


FUJITSU Software

Systemwalker

Service Catalog Manager

A decorative horizontal band with a red-to-dark-red gradient, featuring abstract, glowing white and red lines that swirl and intersect, creating a sense of motion and technology.

ServerView

Resource Orchestrator

Integration Guide

Windows/Linux

B1WS-1164-02ENZ0(00)
July 2014

Preface

Purpose of This Document

This document explains the introduction procedure of ServerView Resource Orchestrator (ROR) integration feature of Systemwalker Service Catalog Manager V15.3.1.

The purpose of this manual is as follows:

- To learn to be able to introduce ServerView Resource Orchestrator integration feature of Systemwalker Service Catalog Manager

Intended Readers

This document is intended for people who introduce ServerView Resource Orchestrator integration feature of Systemwalker Service Catalog Manager.

This document assumes that readers already have the following knowledge:

- Basic knowledge of the operating system being used.

Structure of This Document

This document is structured as follows:

[Chapter 1 Abstract](#)

Explains abstract.

[Chapter 2 Usage Scenarios](#)

Explains usage scenarios

[Chapter 3 Setup](#)

Explains Setup.

[Chapter 4 Importing Certification](#)

Explains importing the certification.

[Chapter 5 Creating and Publishing Service](#)

Explains creating and publishing service.

[Chapter 6 Unsetup](#)

Explains unsetup.

[Chapter 7 Operation](#)

Explains operation.

[Chapter 8 Modifying Settings](#)

Explains modifying settings.

[Appendix A Configuration Settings for APP and Service Controller](#)

Explains configuration settings for APP and service controller.

[Appendix B Service Parameters for ROR Integration Feature](#)

Explains service parameters for ROR integration feature.

[Appendix C Command for Creating Technical Service Definition](#)

Explains command for creating technical service definition.

[Appendix D Example to Register the Service Controller](#)

Explains example to register the service controller.

Appendix E Note on ROR to be Integrated

Explains note on ROR to be integrated.

Appendix F Setup in AML_SP Authenticate mode

Explains setup in SAML_SP Authentication mode.

Conventions Used in This Document

The following names and symbols are used for explanation in the manuals.

- Product name

The manuals refer to Systemwalker Service Catalog Manager V15 as "Systemwalker Service Catalog Manager", omitting "V15".

- Manual name

- The manual sometimes refers to themselves as "this document".
- The titles of the manuals for this product are sometimes abbreviated to "Installation Guide" or "Operator's Guide" for example, omitting "Systemwalker Service Catalog Manager V15" in front of the manual name.

- Operating system specific information

This document provides the information about server operating systems using this product that is common to both the Windows version and the Linux version. Read only the information that is relevant to the operating system for the server that is being used.

Information that is only relevant to particular operating systems is distinguished from common information by attaching the following symbols:

- Headline[Windows]

The entire description of the title and sub-header is a topic specific to the Windows edition.

- Headline[Linux]

The entire description of the title and sub-header is a topic specific to the Linux edition.

If the description differs between the Windows and Linux editions, each description is distinguished by adding words "For Windows system, ..." and "For Linux system, ..." and explained separately.

- Symbols

- [] symbols

Window names, menu names and window item names provided by Systemwalker Service Catalog Manager are surrounded by these symbols.

- Symbols used in command

The symbols used with commands are explained below:

Entry example

[PARA= { a b c ... }]

Meaning of each symbol

Symbol	Meaning
[]	Items enclosed in square brackets are optional.
{ }	Select one of the items enclosed in braces ({ }).
—	When all optional items enclosed in square brackets ([]) are omitted, the default value indicated by an underscore (_) is used.
	Select one of the items separated by vertical bars.
...	The item immediately before the ellipsis (...) can be repeatedly specified.

- Symbols used in the manual

The following note types are used in the manuals:

 **Note**

This note type highlights particularly important points.

 **Point**

This note type highlights information that is worth remembering.

 **Information**

This note type indicates additional reference information.

 **See**

This note type indicates references to other sources.

- Notations of Operating Systems

This document abbreviates Operating systems as follows.

Official name	Abbreviation	
Microsoft(R) Windows Server(R) 2008 Standard Microsoft(R) Windows Server(R) 2008 Enterprise	Windows 2008	Windows
Microsoft(R) Windows Server(R) 2012 Standard Microsoft(R) Windows Server(R) 2012 Datacenter	Windows 2012	
Microsoft(R) Windows Server(R) 2012 R2 Standard Microsoft(R) Windows Server(R) 2012 R2 Datacenter	Windows 2012 R2	
Red Hat Enterprise Linux 6 (for Intel64) Red Hat Enterprise Linux 6 (for x86) Red Hat Enterprise Linux 5 (for Intel64) Red Hat Enterprise Linux 5 (for x86)	Linux	

Export Restrictions

Exportation/release of this document may require necessary procedures in accordance with the regulations of your resident country and/or US export control laws.

Trademarks

Systemwalker, ServerView and Interstage are registered trademarks of Fujitsu Limited.

Microsoft, Internet Explorer, Windows, Windows Server are trademarks or registered trademarks of Microsoft Corporation in the United States and other countries.

Linux is a trademark or registered trademark of Mr. Linus Torvalds in the United States and other countries.

Red Hat and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc. in the United States and other countries.

Other company names and product names are trademarks or registered trademarks of respective companies.

The company names, system names, product names and other proprietary names that appear in this document are not always accompanied by trademark symbols (TM or (R))

Issue Date and Version

Edition	Manual code
First edition December 2013	B1WS-1164-01ENZ0(00)
Second edition July 2014	B1WS-1164-02ENZ0(00)

Notice

No part of the content of this manual may be reproduced without the written permission of Fujitsu Limited.
The contents of this manual may be changed without notice.

Copyright

Copyright 2010-2014 FUJITSU LIMITED

Contents

Chapter 1 Abstract.....	1
1.1 ServerView Resource Orchestrator Integration Feature.....	1
1.2 Operating Condition.....	2
Chapter 2 Usage Scenarios.....	3
Chapter 3 Setup.....	4
3.1 Prerequisites and Preparation.....	4
3.1.1 Install and setup CT-MG.....	4
3.1.2 Database.....	4
3.1.3 SMTP Server.....	5
3.1.4 Checking Configuration Settings.....	5
3.2 Setup for ROR Integration.....	6
3.2.1 Setup.....	6
Chapter 4 Importing Certification.....	11
4.1 Importing and Confirming Certification of Main Domain.....	11
4.1.1 Exporting and Importing Certification of Main Domain.....	11
4.1.2 Confirming the Server Information of Certification.....	12
4.2 Importing and Confirming ROR Server Certification.....	12
4.2.1 Export the Server Certification of ROR.....	12
4.2.2 Import the Certification.....	13
4.2.3 Confirming the Server Information of Certification.....	14
Chapter 5 Creating and Publishing Service.....	15
Chapter 6 Unsetup.....	18
6.1 Unsetup the ROR Integration feature.....	18
6.1.1 Tasks before Unsetup.....	18
6.1.2 Unsetup.....	18
Chapter 7 Operation.....	20
7.1 Start/Stop.....	20
7.1.1 Prerequisites.....	20
7.1.2 Start.....	20
7.1.3 Stop.....	20
7.2 Customize Text.....	20
7.2.1 Text List for ROR Integration Feature.....	20
7.3 Manage Subscription.....	21
Chapter 8 Modifying Settings.....	23
8.1 Change Configuration Settings of APP and Service Controller.....	23
8.1.1 Tasks before Changing.....	23
8.1.2 Changing Configuration Settings.....	23
8.2 Modifying Port Number of Database.....	25
8.2.1 Modifying Port Number of Connection Pool.....	25
8.2.2 Stopping ROR Integration Feature.....	26
8.2.3 Modifying Port Number of Database.....	26
8.2.4 Starting ROR Integration Feature.....	26
8.3 Modifying Port Number of APP Domain.....	26
8.3.1 Modifying Admin Port of Java EE Execution Environment.....	27
8.3.2 Modifying HTTP Listener Port Number.....	27
8.3.3 Modifying HTTP SSL Listener Port Number.....	28
8.3.4 Modifying IIOP Listener Port Number.....	28
8.3.5 Modifying IIOP Listener Port Number for SSL Communication.....	28
8.3.6 Modifying IIOP Listener Port Number for Client Authentication of SSL Communication.....	28

8.3.7 Modifying RMI registry connection port number used by JMX connector.....	29
8.3.8 Modifying Port Number for JMS Host and RMI Registry for Message Queue broker.....	29
8.4 Modifying SMTP Server Settings.....	29
8.4.1 Modifying SMTP Server.....	30
8.4.2 Modifying Mail Address.....	30
8.4.3 Modifying SMTP Authentication.....	30
8.4.4 Modifying SMTP User.....	30
8.4.5 Modifying SMTP Password.....	31
8.4.6 Modifying SMTP Server Port.....	31
8.5 Changing Administrator's Password of Java EE Execution Environment.....	31
8.6 Options of Admin Command.....	32
8.7 Admin Port Number of Java EE Execution Environment.....	32
Appendix A Configuration Settings for APP and Service Controller.....	33
A.1 Configuration Settings of APP.....	33
A.2 Configuration Settings of Service Controller.....	34
Appendix B Service Parameters for ROR Integration Feature.....	36
B.1 All Scenarios.....	36
B.2 L-Platform Provisioning and Scaling.....	37
B.3 Virtual server Provisioning.....	38
Appendix C Command for Creating Technical Service Definition.....	39
Appendix D Example to Register the Service Controller.....	41
D.1 Prerequisites.....	41
D.2 Registering technology Manager.....	41
D.3 Setup Example [Windows].....	41
D.3.1 Configuring setting files.....	42
D.3.2 Executing setting commands.....	42
D.3.3 Importing ROR Server Certification.....	43
D.4 Setup Example [Linux].....	43
D.4.1 Configuring setting files.....	43
D.4.2 Executing setting commands.....	43
D.4.3 Importing ROR Server Certification.....	44
Appendix E Note on ROR to be Integrated.....	45
Appendix F Setup in AML_SP Authenticate mode.....	49
F.1 Tasks before Setup.....	49
F.1.1 Changing Setting File.....	49
F.1.2 Executing Setup Command.....	49
F.2 Tasks After Setup.....	49
F.2.1 Changing Configuration Settings.....	49

Chapter 1 Abstract

1.1 ServerView Resource Orchestrator Integration Feature

ServerView Resource Orchestrator (ROR) integration feature provides ROR feature as the services on Systemwalker Service Catalog Manager (CT-MG). The services are based on the typical usage scenarios for ROR. The supported scenarios are followings:

- Provisioning and scaling of L-Platform (logical platforms)
- Adding and reducing of virtual server by reconfiguration
- Changing of CPU number of each virtual server by reconfiguration
- Start and stop for L-Platform
- Assignment of a single virtual server (logical servers) on an existing L-Platform
- Unsubscribing or removing of L-Platform or virtual server

Refer to “[Chapter 2 Usage Scenarios](#)” for the detailed scenarios.

ROR integration feature is executed on Asynchronous Provisioning Platform (APP), which is provided in order to support the applications which require asynchronous provisioning. So, in order to use ROR integration feature, APP is required to install and configure. APP is installed as the domain for APP (app-domain) and application on Java EE execution environment, and APP supports the communication between main CT-MG and service applications, which require asynchronous handling. Refer to “[Chapter 3 Setup](#)” for how to install and configure APP.

The service application of CT-MG running on APP is called as “service controller”. The service controller for ROR integration feature is “RORIntegration”. “RORIntegration” executes the provisioning and scaling for L-Platform and virtual server. Refer to “[Chapter 4 Importing Certification](#)” for how to setup ROR Integration feature.

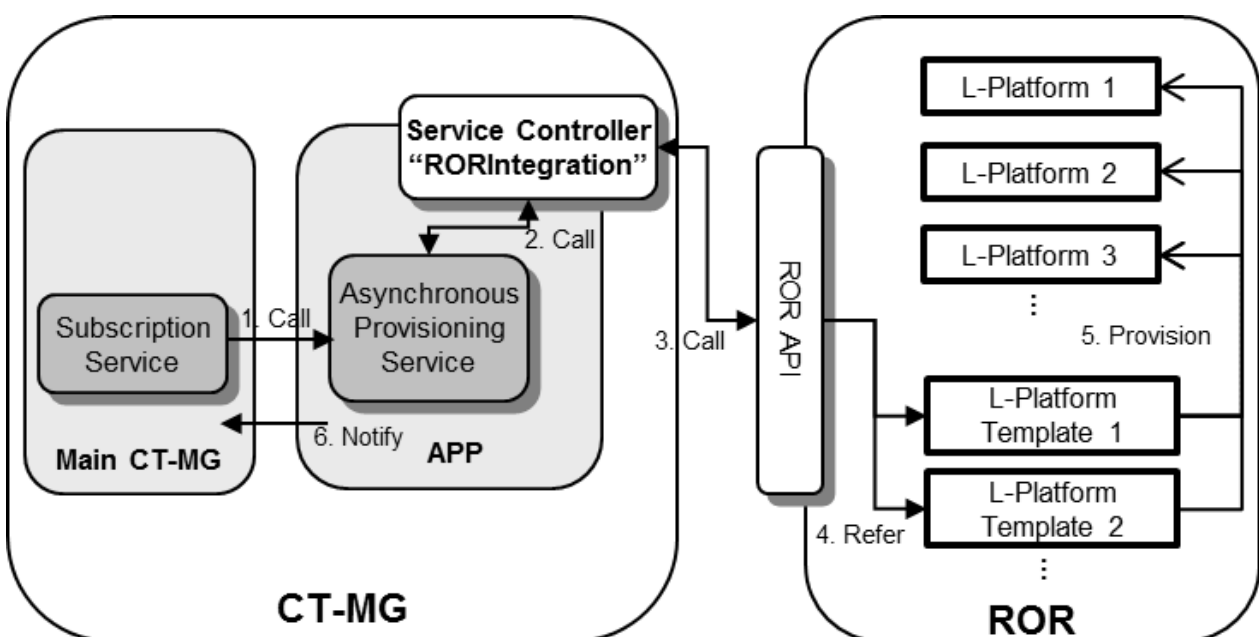
Before setup ROR Integration, the authentication mode of users and Web service must be defined. ROR Integration supports INTERNAL and SAML_SP authentication mode. The default setting is INTERNAL authentication mode.

Define the authentication mode according to that of CT-MG. Ask Operator organization about the authentication mode of CT-MG.

Refer to “[Chapter 3 Setup](#)” in detail how to setup ROR Integration in INTERNAL authentication mode.

Refer to “[Appendix F Setup in AML_SP Authenticate mode](#)” in detail how to setup ROR Integration in SAML_SP authentication mode.

After setup of ROR Integration feature, by creating service working on CT-MG, ROR integration feature is published to customer organizations. Refer to “[Chapter 5 Creating and Publishing Service](#)” for how to create and publish service.



1.2 Operating Condition

ROR integrating with CT-MG must satisfy the one of following conditions:

- ServerView Resource Orchestrator Cloud Edition V3.1.1
- ServerView Resource Orchestrator Cloud Edition V3.1.2

Chapter 2 Usage Scenarios

ROR is the platform software for private clouds, for realizing effective use and streamlining of operation and management. The Infrastructure administrator of ROR modifies and tunes the configuration settings for logical platforms (L-Platform) and logical servers (virtual server) based on the needs from customers. Using L-Platform, Infrastructure administrator can provide, for example, request specific servers and operating systems, firewalls, load balancers, or pre-installed software and databases, based on the requirement from the customers. Virtual servers can be added and removed dynamically as required.

The basic configurations of L-Platform for typical usage scenarios are defined by the ROR Infrastructure administrator in so-called L-Platform templates. For example, L-Platform template may define the resources such as two application virtual servers. Different L-Platform templates can be made available for small, medium, and large scale operation. Customers can provision L-Platform based on a template which is reconfigured according to their needs.

The RORIntegration service controller provides for a basic integration feature of ROR with CT-MG. After the service controller has been deployed and configured in APP and appropriate technical and marketable services have been defined in CT-MG, the following usage scenarios are supported:

- **Provisioning of L-Platform:** This scenario is to create L-Platform for customer organization using L-Platform template created on ROR previously. ROR tenant administrator previously creates the L-Platform template on ROR, and technology provider/supplier organizations create and publish the technical service definition/marketable service in order to create L-Platform based on the L-Platform template created previously. When an administrator of customer organization subscribes to the published service, the L-Platform name can be specified as the parameter of the service. When an administrator of customer organization subscribes to the service, ROR creates the L-Platform based on the L-Platform template through the service controller. If the steps to create the L-Platform are completed successfully, the L-Platform is ready to use for the customer.
- **Adding and reducing of virtual server by reconfiguration:** This scenario is to add/reduce the virtual servers to/from the L-Platform subscribed by the customer. By changing the corresponding parameters in the existing subscription by the administrator of customer organization, ROR adds/reduces the number of virtual servers to/from their L-Platform through the service controller. If all steps to add/reduce the number of virtual servers are completed successfully, the virtual servers are ready to use based on the changed parameters.
- **Changing of CPU number of each virtual server by reconfiguration:** This scenario is to change the number of CPU to the virtual servers in the L-Platform subscribed by the customer. By changing the corresponding parameters in an existing subscription by an administrator of customer organization, ROR changes the number of CPU to each virtual server in their L-Platform through the service controller. If all steps to change the number of CPU are completed successfully, the virtual servers are ready to use based on the changed parameters.
- **Start and stop for L-Platform:** This scenario is to start/stop virtual servers in L-Platform which is subscribed by customer organization. After customer organization subscribes the service based on the provisioning of L-Platform scenario and assigns the user to the subscription, and then the user is ready to start/stop virtual servers in L-Platform through marketplace portal.
- **Assignment of a single virtual server on an existing L-Platform:** This scenario is to add virtual server for customer organization using L-Platform created on ROR previously. ROR tenant administrator previously creates the L-Platform on ROR, and technology provider/supplier organizations create and publish the technical service definition/marketable service in order to add virtual server to the L-Platform created previously. When an administrator of customer organization subscribes to the published service, the virtual server name can be specified as the parameter of the service. When an administrator of customer organization subscribes to the service, ROR adds the virtual server through the service controller. If the steps to add the virtual server are completed successfully, the virtual server is ready to use for the customer.
- **Unsubscribing of L-Platform or removing of virtual server:** This scenario is to unsubscribe L-Platform or remove virtual server subscribed by customer organization. When the customer terminates the subscription for L-Platform or virtual server, ROR unsubscribes the L-Platform or removes the virtual server through the service controller. The subscription is terminated independent on whether this is successful.

If an operation fails on the ROR side, the corresponding subscription in CT-MG remains pending (except when terminating a subscription). The service controller informs its responsible technology provider organization by email of any incomplete provisioning or delete operation in ROR.

In ROR, the virtual platforms and servers created for CT-MG subscriptions are managed in the same way as other L-Platform and virtual servers. They can be viewed and monitored with the standard ROR tools.

Chapter 3 Setup

This chapter explains how to setup ROR Integration.

Note

The procedure described in this chapter requires the administrative privileges to execute. And, the procedure described in this chapter requires the Operator who installs CT-MG.

Information

As for the example procedure described in this chapter and "Chapter 4 Importing Certification", refer to "Appendix D Example to Register the Service Controller".

3.1 Prerequisites and Preparation

This section explains the prerequisites and preparation to setup ROR Integration.

3.1.1 Install and setup CT-MG

ROR integration feature runs on the same server where CT-MG is installed. Confirm following items in advance:

- Completion to install and setup CT-MG for standalone configuration
- Running of CT-MG database. Refer to "Installation Guide" in detail about starting CT-MG database.
- You must have registered a technology provider.
- A fully functional ROR installation must be available.
- In ROR, a tenant must be created for CT-MG technology provider. And, the resource configuration accessible for this tenant, introduction of tenant user and tenant administrator, and creation of L-Platform template must be completed.
- Check the version of ServerView Operations Manager used by ROR. Refer to "Appendix E Note on ROR to be Integrated" in detail.
- Check that the connection is allowed between main domain of CT-MG and APP domain of ROR Integration. It is necessary to set required communication be allowed in the security software and firewall. Refer to "3.2.1 Setup" for the required hostname, IP address and port number. Refer to the security software and OS manuals for the information on how to set required communication be allowed in the security software and firewall.

Refer to "Installation Guide" and "Operator's Guide" for detail.

3.1.2 Database

ROR Integration saves its data to the database. The database is shared which is used by CT-MG itself. So, before introducing ROR Integration, it is required to change the configure settings of the database and to restart the database.

Configure Settings

Modify the following files:

[Windows]

```
%SWCTMG_HOME%\pgctbss\data\postgresql.conf
```

[Linux]

```
/var/opt/FJSVctbss/pgsql/data/postgrsql.conf
```

Modify the parameters according to the following process:

1. **Add** 50 to the existing value (default: 50) of “max_prepared_transactions” property (example: 100).
2. **Add** 210 to the existing value (default: 210) of “max_connections” property (example: 420).

Example:

```
max_prepared_transactions=100
max_prepared_transactions=420
```

These properties are the high limit for the concurrent connection to the database.

Take care for following points: this value is combined and used with the setting value of JDBC pool size. When you changed the JDBC pool size, it is also required to change the value of max_connections. In detail, refer to the “Tuning Performance” section in “Operator’s Guide”.

3. Save the files.

Reboot the database in order to activate the change the setting values. As for rebooting the database, refer to the “Start/Stop” section in “Installation Guide”.



Before rebooting the database, stop Systemwalker Service Catalog Manager Server service and Systemwalker Service Catalog Manager Indexer service. Refer to “9.1 Start/Stop” in “Installation Guide” in detail.

3.1.3 SMTP Server

ROR Integration requires the E-mail function. Prepare the SMTP server where E-mail can be used.

When some problems (such as about registration of subscription and assigning) occur, ROR Integration send requests to the SMTP server preregistered on the same server.

The settings about SMTP server are defined in “app_glassfish.properties” file in “[3.1.4 Checking Configuration Settings](#)”.

3.1.4 Checking Configuration Settings

In case that you have changed the installation environment, configuration settings for ROR Integration must be checked before executing ROR Integration setup command.

Following setting file are registered in the files in the subdirectory "setup" under "app" directory.

- db.properties: the file to register configuration settings for the database setup and access.

As for db.url and db.port, the values are specified based on the values when CT-MG is setup, and they should be modified according to the port number of CT-MG database. In case that you changed the port number of database after CTMG setup, specify the value after changing.

- db.url=jdbc:postgresql://localhost:[the port number of database]/bssapp
- db.port=[the port number of database]

Following three setting files are registered in the files in the subdirectory "files" under "setup" directory.

- app_glassfish.properties: the file to register configuration settings for the domain for APP.

As for MAIL_HOST and MAIL_PORT, the values are specified based on the values when CT-MG is setup, and they should be modified according to the SMTP server information sending mail. In case that you changed the SMTP server information sending mail after CTMG setup, specify the value after changing.

- MAIL_HOST=[hostname of SMTP server]
- MAIL_PORT=[port number of SMTP server]

- app_configsettings.properties: the file to register configuration settings for APP

As for APP_BASE_URL, the values are specified based on the values when CT-MG is setup, and they should be modified according to the host name or IP address of CT-MG server used for access URL to APP portal. In case that you changed the host name or IP address of CT-MG server after CTMG setup, specify the value after changing

- APP_BASE_URL=http://[the host name or IP address of CT-MG server]:%A_HTTP_LISTENER_PORT%/fujitsu-bss-app

After executing setup, this setting is registered to bssapp database.

- app_org_configsettings_controller.properties: the file to register configuration settings for service controller

As for IAAS_API_LOCALE, this should be modified according to the locale used for access to ROR API in case that you changed the locale (“ja” or “en”).

- IAAS_API_LOCALE=[locale used for access to ROR API (“ja” or “en”)]

After executing setup, this setting is registered to bssapp database.

The procedure to change configuration settings is following:

1. create a backup of the files for future reference,.
2. Save the files to the directory where they are registered.
3. Open each of the objective files with an editor.
4. Check the values of items in each file and adapt them to your environment.
- 5.

Note

- If you install everything on the local system, use either the host name or localhost in all configuration files for all URLs that need to be resolved by APP.

Do not mix the specification of host names and localhost. <server> of BSS_WEBSERVICE_URL which is specified in ROR Integration setup command must be same as the information specified in CN of the owner for server certification of bes-domain.

- The host name or IP address of APP_BASE_URL in app_configsettings.properties file is used for name resolution by client. Use the host name available for name resolution or IP address available.

3.2 Setup for ROR Integration

This section explains how to setup ROR Integration.

Note

In case that you specified the password of OS user for database in setup for CT-MG, specify the password as the environmental variable “SWCTMG_DBUSER_PASSWORD”. In case that you did not specify the password, omit specifying environmental variable. Refer to “Installation Guide” for detail of the password of OS user for database.

3.2.1 Setup

This subsection explains the procedure to setup ROR Integration.

Executing setup command

Execute following procedure:

1. Log in as the OS administrator.
Log in as the OS administrator to the server where ROR Integration feature is setup.

2. Open the command prompt (Windows) or a terminal session (Linux).
3. Execute the setup command for ROR Integration.

[Windows]

```
%SWCTMG_HOME%\setup\swctmg_setupRORInteg <AS_APP_ADMIN_USER> <AS_APP_ADMIN_PASSWORD>
<AS_APP_BASE_PORT> <APP_ADMIN_MAIL_ADDRESS> <BSS_WEBSERVICE_HOST_PORT> <BSS_USER_KEY>
<BSS_USER_PWD> <BSS_ORGANIZATION_ID> <IAAS_API_USER> <IAAS_API_PWD> <IAAS_API_TENANT>
<IAAS_API_HOST_PORT>
```

[Linux]

```
/opt/FJsvctbss/setup/swctmg_setupRORInteg.sh <AS_APP_ADMIN_USER> <AS_APP_ADMIN_PASSWORD>
<AS_APP_BASE_PORT> <APP_ADMIN_MAIL_ADDRESS> <BSS_WEBSERVICE_HOST_PORT> <BSS_USER_KEY>
<BSS_USER_PWD> <BSS_ORGANIZATION_ID> <IAAS_API_USER> <IAAS_API_PWD> <IAAS_API_TENANT>
<IAAS_API_HOST_PORT>
```

The strings covered by <> shows the parameter, and all of the following parameters must be specified in order from No.1. Also, an ASCII space character must be put between parameters. Refer to “B.1 Port Number List” in “Installation Guide” for the information on the port numbers used by the domain for APP.

Table 3.1 ROR Integration Setup Parameter List

No.	Parameter name	Mandatory	Explanation
1	AS_APP_ADMIN_USER	Yes	User name of Java EE execution environment. It will be set to the user name for the administrator of Java EE execution environment for APP domain. Example: Administrator
2	AS_APP_ADMIN_PASSWORD	Yes	Password of Java EE execution environment. It will be set to the password for the administrator of Java EE execution environment for APP domain. Example: User1234
3	AS_APP_BASE_PORT	Yes	Base port number for Java EE execution environment (APP domain). Each port of APP domain will be set to the number which each port number is added to this base number. Example: 8800
4	APP_ADMIN_MAIL_ADDRESS	Yes	The email address which is used for sending notifications of information. To this email address, notifications are sent in case that there are some troubles in APP operation. Example: admin@example.com
5	BSS_WEBSERVICE_HOST_PORT	Yes	The hostname and port number for accessing to main domain by APP. The hostname must be same as the as the information specified in CN of the owner for server certification of main domain. As for checking the information, refer to “ 4.1.2 Confirming the Server Information of Certification ”. Specify this parameter according to the form, “<hostname>:<port number>”. Example: SERVER001:8081
6	BSS_USER_KEY	Yes	The user key for technology manager accessing to main domain. Specify the user key which you receive with the confirmation email for your user account. And, use the user key of administrator in the organization which is registered to CT-MG. Example: 10000

No.	Parameter name	Mandatory	Explanation
7	BSS_USER_PWD	Yes	The BSS user password for technology manager accessing to main domain. Specify the password of technology manager of BSS_USER_KEY. Example: admin123
8	BSS_ORGANIZATION_ID	Yes	The ID of the technology provider organization in CT-MG who is to register the technical service for ROR integration feature. Specify the organization ID where the technology manager of BSS_USER_KEY belongs. Example: ca4cbd74
9	IAAS_API_USER	Yes	The user ID in ROR. This is used for access to the tenant in ROR. This ROR user requires Tenant Administrator role. Example: ctmg.ror
10	IAAS_API_PWD	Yes	The password of the user ID in ROR. Specify the password of ROR user specified in IAAS_API_USER. Example: ctmg.ror
11	IAAS_API_TENANT	Yes	The tenant name of ROR. Specify the tenant name to which the user specified in "IAAS_API_USER" belongs. Example: ctmgtenant
12	IAAS_API_HOST_PORT	Yes	The hostname and port number of ROR L-Platform API. Hostname must be same as the information specified in server certification of ROR. As for checking the information, refer to " 4.2.3 Confirming the Server Information of Certification ". Specify this parameter according to the form, "<hostname>:<port number (default: 8014)>". Example: server002:8014

Example:

[Windows]

```
%SWCTMG_HOME%\setup\swctmg_setupRORInteg Administrator User1234 8800 admin@example.com
SERVER001:8081 10000 admin123 ca4cbd74 ctmg.ror ctmg.ror ctmgtenant server002:8014
```

[Linux]

```
/opt/FJSVctbss/setup/swctmg_setupRORInteg.sh Administrator User1234 8800 admin@example.com
SERVER001:8081 10000 admin123 ca4cbd74 ctmg.ror ctmg.ror ctmgtenant server002:8014
```

Note

AS_APP_ADMIN_USER must be specified by alphanumeric letters, underscore(_),hyphen(-) and period(.).

AS_APP_ADMIN_PASSWORD must be specified by alphanumeric letters, underscore(_),hyphen(-) and period(.) and at least 8 characters in length.

AS_APP_BASE_PORT must be specified by numeric letters in the 0 to 65359 range.

BSS_USER_KEY must be specified by alphanumeric letters, and at least over 1000.

BSS_USER_PWD must be specified in at least 6 characters in length.

Port numbers for APP domain will use are following eight numbers: the each port number of APP domain when AS_APP_BASE_PORT is specified to 8800 is described.

8880: HTTP listener (Base port + 80)

8881: HTTP SSL listener (Base port + 81)

8848: JavaEE HTTP listener. This will be used as AS_ADMIN_DOMAIN_PORT in unsetup. (Base port + 48)

8886: JMX connector listener (Base port + 86)

8876: JMS host (Base port + 76)

8976: RMI registry for Message Queue broker (JMS host port + 100)

8837: IIOP listener (Base port + 37)

8838: IIOP SSL listener (Base port + 38)

8839: IIOP listener for client authentication of SSL communication (Base port + 39)

Only in executing the setup command, APP domain will use following two numbers temporarily: following two port numbers are not used after you execute setup command. The each port number of APP domain when AS_APP_BASE_PORT is specified to 8800 is described.

8809 (Base port + 9)

8866 (Base port + 66)



Confirm execution

A message is displayed prompting you to confirm execution of the setup.

To execute enter [y], to abort enter [n], then press the ENTER key.

```
swctmg_setup: INFO: 138: Are you sure you want to start setup Systemwalker Catalog Manager ROR
Integration? (y/n)[n]
```

Start the setup

Following message will be displayed when setup procedure starts.

```
swctmg_setup: INFO: 141: Systemwalker Service Catalog Manager ROR Integration setup start.
```

Confirm the completion

Following message will be displayed when setup procedure completes.

```
swctmg_setup: INFO: 143: Systemwalker Service Catalog Manager ROR Integration setup end.
```



Note

Depending on the environment, it takes around several minutes for setup to complete. Do not terminate the command while it is running to close the command prompt or a terminal session.



Information

When you failed to execute setup command, please handle according to the message displayed on command prompt and shown in the following log files:

[Windows]

- %SWCTMG_HOME%\logs\swctmg_setupRORInteg.log: General setup for ROR Integration
- %SWCTMG_HOME%\logs\build-db-ant_RORInteg.log: Setting up for database
- %SWCTMG_HOME%\logs\build-glassfish-setup-ant_RORInteg.log: Setting up for Java EE execution environment

[Linux]

- /var/opt/FJSVctbss/logs/swctmg_setupRORInteg.log: General setup for ROR Integration

- /var/opt/FJSVctbss/logs/build-db-ant_RORInteg.log: Setting up for database

/var/opt/FJSVctbss/logs/build-glassfish-setup-ant_RORInteg.log: Setting up for Java EE execution environment



Chapter 4 Importing Certification

This chapter explains how to import the certifications.



The procedure described in this chapter requires the administrative privileges to execute.

4.1 Importing and Confirming Certification of Main Domain

APP runs as the application of CT-MG, and calls Web service of main CT-MG. In order to call Web service, it is required to import the certification of main CT-MG to the truststore in app-domain.



This section explains how to import the certification which is registered as default. In case that the certification of main domain is newly registered before ROR Integration setup, contact to Operator organization and import the certification newly registered to the truststore of APP domain.

4.1.1 Exporting and Importing Certification of Main Domain

Import the certification as follows:

1. Open the command prompt (Windows) or a terminal session (Linux).
2. Export the certification from main domain by executing following command:

[Windows]

```
%SWCTMG_HOME%\jdk7\bin\keytool -export -rfc -alias slas -keystore %SWCTMG_HOME%\glassfish3\glassfish\domains\bes-domain\config\keystore.jks -file ctmgbss.crt -storepass changeit
```

[Linux]

```
/opt/FJsvctbss/jdk7/bin/keytool -export -rfc -alias slas -keystore /opt/FJsvctbss/glassfish3/glassfish/domains/bes-domain/config/keystore.jks -file ctmgbss.crt -storepass changeit
```

3. Import the certification to the truststore in app-domain by executing following command:

[Windows]

```
%SWCTMG_HOME%\jdk7\bin\keytool -import -file ctmgbss.crt -trustcacerts -alias ctmgbss -keystore %SWCTMG_HOME%\glassfish3\glassfish\domains\app-domain\config\cacerts.jks -storepass changeit
```

[Linux]

```
/opt/FJsvctbss/jdk7/bin/keytool -import -file ctmgbss.crt -trustcacerts -alias ctmgbss -keystore /opt/FJsvctbss/glassfish3/glassfish/domains/app-domain/config/cacerts.jks -storepass changeit
```

After executing above command, the prompt displayed asking if you trust the certification. Input “y” and import.

4. Check that the certification “ctmgbss” is imported to the truststore in app-domain by executing following command:

[Windows]

```
%SWCTMG_HOME%\jdk7\bin\keytool -list -keystore %SWCTMG_HOME%\glassfish3\glassfish\domains\app-domain\config\cacerts.jks -storepass changeit
```

[Linux]

```
/opt/FJSVctbss/jdk7/bin/keytool -list -keystore /opt/FJSVctbss/glassfish3/glassfish/domains/app-domain/config/cacerts.jks -storepass changeit
```

5. Restarting app-domain is required in order to activate the imported certification. When the app-domain is running, restart app-domain. Refer to “7.1 Start/Stop” in detail how to restart.

Note

- The password of keystore is specified after the option “-storepass”. Change the password of keystore if it is not set as “changeit”.
- The certification file “ctmgbss.crt” is created in the folder where above command is executed. Delete it as necessary.

4.1.2 Confirming the Server Information of Certification

The CN of owner of server certification exported in “4.1.1 Exporting and Importing Certification of Main Domain” can be confirmed by following command:

[Windows]

```
%SWCTMG_HOME%\jdk7\bin\keytool -printcert -file [file name of ROR server certification] -storepass changeit
```

[Linux]

```
/opt/FJSVctbss/jdk7/bin/keytool -printcert -file [file name of ROR server certification] -storepass changeit
```

Following information displays to execute the command, so confirm the value of CN:

```
Owner: CN=WIN-UBVC92LJ386, OU=GlassFish, O=Oracle Corporation, L=Santa Clara, ST=California, C=US
Issuer: CN=WIN-UBVC92LJ386, OU=GlassFish, O=Oracle Corporation, L=Santa Clara, ST=California, C=US
.
.
.
```

4.2 Importing and Confirming ROR Server Certification

1. It is required to import the server certification of ROR to the truststore in app-domain so that the communication between the service controller and ROR is done with SSL. This section explains how to export the server certification of ROR as a file, to import it to the truststore in app-domain and to confirm the server information of ROR server certification.

4.2.1 Export the Server Certification of ROR

This subsection explains how to export the server certification of ROR and to save as a file.

The objective server to export the ROR server certification is the admin server of ROR, not the server where CTMG and ROR integration feature are setup.

Point

The exported certification file is copied and used in the server where ROR Integration feature is setup.

Remove the certification file when it is not needed.

Export with Web browser

This explains how to export the certification with Internet Explore as Web browser. And, Internet Explore must be opened with administrative right.

1. Access to the login page of ROR console with Web browser.

Access to following URL with Web browser:

```
https://<FQDN of admin server>:8014/cfmgapi/endpoint
```

The default port number of ROR API is 8014.

2. Display the certification.

Display the [Certificate] page to choose [View certificate], clicking the security status bar of Web browser, or where “Certificate Error” displays with your mouse

3. Export the certification

Click [Detail] tab on [Certificate] page, and click [Copy to file] button.

Export the certification according to the information in the displayed page.

The type for exporting file does not have to be changed as the default “DER encoded binary X.509”

Export with command

Export the certification using “scsexppfx” command included in ROR.

In order to execute with the command, the password of Interstage certificate environment and the nickname of certification are required.

Refer to “ServerView Resource Orchestrator Cloud Edition Setup Guide” in “ServerView Resource Orchestrator Cloud Edition” in detail. In the explanation of “Importing a Certificate to ServerView SSO Authentication Server, how to export is described.

4.2.2 Import the Certification

This subsection explains how to import the exported server certification of ROR to the truststore in app-domain.

Import the certification in following procedure.

1. Open the command prompt (Windows) or a terminal session (Linux).
2. Copy the created file in “[4.2.1 Export the Server Certification of ROR](#)” to current folder.
The file name is assumed as “ctmgror.cer” in the explanation of this section.
3. Execute following command to import the certification to the truststore in app-domain:

[Windows]

```
%SWCTMG_HOME%\jdk7\bin\keytool -import -file ctmgror.cer -trustcacerts -alias ctmgror -keystore %SWCTMG_HOME%\glassfish3\glassfish\domains\app-domain\config\cacerts.jks -storepass changeit
```

[Linux]

```
/opt/FJVSctbss/jdk7/bin/keytool -import -file ctmgror.cer -trustcacerts -alias ctmgror -keystore /opt/FJVSctbss/glassfish3/glassfish/domains/app-domain/config/cacerts.jks -storepass changeit
```

After executing above command, the prompt displayed asking if you trust the certification. Input “y” and import.

4. Check that the certification “ctmgror” is imported to the truststore in app-domain by executing following command:

[Windows]

```
%SWCTMG_HOME%\jdk7\bin\keytool -list -keystore %SWCTMG_HOME%\glassfish3\glassfish\domains\app-domain\config\cacerts.jks -storepass changeit
```

[Linux]

```
/opt/FJVSctbss/jdk7/bin/keytool -list -keystore /opt/FJVSctbss/glassfish3/glassfish/domains/app-domain/config/cacerts.jks -storepass changeit
```

5. Restarting app-domain is required in order to activate the imported certification. When the app-domain is running, restart app-domain. Refer to “7.1 Start/Stop” in detail how to restart.

Note

- Restarting app-domain is required in order to activate the imported certification.
- The password of keystore is specified after the option “-storepass”. Change the password of keystore if it is not set as “changeit”.
- Delete the exported file of ROR server certification as necessary.

4.2.3 Confirming the Server Information of Certification

The server information of certification is required to be same as the server name of URL used for the service controller to communicate with ROR.

The information of server name can be confirmed in following procedure:

Confirm with Web browser

Click [Issuer] field in the page displayed by clicking [Detail] tab in the certification displayed in “4.2.1 Export the Server Certification of ROR”.

The server information is shown in the line of CN.

Example: CN = SERVER001

Confirm with command

Copy the certification file exported in “4.2.1 Export the Server Certification of ROR” to the server where CT-MG is setup.

The CN of owner of server certification can be confirmed by following command:

[Windows]

```
%SWCTMG_HOME%\jdk7\bin\keytool -printcert -file [file name of ROR server certification] -storepass changeit
```

[Linux]

```
/opt/FJSVctbss/jdk7/bin/keytool -printcert -file [file name of ROR server certification] -storepass changeit
```

Following information displays to execute the command, so confirm the value of CN:

```
Owner: CN=WIN-UBVC92LJ386, OU=GlassFish, O=Oracle Corporation, L=Santa Clara, ST=California, C=US
Issuer: CN=WIN-UBVC92LJ386, OU=GlassFish, O=Oracle Corporation, L=Santa Clara, ST=California, C=US
.
.
.
```

Chapter 5 Creating and Publishing Service

This chapter explains how to create the service of CT-MG.

In order to execute the scenarios, the supplier in CT-MG needs to define appropriate services in CT-MG:

1. Create a technical service and import it to CT-MG as technology provider. Or, send the created technical service to the technology provider.

Make the technical service definitions referring to the following technical service definitions for necessary parameters and basic information for settings.

[Windows]

- For the scenario “Provisioning and scaling of L-Platform”: TechnicalService_VirtualPlatform.xml
- For the scenario “Adding virtual server”: TechnicalService_VirtualServer.xml
- the folder where technical service definitions are registered

[Windows]

```
%SWCTMG_HOME%\app\samples
```

[Linux]

```
/opt/FJSVctbss/app/samples
```

Refer to “[Appendix B Service Parameters for ROR Integration Feature](#)” for detailed information.

The command is available to easily create the technical service definition for the scenario “Provisioning and scaling of L-Platform”. Refer to “[Appendix C Command for Creating Technical Service Definition](#)” for detailed information.

2. Define marketable services as supplier of CT-MG using created technical service, and publish them to the Marketplace Portal, so that it is available to subscribe to the services, change and terminate the subscription.

Note

Confirm that following L-Platform templates and image information are prepared exist in ROR.

- As for L-Platform template, register one image.
- In order to use the template of technical service definition without change, the L-Platform must allow for configuring up to 6 virtual servers. Configure the max number of L-Server for L-Platform template to 6. And, configure the max number of CPU for image information to 4. In case that the max number of L-Server on L-Platform template differs from the number of virtual servers in marketable service, the number and status of available virtual servers on ROR are to differ from that of subscription on CT-MG.
- As for the L-Platform, register one segment.

When changing the number of CPU and virtual server, ROR Integration feature stops the objected virtual server. Confirm to Customer organization subscribing the service, and confirm that no users are using the virtual server.

Do not change or remove the virtual servers and L-Platform directly on ROR which are made by ROR Integration feature. If they are changed or removed, the problems might occur such that the configuration and status differences of subscription would be made and the technical service could not be deleted.

In case that the subscriptions to the services for ROR integration feature fail, refer to the error message shown in confirmation page and following logs:

[Windows]

```
%SWCTMG_HOME%\glassfish3\glassfish\domains\app-domain\logs\app-ror.log: the log of ROR Integration feature
```

```
%SWCTMG_HOME%\glassfish3\glassfish\domains\app-domain\logs\server.log: the server log of app-domain
```

[Linux]

```
/opt/FJSVctbss/glassfish3/glassfish/domains/app-domain/logs/app-ror.logs: the log of ROR Integration feature
```

/opt/FJSVctbss/glassfish3/glassfish/domains/app-domain/logs/server.log: the server log of app-domain

The examples for failed subscriptions are following:

1. ERROR process failed com.fujitsu.bss.app.ror.exceptions.RORException: Command failed: StopLServer Status: ERROR Message: PAPI00200 System Error Occurred.[HTTP Status Code[409] is illegal.]

The configuration of ServerView Operations Manager might not be done. Refer to ”[Appendix E Note on ROR to be Integrated](#)” in detail for how to configure.

2. ERROR Problem while scaling up: ... [code:62514][message:Selectable VM host not found. (not enough CPU or memory available)]

The CPU and memory resources for VM Pool might be short. Refer to “ServerView Resource Orchestrator Cloud Edition Messages” included in ServerView Resource Orchestrator Cloud Edition in detail.

3. Failed to access the WSDL at: https://<hostname>:<port number>/IdentityService/v1.6/BASIC?wsdl.

It might be failed to import the certification of main domain, or hostname might different from the information specified in CN of the owner for server certification of bes-domain. Refer to “[Appendix A Configuration Settings for APP and Service Controller](#)” and “[Appendix D Example to Register the Service Controller](#)” in detail.

When the subscription of ROR Integration is terminated, the name of L-Platform or virtual server cannot be re-used which was used in the terminated subscription until the L-Platform or virtual server is completely terminated.

In case that the operations to subscribe or change L-Platform are executed by customer organization, the error might be occurred in the procedure to stop L-Platform and the operation might be suspended status.

In these cases, resume the operations by following procedure:

1. Open the email of error information notified to the email address specified in APP_ADMIN_MAIL_ADDRESS.
2. On ROR console, stop the virtual servers which fail to stop according to the notified information.
3. Access to the URL described in the notification email.
4. Specify the user ID and password of technology manager which are specified in BSS_USER_KEY and BSS_USER_PWD.

Point

When subscribing the service for ROR integration feature, the master virtual server is provisioned as the first virtual server. And the slave virtual server is added as the second or later virtual server. When deleting the virtual server as the second or later, the newer virtual server is deleted in order.

- As for the “MASTER_TEMPLATE_ID” specified in the technical service definition, specify the ID of image information of virtual server registered in L-Platform template specified in SYSTEM_TEMPLATE_ID.
- As for the “SLAVE_TEMPLATE_ID” specified in the technical service definition, specify the ID of image information of virtual server to be added/reduced in the provisioned L-Platform. The same value as that of “MASTER_TEMPLATE_ID” can be specified
- Make sure to use an image information ID for SLAVE_TEMPLATE_ID which allows the slave servers to run with the same ServerType, NetworkId, HostPool, and StoragePool as the master server. The reason is that the ROR service controller uses these properties of the master server for each newly created slave server.
- Users should not be able to enter a value for this parameter. This means the parameter should not be configurable for customers. Or, in case you specify more than one image, have fixed parameter options for selection.
- Specify the image information ID to SLAVE_TEMPLATE_ID which are based on the same virtualization software as MASTER_TEMPLATE_ID.

The IP addresses and passwords of virtual servers are noticed by email to the user assigned to the service for ROR integration feature after completion of subscribing and assigning to the service. And, in “My subscriptions” menu, the IP addresses and passwords of virtual servers can be confirmed which are assigned to the subscription.

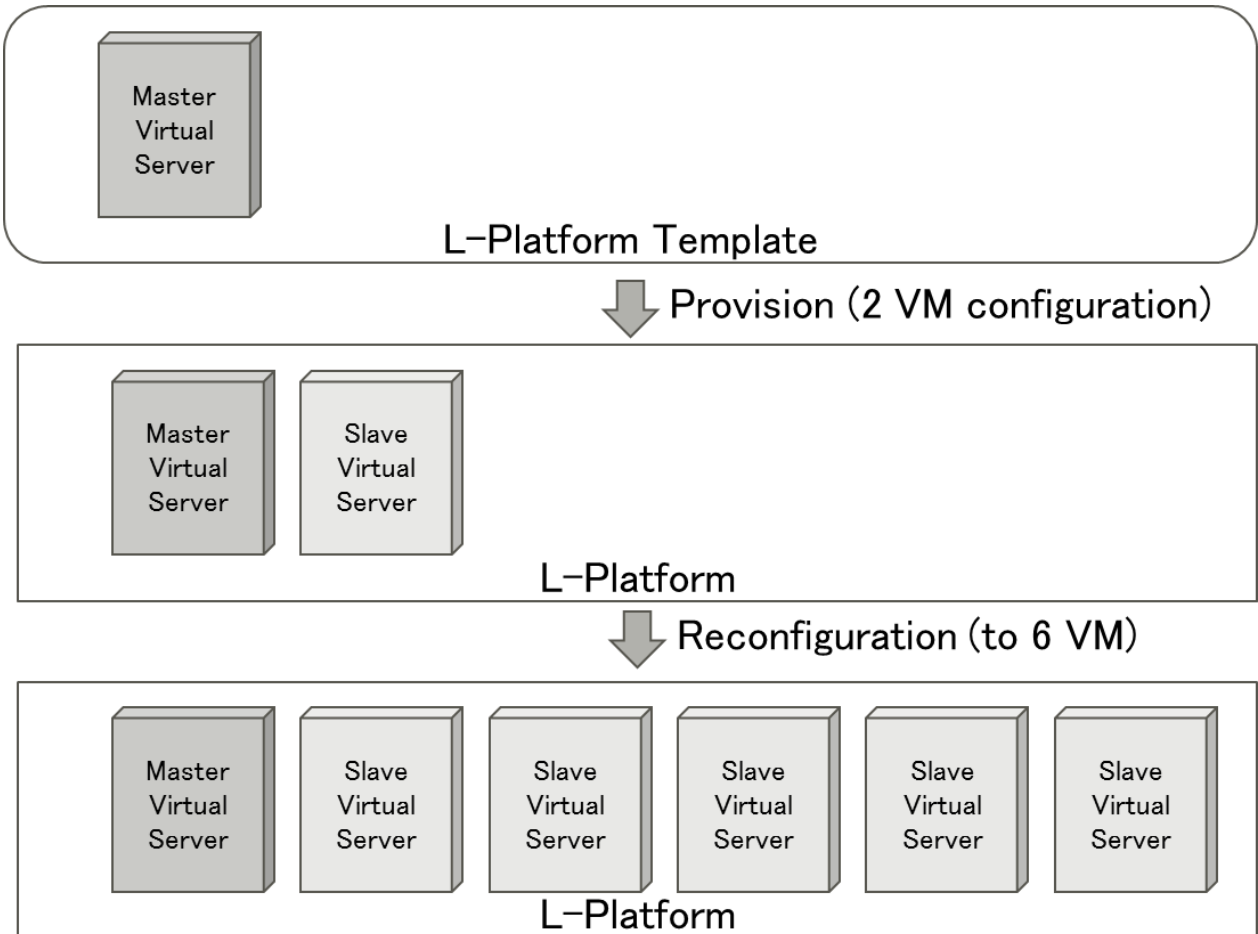
- As for the OS user name to access to the virtual servers, inform to the customer subscribing the service. For example, send email including the list of virtual servers and their access information.

In case that main domain stops when L-Platform or virtual server is being provisioned, the subscription and provisioning process might stop. In this case, resume the subscription and provisioning process by following procedure:

1. Open the email notified to the email address specified in APP_ADMIN_MAIL_ADDRESS, when the subscription and provisioning process stop.
2. Access to the URL described in the notification email.
3. Specify the user ID and password of technology manager which are specified in BSS_USER_KEY and BSS_USER_PWD.

Not execute the operation to stop L-Platform on “My subscriptions” soon after the subscription and changing are completed for L-Platform, or soon after the operation to start L-Platform. In case that this operation is executed, the operations and changing for the subscription might not be able to execute after this operations.

In this case, contact to supplier organization, or directly access to and stop the virtual servers to which the stopping operation is executed.



Chapter 6 Unsetup

This chapter explains how to unsetup ROR integration feature.

6.1 Unsetup the ROR Integration feature

This section explains how to unsetup ROR integration feature.

6.1.1 Tasks before Unsetup

Backup resources

Back up environment resources if necessary before unsetup ROR integration feature. Refer to "9.4 Online backup and restoration" in "Installation Guide" for details.

Delete marketable service and technical service definition

Delete the marketable service and technical service definition for the service controller registered to Systemwalker Service Catalog Manager. Refer to "Supplier's Guide" and "Technology Provider's Guide" for details.

Confirm database port

Confirm the port number of database specified in db.properties. Refer to "3.1.4 Checking Configuration Settings" in detail.

6.1.2 Unsetup

This subsection explains the procedure of ROR Integration feature unsetup

Execute the unsetup command

1. Log in as the OS administrator.

Log in as OS administrator to the server from which the ROR Integration feature will be unsetup.

2. Use the following command to execute the unsetup procedure.

[Windows]

```
%SWCTMG_HOME%\setup\swctmg_unsetupRORInteg
```

[Linux]

```
/opt/FJSVctbss/setup/swctmg_unsetupRORInteg.sh
```

Confirm execution

A message is displayed prompting you to confirm execution to unsetup.

To execute enter [y], to abort enter [n], then press the ENTER key.

```
swctmg_unsetup: INFO: 139: Are you sure you want to start unsetup Systemwalker Catalog Manager ROR  
Integration? (y/n)[n]
```

Start the unsetup

The following message is displayed when you start unsetup:

```
swctmg_unsetup: INFO: 144: Systemwalker Service Catalog Manager ROR Integration unsetup start
```

Confirm completion

The following message is displayed when unsetup is complete

swctmg_unsetup: INFO: 146: Systemwalker Service Catalog Manager ROR Integration unsetup end.

Chapter 7 Operation

This chapter explains the operations of ROR integration feature.

7.1 Start/Stop

This section explains how to start and stop ROR integration feature.

7.1.1 Prerequisites

Start the database of Systemwalker Service Catalog Manager. Refer to “9.1 Start/Stop” in “Installation Guide” in detail.

7.1.2 Start

This subsection explains how to start ROR integration feature.

Execute following command:

[Windows]

```
net start "Systemwalker Service Catalog Manager APP Server"
```

[Linux]

```
service swctmgapp start
```

7.1.3 Stop

This subsection explains how to stop ROR integration feature.

Execute following command:

[Windows]

```
net stop "Systemwalker Service Catalog Manager APP Server"
```

[Linux]

```
service swctmgapp stop
```

7.2 Customize Text

This section explains how to customize the text used in ROR Integration feature.

7.2.1 Text List for ROR Integration Feature

Change following texts in necessary which are shown in marketplace portal. Refer to “Marketplace Owner’s Guide” in detail how to customize.

- Text: pending (the status of subscription)
Key: SubscriptionStatus.PENDING
- pending update (the status of subscription)
Key: SubscriptionStatus.PENDING_UPD
- Value [minimum - maximum] (the explanation for service parameter)
Key: service.parameter.value

- My Subscriptions (the navigation menu and menu title)
 - Key: navigation.subscriptions
 - Key: marketplace.subscriptions.title
 - Key: catalog.title
- Show (the button on “Subscriptions” page)
 - Key: marketplace.account.button.show
- Save (the button on “Configuration” tab on “Subscriptions”)
 - Key: button.save

Note

The key “button.save” is used as “Save” button on the other pages such as “Add User” and “New billing address” pages.

7.3 Manage Subscription

This section explains how to manage the subscriptions of ROR Integration feature.

If the provisioning or modification of a virtual system fails on the ROR side or if there are problems in the communication between the participating systems, the corresponding subscription in CT-MG remains pending. Integration feature informs the technology managers of its responsible technology provider organization by email of any incomplete provisioning, modification, or delete operation in ROR.

After getting the email notification, you can then take the appropriate actions to solve the problem in ROR or in the communication. For example, you could remove an incomplete virtual platform or server, or you could restore a missing connection.

After solving the problem, ROR Integration feature and CT-MG need to be synchronized accordingly. You do this by triggering a corresponding action in the APP component. Proceed as follows:

1. Work as a technology manager of the technology provider organization which is responsible for the ROR service controller.
2. Invoke the instance status interface of APP for the ROR service controller by opening the following URL in a Web browser:

```
http://<server>:<port>/fujitsu-bss-app/controller/?cid=ess.ror
```

Specify the hostname or IP address of the server where CT-MG is running to <server>, and the HTTP listener port of APP domain (example: 8880) to <port>

3. On the log in page, specify the user ID and password of the technology manager who is providing the technical service for ROR Integration feature.

After logging in, the Web page shows all subscriptions for ROR, including detailed information such as the customer organization, the ID of the related ROR instance, and the provisioning status.
4. Find the subscription for which you solved the problem in the most recent provisioning, modification, or deprovisioning operation.
5. In the Action column, select the action for the ROR integration components to execute next. Possible actions are the following:
 - RESUME: to resume the processing of a provisioning operation in APP which was suspended.
 - SUSPEND: to suspend the processing of a provisioning operation in APP, for example, when ROR does not respond.
 - UNLOCK: to remove the lock for an ROR instance in APP.
 - DELETE: to terminate the subscription in CT-MG and remove the instance in APP, but keep the virtual platform or server in ROR for later use. For this action, the service manager role is required in addition
 - DEPROVISION: to terminate the subscription in CT-MG, remove the instance in APP, and deprovision the virtual platform or server in ROR. For this action, the service manager role is required in addition.
 - ABORT_PENDING: to abort a pending provisioning or modification operation in CT-MG.
 - COMPLETE_PENDING: to complete a pending provisioning or modification operation in CT-MG.

6. Click Execute to invoke the selected action.

Chapter 8 Modifying Settings

This chapter explains how to modify the settings of ROR Integration.

8.1 Change Configuration Settings of APP and Service Controller

This section explains how to change the configuration settings of APP and service controller.

8.1.1 Tasks before Changing

ROR integration feature runs on the same server where CT-MG is installed. Confirm following items in advance:

- Completion to setup ROR Integration.
- Running of CT-MG database. Refer to “Installation Guide” in detail about starting CT-MG database.

8.1.2 Changing Configuration Settings

This subsection explains the procedure to change ROR Integration.

Executing setup command

Execute following procedure:

1. Log in as the OS administrator.
Log in as the OS administrator to the server where ROR Integration feature is setup.
2. Open the command prompt (Windows) or a terminal session (Linux).
3. Execute the changing command for ROR Integration.

[Windows]

```
%SWCTMG_HOME%\setup\swctmg_changeRORInteg "<Parameter name>=<value after changing>"
```

[Linux]

```
/opt/FJSVctbss/setup/swctmg_changeRORInteg.sh <Parameter name>=<value after changing>
```

In <parameter name>=<value after changing>, the parameter must be specified which is to be changed, from the according to following table. Also, an ASCII space character must be put between parameters. One to twelve parameters can be set. Refer to “[Appendix A Configuration Settings for APP and Service Controller](#)” in detail for each parameter.

[Windows]

```
"<Parameter name>=<value after changing>"
```

[Linux]

```
<Parameter name>=<value after changing>
```

Table 8.1 ROR Integration Setup Parameter List

No.	Parameter name	Mandatory	説明
1	APP_BASE_URL	No	The URL used to access APP. Specify this parameter according to the form, APP_BASE_URL=http://<server>:<port>/fujitsu-bss-app <server> is used for name resolution by client. Use the host name available for name resolution or IP address available to access by client for <server>. Use the port number for HTTP listener of app-domain (default: 8880) for <port>.

No.	Parameter name	Mandatory	説明
			Example: APP_BASE_URL=http://SERVER001:8081/fujitsu-bss-app
2	APP_TIMER_INTERVAL	No	The interval (in milliseconds). With this interval, APP polls the status of instances. Example: APP_TIMER_INTERVAL=15000
3	APP_ADMIN_MAIL_ADDRESS	No	The email address which is used for sending notifications of information. To this email address, notifications are sent in case that there are some troubles in APP operation. Example: admin@example.com
4	BSS_WEBSERVICE_HOST_PORT	No	The hostname and port number for accessing to main domain by APP. The hostname must be same as the as the information specified in CN of the owner for server certification of main domain. As for checking the information, refer to “ 4.1.2 Confirming the Server Information of Certification ”. Specify this parameter according to the form, “<hostname>:<port number>”. Example: SERVER001:8081
5	BSS_USER_KEY	No	The user key for technology manager accessing to main domain. Specify the user key which you receive with the confirmation email for your user account. And, use the user key of administrator in the organization which is registered to CT-MG. Example: 10000
6	BSS_USER_PWD	No	The BSS user password for technology manager accessing to main domain. Specify the password of technology manager of BSS_USER_KEY. Example: admin123
7	BSS_ORGANIZATION_ID	No	The ID of the technology provider organization in CT-MG who is to register the technical service for ROR integration feature. Specify the organization ID where the technology manager of BSS_USER_KEY belongs. Example: ca4cbd74
8	IAAS_API_LOCALE	No	The locale to be used for accessing ROR API. Specify the locale of ROR (“en” or “ja”).
9	IAAS_API_USER	No	The user ID in ROR. This is used for access to the tenant in ROR. This ROR user requires Tenant Administrator role. Example: ctmg.ror
10	IAAS_API_PWD	No	The password of the user ID in ROR. Specify the password of ROR user specified in IAAS_API_USER. Example: ctmg.ror
11	IAAS_API_TENANT	No	The tenant name of ROR. Specify the tenant name to which the user specified in “IAAS_API_USER” belongs. Example: ctmgtenant
12	IAAS_API_HOST_PORT	No	The hostname and port number of ROR L-Platform API. Hostname must be same as the information specified in server certification of ROR. As for checking the information, refer to “ 4.2.3 Confirming the Server Information of Certification ”.

No.	Parameter name	Mandatory	説明
			Specify this parameter according to the form, “<hostname>:<port number (default: 8014)>”. Example: server002:8014

Example:

[Windows]

```
%SWCTMG_HOME%\setup\swctmg_changeRORInteg "APP_BASE_URL=http://SERVER001:8081/fujitsu-bss-app"
```

[Linux]

```
/opt/FJSVctbss/setup/swctmg_changeRORInteg.sh APP_BASE_URL=http://SERVER001:8081/fujitsu-bss-app
```

Note

APP_TIMER_INTERVAL must be specified alphanumeric number, and from 1 to 180000.

BSS_USER_KEY must be specified by alphanumeric letters and at least over 1000.

BSS_USER_PWD must be specified in at least 8 characters in length.

Confirm the completion

Following message will be displayed when the change procedure completes.

```
swctmg_setup: INFO: 140: Changed Systemwalker Service Catalog Manager ROR Integration successfully.  
Please restart APP domain to reflect the change.
```

Restarting app-domain

Restarting app-domain is required in order to activate the change. Refer to “[7.1 Start/Stop](#)” in detail how to restart.

8.2 Modifying Port Number of Database

This section explains how to modify the port number to connect for ROR Integration when the port number is changed used by the database of this product.

Note

- ROR Integration feature must be running in order to execute the commands.
- The admin port number of Java EE execution environment must be specified as a command option. Refer to “[8.7 Admin Port Number of Java EE Execution Environment](#)” for the information on how to check the port number.

Refer to “[8.6 Options of Admin Command](#)” for the information on the command option.

The explanation for the commands in this section assumes that the options are specified by the following environment variable.

[Windows]

%OPTION%

[Linux]

\$OPTION

8.2.1 Modifying Port Number of Connection Pool

Modify the destination port number used by connection pool so that it can connect to the database.

Use following command to modify the setting.

[Windows]

```
"%SWCTMG_HOME%\glassfish3\bin\asadmin" %OPTION% set server.resources.jdbc-connection-  
pool.BSSAppPool.property.portNumber=<PORT NO>
```

[Linux]

```
/opt/FJSSVctbss/glassfish3/bin/asadmin $OPTION set server.resources.jdbc-connection-  
pool.BSSAppPool.property.portNumber=<PORT NO>
```

8.2.2 Stopping ROR Integration Feature

Stop ROR Integration feature referring to “[7.1 Start/Stop](#)”.

8.2.3 Modifying Port Number of Database

Modify the port number of database of CT-MG referring to “8.2 Modifying Port Number of Database” in “Installation Guide”.

8.2.4 Starting ROR Integration Feature

Start ROR Integration feature referring to “[7.1 Start/Stop](#)”.

8.3 Modifying Port Number of APP Domain

This section explains how to modify the port number used by APP domain.

The port numbers explained in this section can be modified by commands. Execute them on Command Prompt or console.



Note

- ROR Integration feature must be running in order to execute the commands.
- The modification will become effective after restarting ROR Integration service. However, following port will become effective just after executing the modification command:
 - HTTP listener port
 - HTTP SSL listener port
- The admin port number of Java EE execution environment must be specified as a command option. Refer to “[8.7 Admin Port Number of Java EE Execution Environment](#)” for the information on how to check the port number.

Refer to “[8.6 Options of Admin Command](#)” for the information on the command option.

The explanation for the commands in this section assumes that the options are specified by the following environment variable.

[Windows]

%OPTION%

[Linux]

\$OPTION



Information

The parameters are available to check the setting value of the installation environment by executing check command. The objected parameters are those which are modified by “set” subcommand of “asadmin” command for the way to modify installation environment described in this chapter.

The check command is following:

```
<absolute path of "asadmin" command> <OPTION> get <parameter>
```

As for absolute path of “asadmin” command and parameter, refer to the example for each command.

As for OPTION of check command, refer to “[8.6 Options of Admin Command](#)”.

As for the example of check command refer to “[8.7 Admin Port Number of Java EE Execution Environment](#)”.

8.3.1 Modifying Admin Port of Java EE Execution Environment

Use following commands to modify the setting.

[Windows]

1. Change admin port of Java EE Execution Environment.

```
"%SWCTMG_HOME%\glassfish3\bin\asadmin" %OPTION% set server-config.network-config.network-listeners.network-listener.admin-listener.port=<PORT NO>
```

2. Stop the domain of which admin port was changed above.

```
"%SWCTMG_HOME%\glassfish3\bin\asadmin" -H <hostname, other than "localhost"> -p <the old admin port number> stop-domain
```

3. Start ROR Integration feature referring to “[7.1 Start/Stop](#)”.

[Linux]

1. Change admin port of Java EE Execution Environment.

```
/opt/FJSPVctbss/glassfish3/bin/asadmin $OPTION set server-config.network-config.network-listeners.network-listener.admin-listener.port=<PORT NO>
```

2. Stop the domain of which admin port was changed above.

```
/opt/FJSPVctbss/glassfish3/bin/asadmin -H <hostname, other than "localhost"> -p <the old admin port number> stop-domain
```

3. Start ROR Integration feature referring to “[7.1 Start/Stop](#)”..

8.3.2 Modifying HTTP Listener Port Number

Executing the command to modify

Use following command to modify the setting.

[Windows]

```
"%SWCTMG_HOME%\glassfish3\bin\asadmin" %OPTION% set server-config.network-config.network-listeners.network-listener.http-listener-1.port=<PORT NO>
```

[Linux]

```
/opt/FJSPVctbss/glassfish3/bin/asadmin $OPTION set server-config.network-config.network-listeners.network-listener.http-listener-1.port=<PORT NO>
```

Modifying the port number

1. Change the port number of APP_BASE_URL. Refer to “[8.1 Change Configuration Settings of APP and Service Controller](#)” in detail.
2. Change the port number in the technical service definition, log in to admin portal as technology manager and import the technical service. Refer to “[Technology Provider’s Guide](#)” in detail.

8.3.3 Modifying HTTP SSL Listener Port Number

Executing the command to modify

Use following command to modify the setting.

[Windows]

```
"%SWCTMG_HOME%\glassfish3\bin\asadmin" %OPTION% set server-config.network-config.network-listeners.network-listener.http-listener-2.port=<PORT NO>
```

[Linux]

```
/opt/FJSVctbss/glassfish3/bin/asadmin $OPTION set server-config.network-config.network-listeners.network-listener.http-listener-2.port=<PORT NO>
```

8.3.4 Modifying IIOP Listener Port Number

Use following command to modify the setting.

[Windows]

```
"%SWCTMG_HOME%\glassfish3\bin\asadmin" %OPTION% set server-config.iiop-service.iiop-listener.orb-listener-1.port=<PORT NO>
```

[Linux]

```
/opt/FJSVctbss/glassfish3/bin/asadmin $OPTION set server-config.iiop-service.iiop-listener.orb-listener-1.port=<PORT NO>
```

8.3.5 Modifying IIOP Listener Port Number for SSL Communication

Use following command to modify the setting.

[Windows]

```
"%SWCTMG_HOME%\glassfish3\bin\asadmin" %OPTION% set server-config.iiop-service.iiop-listener.SSL.port=<PORT NO>
```

[Linux]

```
/opt/FJSVctbss/glassfish3/bin/asadmin $OPTION set server-config.iiop-service.iiop-listener.SSL.port=<PORT NO>
```

8.3.6 Modifying IIOP Listener Port Number for Client Authentication of SSL Communication

Use following command to modify the setting.

[Windows]

```
"%SWCTMG_HOME%\glassfish3\bin\asadmin" %OPTION% set server-config.iiop-service.iiop-listener.SSL_MUTUALAUTH.port=<PORT NO>
```

[Linux]

```
/opt/FJSVctbss/glassfish3/bin/asadmin $OPTION set server-config.iiop-service.iiop-listener.SSL_MUTUALAUTH.port=<PORT NO>
```

8.3.7 Modifying RMI registry connection port number used by JMX connector

Use following command to modify the setting.

[Windows]

```
"%SWCTMG_HOME%\glassfish3\bin\asadmin" %OPTION% set server.admin-service.jmx-connector.system.port=<PORT NO>
```

[Linux]

```
/opt/FJSVctbss/glassfish3/bin/asadmin $OPTION set server.admin-service.jmx-connector.system.port=<PORT NO>
```

8.3.8 Modifying Port Number for JMS Host and RMI Registry for Message Queue broker

Use following command to modify the setting of JMS host port number. The port number for RMI registry for Message Queue broker will be changed to the JMS host port number + 100.

[Windows]

```
"%SWCTMG_HOME%\glassfish3\bin\asadmin" %OPTION% set server.jms-service.jms-host.default_JMS_host.port=<PORT NO>
```

[Linux]

```
/opt/FJSVctbss/glassfish3/bin/asadmin $OPTION set server.jms-service.jms-host.default_JMS_host.port=<PORT NO>
```

8.4 Modifying SMTP Server Settings

This section explains how to change the setting of SMTP server used by ROR Integration feature.

The setting of SMTP server can be modified by commands. Execute them on Command Prompt or console.



- ROR Integration feature must be running in order to execute the commands.
- The admin port number of Java EE execution environment must be specified as a command option. Refer to “[8.7 Admin Port Number of Java EE Execution Environment](#)” for the information on how to check the port number.

Refer to “[8.6 Options of Admin Command](#)” for the information on the command option.

The explanation for the commands in this section assumes that the options are specified by the following environment variable.

[Windows]

%OPTION%

[Linux]

\$OPTION



The parameters are available to check the setting value of the installation environment by executing check command. The objected parameters are those which are modified by “set” subcommand of “asadmin” command for the way to modify installation environment described in this chapter.

The check command is following:

```
<absolute path of "asadmin" command> <OPTION> get <parameter>
```

As for absolute path of "asadmin" command and parameter, refer to the example for each command.

As for OPTION of check command, refer to "8.6 Options of Admin Command".

As for the example of check command refer to "8.7 Admin Port Number of Java EE Execution Environment".

8.4.1 Modifying SMTP Server

Use following command to modify the SMTP server setting.

[Windows]

```
"%SWCTMG_HOME%\glassfish3\bin\asadmin" %OPTION% set server.resources.mail-resource.mail/  
APPMail.host=<Hostname of SMTP server>
```

[Linux]

```
/opt/FJVSctbss/glassfish3/bin/asadmin $OPTION set server.resources.mail-resource.mail/  
APPMail.host=<Hostname of SMTP server>
```

8.4.2 Modifying Mail Address

This default setting is "service@example.com". Use following command to modify the settings.

[Windows]

```
"%SWCTMG_HOME%\glassfish3\bin\asadmin" %OPTION% set server.resources.mail-resource.mail/  
APPMail.from=<Mail address>
```

[Linux]

```
/opt/FJVSctbss/glassfish3/bin/asadmin $OPTION set server.resources.mail-resource.mail/  
APPMail.from=<Mail address>
```

8.4.3 Modifying SMTP Authentication

This default setting is "false". Use following command to modify the SMTP authentication settings.

[Windows]

```
"%SWCTMG_HOME%\glassfish3\bin\asadmin" %OPTION% set server.resources.mail-resource.mail/  
APPMail.property.mail-smtp-auth=<SMTP authentication(true/false)>
```

[Linux]

```
/opt/FJVSctbss/glassfish3/bin/asadmin $OPTION set server.resources.mail-resource.mail/  
APPMail.property.mail-smtp-auth=<SMTP authentication (true/false)>
```

8.4.4 Modifying SMTP User

This default setting is "saas". Use following command to modify the SMTP server settings.

[Windows]

```
"%SWCTMG_HOME%\glassfish3\bin\asadmin" %OPTION% set server.resources.mail-resource.mail/  
APPMail.user=<SMTP user>
```

[Linux]

```
/opt/FJSTbss/glassfish3/bin/asadmin $OPTION set server.resources.mail-resource.mail/
APPMail.user=<SMTP user>
```

8.4.5 Modifying SMTP Password

This default setting is “password”. Use following command to modify the SMTP password settings.

[Windows]

```
"%SWCTMG_HOME%\glassfish3\bin\asadmin" %OPTION% set server.resources.mail-resource.mail/
APPMail.property.mail-smtp-password=<SMTP password>
```

[Linux]

```
/opt/FJSTbss/glassfish3/bin/asadmin $OPTION set server.resources.mail-resource.mail/
APPMail.property.mail-smtp-password=<SMTP password>
```

8.4.6 Modifying SMTP Server Port

Use following command to modify the SMTP server port settings.

[Windows]

```
"%SWCTMG_HOME%\glassfish3\bin\asadmin" %OPTION% set server.resources.mail-resource.mail/
APPMail.property.mail-smtp-port=<Port number of the SMTP server>
```

[Linux]

```
/opt/FJSTbss/glassfish3/bin/asadmin $OPTION set server.resources.mail-resource.mail/
APPMail.property.mail-smtp-port=<Port number of the SMTP server>
```

8.5 Changing Administrator’s Password of Java EE Execution Environment

This section explains how to change Administrator’s password of Java EE execution environment.

The administrator’s password explained in this section can be modified by commands. Execute them on Command Prompt or console.



- ROR Integration feature must be running in order to execute the commands.
- The modification will become effective after restarting ROR Integration service.
- The admin port number of Java EE execution environment must be specified as a command option. Refer to “[8.7 Admin Port Number of Java EE Execution Environment](#)” for the information on how to check the port number.

Refer to “[8.6 Options of Admin Command](#)” for the information on the command option.

The explanation for the commands in this section assumes that the options are specified by the following environment variable.

[Windows]

%OPTION%

[Linux]

\$OPTION

Use following command to change:

[Windows]

```
"%SWCTMG_HOME%\glassfish3\bin\asadmin" %OPTION% change-admin-password --domaindir %SWCTMG_HOME%\glassfish3\glassfish\domains --domain_name app-domain
```

[Linux]

```
/opt/FJSTbss/glassfish3/bin/asadmin $OPTION change-admin-password --domaindir /opt/FJSTbss/glassfish3/glassfish/domains --domain_name app-domain
```

8.6 Options of Admin Command

This section explains the options of admin command.

The admin port number of Java EE execution environment must be specified as a command option for APP domain. Also the password of Java EE execution environment must be specified.

Refer to “[8.7 Admin Port Number of Java EE Execution Environment](#)” for the information on how to check the port number.

Specify following command options in the case the admin port number has been modified.

Option	Description
-p	Specify the admin port number of Java EE execution environment of the APP domain. If the port has been modified, the execution of the command will fail unless correct value is specified with this option.
-u	Specify the user name of the administrator of Java EE execution environment for APP domain. The user name will be asked after invoking the command if this option is omitted.

Example: Specifying options to the environment variable OPTION

[Windows]

```
SET OPTION=-p 8848 -u Administrator
```

[Linux]

```
export OPTION="-p 8848 -u Administrator"
```

8.7 Admin Port Number of Java EE Execution Environment

This section explains how to confirm the admin port of Java EE execution environment.

Use following command to confirm

[Windows]

```
"%SWCTMG_HOME%\glassfish3\bin\asadmin" %OPTION% get server-config.network-config.network-listeners.network-listener.admin-listener.port
```

[Linux]

```
/opt/FJSTbss/glassfish3/bin/asadmin $OPTION get server-config.network-config.network-listeners.network-listener.admin-listener.port
```

In following example, the port number is the value just after “server-config.network-config.network-listeners.network-listener.admin-listener.port=”.

Example output:

```
server-config.network-config.network-listeners.network-listener.admin-listener.port=8848
```

Appendix A Configuration Settings for APP and Service Controller

This appendix explains the configuration settings for APP and service controller. In order to change the configuration settings for APP and service controller, refer to “[8.1 Change Configuration Settings of APP and Service Controller](#)” in detail.

A.1 Configuration Settings of APP

APP_BASE_URL

```
APP_BASE_URL=http://<server>:<port>/fujitsu-bss-app
```

The URL used to access APP.

Specify the APP_BASE_URL setting as follows:

```
APP_BASE_URL=http://<host>:<port>/fujitsu-bss-app
```

<host> is used for name resolution by client. Use the host name available for name resolution or IP address available to access by client for <host>. Use the port number for HTTP listener of app-domain (default: 8880) for <port>

APP_TIMER_INTERVAL

```
APP_TIMER_INTERVAL=15000
```

The interval (in milliseconds) at which APP polls the status of instances. If you increase the value, provisioning will take longer. If you decrease it, more loading is put on the system.

APP_MAIL_RESOURCE

```
APP_MAIL_RESOURCE=mail/APPMail
```

The JNDI name of the Java EE execution environment mail resource which is used to send mails.

The resource mail/APPMail is created during setup with the parameters defined in the “glassfish.properties” file. The resource mail/APPMail cannot be changed.

APP_ADMIN_MAIL_ADDRESS

```
APP_ADMIN_MAIL_ADDRESS=admin@example.com
```

The email address which is used for sending notifications of information. To this email address, information will be notified in case that trouble occurs when APP is operating.

BSS_WEBSERVICE_URL

```
BSS_WEBSERVICE_URL=https://<server>:<port>/{SERVICE}/v1.6/BASIC?wsdl
```

Required when BSS_AUTH_MODE is set to INTERNAL and basic authentication is used. The hostname and port number of the CT-MG server to be used. The {SERVICE} placeholder must not be replaced.

CT-MG is the HTTPS server while APP is a Web service client. The Web service calls are secured with SSL. The following requirements must be met to establish a connection to CT-MG:

- The CT-MG server must present a valid certificate.
- The CT-MG certificate must be trusted by APP.

For details on certificates, refer to the “Operator's Guide” of the CT-MG user documentation. The value will be set to the part of “<server>:<port>” of this property which is specified in BSS_WEBSERVICE_HOST_PORT in the setup and changing commands for ROR Integration.

BSS_USER_KEY

`BSS_USER_KEY=<userKey>`

The user key for technology manager accessing CT-MG.

Replace <userKey> with the user key which you receive with the confirmation email for your user account. The user must have the administrator role for your organization in CT-MG. “1000” is specified as initial value of this file, assumed that the operator registered after setup of main CT-MG has technology manager role.

BSS_USER_PWD

`BSS_USER_PWD=<password>`

The BSS user password for technology manager accessing CT-MG.

Replace <password> with the plain text password which is valid for the technology manager given in `BSS_USER_KEY=<userKey>`.

BSS_AUTH_MODE

`BSS_AUTH_MODE=INTERNAL`

Specifies whether CT-MG is used for user authentication or whether it acts as a SAML service provider and allows for Web browser single sign-on. The setting must be identical to the `AUTH_MODE` setting in CT-MG.

Possible values: `INTERNAL` (user authentication is used) or `SAML_SP` (acts as a SAML service provider).

Contact the CT-MG platform operator for details on which value to set.

BSS_WEBSERVICE_URL_STS_PORT

`BSS_WEBSERVICE_URL_STS_PORT=https://<server>:<port>/{SERVICE}/v1.6/STS?wsdl`

Required when `BSS_AUTH_MODE` is set to `SAML_SP`. The URL of the CT-MG server to be used. The {SERVICE} placeholder must not be replaced.

APP_KEYSTORE_PASSWORD

`APP_KEYSTORE_PASSWORD=changeit`

Required when `BSS_AUTH_MODE` is set to `SAML_SP`. The password required to access the keystore of the domain used for APP in the domain for APP.

APP_TRUSTSTORE_PASSWORD

`APP_TRUSTSTORE_PASSWORD=changeit`

Required when `BSS_AUTH_MODE` is set to `SAML_SP`. The password required to access the truststore of the domain used for APP in the domain for APP.

A.2 Configuration Settings of Service Controller

CONTROLLER_ID

`CONTROLLER_ID=ess.ror`

Mandatory parameter. “ess.ror” is automatically specified in the setup command for ROR Integration feature. In case to change the configuration settings of service controller with “Appendix F.2.1 change configuration”, you must specify this property.

Default: ess.ror

BSS_ORGANIZATION_ID

`BSS_ORGANIZATION_ID=<OrgID>`

The ID of the technology provider organization in CT-MG who is to register the technical service for ROR integration feature

IAAS_API_LOCALE

IAAS_API_LOCALE=<ja or en>

The locale to be used for accessing ROR API. Specify the locale of ROR (“en” or “ja”).

IAAS_API_USER

IAAS_API_USER=<ROR user ID>

The user ID in ROR. This is used for access to the tenant in ROR. This ROR user requires Tenant Administrator role.

IAAS_API_PWD

IAAS_API_PWD=<the password of ROR user>

Specify the password of the user ID, which is specified in “IAAS_API_USER” used for access to the tenant in ROR. The plain text password will be encrypted automatically in the APP database.

IAAS_API_TENANT

IAAS_API_TENANT=<ROR tenant name>

Specify the tenant name to which the user specified in “IAAS_API_USER” belongs.

IAAS_API_URI

IAAS_API_URI=https://<ROR server>:<port>/cfmgapi/endpoint

Specify the URL of the L-Platform API of ROR. <ROR server> must be same as the information specified in server certification of ROR. As for checking the information, refer to “[4.2.3 Confirming the Server Information of Certification](#)”

The value will be set to the part of “<ROR server>:<port>” of this property which is specified in IAAS_API_HOST_PORT in the setup and changing commands for ROR Integration.

Appendix B Service Parameters for ROR Integration Feature

This appendix explains the parameters of technical services which are handled by the ROR Integration service controller.

B.1 All Scenarios

The following parameters apply to all scenarios:

APP_CONTROLLER_ID

Mandatory. The ID of the service controller on APP as defined in its implementation.

Default: ess.ror

APP_BSS_USER

Mandatory. The user key of the technology manager to be used for service calls to CT-MG. The user must be a member of the technology provider organization for which the service controller has been registered.

Example: 38007

APP_BSS_USER_PWD

Mandatory. The password of the technology manager to be used for service calls to CT-MG.

Example: secret

INSTANCENAME_PATTERN

Mandatory. A regular expression specifying a pattern for the L-platform or virtual server names entered by the users when they subscribe to a corresponding service. If the names do not match the pattern, the subscription is rejected and failed.

Example: ror([a-z0-9]){2,25}

INSTANCENAME_PREFIX

Optional. A string to be prepended to the L-Platform or virtual server names entered by the users when they subscribe to a corresponding service.

Example: ror

INSTANCENAME

Mandatory. The name of the L-Platform or virtual server to be provisioned. This name must be specified by the users when they subscribe to a corresponding service. The string given in INSTANCENAME_PREFIX is prepended to the name. The name including the prefix must match the pattern given in INSTANCENAME_PATTERN.

Example: IASPlatform

MAIL_FOR_COMPLETION

Optional. The address to which emails are to be sent that describe manual steps required to continue an operation. If you specify this parameter, the service controller interrupts the processing of each operation after each step and waits for a notification about the completion of a manual action. Omit this parameter if you do not want to interrupt the processing.

Example: info@company.com

MAIL_FOR_NOTIFICATION

Optional. The address to which emails are to be sent that notify service users or administrators of customer organizations. It is notified to this address that reconfiguration of L-Platform is successful. Such reconfigurations result from changes in the configuration parameters at a corresponding subscription.

Example: info@company.com

B.2 L-Platform Provisioning and Scaling

The following parameters are required for provisioning L-Platform, adding and reducing of virtual server by reconfiguration, changing of CPU number of each virtual server by reconfiguration, and start and stop for L-Platform.

SYSTEM_TEMPLATE_ID

Mandatory. The ID of the ROR template to be used for L-Platforms. As for the template ID, refer to the Template Builder menu Template tab of ROR console.

Example: template-13c8ab3348d

MASTER_TEMPLATE_ID

Mandatory. The ID of the image information to be used for the master virtual server (or the only virtual server) on L-Platform. As for the ID of image information, refer to the Image tab in Template tab of ROR console.

Example: image-13cedef7ed

SLAVE_TEMPLATE_ID

Mandatory. The ID of the image information to be used for the slave virtual servers on L-Platform. The same ID can be specified as that specified as "MASTER_TEMPLATE_ID". As for the ID of image information, refer to the Image tab in Template tab of ROR console. Make sure to use an image information ID for SLAVE_TEMPLATE_ID which allows the slave servers to run with the same ServerType, NetworkId, HostPool, and StoragePool as the master server. The reason is that the ROR service controller uses these properties of the master server for each newly created slave server.

Users should not be able to enter a value for this parameter. This means the parameter should not be configurable for customers. Or, in case you specify more than one image, have fixed parameter options for selection.

Specify the image information ID to SLAVE_TEMPLATE_ID which are based on the same virtualization software as MASTER_TEMPLATE_ID.

Example: image-13c8a812d25

CLUSTER_SIZE

Mandatory. The number of virtual servers to be provisioned on L-Platform. Make sure that the administrator of customer organization can only specify numbers that are supported by the corresponding L-Platform templates. This can be done, for example, by presenting the supported numbers as different parameter options.

Example: 2

COUNT_CPU

Optional. The number of CPUs each virtual server on L-Platform is to have. Make sure that the administrator of customer organization can only specify the same or smaller number than the max CPU number specified in corresponding image information. This can be done, for example, by presenting the supported numbers as different parameter options.

Example: 4

START_VIRTUAL_SYSTEM

Optional. Specify the URL of operation service used for starting L-Platform.

Example: http://localhost:8880/OperationService/AsynchronousOperationProxy?wsdl

STOP_VIRTUAL_SYSTEM

Optional. Specify the URL of operation service used for stopping L-Platform.

Example: http://localhost:8880/OperationService/AsynchronousOperationProxy?wsdl

B.3 Virtual server Provisioning

The following parameters are required for adding virtual server and adding it to existing L-Platform:

VSYS_ID

Mandatory. The ID of the L-Platform to which the new virtual server is to be added. As for the L-Platform ID, get by copying to clipboard from the menu shown by right-clicking on the objective L-Platform on the Management page in L-Platform tab of ROR console.

Example: SampleTe-4LPKTS4KQ

DISKIMG_ID

Mandatory. The resource ID of the image information corresponding to the new virtual server.

Example: image-13c8a812d25

NETWORK_ID

Mandatory. The network ID of the segment where the new virtual server is to be added as for the network ID of the segment, execute GetLPlatformConfiguration and get from <networkId> tag. Refer to “ServerView Resource Orchestrator Cloud Edition Reference Guide (Command/XML)” included in ServerView Resource Orchestrator Cloud Edition in detail.

Example: 4LPKTS4KQ-N-2j0v

VSERVER_TYPE

Mandatory. A string describing the server type. The string must match available one in ROR. As for the server type, confirm from Configuration page of the L-Platform, or the output result of ListServerType. As for ListServerType, refer to “ServerView Resource Orchestrator Cloud Edition Reference Guide (Command/XML)” included in ServerView Resource Orchestrator Cloud Edition in detail.

Example: medium

COUNT_CPU

Optional. The number of CPUs the virtual server is to have. Make sure that the administrator of customer organization can only specify the same or smaller number than the max CPU number specified in corresponding image information. This can be done, for example, by presenting the supported numbers as different parameter options.

Example: 4

VM_POOL

Optional. The VM pool to be used for the new virtual server in ROR. As for VM pool, refer to the Template Builder menu Template tab of ROR console.

Default: VMHostPool

STORAGE_POOL

Optional. The storage pool to be used for the new virtual server in ROR. As for storage pool, refer to the Template Builder menu Template tab of ROR console.

Default: StoragePool

Appendix C Command for Creating Technical Service Definition

This appendix explains how to create technical service definition for the service controller.

The technology provider in Systemwalker Service Catalog Manager registers the technical service created in this appendix, and then the supplier in Systemwalker Service Catalog Manager defines the marketable service based on the technical service definition in this appendix.



Note

As for the command for creating technical service definition, the scenario “Provisioning and scaling of L-Platform” is only supported.

Create technical service definition

In order to create the technical service definition for the service controller, execute following command:

[Windows]

```
%SWCTMG_HOME%\ror\bin\ror servicedef.bat [-t TEMPLATE] [-i SERVICE_ID] [-u URL] [-v VM] [-c CPU] [-o {on|off}] [-f FILE]
```

[Linux]

```
/opt/FJSVctbss/ror/bin/ror servicedef.sh [-t TEMPLATE] [-i SERVICE_ID] [-u URL] [-v VM] [-c CPU] [-o {on|off}] [-f FILE]
```

Table C.1 Parameter list of the command to create technical service definition for service controller

No.	Specified option	Parameter name	mandatory	Explanation
1	-t	TEMPLATE	No	Specify the path name of template file. When omitted, following file is used: [Windows] %SWCTMG_HOME%\ror\template\TechnicalService_VirtualPlatform.xml [Linux] /opt/FJSVctbss/ror/template/TechnicalService_VirtualPlatform.xml
2	-i	SERVICE_ID	No	Specify the ID of created technical service definition. When omitted, the value of template file is not changed and used.
3	-u	URL	No	Specify the protocol, host name and port number for the provisioning service of the service controller. As for the hostname, specify the host name of the server where APP was registered, as for the port number specify the HTTP listener port of APP domain. When omitted, the value of template file is not changed and used. Ex.: -u http://localhost:8880
4	-v	VM	No	Specify the number of VMs available as the parameter of marketable service, with the list style of numbers separated by commas. When omitted, the value of template file is not changed and used. Ex.: -v "2,4,6"
5	-c	CPU	No	Specify the number of CPUs available as the parameter of marketable service, with the list style of numbers separated by commas. When omitted, the value of template file is not changed and used. Ex.: -c "1,2,4"
6	-o	{on off}	No	Specify “on” or “off” whether the start/stop operations for L-Platform are activated. In case that “on” is specified, the operations are activated. In case that “off” is specified,

				<p>the operations are deactivated. In case that “-o” option is omitted, the value of template file is not changed and used.</p> <p>In case that the start/stop operations for L-Platform are activated, the value is used for the access protocol, hostname and port number which is specified in “-u” option. In case that “-u” option is not specified, “http://localhost:8880” is used.</p> <p>Example: -o on</p>
7	-f	FILE	No	Specify the path name of created technical service definition. When omitted, the contents of technical service definition file are displayed to standard output.

To display how to use the command to create the technical service definition for the service controller, execute following command:

[Windows]

```
rorservicedef.bat -h
```

[Linux]

```
rorservicedef.sh -h
```



Note

The “-k” and “-p” options which were provided in V15.3.0 are not required to specify after V15.3.1. After V15.3.1, the user key and password of the user of technology provider organization are specified in the setup command of ROR Integration feature, not the technical service definition file.

Register technical service definition and marketable service

Register the technical service definition and define marketable service based on the registered technical service definition. Refer to “Supplier’s Guide” and “Technology Provider’s Guide” for details.

Appendix D Example to Register the Service Controller

This appendix explains how to register the service controller with the actual example.

D.1 Prerequisites

This section explains following prerequisites for the example:

- Completion for install and setup CT-MG according to “Installation Guide”
- Using the recommended parameters for the install and setup
- Setting no password for the OS user for the database
- Technology manager role for the Operator

D.2 Registering technology Manager

This section explains how to register technology manager.

In the example in this appendix, the first operator organization and the user with operator user role are assumed to have the technology provider organization role and the technology manager role.

1. Log in to Admin Portal

Access to and log in Admin Portal as first operator.

For the first operator, following access information are assigned as initial values:

- User ID: administrator
- User key: 1000
- Initial password: admin123

To access to login page of Admin Portal, activate Web browser and specify following URL to its address:

`http://[server host name]:[port number]/fujitsu-bss-portal/`

2. Configure to technology provider

Add the role of technology provider to the operator organization.

Open the “Manage organization” page in “Operation” menu.

Input PLATFORM_OPERATOR to “Organization ID”.

Check the check box of technology provider in “Organization role” item.

Input the other required items.

Click “Save” button.

3. Add technology manager role to the operator user.

Open the “Manage users” in “Account” menu.

Choose user ID of “administrator” in “Select the user whose data you want to change:” item.

Check the check box of technology manager in “User role” item.

Input the other required items.

Click “Save” button.

D.3 Setup Example [Windows]

This section explains the setup example on Windows.

D.3.1 Configuring setting files

Change the items in the setting files which are required to change.

1. Change the setting file for the database

Open the following setting file with an editor:

```
%SWCTMG_HOME%\pgctbss\data\postgresql.conf
```

Add 50 to the existing value of “max_prepared_transactions” property.

Add 210 to the existing value of “max_connections” property.

Example:

```
max_prepared_transactions=100
max_connections=420
```

D.3.2 Executing setting commands

Execute the setting commands to setup APP and the service controller.

Execute following setting commands:

1. Stop and Start Systemwalker Service Catalog Manager

```
net stop "Systemwalker Service Catalog Manager Server"

net stop "Systemwalker Service Catalog Manager Indexer Server"

net stop "Systemwalker Service Catalog Manager DB Service"

net start "Systemwalker Service Catalog Manager DB Service"

net start "Systemwalker Service Catalog Manager Indexer Server"

net start "Systemwalker Service Catalog Manager Server"
```

2. Setup ROR Integration

```
%SWCTMG_HOME%\setup\swctmg_setupRORInteg Administrator User1234 8800 admin@example.com
SERVER001:8081 1000 admin123 PLATFORM_OPERATOR ctmg.ror ctmg.ror ctmgtenant server002:8014

%SWCTMG_HOME%\jdk7\bin\keytool -export -rfc -alias slas -keystore %SWCTMG_HOME%
\glassfish3\glassfish\domains\bes-domain\config\keystore.jks -file ctmgbss.crt -storepass
changeit

%SWCTMG_HOME%\jdk7\bin\keytool -import -file ctmgbss.crt -trustcacerts -alias ctmgbss -keystore
%SWCTMG_HOME%\glassfish3\glassfish\domains\app-domain\config\cacerts.jks -storepass changeit

del ctmgbss.crt

%SWCTMG_HOME%\jdk7\bin\keytool -list -keystore %SWCTMG_HOME%\glassfish3\glassfish\domains\app-
domain\config\cacerts.jks -storepass changeit

net stop "Systemwalker Service Catalog Manager APP Server"

net start "Systemwalker Service Catalog Manager APP Server"
```



Note

Refer to “[3.2.1 Setup](#)” in detail for the parameters specified for execution of swctmg_setupRORInteg command.

The password required to input in executing “asadmin” command is specified as the following initial value of item “glassfish.app.domain.admin.pwd” in setting file for the domain for APP “glassfish.properties”.

- User1234

D.3.3 Importing ROR Server Certification

It is required to import the server certification of ROR to the truststore in app-domain so that the communication between the service controller and ROR is done.

To import the certification, refer to “4.2 Importing and Confirming ROR Server Certification”.

D.4 Setup Example [Linux]

This section explains the setup example on Linux.

D.4.1 Configuring setting files

Change the items in the setting files which are required to change.

Open the following setting file with an editor:

1. Change the setting file for the database

Open the following setting file with an editor:

```
/var/opt/FJSVctbss/pgsql/data/postgresql.conf
```

Add 50 to the existing value of “max_prepared_transactions” property.

Add 210 to the existing value of “max_connections” property.

Example:

```
max_prepared_transactions=100  
max_connections=420
```

D.4.2 Executing setting commands

Execute the setting commands to setup APP and the service controller.

Execute following setting commands:

1. Stop and Start Systemwalker Service Catalog Manager

```
service swctmgserver stop  
  
service swctmgindexer stop  
  
/opt/FJSVctbss/bin/swctmg_stopdb.sh  
  
/opt/FJSVctbss/bin/swctmg_startdb.sh  
  
service swctmgindexer start  
  
service swctmgserver start
```

2. Setup ROR Integration

```
/opt/FJSVctbss/setup/swctmg_setupRORInteg.sh Administrator User1234 8800 admin@example.com  
SERVER001:8081 1000 admin123 PLATFORM_OPERATOR ctmg.ror ctmg.ror ctmgtenant server002:8014  
  
/opt/FJSVctbss/jdk7/bin/keytool -export -rfc -alias slas -keystore /opt/FJSVctbss/glassfish3/  
glassfish/domains/bes-domain/config/keystore.jks -file ctmgbss.crt -storepass changeit
```

```
/opt/FJSVctbss/jdk7/bin/keytool -import -file ctmgbss.crt -trustcacerts -alias ctmgbss -
keystore /opt/FJSVctbss/glassfish3/glassfish/domains/app-domain/config/cacerts.jks -storepass
changeit

rm ctmgbss.crt

/opt/FJSVctbss/jdk7/bin/keytool -list -keystore /opt/FJSVctbss/glassfish3/glassfish/domains/app-
domain/config/cacerts.jks -storepass changeit

service swctmgapp stop

service swctmgapp start
```

Note

Refer to “[3.2.1 Setup](#)” in detail for the parameters specified for execution of `swctmg_setupRORInteg` command.

The password required to input in executing “`asadmin`” command is specified as the following initial value of item “`glassfish.app.domain.admin.pwd`” in setting file for the domain for APP “`glassfish.properties`”.

- User1234

D.4.3 Importing ROR Server Certification

It is required to import the server certification of ROR to the truststore in app-domain so that the communication between the service controller and ROR is done with SSL.

To import the certification, refer to “[4.2 Importing and Confirming ROR Server Certification](#)”.

Appendix E Note on ROR to be Integrated

You need to configure the TLS/SSL communication settings of ServerView Operations Manager if the version of ServerView Operations Manager used by ROR is 6.10 or later. Follow the steps below to change the setting on the ROR server to be integrated.

Note

Please back up the files to be edited beforehand.

As for the file "standalone.xml", the content of it is to be changed to original contents. Change the file again after ServerView Operations Manager is restarted.

1. Stop manager of ServerView Resource Orchestrator.

Refer to the manual of ServerView Resource Orchestrator for how to stop the manager.

2. Edit following file.

[Windows]

```
<ServerView Suite installation folder>\jboss\standalone\configuration\standalone.xml
```

[Linux]

```
/opt/fujitsu/ServerViewSuite/jboss/standalone/configuration/standalone.xml
```

Look up the XML section <subsystem xmlns="urn:jboss:domain:web:1.1" ...>, and add there the attribute cipher-suite to the XML tag <ssl ...> as follows.

[Before change]

```
<subsystem xmlns="urn:jboss:domain:web:1.1" default-virtual-server="default-host"
native="false">
  <configuration>
    <jsp-configuration x-powered-by="false" display-source-fragment="false"/>
  </configuration>
  <connector name="http" protocol="HTTP/1.1" scheme="http" socket-binding="http"/>
  <connector name="https" protocol="HTTP/1.1" scheme="https" socket-binding="https"
secure="true">
    <ssl name="https" password="changeit" certificate-key-file="../standalone/svconf/pki/
keystore" verify-client="false"/>
  </connector>
  <virtual-server name="default-host" enable-welcome-root="false"/>
</subsystem>
```

[After change]

```
<subsystem xmlns="urn:jboss:domain:web:1.1" default-virtual-server="default-host"
native="false">
  <configuration>
    <jsp-configuration x-powered-by="false" display-source-fragment="false"/>
  </configuration>
  <connector name="http" protocol="HTTP/1.1" scheme="http" socket-binding="http"/>
  <connector name="https" protocol="HTTP/1.1" scheme="https" socket-binding="https"
secure="true">
    <connector name="https" protocol="HTTP/1.1" scheme="https" socket-binding="https"
secure="true">
      <ssl name="https" password="changeit" certificate-key-file="../standalone/svconf/pki/
keystore" cipher-
suite="TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,SSL_RSA_WITH_RC4_128_SHA,SS
L_RSA_WITH_3DES_EDE_CBC_SHA,SSL_RSA_WITH_RC4_128_MD5,TLS_EMPTY_RENEGOTIATION_INFO_SCSV,TLS_RSA_
WITH_NULL_SHA256,SSL_RSA_WITH_NULL_SHA,SSL_RSA_WITH_DES_CBC_SHA,SSL_RSA_WITH_NULL_MD5,SSL_RSA_E
XPORT_WITH_RC4_40_MD5,SSL_RSA_EXPORT_WITH_DES40_CBC_SHA,TLS_KRB5_WITH_RC4_128_SHA,TLS_KRB5_WITH
```

```

    RC4_128_MD5,TLS_KRB5_WITH_3DES_EDE_CBC_SHA,TLS_KRB5_WITH_3DES_EDE_CBC_MD5,TLS_KRB5_WITH_DES_CB
    C_SHA,TLS_KRB5_WITH_DES_CBC_MD5,TLS_KRB5_EXPORT_WITH_RC4_40_SHA,TLS_KRB5_EXPORT_WITH_RC4_40_MD5
    ,TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA,TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5" verify-client="false"/
>
    </connector>
    <virtual-server name="default-host" enable-welcome-root="false"/>
</subsystem>

```

3. Edit following file.

[Windows]

```
<ServerView Suite installation folder>\opends\config\schema\02-config.ldif
```

[Linux]

```
/opt/fujitsu/ServerViewSuite/opends/config/schema/02-config.ldif
```

Change the objectclasses declaration ds-cfg-administration-connector so that May line looks like this:

[Before change]

```

objectClasses: ( 1.3.6.1.4.1.26027.1.2.183
  NAME 'ds-cfg-administration-connector'
  SUP top
  STRUCTURAL
  MUST ( cn $
    ds-cfg-listen-port $
    ds-cfg-key-manager-provider $
    ds-cfg-trust-manager-provider $
    ds-cfg-ssl-cert-nickname )
  MAY ( ds-cfg-listen-address )
  X-ORIGIN 'OpenDS Directory Server' )

```

[After change]

```

objectClasses: ( 1.3.6.1.4.1.26027.1.2.183
  NAME 'ds-cfg-administration-connector'
  SUP top
  STRUCTURAL
  MUST ( cn $
    ds-cfg-listen-port $
    ds-cfg-key-manager-provider $
    ds-cfg-trust-manager-provider $
    ds-cfg-ssl-cert-nickname )
  MAY ( ds-cfg-listen-address )
  MAY ( ds-cfg-listen-address $ ds-cfg-ssl-cipher-suite $ ds-cfg-ssl-protocol )
  X-ORIGIN 'OpenDS Directory Server' )

```

4. Edit following file.

[Windows]

```
<ServerView Suite installation folder>\opends\config\config.ldif
```

[Linux]

```
/opt/fujitsu/ServerViewSuite/opends/config/config.ldif
```

Add the attributes ds-cfg-ssl-cipher-suite and ds-cfg-ssl-protocol to the entry cn=LDAPS Connection Handler,cn=Connection Handlers,cn=config as follows.

[Before change]

```

dn: cn=LDAPS Connection Handler,cn=Connection Handlers,cn=config
objectClass: ds-cfg-ldap-connection-handler

```

```
objectClass: top
objectClass: ds-cfg-connection-handler
ds-cfg-ssl-client-auth-policy: optional
ds-cfg-key-manager-provider: cn=JKS,cn=Key Manager Providers,cn=config
ds-cfg-ssl-cert-nickname: svcs_cms
ds-cfg-trust-manager-provider: cn=JKS,cn=Trust Manager Providers,cn=config
ds-cfg-max-blocked-write-time-limit: 2 minutes
ds-cfg-allow-tcp-reuse-address: true
ds-cfg-allow-start-tls: false
ds-cfg-send-rejection-notice: true
ds-cfg-allow-ldap-v2: true
cn: LDAPS Connection Handler
ds-cfg-use-tcp-no-delay: true
ds-cfg-enabled: true
ds-cfg-java-class: org.opens.server.protocols.ldap.LDAPConnectionHandler
ds-cfg-keep-stats: true
ds-cfg-max-request-size: 5 megabytes
ds-cfg-accept-backlog: 128
ds-cfg-buffer-size: 4096 bytes
ds-cfg-listen-address: 0.0.0.0
ds-cfg-num-request-handlers: 2
ds-cfg-listen-port: 1474
ds-cfg-use-ssl: true
ds-cfg-use-tcp-keep-alive: true
```

[After change]

```
dn: cn=LDAPS Connection Handler,cn=Connection Handlers,cn=config
objectClass: ds-cfg-ldap-connection-handler
objectClass: top
objectClass: ds-cfg-connection-handler
ds-cfg-ssl-client-auth-policy: optional
ds-cfg-key-manager-provider: cn=JKS,cn=Key Manager Providers,cn=config
ds-cfg-ssl-cert-nickname: svcs_cms
ds-cfg-trust-manager-provider: cn=JKS,cn=Trust Manager Providers,cn=config
ds-cfg-max-blocked-write-time-limit: 2 minutes
ds-cfg-allow-tcp-reuse-address: true
ds-cfg-allow-start-tls: false
ds-cfg-send-rejection-notice: true
ds-cfg-allow-ldap-v2: true
cn: LDAPS Connection Handler
ds-cfg-use-tcp-no-delay: true
ds-cfg-enabled: true
ds-cfg-java-class: org.opens.server.protocols.ldap.LDAPConnectionHandler
ds-cfg-keep-stats: true
ds-cfg-max-request-size: 5 megabytes
ds-cfg-accept-backlog: 128
ds-cfg-buffer-size: 4096 bytes
ds-cfg-listen-address: 0.0.0.0
ds-cfg-num-request-handlers: 2
ds-cfg-listen-port: 1474
ds-cfg-use-ssl: true
ds-cfg-ssl-cipher-suite: TLS_RSA_WITH_AES_128_CBC_SHA256
ds-cfg-ssl-cipher-suite: TLS_RSA_WITH_AES_128_CBC_SHA
ds-cfg-ssl-cipher-suite: SSL_RSA_WITH_RC4_128_SHA
ds-cfg-ssl-cipher-suite: SSL_RSA_WITH_3DES_EDE_CBC_SHA
ds-cfg-ssl-cipher-suite: SSL_RSA_WITH_RC4_128_MD5
ds-cfg-ssl-cipher-suite: TLS_EMPTY_RENEGOTIATION_INFO_SCSV
ds-cfg-ssl-cipher-suite: TLS_RSA_WITH_NULL_SHA256
ds-cfg-ssl-cipher-suite: SSL_RSA_WITH_NULL_SHA
ds-cfg-ssl-cipher-suite: SSL_RSA_WITH_DES_CBC_SHA
ds-cfg-ssl-cipher-suite: SSL_RSA_WITH_NULL_MD5
ds-cfg-ssl-cipher-suite: SSL_RSA_EXPORT_WITH_RC4_40_MD5
```

```
ds-cfg-ssl-cipher-suite: SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
ds-cfg-ssl-cipher-suite: TLS_KRB5_WITH_RC4_128_SHA
ds-cfg-ssl-cipher-suite: TLS_KRB5_WITH_RC4_128_MD5
ds-cfg-ssl-cipher-suite: TLS_KRB5_WITH_3DES_EDE_CBC_SHA
ds-cfg-ssl-cipher-suite: TLS_KRB5_WITH_3DES_EDE_CBC_MD5
ds-cfg-ssl-cipher-suite: TLS_KRB5_WITH_DES_CBC_SHA
ds-cfg-ssl-cipher-suite: TLS_KRB5_WITH_DES_CBC_MD5
ds-cfg-ssl-cipher-suite: TLS_KRB5_EXPORT_WITH_RC4_40_SHA
ds-cfg-ssl-cipher-suite: TLS_KRB5_EXPORT_WITH_RC4_40_MD5
ds-cfg-ssl-cipher-suite: TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA
ds-cfg-ssl-cipher-suite: TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5
ds-cfg-ssl-protocol: SSLv2Hello
ds-cfg-ssl-protocol: SSLv3
ds-cfg-ssl-protocol: TLSv1
ds-cfg-use-tcp-keep-alive: true
```

In the same configuration file, change the attribute `ds-cfg-listen-address` of the entry `dn: cn=Administration Connector,cn=config` as follows.

[Before change]

```
dn: cn=Administration Connector,cn=config
objectClass: ds-cfg-administration-connector
objectClass: top
ds-cfg-listen-address: 0.0.0.0
ds-cfg-listen-port: 4444
cn: Administration Connector
ds-cfg-key-manager-provider: cn=Administration,cn=Key Manager Providers,cn=config
ds-cfg-ssl-cert-nickname: svcs_cms
ds-cfg-trust-manager-provider: cn=Administration,cn=Trust Manager Providers,cn=config
```

[After change]

```
dn: cn=Administration Connector,cn=config
objectClass: ds-cfg-administration-connector
objectClass: top
ds-cfg-listen-address: 127.0.0.1
ds-cfg-listen-port: 4444
cn: Administration Connector
ds-cfg-key-manager-provider: cn=Administration,cn=Key Manager Providers,cn=config
ds-cfg-ssl-cert-nickname: svcs_cms
ds-cfg-trust-manager-provider: cn=Administration,cn=Trust Manager Providers,cn=config
```

- Restart ServerView Operations Manager by following command(s).

[Windows]

```
net stop "SVJBASSVC"
net start "SVJBASSVC"
```

[Linux]

```
/etc/init.d/sv_jboss restart
```

- Start manager of ServerView Resource Orchestrator.

Refer to the manual of ServerView Resource Orchestrator for how to start the manager.

Appendix F Setup in AML_SP Authenticate mode

This appendix explains how to setup ROR Integration feature in SAML_SP authentication mode.

F.1 Tasks before Setup

In case that you setup ROR Integration feature in SAML_SP authentication mode, you need to change the configuration settings for ROR Integration feature.

F.1.1 Changing Setting File

In case that SAML_SP authentication mode is used, the parameter value is required to change of setting file “app_configsettings.properties”. The setting file is registered in the subdirectory (setup) under “app” directory

Edit the files according to following procedure:

- Edit following file:

[Windows]

```
%SWCTMG_HOME%\setup\files\app_configsettings.properties
```

[Linux]

```
/opt/FJSVctbss/setup/files/app_configsettings.properties
```

The parameters to change the values are following:

- BSS_AUTH_MODE
- BSS_WEBSERVICE_URL_STS_PORT
- APP_KEYSTORE_PASSWORD
- APP_TRUSTSTORE_PASSWORD

Refer to “[Appendix A Configuration Settings for APP and Service Controller](#)” in detail for parameters.

F.1.2 Executing Setup Command

Execute setup command for ROR Integration feature. Refer to “[Chapter 3 Setup](#)” in detail.

F.2 Tasks After Setup

This section explains the tasks after setup.

F.2.1 Changing Configuration Settings

In case that you want to change the configuration settings for ROR Integration feature which are not described in “[Chapter 8 Modifying Settings](#)”, the procedure is following:

Edit configuration settings files

1. In case that you change APP settings, copy following file:

[Windows]

```
%SWCTMG_HOME%\setup\files\app_configsettings.properties
```

[Linux]

```
/opt/FJSVctbss/setup/files/app_configsettings.properties
```


The folder to copy is following:

[Windows]

```
%SWCTMG_HOME%\app\setup
```

[Linux]

```
/opt/FJSVctbss/app/setup
```

2. In case that you change service controller settings, copy following file:

[Windows]

```
%SWCTMG_HOME%\setup\files\app_org_configsettings_controller.properties
```

[Linux]

```
/opt/FJSVctbss/setup/files/app_org_configsettings_controller.properties
```

The folder to copy is following:

[Windows]

```
%SWCTMG_HOME%\app\setup\controller
```

[Linux]

```
/opt/FJSVctbss/app/setup/controller
```

3. Edit the copied file.

Add the parameter and its value to be changed. Excluding the `CONTROLLER_ID`, the parameters are not required to add which are not changed.

Refer to “[Appendix A Configuration Settings for APP and Service Controller](#)” in detail for parameters.

4. Change the name of copied file.

- `app_configsettings.properties` (Before): `configsettings.properties` (After)
- `app_org_configsettings_controller.properties` (Before): `configsettings_controller.properties` (After)

Execute commands

1. Make sure that the database is running.
2. Open the command prompt (Windows) or a terminal session (Linux).
3. Set the absolute path of “psql” as the environment variable “`DB_INTERPRETER`”: “psql” is the management command of database management system of CT-MG.

[Windows]

```
set DB_INTERPRETER=%SWCTMG_HOME%\fjsvp91_64\bin\psql.exe
```

[Linux]

```
export DB_INTERPRETER=/opt/FJSVctbss/fjsvp91/bin/psql
```

[Linux]

Set the library directory of database management system as the environment variable “`LD_LIBRARY_PATH`”: “`LD_LIBRARY_PATH`” is required for database management system to execute the management command for Linux only.

```
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/FJSVctbss/fjsvp91/lib
```

4. Specify the home directory of Java Development Kit (JDK) version 7 by environment variable.

[Windows]

```
set JAVA_HOME=%SWCTMG_HOME%\jdk7
```

[Linux]

```
export JAVA_HOME=/opt/FJSVctbss/jdk7
```

5. In case that you specified the password of OS user for database in setup for Systemwalker Service Catalog Manager, specify the password as the value of “-Ddb.admin.pwd” option. In case that you did not specify the password, drop the “-Ddb.admin.pwd” option. Refer to “Installation Guide” for detail of the password of OS user for database.
6. Update the configuration settings of APP by executing the build-db.xml file in the subdirectory (setup) under “app” directory as follows:

[Windows]

```
%SWCTMG_HOME%\ant\bin\ant -f %SWCTMG_HOME%\app\setup\build-db.xml updateConfigSettings -  
Ddb.admin.user=pgctbss -Ddb.admin.pwd=<the password of OS user for database specified in setup  
for Systemwalker Service Catalog Manager>
```

[Linux]

```
/opt/FJSVctbss/ant/bin/ant -f /opt/FJSVctbss/app/setup/build-db.xml updateConfigSettings -  
Ddb.admin.user=pgctbss -Ddb.admin.pwd=<the password of OS user for database specified in setup  
for Systemwalker Service Catalog Manager>
```

7. Update the configuration settings of service controller by executing the build-db.xml file in the subdirectory (setup) under “app” directory as follows:

[Windows]

```
%SWCTMG_HOME%\ant\bin\ant -f %SWCTMG_HOME%\app\setup\build-db.xml  
updateConfigSettingsController -Ddb.admin.user=pgctbss -Ddb.admin.pwd=<the password of OS user  
for database specified in setup for Systemwalker Service Catalog Manager>
```

[Linux]

```
/opt/FJSVctbss/ant/bin/ant -f /opt/FJSVctbss/app/setup/build-db.xml  
updateConfigSettingsController -Ddb.admin.user=pgctbss -Ddb.admin.pwd=<the password of OS user  
for database specified in setup for Systemwalker Service Catalog Manager>
```

8. Restarting app-domain is required in order to activate the changed value. Refer to “7.1 Start/Stop” in detail how to restart.