FUJITSU

# FUJITSU Software Enterprise Service Catalog Manager V16.0.0

# IaaS Integration Guide

Windows(64)

B1WS-1259-01ENZ0(00)
February 2016

# Preface

## Purpose of This Document

This document explains the introduction procedure of IaaS integration feature of Enterprise Service Catalog Manager V16.0.0.

The purpose of this manual is as follows:

- To learn to be able to introduce IaaS integration feature of Enterprise Service Catalog Manager

## Intended Readers

This document is intended for people who introduce IaaS integration feature of Enterprise Service Catalog Manager.

This document assumes that readers already have the following knowledge:

- Basic knowledge of the operating system being used.
- Basic knowledge of IaaS.

## Structure of This Document

This document is structured as follows:

Appendix F Setup in SAML_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 Enterprise Service Catalog Manager V16 as "Enterprise Service Catalog Manager", omitting "V16".

- 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 "Enterprise Service Catalog Manager V16" 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 Enterprise 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<br>Microsoft(R) Windows Server(R) 2008 Enterprise | Windows 2008 | Windows |
| Microsoft(R) Windows Server(R) 2012 Standard<br>Microsoft(R) Windows Server(R) 2012 Datacenter | Windows 2012 | |
| Microsoft(R) Windows Server(R) 2012 R2 Standard<br>Microsoft(R) Windows Server(R) 2012 R2 Datacenter | Windows 2012 R2 | |

## 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



.

## Issue Date and Version

| Edition | Manual code |
|---|---|
| First edition February 2016 | B1WS-1259-01ENZ0(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

# Contents

# Chapter 1 Abstract

## 1.1 Abstract of IaaS Integration Feature

IaaS integration feature provides feature of IaaS to be integrated as the services on Enterprise Service Catalog Manager (CT-MG). The services are based on the typical usage scenarios for the IaaS. The supported IaaS are followings:

- ServerView Resource Orchestrator
- Amazon Web Services (Amazon Elastic Compute Cloud)
- OpenStack (OpenStack Heat)
- FUJITSU Cloud IaaS Trusted Public S5

Refer to "Chapter 2 Usage Scenarios" for the scenarios that are supported by each IaaS and their details.

IaaS 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 of IaaS integration feature calls IaaS API and deploys instances.

The service controller of each IaaS integration feature runs on separate APP in CT-MG.

Before setup IaaS Integration, the authentication mode of users and Web service must be defined. IaaS 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 IaaS Integration in INTERNAL authentication mode.

Refer to "Appendix F Setup in SAML_SP Authenticate mode" in detail how to setup IaaS Integration in SAML_SP authentication mode.

After setup of IaaS Integration feature, by creating service working on CT-MG, IaaS integration feature is published to customer organizations. Refer to "Chapter 5 Creating and Publishing Service" for how to create and publish service.

## 1.2 ServerView Resource Orchestrator Integration Feature

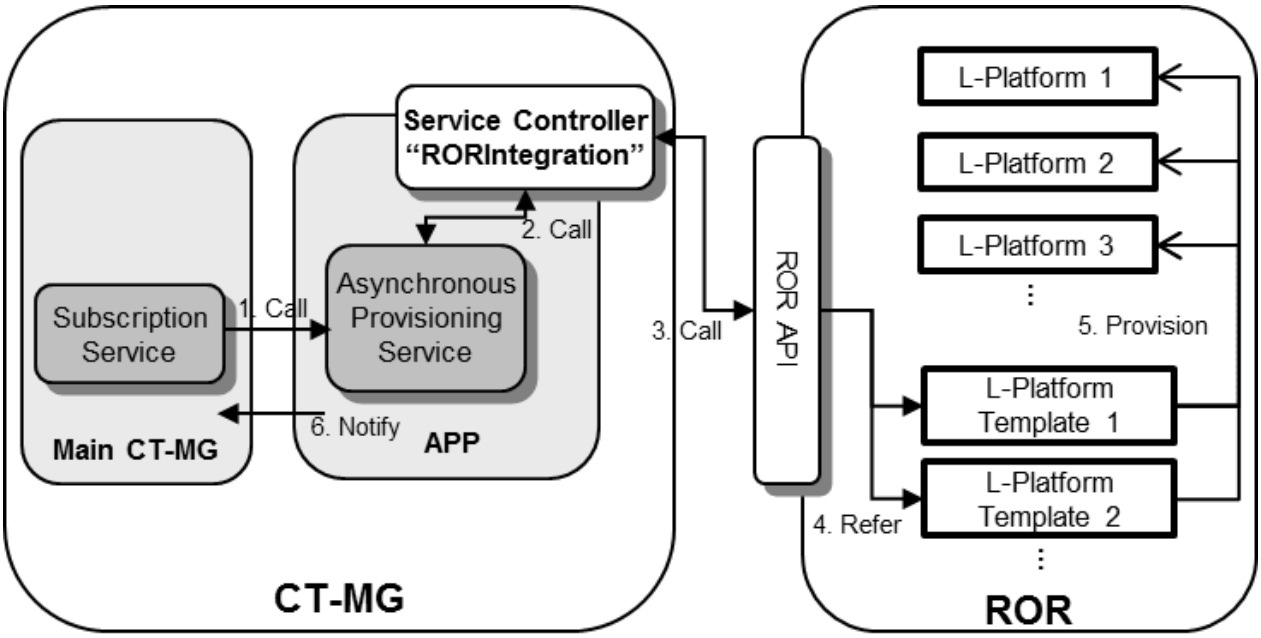
### 1.2.1 What is ServerView Resource Orchestrator Integration Feature

ServerView Resource Orchestrator (ROR) integration feature provides ROR feature as the services on Enterprise 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.

The service controller for ROR integration feature is "RORIntegration". "RORIntegration" executes the provisioning and scaling for L-Platform and virtual server.




## 1.2.2 Operating Condition of ROR Integration Feature

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

To use ROR Integration feature, install and set up Enterprise Service Catalog Manager with standalone configuration. In case of distributed database configuration, ROR Integration feature cannot be set up.

# 1.3 Amazon Web Services Integration Feature

## 1.3.1 What is Amazon Web Services Integration Feature

Amazon Web Services (AWS) integration feature provides AWS feature as the services on Enterprise Service Catalog Manager (CT-MG). The services are based on the typical usage scenarios for AWS. The supported scenarios are followings:

- Provisioning of Amazon EC2 instance
- Start and stop for Amazon EC2 instance
- Automatic execution of user-specific configuration data
- Termination for Amazon EC2 instance

Refer to "Chapter 2 Usage Scenarios" for the detailed scenarios.

The service controller for AWS integration feature is "AWSIntegration". "AWSIntegration" executes AWS API to provision Amazon EC2 instance.

## 1.3.2 Operating Condition of AWS Integration Feature

To use AWS Integration feature, install and set up Enterprise Service Catalog Manager with standalone configuration. In case of distributed database configuration, AWS Integration feature cannot be set up.

# 1.4 OpenStack Integration Feature

## 1.4.1 What is OpenStack Integration Feature

OpenStack integration feature provides OpenStack feature as the services on Enterprise Service Catalog Manager (CT-MG). The services are based on the typical usage scenarios for OpenStack. The supported scenarios are followings:

- Provisioning of Stack
- Start and stop for Stack
- Termination for Stack

Refer to "Chapter 2 Usage Scenarios" for the detailed scenarios.

The service controller for OpenStack integration feature is "OSIntegration". "OSIntegration" executes OpenStack Heat API to provision Stack.

## 1.4.2 Operating Condition of OpenStack Integration Feature

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

- Release version
  - Icehouse
- API version of components
  - Keystone: OpenStack Identity API v2.0
  - Heat: OpenStack Orchestration API v1.0

To use OpenStack Integration feature, install and set up Enterprise Service Catalog Manager with standalone configuration. In case of distributed database configuration, OpenStack Integration feature cannot be set up.

# 1.5 FUJITSU Cloud IaaS Trusted Public S5 Integration Feature

## 1.5.1 What is FUJITSU Cloud IaaS Trusted Public S5 Integration Feature

FUJITSU Cloud IaaS Trusted Public S5 (TPS5) integration feature provides TPS5 feature as the services on Enterprise Service Catalog Manager (CT-MG). The services are based on the typical usage scenarios for TPS5. The supported scenarios are followings:

- Provisioning of virtual system
- Adding and reducing of virtual server by reconfiguration
- Changing of CPU number of each virtual server by reconfiguration
- Start and stop for virtual system
- Unsubscribing of virtual system

Refer to "Chapter 2 Usage Scenarios" for the detailed scenarios.

The service controller for TPS5 integration feature is "TPS5Integration". "TPS5Integration" executes TPS5 API to provisionvirtualsystem.

## 1.5.2 Operating Condition of TPS5 Integration Feature

To use TPS5 Integration feature, install and set up Enterprise Service Catalog Manager with standalone configuration. In case of distributed database configuration, TPS5 Integration feature cannot be set up.

Note

TPS5 Integration feature which is explained in this section cannot be used.

The TPS5 libraries that you download from the FUJITSU Cloud IaaS Trusted Public S5 Service Portal and be integrated in the TPS5 service controller installation environment before installing the TPS5 integration package do not work properly. Request the valid libraries from your FUJITSU support organization.

# Chapter 2 Usage Scenarios

## 2.1 Usage Scenarios of ROR Integration Feature

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 server s 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.

## 2.2 Usage Scenarios of AWS Integration Feature

Amazon Web Services (AWS) is a collection of remote computing services that together make up a Cloud computing platform offered by Amazon. Amazon Elastic Compute Cloud (Amazon EC2) is one of the central Web services of AWS. It provides computing capacities in the Cloud and allows you to quickly scale these capacities as your computing requirements change.

Amazon EC2 allows customers to provision and use virtual servers on which to run their applications. Each virtual server is based on an Amazon Machine Image (AMI). An AMI serves as the basic unit of deployment for services delivered with Amazon EC2. AWS customers can either request pre-configured AMIs or they can create their own images. They can provision their images with a variety of operating systems and load them with custom application environments.

The integration of AWS with CT-MG provides for an Infrastructure as a Service (IaaS) solution that leverages the features of both products: Through services, which are published on a marketplace in CT-MG, users can request and use virtual servers in Amazon EC2. The usage costs can be calculated and charged by means of the CT-MG billing and payment services.

The AWSIntegration service controller provides for a basic integration feature of AWS 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 Amazon EC2 instance**: This scenario is to create EC2 instance for customer organization using AMI created on AWS. Technology provider/Supplier organizations create and publish the technical service definition/marketable service in order to create EC2 instance based on the AMI. When an administrator of customer organization subscribes to the published service, the name of EC2 instance can be specified as the parameter of the service. When an administrator of customer organization subscribes to the service, AWS creates the EC2 instance based on the specified AMI through the service controller. If the steps to create the EC2 instance are completed successfully, the EC2 instance is ready to use for the customer.
- **Start and stop for Amazon EC2 instance**: This scenario is to start/stop EC2 instance which is subscribed by customer organization. After customer organization subscribes the service based on the provisioning of EC2 instance scenario and assigns the user to the subscription, and then the user is ready to start/stop EC2 instance through marketplace portal.
- **Automatic execution of user-specific configuration data**: When a customer subscribes to a corresponding service on a CT-MG marketplace, he has the option of passing user-specific configuration data to the Amazon EC2 instance to be provisioned. The data can be used to modify the static information defined in the underlying AMI. Thus, the customer can, for example, perform automated configuration tasks or run scripts.
- **Termination for Amazon EC2 instance**: This scenario is to terminate EC2 instance subscribed by customer organization. When the customer terminates the subscription for EC2 instance, AWS terminates the EC2 instance through the service controller. The subscription is terminated independent on whether this is successful.

The service controller informs its responsible technology provider organization by email of any incomplete provisioning or delete operation in AWS.

In AWS, the EC2 instances created for CT-MG subscriptions are managed in the same way as other EC2 instance. They can be viewed and monitored with the standard AWS tools.

Modifying a subscription and thereby triggering modifications of the EC2 instance in AWS is not supported.

Note

In the scenario "Start and stop for Amazon EC2 instance", when restarting EC2 instance, access information including IP address is automatically changed. After restarting EC2 instance, connect to the EC2 instance based on the updated access information shown in [My subscriptions] menu on service portal.

## 2.3 Usage Scenarios of OpenStack Integration Feature

OpenStack is an open-source cloud operating system that controls large pools of processing, storage, and networking resources throughout a data center.

OpenStack allows users to deploy virtual systems which handle different tasks for managing a cloud environment. It makes horizontal scaling easy, which means that tasks which benefit from running concurrently can easily serve users by spinning up more resources. For example, a mobile application which needs to communicate with a remote server might be able to divide the work of communicating with each user across many different resources, all communicating with one another but scaling quickly and easily as the application gains more users.

OpenStack includes the orchestration component, which is called as "Heat". OpenStack Heat offers template-based mechanisms for describing cloud applications. Through both an OpenStack ReST API and a CloudFormation-compatible Query API, Heat provides Heat Orchestration Template (HOT) and compatibility with existing template formats, for example with the AWS CloudFormation (CFN) template format. The flexible template format of OpenStack enables application developers to describe and automate the deployment of infrastructure, services, and applications. Collections of resources (e.g. networks, servers, or storage) can be deployed from a single template. The template serves as an orchestration document that details everything needed to carry out the orchestration. Once instantiated, the resources are also referred to as stacks.

As for this template file, OpenStack Integration feature supports JSON format which is described with CFN compatible style, and YAML format which is described with HOT style.

The integration of OpenStack with CT-MG provides for an Infrastructure as a Service (IaaS) solution that leverages the features of both products: Through services, which are published on a marketplace in CT-MG, users can request and use virtual systems in OpenStack. The usage costs can be calculated and charged by means of the CT-MG billing and payment services.

The OSIntegration service controller provides for a basic integration feature of OpenStack Heat 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 Stack:** This scenario is to create Stack for customer organization using a Heat template. Technology provider/Supplier organizations create and publish the technical service definition/marketable service in order to create Stack based on the Heat template. When an administrator of customer organization subscribes to the published service, the name of Stack can be specified as the parameter of the service. When an administrator of customer organization subscribes to the service, OpenStack Heat creates the Stack based on the specified template through the service controller. If the steps to create the Stack are completed successfully, the Stack and its virtual machines are ready to use for the customer.
- **Start and stop for Stack:** This scenario is to start/stop Stack which is subscribed by customer organization. After customer organization subscribes the service based on the provisioning of Stack scenario and assigns the user to the subscription, and then the user is ready to start/stop Stack through marketplace portal.
- **Termination for Stack:** This scenario is to terminate Stack subscribed by customer organization. When the customer terminates the subscription for Stack, OpenStack terminates the Stack through the service controller. The subscription is terminated independent on whether this is successful.

The service controller informs its responsible technology provider organization by email of any incomplete provisioning or delete operation in OpenStack.

In OpenStack, the Stack created for CT-MG subscriptions are managed in the same way as other Stack. They can be viewed and monitored with the standard OpenStack dashboard.

Modifying a subscription and thereby triggering modifications of the Stack in OpenStack is not supported.

## 2.4 Usage Scenarios of TPS5 Integration Feature

FUJITSU Cloud IaaS Trusted Public S5 (TPS5) gives you on-demand access to a shared pool of virtual, fully configured server, storage, and network resources hosted in FUJITSU's global network of data centers. The provisioning of computing resources in the Cloud allows you to rapidly scale and flex your infrastructure to support new business initiatives or roll out services.

On virtual systems, users can, for example, request specific servers and operating systems, firewalls, load balancers, middleware services or databases. Servers can be added and removed dynamically as required.

The integration of TPS5 with CT-MG provides for an Infrastructure as a Service (IaaS) solution that leverages the features of both products: Through services, which are published on a marketplace in CT-MG, users can request and use virtual systems in TPS5. The usage costs can be calculated and charged by means of the CT-MG billing and payment services.

The TPS5Integration service controller provides for a basic integration feature of TPS5 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 virtual system:** This scenario is to create virtual system for customer organization using system template created on TPS5 previously. TPS5 resource administrator previously creates the system template on TPS5, and technology provider/supplier organizations create and publish the technical service definition/marketable service in order to create virtual system based on the system template created previously. When an administrator of customer organization subscribes to the published service, the virtual system name can be specified as the parameter of the service. When an administrator of customer organization subscribes to the service, TPS5 creates the virtual system based on the system template through the service controller. If the steps to create the virtual system are completed successfully, the virtual system 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 virtual system subscribed by the customer. By changing the corresponding parameters in the existing subscription by the administrator of customer organization, TPS5 adds/reduces the number of virtual servers to/from their virtual system 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 type of virtual server by reconfiguration:** This scenario is to change the type to the virtual servers added by the customer. By changing the corresponding parameters in an existing subscription by an administrator of customer organization, TPS5 changes the type to each virtual server through the service controller. If all steps to change the type are completed successfully, the virtual servers are ready to use based on the changed parameters.
- **Start and stop for virtual system:** This scenario is to start/stop virtual servers in virtual system which is subscribed by customer organization. After customer organization subscribes the service based on the provisioning of virtual system scenario and assigns the user to the subscription, and then the user is ready to start/stop virtual servers in virtual system through marketplace portal.
- **Unsubscribing of virtual system:** This scenario is to unsubscribe virtual system subscribed by customer organization. When the customer terminates the subscription for virtual system, TPS5 unsubscribes the virtual system through the service controller. The subscription is terminated independent on whether this is successful.

If an operation fails on the TPS5 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 TPS5.

In TPS5, the virtual systems and servers created for CT-MG subscriptions are managed in the same way as other TPS5 and virtual servers. They can be viewed and monitored with the standard TPS5 tools.

# Chapter 3 Setup

This chapter explains how to setup IaaS 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 for ROR Integration Feature".

## 3.1 Prerequisites and Preparation

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

### 3.1.1 Install and setup CT-MG

IaaS 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.
- Check that the connection is allowed between main domain of CT-MG and APP domain of IaaS Integration. It is necessary to set required communication be allowed in the security software and firewall. Refer to "3.2.2 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

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

#### Configure Settings

Confirm the following files:

[Windows]

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

Confirm and modify the parameters according to the following process:

1. Confirm the value (default: 210) of "max_connections" property.

   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".

   Example: in case to modify to "300"

```
max_connections=300
```

2. Save the files.
3. 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"..

**Note**

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

## 3.1.3 SMTP Server

IaaS 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, IaaS 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 IaaS Integration must be checked before executing IaaS Integration setup command.

Configuration settings file "db.properties" is saved in following directory.

[Windows] %FSCTMG_HOME%\app\setup\databases\app_db

- db.properties: the file to register configuration settings for setting up and accessing to database

  The values of db.url and db.port are specified with those in CT-MG setting up, and they have to be same as the database port number of CT-MG. In case that the database port number was changed after setting up CT-MG, specify the port number after changed.

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

**Point**

The described "setup" folder in this section is for ROR Integration feature. In case that AWS and OpenStack Integration feature are used, please replace "setup" folder as following:

[Windows]

%FSCTMG_HOME%\app\setup (ROR), %FSCTMG_HOME%\app\setupaws (AWS), %FSCTMG_HOME%\app\setupos (OpenStack), %FSCTMG_HOME%\app\setups5 (TPS5)

Also, in the above db.url, "bssapp" is for ROR Integration. In case of using AWS, OpenStack and TPS5 Integration feature, please replace "bssawsapp", "bssosapp" and "bsss5app".

Following three setting files are registered in following directory:

[Windows] %FSCTMG_HOME%\setup\files

- 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%/oscm-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

  In case of using ROR Integration feature, 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.

- 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.

In case that you specified the password of OS user for database in setup for CT-MG, specify the password as the environmental variable "FSCTMG_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 Prerequisites

This subsection explains prerequisites for setting up ROR Integration feature.

- 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.

## 3.2.2 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.

3. Execute the setup command for ROR Integration.

   [Windows]

```
%FSCTMG_HOME%\setup\fsctmg_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>
```

   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.<br><br>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.<br><br>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.<br><br>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 operation of APP used for each IaaS integration feature.<br><br>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>".<br><br>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 |

| No. | Parameter name | Mandatory | Explanation |
|---|---|---|---|
| | | | key of administrator in the organization which is registered to CT-MG.<br>Example: 10000 |
| 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.<br>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 IaaS integration feature. Specify the organization ID where the technology manager of BSS_USER_KEY belongs.<br>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.<br>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.<br>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.<br>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 "4.3.3 Confirming the Server Information of Certification".<br>Specify this parameter according to the form, "<hostname>:<port number (default: 8014)>".<br>Example: server002:8014 |

Example:

[Windows]

```
%FSCTMG_HOME%\setup\fsctmg_setupRORInteg 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.

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

### Start the setup

Following message will be displayed when setup procedure starts.

```
fsctmg_setup: INFO: 141: Enterprise Service Catalog Manager ROR Integration setup start.
```

### Confirm the completion

Following message will be displayed when setup procedure completes.

```
fsctmg_setup: INFO: 143: Enterprise 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

After executing the setup command of IaaS Integration feature, each APP and service controller are deployed for each IaaS to be integrated. So, technology provider to manage IaaS Integration feature can be changed by each IaaS.

When you failed to execute setup command, please handle according to the message displayed on command prompt and shown in the following log files, where <target IaaS> is one of ROR, AWS, or OS:

- General setup for IaaS integration feature: fsctmg_setup<target IaaS>Integ.log
- Database setup for IaaS integration feature: build-db-ant_<target IaaS>Integ.log
- Java EE execution environment setup for IaaS integration feature: build-glassfish-setup-ant_<target IaaS>Integ.log

The registered folder of above log files are following.

[Windows] %FSCTMG_HOME%\logs

# 3.3 Setup for AWS Integration

This section explains how to setup AWS 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 "FSCTMG_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.

## 3.3.1 Prerequisites

This subsection explains prerequisites for setting up AWS Integration feature.

- As technology manager for managing service controller, AWS account (access key ID and secret access key) is prepared.

## 3.3.2 Setup

This subsection explains the procedure to setup AWS Integration.

### Executing setup command

Execute following procedure:

1. Log in as the OS administrator.

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

2. Open the command prompt.

3. Execute the setup command for AWS Integration.

   [Windows]

```
%FSCTMG_HOME%\setup\fsctmg_setupAWSInteg <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>
```

   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 3.2 AWS Integration Setup Parameter List

| No. | Parameter name | Mandatory | Explanation |
|---|---|---|---|
| 1 | AS_APP_ADMIN_USER | Yes | Refer to the parameter list in "3.2.2 Setup". |
| 2 | AS_APP_ADMIN_PASSWORD | Yes | |
| 3 | AS_APP_BASE_PORT | Yes | |
| 4 | APP_ADMIN_MAIL_ADDRESS | Yes | |
| 5 | BSS_WEBSERVICE_HOST_PORT | Yes | |
| 6 | BSS_USER_KEY | Yes | |
| 7 | BSS_USER_PWD | Yes | |
| 8 | BSS_ORGANIZATION_ID | Yes | |

Example:

[Windows]

```
%FSCTMG_HOME%\setup\fsctmg_setupAWSInteg Administrator User1234 8800 admin@example.com
SERVER001:8081 10000 admin123 ca4cbd74
```

Note

Refer to the Note in "3.2.2 Setup".

### 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.

```
fsctmg_setup: INFO: 149: Are you sure you want to start setup Enterprise Service Catalog Manager AWS
Integration? (y/n)[n]
```

### Start the setup

Following message will be displayed when setup procedure starts.

```
fsctmg_setup: INFO: 152: Enterprise Service Catalog Manager AWS Integration setup start.
```

### Confirm the completion

Following message will be displayed when setup procedure completes.

```
fsctmg_setup: INFO: 154: Enterprise Service Catalog Manager AWS 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

Refer to the Reference in "3.2.2 Setup".

## 3.4 Setup for OpenStack Integration

This section explains how to setup OpenStack 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 "FSCTMG_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.

### 3.4.1 Prerequisites

This subsection explains prerequisites for setting up OpenStack Integration feature.

- A fully functional OpenStack installation must be available.

- In OpenStack, a tenant must be created for CT-MG technology provider. And, the resource configuration accessible for this tenant, introduction of user must be completed.
- Heat template provided by this product does not specify the subnet. In case to use Heat template of this product without changing, make the one subnet of the OpenStack project to be integrated. In case to use multiple subnets of the OpenStack project to be integrated, change the technical service definition and Heat template, so that the subnet can be specified.
- In case that OpenStack to be integrated was built by "pacstack" command, confirm that the port of OpenStack Heat is allowed to communicate with iptables.
- In case that OpenStack to be integrated was built by "pacstack" command, confirm that the configuration settings are adapted for which the traffic of floating IP range (172.24.4.224/28) flows to the bridge (br-ex) connecting to public network.
- As for the Heat template provided by this product, it assigns public IP with EIP, so default pool must be specified. Add (comment-out) following items in "/etc/nova/nova.conf" of OpenStack environment to be integrated. After changing "/etc/nova/nova.conf" file, restart openstack-nova-api and openstack-nova-compute.

  Default_floating_pool=<pool name>
- As for the Heat template to provision Stack, OpenStack Integration feature supports JSON format which is described with AWS CloudFormation (CFN) style, and YAML format which is described with HOT style.

## 3.4.2 Setup

This subsection explains the procedure to setup OpenStack Integration.

### Executing setup command

Execute following procedure:

1. Log in as the OS administrator.

   Log in as the OS administrator to the server where OpenStack Integration feature is setup.
2. Open the command prompt.
3. Execute the setup command for OpenStack Integration.

   [Windows]

```
%FSCTMG_HOME%\setup\fsctmg_setupOSInteg <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> <API_USER_NAME> <API_USER_PWD> <KEYSTONE_API_URL>
<TENANT_NAME> <TEMPLATE_BASE_URL>
```

   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 3.3 OpenStack Integration Setup Parameter List

| No. | Parameter name | Mandatory | Explanation |
|---|---|---|---|
| 1 | AS_APP_ADMIN_USER | Yes | Refer to the parameter list in "3.2.2 Setup". |
| 2 | AS_APP_ADMIN_PASSWORD | Yes | |
| 3 | AS_APP_BASE_PORT | Yes | |
| 4 | APP_ADMIN_MAIL_ADDRESS | Yes | |
| 5 | BSS_WEBSERVICE_HOST_PORT | Yes | |
| 6 | BSS_USER_KEY | Yes | |
| 7 | BSS_USER_PWD | Yes | |
| 8 | BSS_ORGANIZATION_ID | Yes | |

| No. | Parameter name | Mandatory | Explanation |
|---|---|---|---|
| 9 | API_USER_NAME | Yes | The user name to be used to access the tenant for your organization in OpenStack. Once authenticated, this user is authorized to access the Heat API.<br>The user must have the necessary credentials to create and configure virtual systems for the tenant.<br>Example: demo |
| 10 | API_USER_PWD | Yes | The password of the user ID in OpenStack. Specify the password of OpenStack user specified in API_USER_NAME.<br>Example: demo1234 |
| 11 | KEYSTONE_API_URL | Yes | The URL of the Keystone API that is used for authenticating the user name specified in API_USER_NAME. Keystone is the identity service used by OpenStack. Specify the hostname or IP address, port number and version of Keystone API endpoint.<br>Example: http://openstackserver:5000/v2.0 |
| 12 | TENANT_NAME | Yes | The tenant name of OpenStack. Specify the tenant name to which the user specified in "API_USER_NAME" belongs. This tenant name corresponds to "Project name" on OpenStack dashboard.<br>Example: demo |
| 13 | TEMPLATE_BASE_URL | Yes | The URL of directory leading to the Heat templates that are specified in technical service definitions. The file names of the templates to be used are specified when customers subscribe to a corresponding service on CT-MG marketplace. The Heat template files must be registered in the directory, which is specified as this parameter.<br>Example: http://openstackserver:8000/templates/ |

Example:

[Windows]

```
%FSCTMG_HOME%\setup\fsctmg_setupOSInteg Administrator User1234 8800 admin@example.com SERVER001:8081
10000 admin123 ca4cbd74 demo demo1234 http://openstackserver:5000/v2.0 demo http://openstackserver:
8000/templates/
```

Note

Refer to the Note in "3.2.2 Setup".

### 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.

```
fsctmg_setup: INFO: 160: Are you sure you want to start setup Enterprise Service Catalog Manager
OpenStack Integration? (y/n)[n]
```

### Start the setup

Following message will be displayed when setup procedure starts.

```
fsctmg_setup: INFO: 163: Enterprise Service Catalog Manager OpenStack Integration setup start.
```

#### Confirm the completion

Following message will be displayed when setup procedure completes.

```
fsctmg_setup: INFO: 165: Enterprise Service Catalog Manager OpenStack 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

Refer to the Reference in "3.2.2 Setup".

## 3.5 Setup for TPS5 Integration

This section explains how to setup TPS5 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 "FSCTMG_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.

### 3.5.1 Prerequisites

This subsection explains prerequisites for setting up TPS5 Integration feature.

- As technology manager for managing service controller, TPS5 account and his account certification are prepared.
- In TPS5, a resource administrator must be created for CT-MG technology provider. And, the creation of system template and image must be completed.
- Download TPS5 API Library from TPS5 service portal. And then, copy the TPS5 API library of the OViSS_JAVASDK/lib directory to the "applib" subdirectory of the "<CT-MG installation directory>/app/setups5/domains/app_domain" directory.
- Save the account certification to call TPS5 API in the server where TPS5 Integration is set up. The directory to save must be named with alphanumeric characters and slash, excluding space, double and single quotations.

### 3.5.2 Setup

This subsection explains the procedure to setup TPS5 Integration.

#### Executing setup command

Execute following procedure:

1. Log in as the OS administrator.

   Log in as the OS administrator to the server where TPS5 Integration feature is setup.

2. Open the command prompt.

3. Execute the setup command for TPS5 Integration.

   [Windows]

```
%FSCTMG_HOME%\setup\fsctmg_setupS5Integ <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_LOCALE> <IAAS_API_URI> <IAAS_API_KEYSTORE_TYPE>
<IAAS_API_KEYSTORE_PASS> <IAAS_API_KEYSTORE>
```

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 3.4 TPS5 Integration Setup Parameter List

| No. | Parameter name | Mandatory | Explanation |
|---|---|---|---|
| 1 | AS_APP_ADMIN_USER | Yes | Refer to the parameter list in "3.2.2 Setup". |
| 2 | AS_APP_ADMIN_PASSWORD | Yes | |
| 3 | AS_APP_BASE_PORT | Yes | |
| 4 | APP_ADMIN_MAIL_ADDRESS | Yes | |
| 5 | BSS_WEBSERVICE_HOST_PORT | Yes | |
| 6 | BSS_USER_KEY | Yes | |
| 7 | BSS_USER_PWD | Yes | |
| 8 | BSS_ORGANIZATION_ID | Yes | |
| 9 | IAAS_API_LOCALE | ○ | The locale to be used for accessing TPS5 API. Specify the locale of TPS5 ("en" or "ja").<br>Example: en |
| 10 | IAAS_API_URI | ○ | The URL of TPS5 API. Specify the URL of integrating region of TPS5.<br>Example: https://api.oviss.jp.fujitsu.com/ovissapi/endpoint |
| 11 | IAAS_API_KEYSTORE_TYPE | ○ | Spefify the file type of TPS5 account certification to call TPS5 API.<br>Example: pkcs12 |
| 12 | IAAS_API_KEYSTORE_PASS | ○ | Spefify the password of TPS5 account certification to call TPS5 API<br>Example: User12345789012 |
| 13 | IAAS_API_KEYSTORE | ○ | Spefify the directory where TPS5 account certification to call TPS5 API with the full path.<br>Example: C:/Users/Administrator/UserCert.p12 |

Example:

[Windows]

```
%FSCTMG_HOME%\setup\fsctmg_setupS5Integ Administrator User1234 8800 admin@example.com SERVER001:8081
10000 admin123 ca4cbd74 en https://api.oviss.jp.fujitsu.com/ovissapi/endpoint pkcs12 User12345789012
C:/Users/Administrator/UserCert.p12
```

Note

Refer to the Note in "3.2.2 Setup".

### 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.

```
fsctmg_setup: INFO: 171: Are you sure you want to start setup Enterprise Service Catalog Manager TPS5
Integration? (y/n)[n]
```

### Start the setup

Following message will be displayed when setup procedure starts.

```
fsctmg_setup: INFO: 172: Enterprise Service Catalog Manager TPS5 Integration setup start.
```

### Confirm the completion

Following message will be displayed when setup procedure completes.

```
fsctmg_setup: INFO: 174: Enterprise Service Catalog Manager TPS5 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**

Refer to the Reference in "3.2.2 Setup".

# 3.6 Tasks after Setup

This section explains the tasks after setup of IaaS Integration feature.

## 3.6.1 Modify Proxy

In case that the server where IaaS Integration feature is set up accesses to the IaaS to be integrated through the proxy, the proxy and its authentication information must be modified. Refer to "8.8 Modifying Proxy" in detail.

After executing, in order to reflect the modified values, restart APP domain. Refer to "7.1 Start/Stop" for how to restart.

## 3.6.2 Tasks after Setup of AWS Integration Feature

This subsection explains the tasks after setup of AWS Integration feature.

**Note**

Before executing the tasks after setup of AWS Integration feature, import the certifications according to the steps of "Chapter 4 Importing Certification"

### Inputting access key ID and secret access key

In order to call AWS API by AWS Integration feature, access key ID and secret access key must be input to "AWSIntegration". Execute following steps.

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

   ```
   http://<server>:<port>/oscm-app-aws
   ```

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 key and password of the technology manager who is providing the technical service for AWS Integration feature.

   After logging in, the Web page shows the configuration settings of AWS Integration feature.

4. Specify the access key ID and secret access key in the interface.

5. Save the settings.

# Chapter 4 Importing Certification

This chapter explains how to import the certifications.

Note

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.

Note

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 IaaS Integration setup, contact to Operator organization and import the certification newly registered to the truststore of APP domain.

Point

The truststore in this section where authentication is imported is for ROR Integration feature. In case that AWS, OpenStack and TPS5 Integration features are used, please replace the truststore as following:

[Windows]

%FSCTMG_HOME%\glassfish3\glassfish\domains\app-domain\config\cacerts.jks (ROR)

%FSCTMG_HOME%\glassfish3\glassfish\domains\app-aws-domain\config\cacerts.jks (AWS)

%FSCTMG_HOME%\glassfish3\glassfish\domains\app-os-domain\config\cacerts.jks (OpenStack)

%FSCTMG_HOME%\glassfish3\glassfish\domains\app-s5-domain\config\cacerts.jks (TPS5)

### 4.1.1 Exporting and Importing Certification of Main Domain

Import the certification as follows:

1. Open the command prompt.
2. Export the certification from main domain by executing following command:

   [Windows]

   ```
   %FSCTMG_HOME%\jdk7\bin\keytool -export -rfc -alias s1as -keystore %FSCTMG_HOME%
   \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]

   ```
   %FSCTMG_HOME%\jdk7\bin\keytool -import -file ctmgbss.crt -trustcacerts -alias ctmgbss -keystore
   %FSCTMG_HOME%\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]

```
%FSCTMG_HOME%\jdk7\bin\keytool -list -keystore %FSCTMG_HOME%\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 derail 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]

```
%FSCTMG_HOME%\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 Certification of APP Domain

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

Note

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

Point

The truststore in this section where authentication is exported is for ROR Integration feature. In case that AWS and OpenStack Integration features are used, please replace the truststore as following:

[Windows]

ROR:%FSCTMG_HOME%\glassfish3\glassfish\domains\app-domain\config\cacerts.jks

AWS:%FSCTMG_HOME%\glassfish3\glassfish\domains\app-aws-domain\config\cacerts.jks

OpenStack: %FSCTMG_HOME%\glassfish3\glassfish\domains\app-os-domain\config\cacerts.jks

TPS5: %FSCTMG_HOME%\glassfish3\glassfish\domains\app-s5-domain\config\cacerts.jks

### 4.2.1 Exporting and Importing Certification of APP Domain

Import the certification as follows:

1. Open the command prompt.
2. Export the certification from main domain by executing following command:

   [Windows]

   ```
   %FSCTMG_HOME%\jdk7\bin\keytool -export -rfc -alias s1as -keystore %FSCTMG_HOME%
   \glassfish3\glassfish\domains\app-domain\config\keystore.jks -file appror.crt -storepass
   changeit
   ```

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

   [Windows]

   ```
   %FSCTMG_HOME%\jdk7\bin\keytool -import -file appror.crt -trustcacerts -alias appror -keystore
   %FSCTMG_HOME%\glassfish3\glassfish\domains\bes-domain\config\cacerts.jks -storepass changeit
   ```

4. Check that the certification "appror" is imported to the truststore in bes-domain by executing following command:

   [Windows]

   ```
   %FSCTMG_HOME%\jdk7\bin\keytool -list -keystore %FSCTMG_HOME%\glassfish3\glassfish\domains\bes-
   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 Installation in derail 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 "appror.crt" is created in the folder where above command is executed. Delete it as necessary.

### 4.2.2 Confirming the Server Information of Certification

The CN of owner of server certification exported in "4.2.1 Exporting and Importing Certification of APP Domain" can be confirmed by following command:

[Windows]

```
%FSCTMG_HOME%\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
.
.
.
```

## 4.3 Importing and Confirming ROR Server Certification

In case of using ROR integration feature, 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.

## Note

This step is for usage of ROR Integration feature.

In case of usage of AWS Integration feature, this step is not required.

As for OpenStack Integration feature, in case that the URL of HTTPS protocol is specified for setup parameter "KEYSTONE_API_URL" in setting up OpenStack Integration feature, the certification of OpenStack Keystone must be imported to APP domain. Referring to the manual of integrated OpenStack and "4.3.2 Import the Certification", export the certification of OpenStack Keystone and import the exported certification to APP domain. When referring to "4.3.2 Import the Certification", replace the importing certification ("ctmgror.cer" and "ctmgror") to that of OpenStack Keystone, and replace the importing APP domain (app-domain) to the APP domain for OpenStack Integration (app-os-domain).

As for TPS5 Integration feature, the certification of TPS5 site must be imported to APP domain. Referring to the manual of integrated TPS5 and "4.3.2 Import the Certification", export the certification of TPS5 site and import the exported certification to APP domain. When referring to "4.3.2 Import the Certification", replace the importing certification ("ctmgror.cer" and "ctmgror") to that of TPS5, and replace the importing APP domain (app-domain) to the APP domain for TPS5 Integration (app-s5-domain).

【Windows】

```
%FSCTMG_HOME%\jdk7\bin\keytool -export -alias endpoint -keystore <directory of TPS5 API library>\bin
\security\cacerts -file tps5.crt -storepass changeit
```

## 4.3.1 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.

## 4.3.2 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.
2. Copy the created file in "4.3.1 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]

   ```
   %FSCTMG_HOME%\jdk7\bin\keytool -import -file ctmgror.cer -trustcacerts -alias ctmgror -keystore
   %FSCTMG_HOME%\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]

   ```
   %FSCTMG_HOME%\jdk7\bin\keytool -list -keystore %FSCTMG_HOME%\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 derail 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.

## 4.3.3 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 "4.3.1 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 "4.3.1 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]

```
%FSCTMG_HOME%\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.

## 5.1 Creating and Publishing Service of ROR Integration Feature

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.

   - 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]

     ```
     %FSCTMG_HOME%\app\setup\samples
     ```

   Refer to "Appendix B Service Parameters for IaaS 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]

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

%FSCTMG_HOME%\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 org.oscm.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 for ROR Integration Feature" 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.

Your cost calculation for the services should include any external costs for operating the virtual servers in ROR.

## 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.

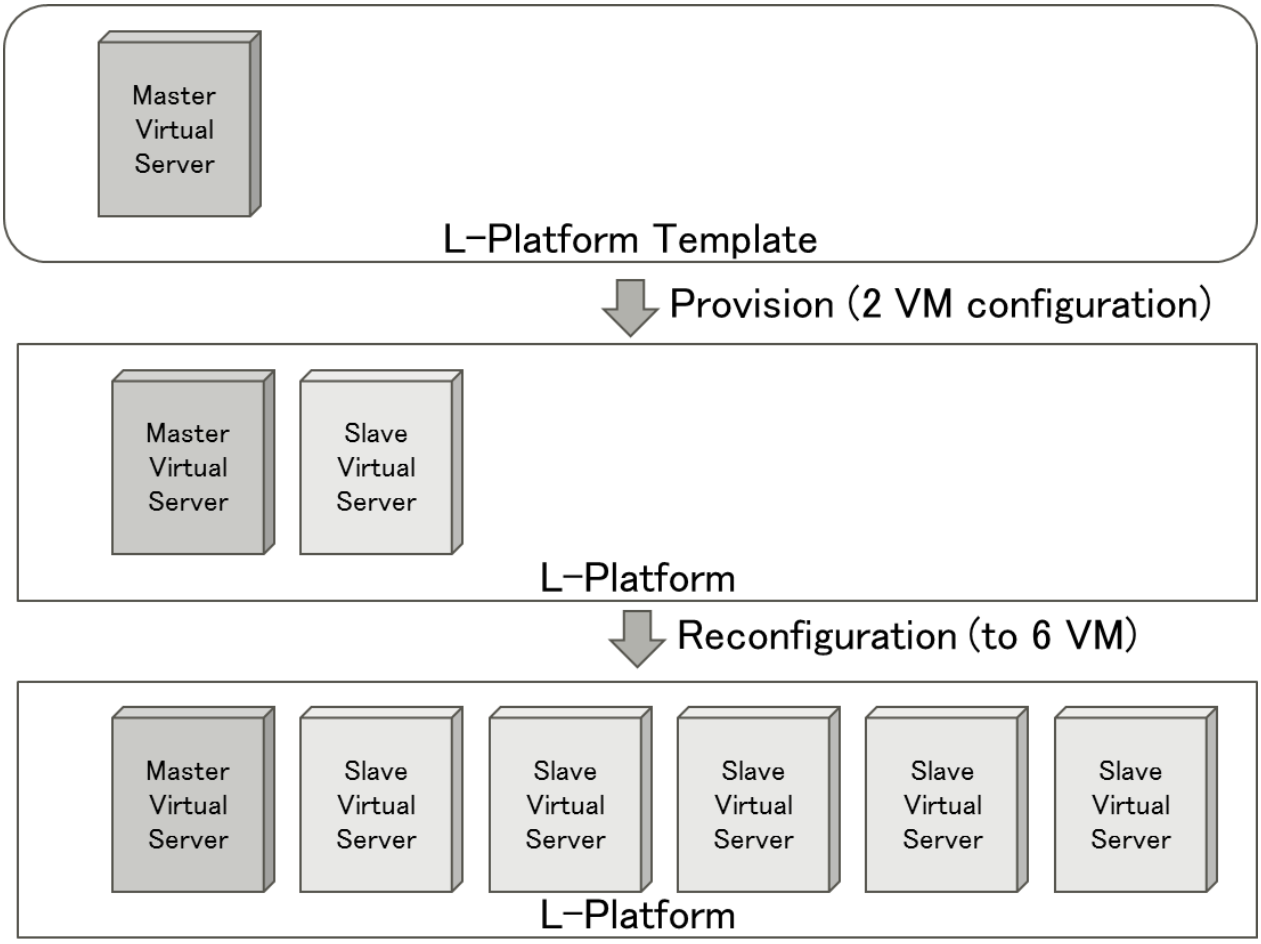
- As for the OS user name to access to the virtual servers, inform to the customer subscribing the service. For example, send email including the list of virtual servers and their access information.

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.




## 5.2 Creating and Publishing Service of AWS Integration Feature

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.

   - The folder where technical service definitions are registered

     [Windows]

     ```
     %FSCTMG_HOME%\app\setupaws\samples\TechnicalService_AWS.xml
     ```

   Refer to "Appendix B Service Parameters for IaaS Integration Feature" for detailed information.

The command is available to easily create the technical service definition. 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

Your cost calculation for the services should include any external costs for operating the virtual servers in Amazon EC2.

## 5.3 Creating and Publishing Service of OpenStack Integration Feature

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.

   - The folder where technical service definitions are registered

     [Windows]

     ```
     %FSCTMG_HOME%\app\setupos\samples\TechnicalService_OpenStack.xml
     ```

   Refer to "Appendix B Service Parameters for IaaS Integration Feature" for detailed information.

   The command is available to easily create the technical service definition. Refer to "Appendix C Command for Creating Technical Service Definition" for detailed information.

   Make the JSON template referring to the following technical service definitions for provisioning Stack.

   - The folder where JSON template is registered

     [Windows]

     ```
     %FSCTMG_HOME%\app\setupos\samples\template.json
     ```

     ```
     %FSCTMG_HOME%\app\setupos\samples\template.yaml
     ```

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

Your cost calculation for the services should include any external costs for operating the virtual servers in OpenStack.

In case that the operation to terminate Stack is executed by customer organization, the error might be occurred in the procedure to terminate Stack and the instances to be terminated might remain on OpenStack dashboard and the instance status interface of APP.

In these cases, restart OpenStack, reset the instance status managed by OpenStack Nova, and then resume the terminating operation on OpenStack dashboard and the instance status interface of APP.

## 5.4 Creating and Publishing Service of TPS5 Integration Feature

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.

   - The folder where technical service definitions are registered

     [Windows]

     ```
     %FSCTMG_HOME%\app\setups5\samples\TechnicalService_VirtualSystem.xml
     ```

   Refer to "Appendix B Service Parameters for IaaS Integration Feature" 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

Your cost calculation for the services should include any external costs for operating the virtual systems in TPS5.

The IP addresses indicated in the subscription details are private addresses. For accessing the virtual servers, a user must start a VPN connection from Internet.

# Chapter 6 Unsetup

This chapter explains how to unsetup IaaS integration feature.

## 6.1 Unsetup the ROR Integration feature

This section explains how to unsetup ROR integration feature.

Note

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

### 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 Enterprise 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]

```
%FSCTMG_HOME%\setup\fsctmg_unsetupRORInteg
```

#### 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.

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

#### Start the unsetup

The following message is displayed when you start unsetup:

```
fsctmg_unsetup: INFO: 144: Enterprise Service Catalog Manager ROR Integration unsetup start.
```

### Confirm completion

The following message is displayed when unsetup is complete

```
fsctmg_unsetup: INFO: 146: Enterprise Service Catalog Manager ROR Integration unsetup end.
```

## 6.2 Unsetup the AWS Integration feature

This section explains how to unsetup AWS integration feature.

Note

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

### 6.2.1 Tasks before Unsetup

Refer to "6.1.1 Tasks before Unsetup".

### 6.2.2 Unsetup

This subsection explains the procedure of AWS 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 AWS Integration feature will be unsetup.

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

   [Windows]

   ```
   %FSCTMG_HOME%\setup\fsctmg_unsetupAWSInteg
   ```

#### 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.

```
fsctmg_unsetup: INFO: 150: Are you sure you want to start unsetup Enterprise Service Catalog Manager
AWS Integration? (y/n)[n]
```

#### Start the unsetup

The following message is displayed when you start unsetup:

```
fsctmg_unsetup: INFO: 155: Enterprise Service Catalog Manager AWS Integration unsetup start.
```

#### Confirm completion

The following message is displayed when unsetup is complete

```
fsctmg_unsetup: INFO: 157: Enterprise Service Catalog Manager AWS Integration unsetup end.
```

## 6.3 Unsetup the OpenStack Integration feature

This section explains how to unsetup OpenStack integration feature.

Note

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

## 6.3.1 Tasks before Unsetup

Refer to "6.1.1 Tasks before Unsetup".

## 6.3.2 Unsetup

This subsection explains the procedure of OpenStack 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 OpenStack Integration feature will be unsetup.

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

   [Windows]

```
%FSCTMG_HOME%\setup\fsctmg_unsetupOSInteg
```

### 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.

```
fsctmg_unsetup: INFO: 161: Are you sure you want to start unsetup Enterprise Service Catalog Manager
OpenStack Integration? (y/n)[n]
```

### Start the unsetup

The following message is displayed when you start unsetup:

```
fsctmg_unsetup: INFO: 166: Enterprise Service Catalog Manager OpenStack Integration unsetup start.
```

### Confirm completion

The following message is displayed when unsetup is complete

```
fsctmg_unsetup: INFO: 168: Enterprise Service Catalog Manager OpenStack Integration unsetup end.
```

# 6.4 Unsetup the TPS5 Integration feature

This section explains how to unsetup TPS5 integration feature.

Note

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

## 6.4.1 Tasks before Unsetup

Refer to "6.1.1 Tasks before Unsetup".

## 6.4.2 Unsetup

This subsection explains the procedure of TPS5 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 TPS5 Integration feature will be unsetup.

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

   [Windows]

```
%FSCTMG_HOME%\setup\fsctmg_unsetupS5Integ
```

### 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.

```
fsctmg_unsetup: INFO: 175: Are you sure you want to start unsetup Enterprise Service Catalog Manager
TPS5 Integration? (y/n)[n]
```

### Start the unsetup

The following message is displayed when you start unsetup:

```
fsctmg_unsetup: INFO: 176: Enterprise Service Catalog Manager TPS5 Integration unsetup start.
```

### Confirm completion

The following message is displayed when unsetup is complete

```
fsctmg_unsetup: INFO: 178: Enterprise Service Catalog Manager TPS5 Integration unsetup end.
```

# Chapter 7 Operation

This chapter explains the operations of IaaS 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 Enterprise Service Catalog Manager. Refer to "9.1 Start/Stop" in "Installation Guide" in detail.

### 7.1.2 Start ROR Integration Feature

This subsection explains how to start ROR integration feature.

Execute following command:

[Windows]

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

### 7.1.3 Stop ROR Integration Feature

This subsection explains how to stop ROR integration feature.

Execute following command:

[Windows]

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

### 7.1.4 Start AWS Integration Feature

This subsection explains how to start AWS integration feature.

Execute following command:

[Windows]

```
net start "Enterprise Service Catalog Manager APP AWS Server"
```

### 7.1.5 Stop AWS Integration Feature

This subsection explains how to stop AWS integration feature.

Execute following command:

[Windows]

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

### 7.1.6 Start OpenStack Integration Feature

This subsection explains how to start OpenStack integration feature.

Execute following command:

[Windows]

```
net start "Enterprise Service Catalog Manager APP OpenStack Server"
```

### 7.1.7 Stop OpenStack Integration Feature

This subsection explains how to stop OpenStack integration feature.

Execute following command:

[Windows]

```
net stop "Enterprise Service Catalog Manager APP OpenStack Server"
```

### 7.1.8 Start TPS5 Integration Feature

This subsection explains how to start TPS5 integration feature.

Execute following command:

[Windows]

```
net start "Enterprise Service Catalog Manager APP TPS5 Server"
```

### 7.1.9 Stop TPS5 Integration Feature

This subsection explains how to stop TPS5 integration feature.

Execute following command:

[Windows]

```
net stop "Enterprise Service Catalog Manager APP TPS5 Server"
```

## 7.2 Customize Text

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

### 7.2.1 Text List for IaaS 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

- Account (the navigation menu and menu title)

  Key: marketplace.account.title

  Key: navigation.myAccount

- Show (the button on "Subscriptions" page)

  Key: marketplace.account.button.show

- Save (the button on "Configuration" tab on "Subscriptions")

  Key: button.save

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 IaaS Integration feature.

If the provisioning or modification of a virtual system fails on the IaaS 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 IaaS.

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

After solving the problem, IaaS 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 IaaS service controller.
2. Invoke the instance status interface of APP for respective service controller by opening the following URL in a Web browser:

   ROR integration feature:

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

   AWS integration feature:

   ```
   http://<server>:<port>/oscm-app/controller/?cid=ess.aws
   ```

   OpenStack integration feature:

   ```
   http://<server>:<port>/oscm-app/controller/?cid=ess.openstack
   ```

   TPS5 integration feature:

   ```
   http://<server>:<port>/oscm-app/controller/?cid=ess.tps5
   ```

   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 IaaS Integration feature.

   After logging in, the Web page shows all subscriptions for IaaS, including detailed information such as the customer organization, the ID of the related instance, and the provisioning status.
4. Find the subscription for which you solved the problem in the most recent provisioning, modification, or deprovisioning operation. Clicking the entry of table displaying on the instance status interface of APP, instance details can be shown. In the instance details, the information are shown correspondind to subscriptions, which are registered in APP database.
5. In the Action column, select the action for the IaaS 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.

**Point**

In case that clock mark is shown in "Run with timer" column on the instance status interface of APP, the timer is running in order to poll with the interval specified as APP_TIMER_INTERVAL.to reset the timer if required, click the link "Reset timer". As for the interval to poll, please refer to the parameter "APP_TIMER_INTERVAL" in "A.1 Configuration Settings of APP".

In case that the timer stops and APP does not poll the instance status, the clock mark is not shown. (Example: when the service parameter "MAIL_FOR_COMPLETION" is specified, and the instance is waiting for a notification about the completion of a manual action.)

## 7.4 Manage APP

When the communication between APP and CT-MG is no longer possible, for example when CT-MG is stopped, APP suspends the processing of requests. An internal flag is set in the APP database: APP_SUSPEND=true, and an email is sent to the address specified in the APP_ADMIN_MAIL_ADDRESS configuration setting.

Contact the CT-MG operator so that he makes sure that CT-MG is up and running again correctly.

You then work as a technology manager of the technology provider organization which is responsible for the IaaS service controller, and you have the following possibilities to resume the processing of requests by APP:

1. Click the link provided in the email.
2. On the log in page, specify the user ID and password of the technology manager who is providing the technical service for IaaS Integration feature.

   APP is restarted instantly. In the APP database, the APP_SUSPEND key is set to false.

As an alternative, you can proceed as follows:

1. In a Web browser, access the base URL of APP, for example:

   ```
   http://<server>:<port>/oscm-app
   ```

   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) of IaaS Integration to <port>.
2. On the log in page, specify the user ID and password of the technology manager who is providing the technical service for IaaS Integration feature.

   After logging in, a message is shown that APP has been suspended due to a communication problem with CT-MG.
3. Click Restart.

   APP is restarted instantly. In the APP database, the APP_SUSPEND key is set to false.

## 7.5 Manage Log Level

Service controller and APP record information such as connection issues in the following log files:

- Log file of service controller

```
%FSCTMG_HOME%\glassfish3\glassfish\domains\app-domain\logs\app-ror.log
```

- Log file of APP

```
%FSCTMG_HOME%\glassfish3\glassfish\domains\app-domain\logs\app-ror.log
```

The logging is based on log4j. The default log level is INFO. You will manage to adapt the log level in following configuration files if necessary.

- Log configuration file of service controller

```
%FSCTMG_HOME%\glassfish3\glassfish\domains\app-domain\config\log4j.ess.ror.properties
```

- Log configuration file of APP

```
%FSCTMG_HOME%\glassfish3\glassfish\domains\app-domain\config\log4j.app.core.properties
```

How to manage the log level is following:

1. Open log configuration file with text editor.
2. Modify the value of "log4j.logger.org.oscm.app".
    a. ERROR: describes error information.
    b. WARN: adding to the information of ERROR, describes information to handle.
    c. INFO: adding to the information of WARN, describes information of correct running.
    d. DEBUG: adding to the information of INFO, describes debug information.
    e. TRACE: adding to the information of DEBUG, describes information of detailed running. This vaule is available to be specified only for ROR Integration fearute.

    Example:

    ```
    log4j.logger.org.oscm.app=INFO
    ```

Every 60 seconds, the IaaS integration feature checks for changes in the log configuration. There is no need to restart IaaS Integration.

Note

Above description is the explanation in the case of ROR Integation feature. In case to manage the log configuration of the other IaaS Integration features, please modify the value to replace the directories and names of the log file.

# Chapter 8 Modifying Settings

This chapter explains how to modify the settings of IaaS 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

Confirm following items before changing the configuration settings of APP and service controller.

- Completion to setup IaaS Integration.
- Running of CT-MG database. Refer to "Installation Guide" in detail about starting CT-MG database.

### 8.1.2 Changing Configuration Settings of ROR Integration Feature

This subsection explains the procedure to change ROR Integration.

#### Executing setup command

Execute following procedure:

1. Open the command prompt.
2. Execute the changing command for ROR Integration.

   [Windows]

   ```
   %FSCTMG_HOME%\setup\fsctmg_changeRORInteg "<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>"
   ```

   Table 8.1 ROR Integration Setup Parameter List

| No. | Parameter name | Mandatory | Explanation |
|---|---|---|---|
| 1 | APP_BASE_URL | No | The URL used to access APP. Specify this parameter according to the form, APP_BASE_URL=http://<server>:<port>/oscm-app<br><br><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>.<br><br>Example: APP_BASE_URL=http://SERVER001:8880/oscm-app |
| 2 | APP_TIMER_INTERVAL | No | The interval (in milliseconds). With this interval, APP polls the status of instances.<br><br>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. |

| No. | Parameter name | Mandatory | Explanation |
|---|---|---|---|
| | | | 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>".<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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 "4.3.3 Confirming the Server Information of Certification".<br>Specify this parameter according to the form, "<hostname>:<port number (default: 8014)>".<br>Example: server002:8014 |

Example:

[Windows]

```
%FSCTMG_HOME%\setup\fsctmg_changeRORInteg "APP_BASE_URL=http://SERVER001:8880/oscm-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.

```
fsctmg_setup: INFO: 140: Changed Enterprise 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 derail how to restart.

## 8.1.3 Changing Configuration Settings of AWS Integration Feature

This subsection explains the procedure to change AWS Integration.

### Executing setup command

Execute following procedure:

1. Open the command prompt.
2. Execute the changing command for AWS Integration.

   [Windows]

   ```
   %FSCTMG_HOME%\setup\fsctmg_changeAWSInteg "<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 seven 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>"
   ```

   Table 8.2 AWS Integration Setup Parameter List

| No. | Parameter name | Mandatory | Explanation |
|---|---|---|---|
| 1 | APP_BASE_URL | No | Refer to the setup parameter list in "8.1.2 Changing Configuration Settings of ROR Integration Feature". |
| 2 | APP_TIMER_INTERVAL | No | |
| 3 | APP_ADMIN_MAIL_ADDRESS | No | |
| 4 | BSS_WEBSERVICE_HOST_PORT | No | |
| 5 | BSS_USER_KEY | No | |
| 6 | BSS_USER_PWD | No | |
| 7 | BSS_ORGANIZATION_ID | No | |

Example:

[Windows]

```
%FSCTMG_HOME%\setup\fsctmg_changeAWSInteg "APP_BASE_URL=http://SERVER001:8880/oscm-app"
```

Note

Refer to the Note in "8.1.2 Changing Configuration Settings of ROR Integration Feature".

### Confirm the completion

Following message will be displayed when the change procedure completes.

```
fsctmg_setup: INFO: 151: Changed Enterprise Service Catalog Manager AWS 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 derail how to restart.

## 8.1.4 Changing Configuration Settings of OpenStack Integration Feature

This subsection explains the procedure to change OpenStack Integration.

### Executing setup command

Execute following procedure:

1. Open the command prompt.
2. Execute the changing command for OpenStack Integration.

   [Windows]

   ```
   %FSCTMG_HOME%\setup\fsctmg_changeOSInteg "<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>"
   ```

Table 8.3 OpenStack Integration Setup Parameter List

| No. | Parameter name | Mandatory | Explanation |
|---|---|---|---|
| 1 | APP_BASE_URL | No | Refer to the setup parameter list in "8.1.2 Changing Configuration Settings of ROR Integration Feature". |
| 2 | APP_TIMER_INTERVAL | No | |
| 3 | APP_ADMIN_MAIL_ADDRESS | No | |
| 4 | BSS_WEBSERVICE_HOST_PORT | No | |
| 5 | BSS_USER_KEY | No | |
| 6 | BSS_USER_PWD | No | |
| 7 | BSS_ORGANIZATION_ID | No | |
| 8 | API_USER_NAME | No | The user name to be used to access the tenant for your organization in OpenStack. Once authenticated, this user is authorized to access the Heat API.<br>The user must have the necessary credentials to create and configure virtual systems for the tenant.<br>Example: demo |
| 9 | API_USER_PWD | No | The password of the user ID in OpenStack. Specify the password of OpenStack user specified in API_USER_NAME. |

| No. | Parameter name | Mandatory | Explanation |
|---|---|---|---|
| | | | Example: demo1234 |
| 10 | KEYSTONE_API_URL | No | The URL of the Keystone API that is used for authenticating the user name specified in API_USER_NAME. Keystone is the identity service used by OpenStack. Specify the hostname or IP address, port number and version of Keystone API endpoint.<br>Example: http://openstackserver:5000/v2.0 |
| 11 | TENANT_NAME | No | The tenant name of OpenStack. Specify the tenant name to which the user specified in "API_USER_NAME" belongs. This tenant name corresponds to "Project name" on OpenStack dashboard.<br>Example: demo |
| 12 | TEMPLATE_BASE_URL | No | The URL of directory leading to the Heat templates that are specified in technical service definitions. The file names of the templates to be used are specified when customers subscribe to a corresponding service on CT-MG marketplace. The Heat template files must be registered in the directory, which is specified as this parameter.<br>Example: http://openstackserver:8000/templates/ |

Example:

[Windows]

```
%FSCTMG_HOME%\setup\fsctmg_changeOSInteg "APP_BASE_URL=http://SERVER001:8880/oscm-app"
```

Note

Refer to the Note in "8.1.2 Changing Configuration Settings of ROR Integration Feature".

### Confirm the completion

Following message will be displayed when the change procedure completes.

```
fsctmg_setup: INFO: 162: Changed Enterprise Service Catalog Manager OpenStack 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 derail how to restart.

## 8.1.5 Changing Configuration Settings of TPS5 Integration Feature

This subsection explains the procedure to change TPS5 Integration.

### Executing setup command

Execute following procedure:

1. Open the command prompt.
2. Execute the changing command for TPS5 Integration.

   [Windows]

   ```
   %FSCTMG_HOME%\setup\fsctmg_changeS5Integ "<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>"
```

Table 8.4 TPS5 Integration Setup Parameter List

| No. | Parameter name | Mandatory | Explanation |
|---|---|---|---|
| 1 | APP_BASE_URL | No | Refer to the setup parameter list in "8.1.2 Changing Configuration Settings of ROR Integration Feature". |
| 2 | APP_TIMER_INTERVAL | No | |
| 3 | APP_ADMIN_MAIL_ADDRESS | No | |
| 4 | BSS_WEBSERVICE_HOST_PORT | No | |
| 5 | BSS_USER_KEY | No | |
| 6 | BSS_USER_PWD | No | |
| 7 | BSS_ORGANIZATION_ID | No | |
| 8 | IAAS_API_LOCALE | No | The locale to be used for accessing TPS5 API. Specify the locale of TPS5 ("en" or "ja").<br>Example: en |
| 9 | IAAS_API_URI | No | The URL of TPS5 API. Specify the URL of integrating region of TPS5.<br>Example: https://api.oviss.jp.fujitsu.com/ovissapi/endpoint |
| 10 | IAAS_API_KEYSTORE_TYPE | No | Spefify the file type of TPS5 account certification to call TPS5 API.<br>Example: pkcs12 |
| 11 | IAAS_API_KEYSTORE_PASS | No | Spefify the password of TPS5 account certification to call TPS5 API<br>Example: User12345789012 |
| 12 | IAAS_API_KEYSTORE | No | Spefify the directory where TPS5 account certification to call TPS5 API with the full path.<br>Example: C:/Users/Administrator/UserCert.p12 |

Example:

[Windows]

```
%FSCTMG_HOME%\setup\fsctmg_changeS5Integ "APP_BASE_URL=http://SERVER001:8880/oscm-app"
```

Note

Refer to the Note in "8.1.2 Changing Configuration Settings of ROR Integration Feature".

### Confirm the completion

Following message will be displayed when the change procedure completes.

```
fsctmg_setup: INFO: 179: Changed Enterprise Service Catalog Manager TPS5 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 derail how to restart.

## 8.2 Modifying Port Number of Database

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

Note

- IaaS 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%

### 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]

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

### 8.2.2 Stopping IaaS Integration Feature

Stop IaaS 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 IaaS Integration Feature

Start IaaS 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

- IaaS Integration feature must be running in order to execute the commands.
- The modification will become effective after restarting IaaS 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%

### 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.

   ```
   "%FSCTMG_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.

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

3. Start IaaS 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]

```
"%FSCTMG_HOME%\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]

```
"%FSCTMG_HOME%\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]

```
"%FSCTMG_HOME%\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]

```
"%FSCTMG_HOME%\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]

```
"%FSCTMG_HOME%\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]

```
"%FSCTMG_HOME%\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]

```
"%FSCTMG_HOME%\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 IaaS Integration feature.

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

### Note

- IaaS 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%

### 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".

### 8.4.1 Modifying SMTP Server

Use following command to modify the SMTP server setting.

[Windows]

```
"%FSCTMG_HOME%\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]

```
"%FSCTMG_HOME%\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]

```
"%FSCTMG_HOME%\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]

```
"%FSCTMG_HOME%\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]

```
"%FSCTMG_HOME%\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]

```
"%FSCTMG_HOME%\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.

Note

- IaaS Integration feature must be running in order to execute the commands.
- The modification will become effective after restarting IaaS 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%

Use following command to change:

[Windows]

```
"%FSCTMG_HOME%\glassfish3\bin\asadmin" %OPTION% change-admin-password --domaindir %FSCTMG_HOME%
\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.<br>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.<br>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
```

## 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]

```
"%FSCTMG_HOME%\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
```

## 8.8 Modifying Proxy

This section explains how to modify the proxy settings of APP domain.

In case that the server where IaaS Integration feature is set up accesses to the IaaS to be integrated through the proxy, the proxy and its authentication information must be modified. Use following commands depending on used server.

### Note

- IaaS Integration feature must be running in order to execute the commands.
- The modification will become effective after restarting IaaS 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%

### Command to modify proxy host

[Windows]

```
"%FSCTMG_HOME%\glassfish3\bin\asadmin" %OPTION% create-jvm-options -Dhttps.proxyHost=<proxy host>
```

### Command to modify proxy port

[Windows]

```
"%FSCTMG_HOME%\glassfish3\bin\asadmin" %OPTION% create-jvm-options -Dhttps.proxyPort=<port number>
```

### Command to modify the authentication user of proxy

[Windows]

```
"%FSCTMG_HOME%\glassfish3\bin\asadmin" %OPTION% create-jvm-options -Dhttps.proxyUser=<authentication
user>
```

### Command to modify the authentication password of proxy

[Windows]

```
"%FSCTMG_HOME%\glassfish3\bin\asadmin" %OPTION% create-jvm-options -
Dhttps.proxyPassword=<authentication password>
```

### Command to modify the host to connect directly

In case that the proxy is modified for APP domain, the host to connect directly must be modified, in order to communicate directly between APP domain and Web service of CTMG without the proxy.

[Windows]

```
"%FSCTMG_HOME%\glassfish3\bin\asadmin" %OPTION% create-jvm-options -Dhttp.nonProxyHosts="localhost|
127.0.0.1|<server host name where CT-MG is running>*"
```

# 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>/oscm-app
```

The URL used to access APP.

Specify the APP_BASE_URL setting as follows:

APP_BASE_URL=http://<host>:<port>/oscm-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 on CT-MG will take longer than the actual provisioning on IaaS. 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}/BASIC
```

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 IaaS Integration.

### BSS_WEBSERVICE_WSDL_URL

```
BSS_WEBSERVICE_WSDL_URL=https://<server>:<port>/oscm/v1.9/{SERVICE}/BASIC?wsdl
```

Mandatory when BSS_AUTH_MODE is set to INTERNAL and basic authentication is used. The version of the CT-MG Web services to be used. The {SERVICE} placeholder must not be replaced.

As for the requirements of this property, please refer to BSS_WEBSERVICE_URL. 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 IaaS 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 manger role.

### BSS_USER_PWD

```
BSS_USER_PWD=_crypt:<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_STS_WEBSERVICE_URL

```
BSS_STS_WEBSERVICE_URL=https://<server>:<port>/{SERVICE}/STS
```

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.

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.

### BSS_STS_WEBSERVICE_WSDL_URL

```
BSS_STS_WEBSERVICE_WSDL_URL=https://<server>:<port>/oscm/v1.9/{SERVICE}/STS?wsdl
```

Mandatory when BSS_AUTH_MODE is set to SAML_SP. The version of the CT-MG Web services 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

### A.2.1 Configuring setting of ROR 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 "F.2.1 Changing Configuration Settings", 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=_crypt:<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 "4.3.3 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.

## A.2.2 Configuring setting of AWS Service Controller

### CONTROLLER_ID

CONTROLLER_ID=ess.aws

Mandatory parameter. "ess.aws" is automatically specified in the setup command for ROR Integration feature. In case to change the configuration settings of service controller with "F.2.1 Changing Configuration Settings", you must specify this property.

Default: ess.aws

### 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 AWS integration feature

### ACCESS_KEY_ID_PWD

ACCESS_KEY_ID_PWD=_crypt:<accessKeyID>

The identifier of the access key for the AWS account.

A technology provider who is responsible for creating technical services for appropriate AMIs needs to have an AWS account to create Amazon EC2 instances. For details about creating an AWS account, refer to the user documentation of Amazon Web Services.

Together with the secret access key, the access key ID is used to authenticate API calls to Amazon EC2.

### SECRET_KEY_PWD

SECRET_KEY_PWD=_crypt:<secretAccessKey>

The secret access key for the AWS account.

Together with the access key ID, the secret access key is used to authenticate API calls to

Amazon EC2.

## A.2.3 Configuring setting of OpenStack Service Controller

### CONTROLLER_ID

CONTROLLER_ID=ess.openstack

Mandatory parameter. "ess.openstack" is automatically specified in the setup command for ROR Integration feature. In case to change the configuration settings of service controller with "F.2.1 Changing Configuration Settings", you must specify this property.

Default: ess.openstack

### 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 OpenStack integration feature

### API_USER_NAME

API_USER_NAME=<OpenStack user name>

The user name to be used to access the tenant for your organization in OpenStack. Once authenticated, this user is authorized to access the Heat API.

The user must have the necessary credentials to create and configure virtual systems for the tenant.

Example: demo

### API_USER_PWD

API_USER_PWD=_crypt:<OpenStack user password>

The password of the user ID in OpenStack. Specify the password of OpenStack user specified in API_USER_NAME.

The plain text password will be encrypted automatically in the APP database.

Example: demo1234

### KEYSTONE_API_URL

KEYSTONE_API_URL=http://<host name or IP address of keystone endpoint>:<port>/<version>

The URL of the Keystone API that is used for authenticating the user name specified in API_USER_NAME. Keystone is the identity service used by OpenStack. Specify the hostname or IP address, port number and version of Keystone API endpoint.

Example: http://openstackserver:5000/v2.0

### TENANT_NAME

The tenant name of OpenStack. Specify the tenant name to which the user specified in "API_USER_NAME" belongs. This tenant name corresponds to "Project name" on OpenStack dashboard.

Example: demo

### TEMPLATE_BASE_URL

TEMPLATE_BASE_URL=http://<host name or IP address of template>:<port>/<directory>/

The URL of directory leading to the Heat templates that are specified in technical service definitions. The file names of the templates to be used are specified when customers subscribe to a corresponding service on CT-MG marketplace. The Heat template files must be registered in the directory, which is specified as this parameter.

Example: http://openstackserver:8000/templates/

## A.2.4 Configuring setting of TPS5 Service Controller

### CONTROLLER_ID

CONTROLLER_ID=ess.tps5

Mandatory parameter. "ess.tps5" is automatically specified in the setup command for TPS5 Integration feature. In case to change the configuration settings of service controller with "F.2.1 Changing Configuration Settings", you must specify this property.

Default: ess.tps5

### 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 TPS5 integration feature

### IAAS_API_LOCALE

IAAS_API_LOCALE=<ja or en>

The locale to be used for accessing TPS5 API. Specify the locale of TPS5 ("en" or "ja").

### IAAS_API_URI

IAAS_API_URI=https://<TPS5 server>:<port>/ovissapi/endpoint

The URL of TPS5 API. Specify the URL of integrating region of TPS5. Specify the port number of TPS5 API for <port> (default: 80, optional)

### IAAS_API_KEYSTORE_TYPE

IAAS_API_KEYSTORE_TYPE=<certification type>

Spefify the file type of TPS5 account certification to call TPS5 API.

### IAAS_API_KEYSTORE_PASS

IAAS_API_KEYSTORE_PASS=_crypt:<certification password>

Spefify the password of TPS5 account certification to call TPS5 API

### IAAS_API_KEYSTORE

IAAS_API_KEYSTORE=<directory of certification>

Spefify the directory where TPS5 account certification to call TPS5 API with the full path.

The account certification to call TPS5 API must be saved in the server where TPS5 Integration is set up. The directory to save must be named with alphanumeric characters and slash, excluding space, double and single quotations.

# Appendix B Service Parameters for IaaS Integration Feature

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

## B.1 Service Parameters for ROR Integration Feature

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

### B.1.1 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. In case that the manager of integrated IaaS needs to change or modify the instance manually on the integrated IaaS side after provisioning the instance from the service of IaaS Integration feature on CT-MG marketplace portal, this parameter should be specified.

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. Remove 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.1.2 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-13cedeaf7ed

### 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. Specify the hostname in this URL, which is same as the information specified in CN of the owner for server certification of APP domain.

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

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

Example: https://SERVER001:8881/OperationService/AsynchronousOperationProxy?wsdl

#### STOP_VIRTUAL_SYSTEM

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

Specify the hostname in this URL, which is same as the information specified in CN of the owner for server certification of APP domain.

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

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

Example: https://SERVER001:8881/OperationService/AsynchronousOperationProxy?wsdl

### B.1.3 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

## B.2 Service Parameters for AWS Integration Feature

### APP_CONTROLLER_ID

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

Default: ess.aws

### APP_BSS_USER

Please refer to "B.1 Service Parameters for ROR Integration Feature".

### APP_BSS_USER_PWD

Please refer to "B.1 Service Parameters for ROR Integration Feature".

### INSTANCENAME_PATTERN

Mandatory. A regular expression specifying a pattern for the EC2 instance 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: aws([a-z0-9]){2,25}

### INSTANCENAME_PREFIX

Optional. A string to be prepended to the EC2 instance names entered by the users when they subscribe to a corresponding service.

Example: aws

### INSTANCENAME

Mandatory. The name of the EC2 instance 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: ec2instance

### IMAGE_NAME

Mandatory. Name of the AMI which is the basis for virtual servers.

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 region, have fixed parameter options for selection.

Example: amzn-ami-minimal-pv-2013.09.0.x86_64-ebs

### INSTANCE_TYPE

Mandatory. The type of the EC2 instance to be provisioned. Any valid Amazon EC2 instance type can be specified. In the sample technical service, the following types are defined:

· t1.micro

· t1.small

· t1.medium

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

Example: t1.micro

### KEY_PAIR_NAME

Mandatory. The key pair name of the virtual server to be instantiated.

The key pair name must be specified by the customer when subscribing to an AWS service. To log in to the instance, technology provider and supplier organization must retrieve this key pair to the customer, and then the customer must enter the key pair name and the associated private key.

Example: my-key-pair

### REGION

Mandatory. The region where the data center hosting the virtual servers is located. Any valid region can be specified. In the sample technical service, the following regions are defined:

· us-west-1 (US West (Northern California) Region)

· us-west-2 (US West (Oregon) Region)

· us-east-1 (US East (Northern Virginia) Region)

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 region, have fixed parameter options for selection.

Example: us-east-1

### SECURITY_GROUP_NAMES

Optional. Comma-separated list of security group names for the virtual server to be instantiated.

A security group acts as a firewall that controls the traffic to an Amazon EC2 instance. An Amazon EC2 instance can be assigned to one or more security groups.

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 security group, have fixed parameter options for selection.

Example: MySecurityGroup

### USERDATA_URL

Optional. URL to access the user data scripts or cloud-init directives for the automatic execution of user-specific configuration data. This URL must be accessible for APP.

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 URL, have fixed parameter options for selection.

Example: http://127.0.0.1:8880/cloud-init/LAMP.script (if the file was created under <app-domain>/docroot/cloud-init/LAMP.script)

### MAIL_FOR_COMPLETION

Please refer to "B.1 Service Parameters for ROR Integration Feature".

### START_VIRTUAL_SYSTEM

Optional. Specify the URL of operation service used for starting EC2 instance. Please refer to "B.1 Service Parameters for ROR Integration Feature" in detail.

Example: https://SERVER001:8881/OperationService/AsynchronousOperationProxy?wsdl

### STOP_VIRTUAL_SYSTEM

Optional. Specify the URL of operation service used for stopping EC2 instance. Please refer to "B.1 Service Parameters for ROR Integration Feature" in detail.

Example: https://SERVER001:8881/OperationService/AsynchronousOperationProxy?wsdl

## B.3 Service Parameters for OpenStack Integration Feature

### APP_CONTROLLER_ID

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

Default: ess.openstack

### APP_BSS_USER

Please refer to "B.1 Service Parameters for ROR Integration Feature".

### APP_BSS_USER_PWD

Please refer to "B.1 Service Parameters for ROR Integration Feature".

### STACK_NAME

Mandatory. The name of the virtual system to be instantiated. This name must be specified by customers when they subscribe to a corresponding service.

The name is restricted to 20 characters. It must start with an alphanumeric character and must not contain any of the following characters:

! " # $ % & ' * + , / : ; < = > ? \ ^ `

OpenStack generates a random number that is appended to the name to make it unique.

Example: stack

### TEMPLATE_NAME

Mandatory. Name of the template file or relative path to the template file which forms the basis for the instance to be instantiated. The template file details everything needed to carry out the resource orchestration in OpenStack. The template must be specified by customers when they subscribe to a corresponding service.

As for this template file, OpenStack Integration feature supports JSON format which is described with CFN compatible style and and YAML format which is described with HOT style.

The template file specified as this parameter must be registered in the directory of URL, which was specified as TEMPLATE_BASE_URL. And, in the technical service of OpenStack Integration, specify the file name of template as the value of this parameter "TEMPLATE_NAME".

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 template, have fixed parameter options for selection.

Example: MyTemplate.json

Note

Parameter "TEMPLATE_NAME" is to be added to the parameter " TEMPLATE_BASE_URL" specified in "configsettings_controller.properties" file.

### ACCESS_INFO_PATTERN

Mandatory. The access information to be output in the subscription details on the marketplace as soon as the provisioning is complete. This information must give all the details the customer needs to access a provisioned instance, e.g. an IP address and a key pair name.

The information must correspond to the output parameters specified in the template file. If the values do not match, the subscription is rejected.

Customers should not be able to enter a value for this parameter, i.e. it should not be configurable.

Example: Key pair name: {KP_Out}; Ip: {IP_Out}

### TP_ImageId

Mandatory. The virtual machine image for the instance to be instantiated. Any valid image of OpenStack to be integrated can be specified.

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.

Example: cedarish for a cedar image.

### TP_InstanceType

Mandatory. The flavor for the instance to be instantiated. The flavor defines the compute, memory, and storage capacity. Any valid OpenStack flavor can be specified.

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 flavor, have fixed parameter options for selection.

Example: m1.small

### TP_KeyName

Mandatory. The key pair name of the instance to be instantiated.

The key pair name must be specified by the customer when subscribing to an OpenStack service. To log in to the instance, the customer must enter the key pair name and the associated private key.

Example: my-key-pair

### TP_*

Optional. Any number of parameters that are mapped from the parameters defined in the template file. The parameters in the template file detail everything needed to carry out the resource orchestration in OpenStack. For each parameter in the template file, there must be a corresponding parameter in the technical service definition.

The parameter names must correspond to the names in the template file. The string TP_ must be prepended to the name. If the names do not match this pattern, the subscription is ignored, and is not to be specified.

Example: TP_InstanceType (in case of INSTANCE_TYPE, the type of virtual server and so on)

### MAIL_FOR_COMPLETION

Please refer to "B.1 Service Parameters for ROR Integration Feature".

### START_VIRTUAL_SYSTEM

Optional. Specify the URL of operation service used for starting Stack.

Example: https://SERVER001:8881/OperationService/AsynchronousOperationProxy?wsdl

### STOP_VIRTUAL_SYSTEM

Optional. Specify the URL of operation service used for stopping Stack.

Example: https://SERVER001:8881/OperationService/AsynchronousOperationProxy?wsdl

## B.4 Service Parameters for TPS5 Integration Feature

This section explains the parameters of technical services which are handled by the TPS5 Integration service controller.

## B.4.1 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.tps5

### APP_BSS_USER

Please refer to "B.1 Service Parameters for ROR Integration Feature".

### APP_BSS_USER_PWD

Please refer to "B.1 Service Parameters for ROR Integration Feature".

### INSTANCENAME_PATTERN

Mandatory. A regular expression specifying a pattern for the virtual system 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: tps5([a-z0-9]){2,25}

### INSTANCENAME_PREFIX

Optional. A string to be prepended to the virtual system names entered by the users when they subscribe to a corresponding service.

Example: tps5

### INSTANCENAME

Mandatory. The name of the virtual system 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: mysystem

### SYSTEM_TEMPLATE_ID

Mandatory. The ID of the system template to be used for virtual system. As for the system template ID, refer to the Template Manager menu of My Portal of TPS5 Service Portal.

Example: mytemplate

### MAIL_FOR_COMPLETION

Please refer to "B.1 Service Parameters for ROR Integration Feature".

### MAIL_FOR_ NOTIFICATION

Please refer to "B.1 Service Parameters for ROR Integration Feature".

### START_VIRTUAL_SYSTEM

Optional. Specify the URL of operation service used for starting virtual system. Please refer to "B.1 Service Parameters for ROR Integration Feature" in detail.

Example: https://SERVER001:8881/OperationService/AsynchronousOperationProxy?wsdl

### STOP_VIRTUAL_SYSTEM

Optional. Specify the URL of operation service used for stopping virtual system. Please refer to "B.1 Service Parameters for ROR Integration Feature" in detail.

Example: https://SERVER001:8881/OperationService/AsynchronousOperationProxy?wsdl

## B.4.2 Adding and Reducing of Virtual Server by Reconfiguring

The following parameters are required for adding adding and reducing of virtual server by reconfiguring:

### VSERVER_<#>

Optional. Boolean specifying whether the additional virtual server is to be instantiated on the virtual platform. Consecutive numbers must be used in the parameter name (#) to uniquely identify each additional virtual server.

Default: true

### VSERVER_<#>_INSTANCENAME

Mandatory in case of using VSERVER_<#>. The name of the virtual server specified in VSERVER_<#>.

Example: WindowsT1

### VSERVER_<#>_NETWORK_ID

Mandatory in case of using VSERVER_<#>. If the virtual platform to which the virtual server is to be added has more than one network, the ID or name of the network must be specified, within the virtual platform to which the virtual server specified in VSERVER_<#> is to be added.

Users should not be able to enter a value for this parameter. The parameter should define fixed

parameter options for selection.

Example: DMZ

### VSERVER_<#>_DISKIMG_ID

Mandatory in case of using VSERVER_<#>. The ID of the TPS5 image to be used for the virtual server specified in VSERVER_<#>.

Users should not be able to enter a value for this parameter. The parameter should define fixed parameter options for selection.

Example: myimage

### VSERVER_<#>_VSERVER_TYPE

Mandatory in case of using VSERVER_<#>. A string describing the type of the virtual server specified in VSERVER_<#>. The string must match one of the server types defined in TPS5.

Example: economy

### VSERVER_<#>_VDISK_NAME

Optional. Name of an additional disk with configurable disk size for the virtual server specified in VSERVER_<#>.

Example: mydisk

### VSERVER_<#>_VDISK_SIZE

Optional. Size of the additional disk for the virtual server specified in VSERVER_<#>.

It is recommended that VDISK_SIZE is defined as one-time parameter, since the modification of the disk size may lead to a loss of data.

Example: 10GB

## B.4.3 Firewall

The following parameters are required for adding the firewall settings.

### FIREWALL_CONFIG

Optional. Configuration setting for managing the communication between the virtual system and the outside network. A firewall can be configured for each active segment (DMZ, SECURE1, and SECURE2).

If more than one firewall rule is required as parameter value, use a semicolon to separate the individual rules. The complete set of rules must not exceed 256 characters. If the parameter value exceeds this maximum length, use FIREWALL_CONFIG_<#> as an additional parameter.

Customers should not be able to enter a value for this parameter, i.e. it should not be configurable. Use FIREWALL_<VARIABLE> to define variables instead.

Example: INTERNET>DMZ("Windows":8080);INTERNET>DMZ("LINUX":443)

### FIREWALL_CONFIG_<#>

Optional. Additional firewall configuration setting if more than 256 characters are needed for specifying the firewall rules.

Use consecutive numbers in the parameter name (<#>) to uniquely identify each additional parameter that is required.

### FIREWALL_<VARIABLE>

Mandatory if FIREWALL_CONFIG or FIREWALL_CONFIG_<#> specify a variable to make a value configurable.

Replace <VARIABLE> with the name of the variable as defined in FIREWALL_CONFIG or FIREWALL_CONFIG_<#>, and enter the required string as parameter value.

Example: in case that FIREWALL_CONFIG=INTERNET>DMZ("${SIP}":80,443), FIREWALL_SIP=Windows

# 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 Enterprise Service Catalog Manager registers the technical service created in this appendix, and then the supplier in Enterprise Service Catalog Manager defines the marketable service based on the technical service definition in this appendix.

## C.1 Command for Creating Technical Service Definition of ROR Integration Feature

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

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]

```
%FSCTMG_HOME%\iaas\bin\rorservicedef.bat [-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:<br>[Windows]<br>%FSCTMG_HOME%\iaas\sample\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.<br>Ex.: -u https://SERVER001:8881 |
| 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.<br>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.<br>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, the operations are deactivated. In case that "-o" option is omitted, the value of template file is not changed and used. |

| | | | | |
|---|---|---|---|---|
| | | | | 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.<br>Example: -o on |
| 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]

```
%FSCTMG_HOME%\iaas\bin\rorservicedef.bat -h
```

### 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.

# C.2 Command for Creating Technical Service Definition of AWS Integration Feature

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

### Create technical service definition

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

[Windows]

```
%FSCTMG_HOME%\iaas\bin\awsservicedef.bat [-t TEMPLATE] [-i SERVICE_ID] [-u URL] [-y INSTANCE_TYPE] [-
r REGION] [-o {on|off}] [-f FILE]
```

Table C.2 Parameter list of the command to create technical service definition for service controller

| No. | Specified option | Parameter name | mandatory | Explanation |
|---|---|---|---|---|
| 1 | -t | TEMPLATE | No | Refer to the parameter list in "C.1 Command for Creating Technical Service Definition of ROR Integration Feature". |
| 2 | -i | SERVICE_ID | No | |
| 3 | -u | URL | No | |
| 4 | -y | INSTANCE_TYPE | No | Specify the name of instance type of VM 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. |
| 5 | -r | REGION | No | Specify the regions (data centers) to provide EC2 instance, 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. |
| 6 | -o | {on\|off} | No | Specify "on" or "off" whether the start/stop operations for EC2 instance are activated. In case that "on" is specified, the operations are activated. In case that "off" is specified, the operations are deactivated. In case that "-o" option is omitted, the value of template file is not changed and used.<br>In case that the start/stop operations for EC2 instance 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.<br>Example: -o on |
| 7 | -f | FILE | No | Refer to the parameter list in "C.1 Command for Creating Technical Service Definition of ROR Integration Feature". |

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

[Windows]

```
%FSCTMG_HOME%\iaas\bin\awsservicedef.bat -h
```

### 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.

## C.3 Command for Creating Technical Service Definition of OpenStack Integration Feature

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

### Create technical service definition

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

[Windows]

```
%FSCTMG_HOME%\iaas\bin\osservicedef.bat [-t TEMPLATE] [-i SERVICE_ID] [-u URL] [-o {on|off}] [-f
FILE]
```

Table C.3 Parameter list of the command to create technical service definition for service controller

| No. | Specified option | Parameter name | mandatory | Explanation |
|---|---|---|---|---|
| 1 | -t | TEMPLATE | No | Refer to the parameter list in "C.1 Command for Creating Technical Service Definition of ROR Integration Feature". |
| 2 | -i | SERVICE_ID | No | |
| 3 | -u | URL | No | |
| 4 | -o | {on\|off} | No | Specify "on" or "off" whether the start/stop operations for Stack are activated. In case that "on" is specified, the operations are activated. In case that "off" is specified, the operations are deactivated. In case that "-o" option is omitted, the value of template file is not changed and used.<br>In case that the start/stop operations for Stack 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.<br>Example: -o on |
| 5 | -f | FILE | No | Refer to the parameter list in "C.1 Command for Creating Technical Service Definition of ROR Integration Feature". |

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

[Windows]

```
%FSCTMG_HOME%\iaas\bin\osservicedef.bat -h
```

### 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 for ROR Integration Feature

This appendix explains how to register the service controller for ROR integration feature 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]/oscm-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:

```
%FSCTMG_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 Enterprise Service Catalog Manager

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

net stop "Enterprise Service Catalog Manager Indexer Server"

net stop "Enterprise Service Catalog Manager DB Service"

net start "Enterprise Service Catalog Manager DB Service"

net start "Enterprise Service Catalog Manager Indexer Server"

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

2. Setup ROR Integration

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

%FSCTMG_HOME%\jdk7\bin\keytool -export -rfc -alias s1as -keystore %FSCTMG_HOME%
\glassfish3\glassfish\domains\bes-domain\config\keystore.jks -file ctmgbss.crt -storepass
changeit

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

del ctmgbss.crt

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

net stop "Enterprise Service Catalog Manager APP Server"
net start "Enterprise Service Catalog Manager APP Server"

%FSCTMG_HOME%\jdk7\bin\keytool -export -rfc -alias s1as -keystore %FSCTMG_HOME%
```

```
\glassfish3\glassfish\domains\app-domain\config\keystore.jks -file appror.crt -storepass
changeit

%FSCTMG_HOME%\jdk7\bin\keytool -import -file appror.crt -trustcacerts -alias appror -keystore
%FSCTMG_HOME%\glassfish3\glassfish\domains\bes-domain\config\cacerts.jks -storepass changeit

del appror.crt

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

net stop "Enterprise Service Catalog Manager Server"
net start "Enterprise Service Catalog Manager Server"
```

Note

Refer to "3.2.2 Setup" in detail for the parameters specified for execution of fsctmg_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 "4.3 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: svs_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.opends.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: svs_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.opends.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: svs_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: svs_cms
ds-cfg-trust-manager-provider: cn=Administration,cn=Trust Manager Providers,cn=config
```

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

   [Windows]

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

   [Linux]

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

6. Start manager of ServerView Resource Orchestrator.

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

# Appendix F Setup in SAML_SP Authenticate mode

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

## F.1 Tasks before Setup

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

### F.1.1 Preparing Metadata Exchange File

From the SAML Identity Provider (IdP) or CT-MG operator, obtain a metadata exchange file in WSDL format generated

with and for the IdP system in use. The metadata includes namespace information required for connecting to the Security Token Service (STS).

Save the metadata exchange file to the following file, overwriting the existing empty file:

```
%FSCTMG_HOME%\app\setup\domains\app_domain\wsit\STSService.xml
```

Open the STSService.xml file and retrieve the value of targetNamespace

Example:

```
http://schemas.microsoft.com/ws/2008/06/identity/securitytokenservice
```

Open the following file, and Replace the placeholder in the namespace tag of the wsit-client.xml file with the

targetNamespace value copied from the STSService.xml file:

```
%FSCTMG_HOME%\app\setup\domains\app_domain\wsit\wsit-client.xml
```

During the installation process, a CT-MG-wsit.jar file is created containing the STSService.xml file as well as the wsit-client.xml file; the .jar file is then copied to:

```
%FSCTMG_HOME%\app\setup\domains\app_domain\lib
```

### F.1.2 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]

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

  The parameters to change the values are following:

  - BSS_AUTH_MODE
  - BSS_STS_WEBSERVICE_URL
  - BSS_STS_WEBSERVICE_WSDL_URL
  - APP_KEYSTORE_PASSWORD
  - APP_TRUSTSTORE_PASSWORD

  Refer to "Appendix A Configuration Settings for APP and Service Controller" in detail for parameters.

### F.1.3 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 IaaS Integration feature which are not described in "Chapter 8 Modifying Settings", the procedure is following:

**Point**

The described file and folder in this section is for ROR Integration feature. In case that AWS and OpenStack Integration feature are used, please replace the described file and folder as following:

[Windows]

%FSCTMG_HOME%\app\setup (ROR)

%FSCTMG_HOME%\app\setupaws (AWS)

%FSCTMG_HOME%\app\setupos (OpenStack)

#### Edit configuration settings files

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

   [Windows]

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

   The folder to copy is following:

   [Windows]

   ```
   %FSCTMG_HOME%\app\setup\databases\app_db
   ```

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

   [Windows]

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

   The folder to copy is following:

   [Windows]

   ```
   %FSCTMG_HOME%\app\setup\databases\app_db
   ```

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.
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=%FSCTMG_HOME%\fjsvpgs91_64\bin\psql.exe
   ```

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

   [Windows]

   ```
   set JAVA_HOME=%FSCTMG_HOME%\jdk7
   ```

5. In case that you specified the password of OS user for database in setup for Enterprise 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/install) under "app" directory as follows:

   [Windows]

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

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

   [Windows]

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

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