HCSC server A.

  To run the system normally under the above conditions, perform the following procedure:
  1. Stop the execution log reference command and system operation GUI.
  2. Specify the request transmission control settings to prevent requests from being sent to HCSC servers B and C.
  3. Stop receptions of HCSC servers B and C (standard and user-defined receptions).
  4. Use the `cjclearpool` command to discard all resource adapter pools of HCSC servers B and C.
  5. Execute the `cscenvupdate` command on HCSC server A.

(b) If the target of rolling update is version 09-00 or later

The `cscenvupdate` command might fail when all of the following conditions exist:

- Service Platform has been set up in a configuration that uses a database and Reliable Messaging.
- Business processes are used.
- The update being performed is the first update performed in the cluster.

In this case, stop online processing, and then perform rolling update, following the procedure in *H.4 Repository migration procedure in the operating environment during rolling update*.

G.5 Setup after an update (in the case of an update from a version earlier than 07-50)

After Service Platform is updated from a version earlier than 07-50, the execution environment requires software setup. This appendix describes how to set up Reliable Messaging.

From version 07-50, creation of a queue definition file is no longer necessary for setting up Reliable Messaging. Therefore, you do not need to create a queue definition file during setup of Reliable Messaging after a version update. However, if an update is from a version earlier than 07-50, you can set up Reliable Messaging by creating a queue definition file in the same way as in the old version.

(a) Creating a queue definition file

Use a sample queue definition file to create the queue definition file (by changing the cluster name). The location of the sample queue definition file is as follows:

Service-Platform-installation-directory\CSC\samples\qconf.txt

The contents of the sample queue definition file are as follows:

```
############################################################
# Cosminexus Reliable Messaging JMS Queue Configuration
# All Rights Reserved. Copyright (C) 2006, Hitachi, Ltd.
############################################################
QueueImplClass=jp.co.Hitachi.soft.reliablemessaging.ra.jms.QueueImpl
Queue.1.DisplayName= CSC<HCSCServer_Name>ACPT_RCVQ
Queue.1.QueueName= CSC<HCSCServer_Name>ACPT_RCVQ
Queue.2.DisplayName= CSC<HCSCServer_Name>ACPT_DBQ
Queue.2.QueueName= CSC<HCSCServer_Name>ACPT_DBQ
```

Copy the above sample queue definition file to a location of your choice, open the file with a text editor, change the <HCSCServer_Name> part in the file as shown below, and then save the file:

- For an HCSC server that is not a cluster, or for HCSC servers that make up a load-balancing cluster:
  <HCSCServer_Name>: HCSC server name
- For HCSC servers that make up an HA cluster:
  <HCSCServer_Name>: Cluster name

(b) Setting the Reliable Messaging configuration property

In addition to the properties shown in *3.1.2(9) Setting up Reliable Messaging*, set the property shown in the following table.

Property name	Explanation	Value to be set
QueueConfigFileName	Location of the queue definition file	Specify the path of the created queue definition file.

H. Performing Repository Migration from an Old Version in the Operating Environment

This appendix describes how to migrate the repository (in accordance with an update to 09-51) in only the operating environment without using the development environment.

For details about how to migrate the repository by using the development environment, see *Appendix G. Migration from an Old Version*. If you choose to convert the existing repository information before or after a version update in the development environment, and to use the converted repository information with the new version, see *Appendix A. Migrating from old version* in the *uCosminexus BPM/ESB Service Platform Basic Development Guide*.

H.1 Versions supporting repository migration

If you update the version of the product from version 08-00 or later to 09-51, you can migrate the repository in the operating environment only. The following table lists the product versions and the corresponding repository versions.

Table H–1: Product versions and corresponding repository versions

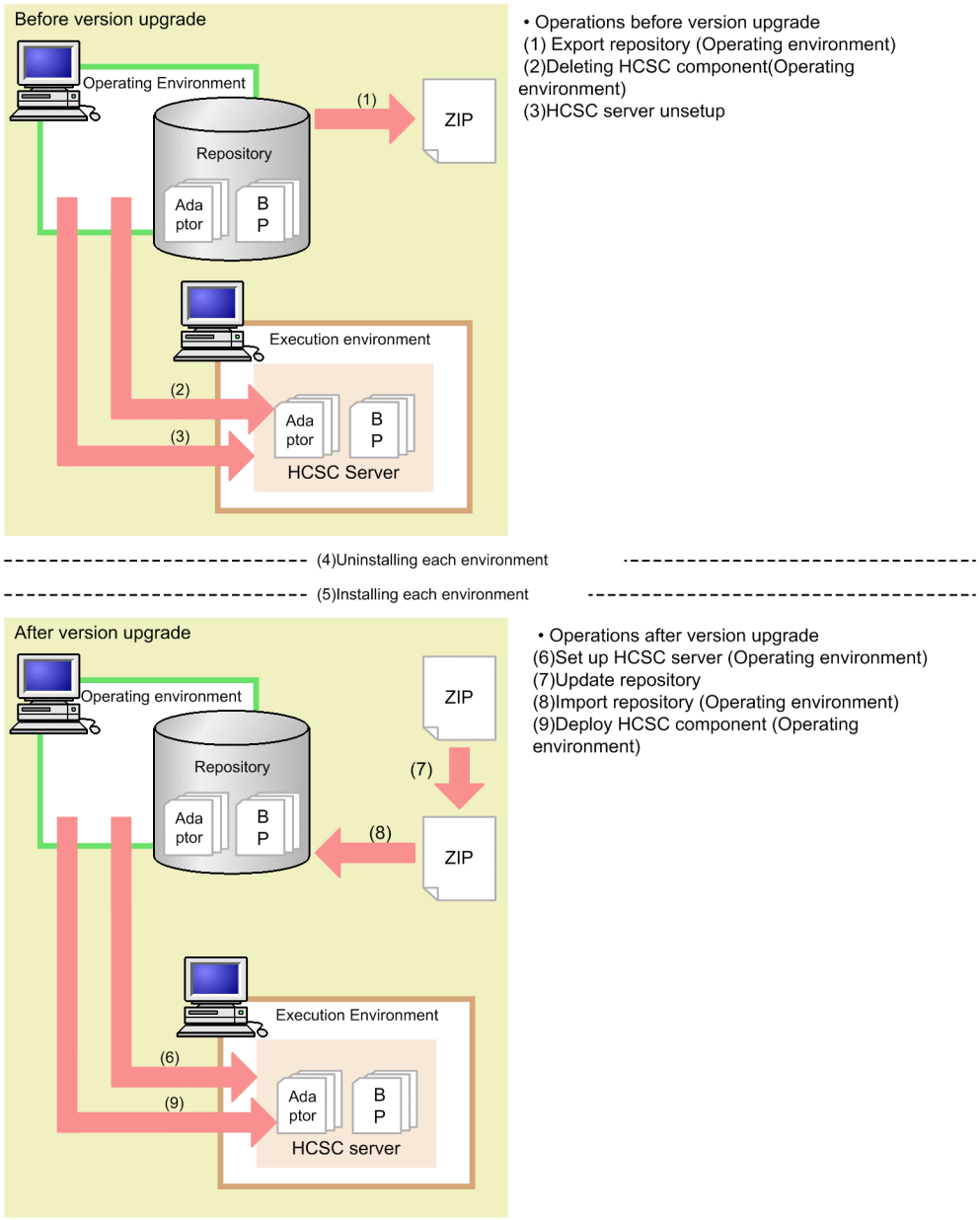
Product version	Repository version
08-00	1.1
08-10	1.2
08-50	1.3
08-51	1.4
08-53	1.5
08-70	1.6
09-00	1.7
09-50	1.8
09-51	1.9

If you want to update the product from a version earlier than 08-00 to 09-51, you can migrate the repository by using the development environment. For details about how to migrate the repository by using the development environment, see *Appendix G. Migration from an Old Version*.

H.2 Repository migration procedure in the operating environment during a new installation

Update Service Platform from the old version to the new version (09-51), following the steps in the figure below (*(1) Export the repository (operating environment)* to *(9) Deploy HCSC components (operating environment)*).

Figure H–1: Migration procedure for a new installation (in the operating environment only)



The steps in Figure H-1 (*(1) Export the repository (operating environment)* to *(9) Deploy HCSC components (operating environment)*) are described below.

For details about the commands used in these steps, see *Chapter 5. Commands (Operating and Execution Environments)* in the *uCosminexus Service Platform Reference Guide*.

(1) Export the repository (operating environment)

Before you update the version, in the operating environment, export the repository as a backup. If there are multiple repositories, export all necessary repositories as backups.

In the operating environment, execute the `cscrepctl` command (with the `-export` option) to export the repository (or repositories).

For details about how to export a repository, see *4.2 Exporting Repository Information*.

(2) Delete HCSC components (operating environment)

Delete all HCSC components deployed on the HCSC server in the execution environment. If there are multiple HCSC servers in the execution environment to be updated, delete all HCSC components from all of those HCSC servers.

In the operating environment, execute the `csccompoundeploy` command, as shown below. This command deletes all HCSC components deployed on the specified HCSC server.

```
csccompoundeploy -csc HCSC-server-name -type {adapter|bp} -name service-adapter's-service-ID
```

(3) Perform unsetup of the HCSC servers

Before you update the version, in the execution environment, perform unsetup of all HCSC servers.

In the operating environment, execute the `cscsvunsetup` command to perform unsetup of all HCSC servers. For a test environment in which Service Platform was set up by using HCSC Easy Setup, use HCSC Easy Setup to perform unsetup.

For details about how to perform unsetup of HCSC servers, see *3.3.5 Unsetting up an HCSC server*.

(4) Uninstall Service Platform in each environment

Uninstall the old version of Service Platform in the operating and execution environments. We recommend that you back up the Service Platform installation directory before uninstalling Service Platform.

Notes

When you perform uninstallation, note the following:

- Before you start uninstallation, terminate all components, such as the J2EE server, Management Server, and PRF, in the execution environment.
- If an embedded database is used, terminate it before you start uninstallation.

Notes applying to an update from a version earlier than 09-00

The products listed below come with Service Platform 09-00 or later. If any of the products listed below have already been installed, we recommend that you uninstall them.

- Service Adapter for Flat Files
- Service Adapter Architect for Flat Files
- Service Adapter for FTP
- Service Adapter Architect for FTP
- Service Adapter for Message Queue
- Service Adapter Architect for Message Queue
- Service Adapter for Object Access
- Service Adapter Architect for Object Access
- Service Adapter for TP1
- Service Adapter Architect for TP1
- Code Conversion - Development Kit
- Code Conversion - Server Runtime
- Code Conversion - Runtime
- TP1/Client/J

(5) Install Service Platform in each environment

Install Service Platform 09-51 to update the version in the operating and execution environments.

(6) Set up an HCSC server (operating environment)

Set up and define the same environment as the previously created HCSC server, based on the following files that were created previously:

- HCSC server configuration definition file
- HCSC server setup definition file
- HCSC server runtime definition file
- User-defined reception runtime definition file

In a test environment, use HCSC Easy Setup to set up an HCSC server.

(7) Update the repository

To continue to use business processes and service adapters that were created in the old version, use the `cscrepupdate` command to update the repository created in the old version.

```
cscrepupdate -inputfile old-repository-ZIP-file-name -outputfile new-repository-ZIP-file-
name
```

(8) Import the repository (operating environment)

Import the repository that was updated in *(7) Update the repository*. Note that you cannot import the repository that was used in the old version.

Execute the `cscrepctl` command (with the `-import` option) in the operating environment.

For details about how to import the repository, see *4.3 Importing a repository*.

(9) Deploy HCSC components (operating environment)

After you have imported the repository information in *(8) Import the repository (operating environment)*, deploy the HCSC components included in the repository information on the HCSC server. Make sure that the resulting environment is the same as the environment existing when the repository was exported in *(1) Export the repository (operating environment)*.

Execute the `csccompodeploy` command (with the `-all` option) in the operating environment.

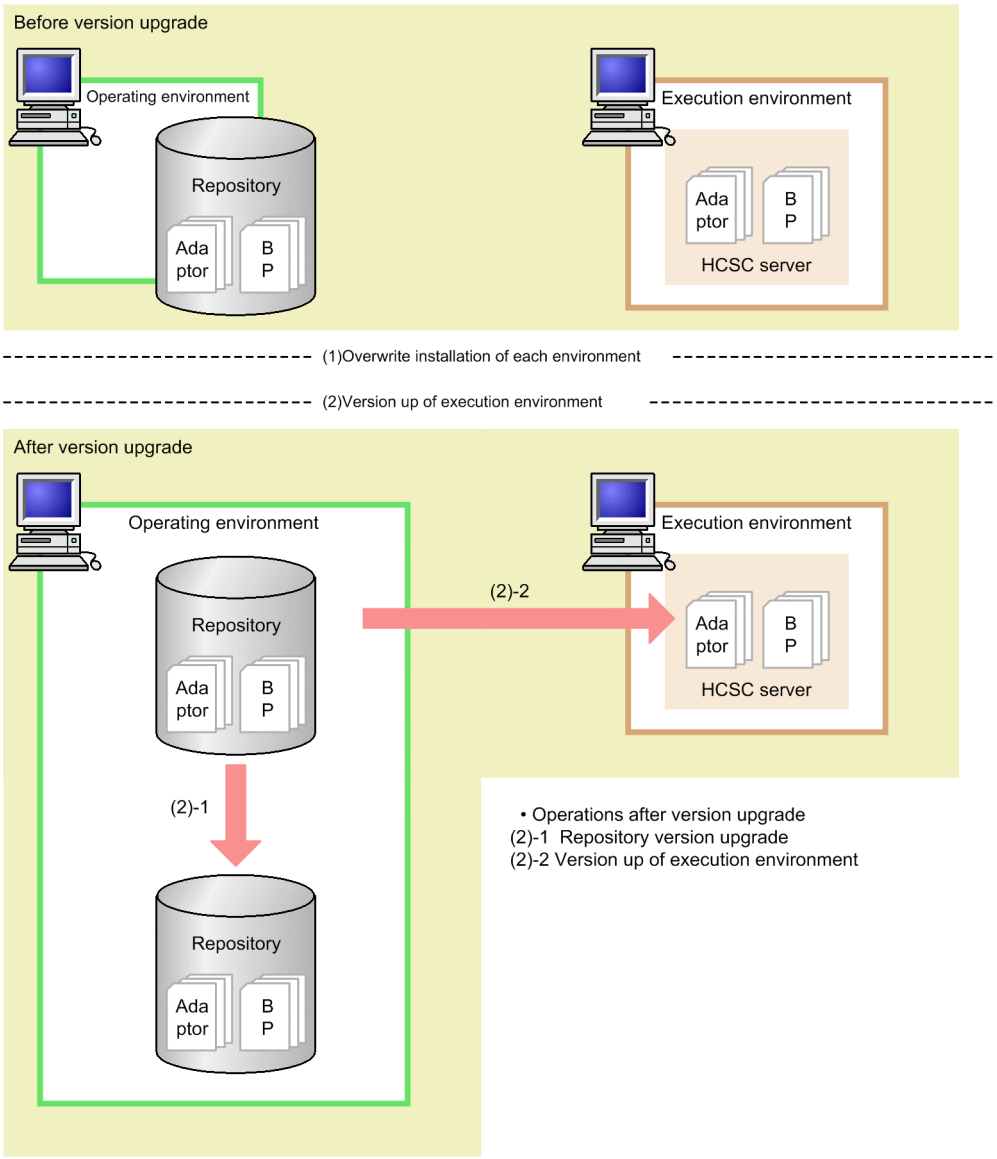
For details about how to deploy HCSC components, see *3.1.8 Deploying a service adapter* and *3.1.13 Deploying a business process*.

After you have deployed the HCSC components, you can perform operations on them as you could before the version was updated.

H.3 Repository migration procedure in the operating environment during update installation

Update Service Platform from the old version to the new version (09-51), following the steps in the below figure (*(1) Perform update installation in each environment* to *(6) Update the version of the execution environment (operating environment)*.

Figure H–2: Migration procedure for an update installation (in the operating environment only)



The steps in Figure H-2 (*(1) Perform update installation in each environment* to *(6) Update the version of the execution environment (operating environment)*) are described below.

For details about the commands used in these steps, see *Chapter 5. Commands (Operating and Execution Environments)* in the *uCosminexus Service Platform Reference Guide*.

(1) Perform update installation in each environment

Update the version of Service Platform by installing Service Platform 09-51 as an update installation in the operating and execution environments. For a test environment in which Service Platform was set up by using HCSC Easy Setup, use HCSC Easy Setup to perform unsetup before you perform update installation, and perform setup again after update installation.

The following shows the prerequisites for update installation in each environment.

Prerequisites:

- The HCSC server has been set up.
- Service Platform and Reliable Messaging are not running.
- The embedded database (if used) is not running.

- The HCSC server, J2EE server, and HCSC components are not running.

Notes

When you perform update installation, note the following:

- Before you start update installation, terminate all components, such as the J2EE server, Management Server, and PRF, in the execution environment.
- If an embedded database is used, terminate it before you start update installation.

Note that update installation overwrites all files other than the files listed below:

- *Service-Platform-installation-directory*\CSC\config\manager\csccmd.properties
- *Service-Platform-installation-directory*\CSC\config\manager\cscmng.properties
- *Service-Platform-installation-directory*\CSC\config\msg\cmdconf.bat
- *Service-Platform-installation-directory*\CSC\inbound-adapter\ftp\config\command\log4j.xml
- *Service-Platform-installation-directory*\CSC\inbound-adapter\ftp\config\FTP_Inbound_Resource_Adapter\serverstatus.properties
- *Service-Platform-installation-directory*\CSC\inbound-adapter\ftp\config\FTP_Inbound_Resource_Adapter\users.properties
- *Service-Platform-installation-directory*\CSC\system\manager\setup\input.properties

(2) Change the class path of the J2EE server

If the version to be updated is earlier than 09-00 and the option definition file for the J2EE server (usrconf.cfg) contains the entries listed below, delete all of them. When you change the definition, we recommend that you use Smart Composer functionality or management portal.

- add.class.path=*TP1-adapter-installation-directory*\lib\adptp1rt.jar
- add.class.path=*file-adapter-installation-directory*\lib\adpffrt.jar
- add.class.path=*Object-Access-adapter-installation-directory*\lib\adpoart.jar
- add.class.path=*Object-Access-adapter-installation-directory*\usrlib\adpoaow.jar
- add.class.path=*Message-Queue-adapter-installation-directory*\lib\adpmqrt.jar
- add.class.path=*FTP-adapter-installation-directory*\lib\adpftprt.jar
- add.class.path=*FTP-adapter-installation-directory*\lib\ftp_common.jar
- add.class.path=*code-conversion-library-installation-directory*\java\codeconv.jar
- add.class.path=*TP1/Client/J-installation-directory*\LIB\TP1Client.jar

(3) Perform migration of old option adapter definition files

Migration of the option adapters that were used in a version earlier than 09-00 requires the tasks described below.

(a) Migration of the TP1 adapter definition files

Copy the TP1 adapter execution-environment property files. The files to be copied and the copy destination directory are as follows:

Files to be copied: *TP1-adapter-installation-directory*\config*.properties

Copy destination: *Service-Platform-installation-directory*\CSC\custom-adapter\TP1\config\

(b) Migration of the file adapter definition files

Copy the file adapter execution-environment property files. The files to be copied and the copy destination directory are as follows:

Files to be copied: *file-adapter-installation-directory*\config*.properties

Copy destination: *Service-Platform-installation-directory*\CSC\custom-adapter\File\config\

(c) Migration of the Object Access adapter definition files

Copy the Object Access adapter execution-environment property files. The files to be copied and the copy destination directory are as follows:

Files to be copied: *Object-Access-adapter-installation-directory*`\config\*.properties`

Copy destination: *Service-Platform-installation-directory*`\CSC\custom-adapter\OA\config\`

(d) Migration of the Message Queue adapter definition files

Copy the Message Queue adapter execution-environment property files. The files to be copied and the copy destination directory are as follows:

Files to be copied: *Message-Queue-adapter-installation-directory*`\config\*.properties`

Copy destination: *Service-Platform-installation-directory*`\CSC\custom-adapter\MQ\config\`

(e) Migration of the FTP adapter definition files

Copy the FTP adapter command definition files and FTP adapter execution-environment property files. The files to be copied and the copy destination directory are as follows:

Files to be copied: *FTP-adapter-installation-directory*`\config\*.properties`

Copy destination: *Service-Platform-installation-directory*`\CSC\custom-adapter\FTP\config\`

(4) Uninstall products

The products listed below come with Service Platform 09-00 or later. If you update Service Platform from a version earlier than 09-00 and any of these products have already been installed, we recommend that you uninstall them.

- Service Adapter for Flat Files
- Service Adapter Architect for Flat Files
- Service Adapter for FTP
- Service Adapter Architect for FTP
- Service Adapter for Message Queue
- Service Adapter Architect for Message Queue
- Service Adapter for Object Access
- Service Adapter Architect for Object Access
- Service Adapter for TP1
- Service Adapter Architect for TP1
- Code Conversion - Development Kit
- Code Conversion - Server Runtime
- Code Conversion - Runtime
- TP1/Client/J

(5) Update Service Platform and Reliable Messaging (execution environment)

Update Service Platform and Reliable Messaging by using the following procedure, which is also required when the version to be updated is earlier than 09-00:

- Execute the update command (`mngenvupdate`).
- Add properties to `mserver.properties` (Management Server environment configuration file).

  The properties to be added are shown below. If you start Management Server without adding these properties, commands whose names begin with `csc` might fail. For details about how to add properties, see *2.1.6(1) Setting mserver.properties (Management Server environment settings file)*.

  ```
  ejbserver.naming.port
  ejbserver.server.edition.settingforce
  ```

(6) Update the version of the execution environment (operating environment)

Update the version of the execution environment from the operating environment.

(a) Prerequisites

The execution environment can be updated when all of the following conditions are satisfied:

- Management Server is running.
- The embedded database (if used) is running.
- The version of the repository is equal to or older than the version of the installation.
- The version of the repository is 08-00 or later (but older than that of the installation).
- (If the FTP inbound adapter is to be used) The resource adapter has already been updated by using the `cjrarupdate` command#.

  #

  For the `cjrarupdate` command, specify the following options and values:

  `-type` option: `rar`

  `-f` option: *Service-Platform-installation-directory*`\CSC\inbound-adapter\ftp\rar\ftp_inbound_adapter.rar`

  For details about the `cjrarupdate` command, see *cjrarupdate (update resource adapter version)* in the *uCosminexus Application Server Command Reference Guide*.

  Note that if you update the FTP inbound adapter from a version earlier than 09-50, the default terminator used for FTP response changes from the OS-dependent line break code to CR-LF. If you do not want to change the terminator, use the `cjgetrarprop` command to obtain the attribute file from the FTP inbound adapter's RAR files, change the definition, and then use the `cjsetrarprop` command to set the attribute file. For details about how to set the attribute file, see *3.2.3(3) Setting up the FTP inbound adapter*.

If the prerequisites listed above are not satisfied, satisfy them in the order in which they are listed.

(b) How to update the version

Execute the `cscenvupdate` command to update the version of the repository and HCSC server.

```
cscenvupdate -csc name-of-the-HCSC-server-to-be-updated
```

If you choose to convert the existing repository information before or after version update in the development environment, and to use the converted repository information with the new version, see *Appendix A. Migrating from old version* in the *uCosminexus BPM/ESB Service Platform Basic Development Guide*.

! Important note

If you stop the HCSC server and update the version of the execution environment while HCSC components are running, the HCSC components will stop when you restart the HCSC server. Therefore, after you restart the HCSC server, you must also restart the HCSC components.

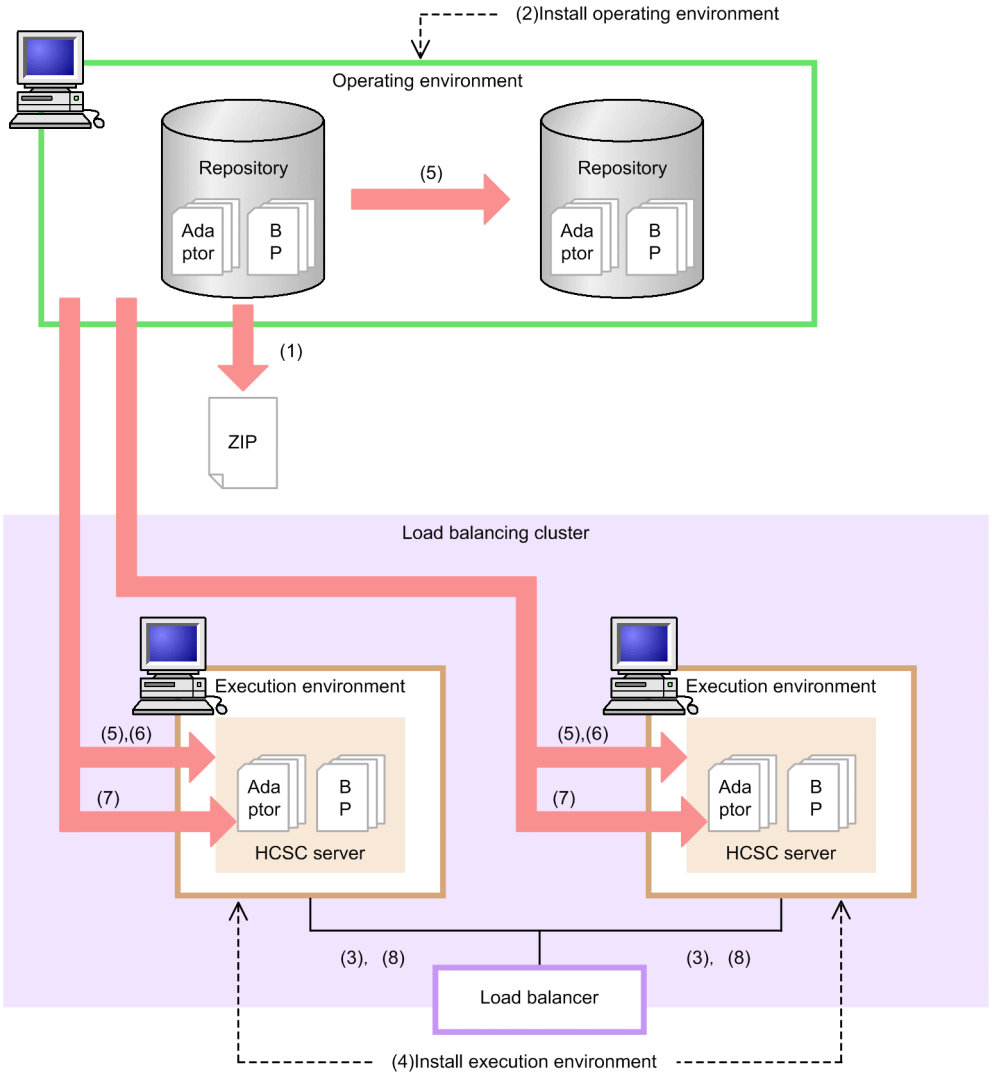
H.4 Repository migration procedure in the operating environment during rolling update

Rolling update is an update installation that is performed without fully stopping the system.

Rolling update requires two or more HCSC servers that make up a load-balancing cluster.

Update Service Platform from the old version to the new version (09-51), following the steps in the below figure (*(1) Export the repository (operating environment)* to *(13) Respecify the request transmission control (load balancer) settings*).

Figure H–3: Migration procedure for a rolling update (in the operating environment only)



• Operation before version upgrade
(1)Export repository (operating environment)

•Version upgrade of operating environment
(2) Install operating environment

•Version upgrade of execution environment
(3) Control sending of requests (Load balancer)
(4) Install execution environment
(5) Version up of execution environment (Operating environment)
(6) Start HCSC server (Operating environment)
(7)Start HCSC component (Operating environment)
(8) Cancelling the control on sending requests

The steps in Figure H-3 (*(1) Export the repository (operating environment)* to *(13) Respecify the request transmission control (load balancer) settings* are described below. The tasks to be performed for the second and following HCSC servers (in the execution environment) are also described below.

For details about the commands used in these steps, see *Chapter 5. Commands (Operating and Execution Environments)* in the *uCosminexus Service Platform Reference Guide*.

! Important note

You cannot perform the following operations in the old system until rolling update finishes:

- Use the `cscsvsetup` command to set up a new HCSC server.

- Use the `csccompodeploy` command to deploy a new HCSC component.

---

(1) Export the repository (operating environment)

Before you update the version, in the operating environment, export the repository as a backup. If there are multiple repositories, export all necessary repositories as backups.

In the operating environment, execute the `cscrepctl` command (with the `-export` option) to export the repository (or repositories).

For details about how to export a repository, see *4.2 Exporting Repository Information*.

(2) Install Service Platform in the operating environment

In the operating environment, install Service Platform 09-51 to update the version. You can install Service Platform as a new installation or an update installation.

To install Service Platform as a new installation:

Perform *(2) Delete HCSC components (operating environment)* to *(5) Install Service Platform in each environment* in *H.2 Repository migration procedure in the operating environment during a new installation*.

To install Service Platform as an update installation:

Perform *(1) Perform update installation in each environment* in *H.3 Repository migration procedure in the operating environment during update installation*.

Note

If the J2EE server, Management Server, PRF, and other components that make up the Service Platform execution environment are running in the environment in which you update-install Service Platform, stop all of them, and then start update installation.

The prerequisites for installation are as follows.

Prerequisites:

- HCSC servers have been set up.
- Service Platform and Reliable Messaging are not running.
- The embedded database (if used) is not running.
- The HCSC server, J2EE server, and HCSC components are not running.

(3) Uninstall products (operating environment)

The products listed below come with Service Platform 09-00 or later. If you update Service Platform from a version earlier than 09-00 and any of these products have already been installed, we recommend that you uninstall them.

- Service Adapter for Flat Files
- Service Adapter Architect for Flat Files
- Service Adapter for FTP
- Service Adapter Architect for FTP
- Service Adapter for Message Queue
- Service Adapter Architect for Message Queue
- Service Adapter for Object Access
- Service Adapter Architect for Object Access
- Service Adapter for TP1
- Service Adapter Architect for TP1
- Code Conversion - Development Kit
- Code Conversion - Server Runtime
- Code Conversion - Runtime

- TP1/Client/J

(4) Specify the request transmission control (load balancer) settings

Specify the load balancer settings so that requests are not sent to the HCSC server being updated. Before doing this, make sure that there no requests are being sent. How to specify the load balancer settings differs depending on the specifications of the load balancer you are using.

(5) Install Service Platform in the execution environment (execution environment)

In the execution environment, install Service Platform 09-51 to update the version.

You can install Service Platform as a new installation or an update installation in the execution environment.

To install Service Platform as a new installation:

Perform *(2) Delete HCSC components (operating environment)* to *(6) Set up an HCSC server (operating environment)* in *H.2 Repository migration procedure in the operating environment during a new installation*.

To install Service Platform as an update installation:

Perform *(1) Perform update installation in each environment* in *H.3 Repository migration procedure in the operating environment during update installation*.

(6) Change the class path of the J2EE server (execution environment)

If the version to be updated is earlier than 09-00 and the option definition file for the J2EE server (`usrconf.cfg`) contains the entries listed below, delete all of them. When you change the definition, we recommend that you use Smart Composer functionality or management portal.

- `add.class.path=`*TP1-adapter-installation-directory*`\lib\adptp1rt.jar`
- `add.class.path=`*file-adapter-installation-directory*`\lib\adpffrt.jar`
- `add.class.path=`*Object-Access-adapter-installation-directory*`\lib\adpoart.jar`
- `add.class.path=`*Object-Access-adapter-installation-directory*`\usrlib\adpoaow.jar`
- `add.class.path=`*Message-Queue-adapter-installation-directory*`\lib\adpmqrt.jar`
- `add.class.path=`*FTP-adapter-installation-directory*`\lib\adpftprt.jar`
- `add.class.path=`*FTP-adapter-installation-directory*`\lib\ftp_common.jar`
- `add.class.path=`*code-conversion-library-installation-directory*`\java\codeconv.jar`
- `add.class.path=`*TP1/Client/J-installation-directory*`\LIB\TP1Client.jar`

(7) Perform migration of old option adapter definition files (execution environment)

Migration of the option adapters that were used in a version earlier than 09-00 requires the tasks described below.

(a) Migration of the TP1 adapter definition files

Copy the TP1 adapter execution-environment property files. The files to be copied and the copy destination directory are as follows:

Files to be copied: *TP1-adapter-installation-directory*`\config\*.properties`

Copy destination: *Service-Platform-installation-directory*`\CSC\custom-adapter\TP1\config\`

(b) Migration of the file adapter definition files

Copy the file adapter execution-environment property files. The files to be copied and the copy destination directory are as follows:

Files to be copied: *file-adapter-installation-directory*`\config\*.properties`

Copy destination: *Service-Platform-installation-directory*`\CSC\custom-adapter\File\config\`

(c) Migration of the Object Access adapter definition files

Copy the Object Access adapter execution-environment property files. The files to be copied and the copy destination directory are as follows:

Files to be copied: *Object-Access-adapter-installation-directory*`\config\*.properties`

Copy destination: *Service-Platform-installation-directory*`\CSC\custom-adapter\OA\config\`

(d) Migration of the Message Queue adapter definition files

Copy the Message Queue adapter execution-environment property files. The files to be copied and the copy destination directory are as follows:

Files to be copied: *Message-Queue-adapter-installation-directory*`\config\*.properties`

Copy destination: *Service-Platform-installation-directory*`\CSC\custom-adapter\MQ\config\`

(e) Migration of the FTP adapter definition files

Copy the FTP adapter command definition files and FTP adapter execution-environment property files. The files to be copied and the copy destination directory are as follows:

Files to be copied: *FTP-adapter-installation-directory*`\config\*.properties`

Copy destination: *Service-Platform-installation-directory*`\CSC\custom-adapter\FTP\config\`

(8) Uninstall products (execution environment)

The products listed below come with Service Platform 09-00 or later. If you update Service Platform from a version earlier than 09-00 and any of these products have already been installed, we recommend that you uninstall them.

- Service Adapter for Flat Files
- Service Adapter Architect for Flat Files
- Service Adapter for FTP
- Service Adapter Architect for FTP
- Service Adapter for Message Queue
- Service Adapter Architect for Message Queue
- Service Adapter for Object Access
- Service Adapter Architect for Object Access
- Service Adapter for TP1
- Service Adapter Architect for TP1
- Code Conversion - Development Kit
- Code Conversion - Server Runtime
- Code Conversion - Runtime
- TP1/Client/J

(9) Update Service Platform and Reliable Messaging (execution environment)

Update Service Platform and Reliable Messaging by using the following procedure, which is also required when the version to be updated is earlier than 09-00:

- Execute the update command (`mngenvupdate`).
- Add properties to `mserver.properties` (Management Server environment configuration file).

  The properties to be added are shown below. If you start Management Server without adding these properties, commands whose names begin with `csc` might fail. For details about how to add properties, see *2.1.6(1) Setting mserver.properties (Management Server environment settings file)*.

  ```
  ejbserver.naming.port
  ejbserver.server.edition.settingforce
  ```

(10) Update the execution environment (operating environment)

Update the version of the execution environment from the operating environment.

(a) Prerequisites

The execution environment can be updated when all of the following conditions are satisfied:

- Management Server is running.
- The embedded database (if used) is running.
- The version of the repository is equal to or older than the version of the installation.
- The version of the repository is 08-00 or later (but older than that of the installation).

If the prerequisites listed above are not satisfied, satisfy them in the order in which they are listed.

(b) How to update the version

Execute the `cscenvupdate` command to update the version of the repository and HCSC server.

```
cscenvupdate -csc name-of-the-HCSC-server-to-be-updated
```

(11) Start the HCSC server (operating environment)

Start the updated HCSC server.

(12) Start the HCSC components (operating environment)

Start the HCSC components that are deployed on the HCSC server whose version was updated in *(10) Update the execution environment (operating environment)*.

(13) Respecify the request transmission control (load balancer) settings

Respecify the load balancer settings so that requests are sent to the updated HCSC server. How to specify the load balancer settings differs depending on the specifications of the load balancer you are using.

(14) Perform tasks on the HCSC servers other than the first HCSC server (execution environment)

On all HCSC servers that make up the load-balancing cluster, perform *(4) Specify the request transmission control (load balancer) settings* to *(13) Respecify the request transmission control (load balancer) settings*.

If you choose to convert the existing repository information before or after version update in the development environment, and to use the converted repository information with the new version, see *Appendix A. Migrating from old version* in the *uCosminexus BPM/ESB Service Platform Basic Development Guide*.

(15) Notes on rolling update

The notes that apply to rolling update are the same as the notes that apply to update of the development environment, operating environment, and execution environment. For notes on rolling update, see *G.4(15) Notes on rolling update*.

H.5 Setup after update

After the update, perform the same setup as the one performed after update of the development environment, operating environment, and execution environment. For the points to be noted after the version is updated, see *G.5 Setup after an update (in the case of an update from a version earlier than 07-50)*.

I. Glossary

For the terminology used in manual,

See "Application Server and BPM/ESB Platform Terminology Guide".

Index

Numerics

A

B

C

D

E

F

H

I

J

L

M

N

O

P

R

S

T

U

V

W

X