FUJITSU

December 2017

Contents

About this Manual

This manual describes how to get started with FUJITSU Software Enterprise Service Catalog Manager - hereafter referred to as Catalog Manager (CT-MG).

The manual is structured as follows:

Chapter	Description
	Provides an overview of CT-MG, its architecture, and the distribution media.
	Describes the prerequisites that must be fulfilled and the preparations you need to take before installing and deploying CT-MG.
	Describes how to install CT-MG with the help of the utilities which are shipped with the software.
	Describes how to update CT-MG.
	Describes how to uninstall CT-MG.
	Describes the resources required for CT-MG on the application server.
	Describes the CT-MG configuration settings.

Readers of this Manual

This manual is directed to operators who deploy, configure, use, and setup CT-MG in a SUSE OpenStack Cloud 7 environment.

It assumes that you are familiar with the following:

- Administration of the operating systems in use, including the adaption and execution of batch files or shell scripts.
- Java EE technology, particularly as to the deployment on application servers.
- SUSE OpenStack Cloud 7 administration and usage.
- CT-MG concepts as explained in the *Overview* manual.

Abbreviations

This manual uses the following abbreviations:

API	Application Programming Interface
CT-MG	Catalog Manager
DBMS	Database Management System
EJB	Enterprise JavaBeans
IdP	SAML Identity Provider
JMS	Java Message Service
LDAP	Lightweight Directory Access Protocol

PaaS	Platform as a Service
PSP	Payment Service Provider
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SOAP	Simple Object Access Protocol
STS	Security Token Service
WSDL	Web Services Description Language
WSIT	Web Services Interoperability Technologies

The term "Windows" is used to denote the different Microsoft Windows operating systems supported by CT-MG. "UNIX" stands for the supported UNIX operating systems, "Linux" for the supported Linux systems.

1 Introduction

Describes Chapter 1

1.1 What is CT-MG

Catalog Manager (CT-MG) is a set of services which provide all business-related functions and features required for turning on-premise applications and tools into "as a Service" (aaS) offerings and using them in the Cloud. This includes ready-to-use account and subscription management, online service provisioning, billing and payment services, and reporting facilities.

With its components, CT-MG covers all the business-related aspects of a Platform as a Service (PaaS) or Cloud platform. It supports software vendors as well as their customers in leveraging the advantages of Cloud Computing:

- Sharing: Through the Internet, many customers use applications which are installed centrally and share a common IT infrastructure. Each customer's security and privacy are not sacrificed, but even improved by the concentration of security means and expertise at the data centers.
- Pay-per-use: Software vendors as well as their customers only pay for the services they actually use, without upfront investment or entry costs for both human and non-human resources. Customers simply subscribe to the services they like to use and pay for what they consume.
- Centralized management: Cloud application providers maintain and operate the applications centrally for all their customers. This substantially reduces installation and maintenance costs for all participants.

Integration with CT-MG does not require software vendors to design or implement their applications in a specific way. Instead, CT-MG offers open and standards-based interfaces, which enable software vendors to:

- Easily and rapidly provide new as well as existing applications with the required business services without the need of rewriting existing applications or changing their development environment.
- Leverage an open platform suitable for multiple sales channels such as online marketplaces, value-added resellers, system integrators, and direct sales.

While being open in its interfaces, CT-MG provides all the required ways and means to ensure customer privacy and data security.

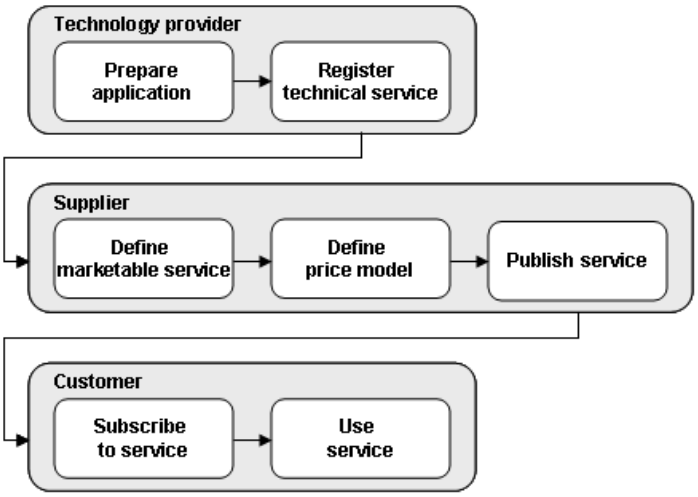
CT-MG is typically operated and used in a SaaS environment. It supports, however, all types of "as-a-Service" environments.

1.2 Usage Scenarios

CT-MG supports a variety of usage scenarios. The following sections describe typical scenarios and provide an overview of the participating users and organizations.

Basic Usage Scenario

The basic scenario of deploying and using applications as services in the CT-MG framework involves the following users and organizations:



1. **Technology providers** (e.g. independent software vendors) technically prepare their applications for usage in the Cloud and integrate them with CT-MG. They register the applications as technical services in CT-MG.
2. **Suppliers** (e.g. independent software vendors or sales organizations) define service offerings, so-called marketable services, for the technical services in CT-MG. They publish the services to a marketplace.
3. **Customers** register themselves or are registered by an authorized organization in CT-MG and subscribe to one or more services. Users appointed by the customers work with the underlying applications under the conditions of the corresponding subscriptions.

Extended Usage Scenarios

The suppliers who define marketable services may involve additional users and organizations in offering and selling these services:

- **Brokers** support suppliers in establishing relationships to customers by offering the suppliers' services on a marketplace. A service subscription is a contract between the customer and the supplier.
- **Resellers** offer services defined by suppliers to customers applying their own terms and conditions. A service subscription establishes a contract between the customer and the reseller.

Brokers and resellers usually receive their share of a supplier's revenue. CT-MG provides the means to define these revenue shares and calculate and retrieve the actual amounts from the service usage fees.

CT-MG Across Usage Scenarios

In addition to technology providers, suppliers, resellers, brokers, and customers, the following users are involved in the preparation and operation of CT-MG and the applications integrated with it:

- **Marketplace owners** are responsible for administrating and customizing the marketplaces to which services are published.
- **Operators** are responsible for deploying and maintaining CT-MG.

CT-MG offers features and functions which are of relevance for all these participating parties. These include a state-of-the-art user interface, account and identity management, and external process control. Public Web services and application programming interfaces (APIs) are available by which developers can integrate applications and external systems with CT-MG.

1.3 CT-MG Architecture

CT-MG is implemented in Java, using Java Platform, Enterprise Edition (Java EE) technology. It is deployed on an application server supporting this technology.

The following figure provides an overview of the architecture:

CT-MG has a three-tier architecture:

- The **presentation layer** in the application server's Web container includes the **user interface** (administration portal and marketplaces), realized as JavaServer Faces. Users access the user interface in Web browsers. In addition, CT-MG provides a **command line tool**, which operators can install to carry out their tasks from a command shell instead of the administration portal.
- The **business logic** is implemented in Enterprise JavaBeans (EJB). Both the Enterprise JavaBeans and the **public Web services** are available in the application server's EJB container. The public Web services and their interfaces are mainly used for integrating applications and external systems with CT-MG. However, they can also be employed for accessing CT-MG functionality from a Web service client. HTTPS must be used for communication with the public Web services.
- CT-MG **persists** its data through the Java Persistence API in **relational databases**.

For informing users about relevant issues (e.g. their registration or assignment to a subscription), CT-MG must have access to a mail server.

1.4 Organizations and User Roles

Each user working in CT-MG is a member of a specific organization. An organization typically represents a company, but it may also stand for a department of a company or a single person. Each organization in CT-MG has a unique account and ID as well as one or more of the following roles: **operator**, **technology provider**, **supplier**, **reseller**, **broker**, **marketplace owner**, **customer**.

Customers can register themselves with CT-MG or be registered by a supplier, reseller, broker, or operator. In any case, an organization with the customer role is created. Organizations with other roles can also act as customers, i.e. they are implicitly assigned the customer role. These organizations are created and assigned their roles as follows:

- When CT-MG is installed, an organization with the operator role is created.

- Operators can assign the supplier, reseller, broker, and technology provider role to any existing organization or create new organizations with these roles.
- When operators create a marketplace, they specify an existing organization as its owner. In this way, the organization is assigned the marketplace owner role.

The roles of an organization determine which features are available to its users at the CT-MG interfaces and which roles the users can be assigned. These user roles control the actions an individual user is allowed to carry out:

- **Standard user**: Users with this non-privileged role can work with services their organization has subscribed to. Every user registered in CT-MG automatically is a standard user. Additional user roles must be assigned explicitly by an administrator.
- **Administrator**: Each organization must have at least one user with this role. An administrator can manage the organization's account and subscriptions as well as its users and their roles. The first administrator of an organization is defined when the organization is created.
- **OU administrator**: The users of an organization can be grouped in organizational units (OUs). The OU administrator role allows a user to manage the organizational units for which he has been appointed as an administrator, to create, modify, and terminate subscriptions for these units, as well as generate reports for cost-controlling purposes.
- **Subscription manager**: This role allows a user to subscribe to services and manage his own subscriptions. Unlike administrators, subscription managers are not permitted to work on subscriptions belonging to others or on subscription data related to billing and payment.
- **Technology manager**: This role allows a user to define technical services. It can be assigned to users of technology provider organizations.
- **Service manager**: This role allows a user to define marketable services and price models as well as publish marketable services. It can be assigned to users of supplier organizations.
- **Reseller**: This role allows a user to publish a supplier's marketable services applying different terms and conditions. It can be assigned to users of reseller organizations.
- **Broker**: This role allows a user to publish a supplier's marketable services without changing the terms and conditions defined by the supplier. It can be assigned to users of broker organizations.
- **Marketplace manager**: This role allows a user to define the organizations who are permitted to access a marketplace and publish services to it as well as update and customize a marketplace. This role can be assigned to users of marketplace owner organizations. It is automatically assigned to all administrators of the marketplace owner organization when a marketplace is created.
- **Operator**: This role allows a user to carry out configuration and maintenance tasks, manage organizations, and create marketplaces. The first operator is created together with its operator organization when CT-MG is installed.

2 Introduction

Describes Chapter 2

2.1 Deploying

Describes the deployment steps

2.2 Configuring

Required configuration steps BEFORE deploying OSCM

2.3 Results

Describes what is available once OSCM has been deployed.

3 Next Steps

After you have successfully completed the deployment of CT-MG, you can optionally change the URL to be used for accessing the CT-MG administration portal and the marketplaces. You can then start to set up the CT-MG organizations using the CT-MG administration portal.

Setting the Context Root

By default, the context root of the URL used for accessing the CT-MG administration portal and the marketplaces is `oscm-portal`. You can change this setting in the application server administration console. In addition, you need to adapt the `BASE_URL_HTTPS` configuration setting, and, if specified, the `BASE_URL` configuration setting, in CT-MG.

Proceed as follows:

1. In the application server administration console:
   1. Go to **Applications -> oscm-portal -> Edit** and set the **Context Root** as required.
   2. Go to **Applications -> oscm-portal-help -> Edit** and set the **Context Root** analogously to the one for `oscm-portal`.

      Example: If you set the context root for `oscm-portal` to `MyPortal`, set it to `MyPortal-help` for `oscm-portal-help`.
2. In the CT-MG administration portal, go to **Operation -> Update Configuration Settings** and change the `BASE_URL_HTTPS` configuration setting, and, if specified, the `BASE_URL` configuration setting, accordingly. See below for details on accessing CT-MG.

Accessing CT-MG

You can access the CT-MG administration portal in a Web browser using an URL in the following format:

`https://<server>:<port>/<context-root>/<tenant-id>` or

`http://<server>:<port>/<context-root>/<tenant-id>`

`<server>` is the host of the application server where CT-MG has been deployed. `<port>` is the port to address the application server (default: `8080` for HTTP, `8081` for HTTPS). `<context-root>` is the context root of CT-MG (default: `oscm-portal`). `<tenant-id>` is the ID of the tenant specified when installing CT-MG in SAML_SP mode. If installed in INTERNAL mode, the tenant ID is not appended to the URL.

You are prompted for a user ID and password.

The initial credentials are the following:

User ID: `administrator`

Password: `admin123`

It is recommended that you change the initial password in the CT-MG administration portal (**Change Password** page in the **Account** menu).

Connecting to the BIRT Report Engine

Adjust the `REPORT_ENGINEURL` configuration setting in CT-MG as follows:

In the CT-MG administration portal, choose **Update configuration settings** in the **Operation** menu. Change the host IP address and port to the ones of the application server to which you deployed the report engine:

```
http://<host IP address>:<port>/birt/frameset?
    __report=${reportname}.rptdesign&SessionId=${sessionid}
   &__locale=${locale}&WSDLURL=${wsdlurl}&SOAPEndPoint=${soapendpoint}
   &wsname=Report&wsport=ReportPort
```

Creating an Additional Operator Account

The creation of an additional operator account for your organization is useful, for example, to be able to delegate operational tasks or to unlock other operator accounts in case the password has been forgotten. Proceed as follows:

In the CT-MG administration portal, choose **Register new users** in the **Account** menu. Enter the relevant user data and assign at least the **Operator** role.

Changing the CT-MG Configuration

Refer to the *Operator's Guide* in case you need to change the configuration of your CT-MG installation.

3.1 Tool Support for Operating CT-MG

CT-MG provides operator functions in its administration portal that support you in performing on-demand maintenance and operation tasks. For some functions, you can also use the operator client, which is available as a command line tool.

CT-MG Administration Portal

You can access the CT-MG administration portal in a Web browser using an URL in the following format:

`http://<server>:<port>/<context-root>`

`<server>` is the application server where CT-MG has been deployed. `<port>` is the port to address the application server (default: `8080` for HTTP, `8081` for HTTPS). `<context-root>` is the context root of CT-MG (default: `oscm-portal`).

You are prompted for the user ID and password. The initial credentials are as follows:

User ID: `administrator`

Password: `admin123`

It is recommended that you change the initial password in the CT-MG administration portal (**Change Password** page in the **Account** menu).

After login, the operator functionality is available in the **Operation** menu.

Command Line Tool

The command line tool provides a subset of the functions that are available in the **Operation** menu in the CT-MG administration portal.

The command line tool is provided in the CT-MG installation package, `oscm-install-pack.zip`, as `oscm-operatorclient.zip`. The contents of this package can be made available in your environment as follows:

1. Extract the contents of the `oscm-operatorclient.zip` file to a separate directory on the system where you have installed CT-MG. The directory contains the required configuration files, jar files, and scripts.
2. Set the `GLASSFISH_HOME` environment variable to the directory where you have installed the application server.
3. Run the `prepareCP.cmd` script located in the directory to which you extracted the `oscm-operatorclient.zip` file. This script copies the required `.jar` files from the application server installation directory.
4. Adapt the settings in the `env.properties` file to your environment. This file is located in the directory to which you extracted the `oscm-operatorclient.zip` file.

For executing a command, change to the directory to which you extracted the `oscm-operatorclient.zip` file.

Command Syntax:

The syntax of all available commands is as follows:

```
<JAVA_HOME>/bin/java -jar lib/oscm-operatorsvc-client.jar
 <userkey> <password>
 <command> <parameter>
```

where

`<JAVA_HOME>` is the installation directory of your JDK (for example `C:\XXX\jdk1.8.0_121`).

`userkey` is the numeric key of the operator. The key of the initial operator is `1000`.

`password` is the password of the operator. The initial passwort is `admin123`.

`command` is the command to be executed.

`parameter` is a command parameter to be set.

You can change the initial password in the CT-MG administration portal (**Change Password** page in the **Account** menu).

4 CT-MG in SUSE OpenStack Cloud

CT-MG is installed as a workload in the SUSE Openstack Cloud (SOC).

The OSCM installation on SOC consists of the following main steps:

- Create OpenStack resources for CT-MG
- Pull Docker images (oscm, app and database) from specified repository, configure and run containers.

OpenStack Resources for OSCM

The following resources are created in OpenStack:

oscm project

oscm user (with corresponding roles)

oscm.medium flavor

oscm keypair

oscm stack with 2 cinder volumes (for database and application data - config, logs)

oscm stack with 1 instance with the 2 cinder volumes attachments (virtual machine based on SLES where oscm docker containers will run)

Both stacks are created with using heat templates (can be found in the crowbar-openstack code).

```
crowbar-openstack/chef/cookbooks/oscm/files/default/volumes.yaml
crowbar-openstack/chef/cookbooks/oscm/files/default/applications.yaml
```

The Docker part (pull, configure, start containers) runs via cloud init on the first start of the instance (VM). The scripts can be found at the following location:

```
crowbar-openstack/chef/cookbooks/oscm/files/default/user-data
```

The other resources mentioned are created in the chef recipe of the oscm barclamp:

```
crowbar-openstack/chef/cookbooks/oscm/recipes/server.rb
```

Tip: Locate all oscm barclamp code in the crowbar-framework search for string "oscm"

OSCM Passwords

There are 3 different layers where we deal with OSCM passwords:

OpenStack: user "oscm" with password "oscm". Can be changed by the OSCM operator in Horizon dashboard or with command line client from OpenStack.

Glassfish admin credentials (user: "oscm", password: generated from openstack), Glassfish keystores (password generated by openstack), Postgres (user "postgres", password: generated from openstack)

OSCM applicaltion (platform operator user: "administrator", password: "admin123").

The passwords for the glassfish and postgres are random strings, found as resource in the stack. They are generated, because otherwise they will be visible on the Horizon dashboard by stack overview.

They are displayed as stack resource of type OS::Heat::RandomString.

The value of the password can be shown on command line on controller node (be sure to use environment for oscm - oscm project and user). The following example shows the resource "as_admin_password" from the stack "oscm-instances" displayed also on the picture bellow.

```
openstack stack resource show -f shell oscm-instances as_admin_password
```

Output can be as following (the value of the password is 2lkXaVAZbsTbbgZmkdrGjy8WXrcvRXwG).

```
attributes="{u'value': u'2lkXaVAZbsTbbgZmkdrGjy8WXrcvRXwG'}"
creation_time="2017-04-18T07:56:24Z"
description=""
 links="[{u'href': u'http://192.168.53.2:8004/v1/df18d51e5f684ee0873acd69bb6426b4/s
 u'rel': u'self'},
 {u'href': u'http://192.168.53.2:8004/v1/df18d51e5f684ee0873acd69bb6426b4/stacks/os
 u'rel': u'stack'}]"
logical_resource_id="as_admin_password"
physical_resource_id="oscm-instances-as_admin_password-d4ezt64jm67x"
required_by="[u'user_data_params']"
resource_name="as_admin_password"
resource_status="CREATE_COMPLETE"
resource_status_reason="state changed"
 resource_type="OS::Heat::RandomString"
updated_time="2017-04-18T07:56:24Z"
```

[[!StackResources.PNG!]] [Click to start editing]

SSL Encryption

OSCM uses https for communication but also for client authentication (APP). [[!ssl.png!]]

The default s1as certificates of oscm and app domains are used for the https between the containers. From security point of view it is acceptable, since it is not public network. Nevertheless, the s1as certificates are generated for each container installation (otherwise each OSCM container in the world would use the same certificates!) This is done in scripts for cloud init.

For the web part, the cloud administrator can choose if http or https is required at installation time. In case of https, it has a possibility to specify secure certificates (not self-signed s1as that the scripts generate).

In the development/test environment we are using the floating IP for accessing the web part of OSCM. In production environment, there are domain names, for which also the secure certificates are signed (CN=<domain name>).

Since APP uses the client_auth for SOAP with certificates, the CN in the certificate must match the app host name (it is specified to be "app" docker host, for oscm the docker host is "web"). This means the secure certificates with real domain name cannot be used for the https for SOAP.

So separate http listeners by glassfish server will be used for SOAP with s1as as certificate (at least for APP), and if secure certificates used for web, this certificate will be applied for the http listeners for web part.

It can be configurated in domain.xml -> secure http listener, cert-nick).

However SOAP API is also public as the UI, but for now there is no plan for some SOAP integration in SUSE environment.