FUJITSU

FUJITSU Software Enterprise Service Catalog Manager V16.1

Trusted Public S5 Integration (GlassFish)

B1WS-1265-02
September 2016

Contents

About this Manual

This manual describes the integration of FUJITSU Cloud IaaS Trusted Public S5 (TPS5) with FUJITSU Software Enterprise Service Catalog Manager - hereafter referred to as Catalog Manager (CT-MG).

This manual is structured as follows:

Chapter	Description
Introduction on page 8	Provides an overview of the CT-MG TPS5 integration, the components involved, and the supported usage scenarios.
Installing the TPS5 Integration Software on page 10	Describes how to prepare and carry out the installation of the TPS5 integration software.
Creating and Publishing Services on page 22	Describes how to create and publish services for TPS5 in CT-MG.
Using TPS5 Services in CT-MG on page 24	Describes how to provision, modify, and deprovision virtual systems in TPS5 through services in CT-MG.
Administrating the TPS5 Integration on page 26	Describes administration tasks related to the CT-MG TPS5 integration.
Uninstallation on page 31	Describes how to uninstall the CT-MG TPS5 integration software.

Readers of this Manual

This manual is intended for operators who want to offer virtual systems controlled by TPS5 through services on a marketplace provided by CT-MG. It assumes that you have access to an existing CT-MG installation and to a TPS5 platform. In addition, you should have basic knowledge of TPS5 and you should be familiar with the concepts and administration of CT-MG.

Notational Conventions

This manual uses the following notational conventions:

Add	The names of graphical user interface elements like menu options are shown in boldface.
`init`	System names, for example command names and text that is entered from the keyboard, are shown in Courier font.
`<variable>`	Variables for which values must be entered are enclosed in angle brackets.
`[option]`	Optional items, for example optional command parameters, are enclosed in square brackets.
`one | two`	Alternative entries are separated by a vertical bar.
`{one | two}`	Mandatory entries with alternatives are enclosed in curly brackets.

Abbreviations

This manual uses the following abbreviations:

APP	Asynchronous Provisioning Platform
CT-MG	Catalog Manager
DBMS	Database Management System
IaaS	Infrastructure as a Service
IdP	SAML Identity Provider
SAML	Security Assertion Markup Language
STS	Security Token Service
TPS5	Trusted Public S5
WSDL	Web Services Description Language
WSIT	Web Services Interoperability Technologies

Available Documentation

The following documentation on CT-MG is available:

- *Overview:* A PDF manual introducing CT-MG. It is written for everybody interested in CT-MG and does not require any special knowledge.
- *Online Help:* Online help pages describing how to work with the administration portal of CT-MG. The online help is intended for and available to everybody working with the administration portal.
- *Installation Guide (GlassFish):* A PDF manual describing how to install and uninstall CT-MG. It is intended for operators who set up and maintain CT-MG in their environment.
- *Operator's Guide:* A PDF manual for operators describing how to administrate and maintain CT-MG.
- *Technology Provider's Guide:* A PDF manual for technology providers describing how to prepare applications for usage in a SaaS model and how to integrate them with CT-MG.
- *Supplier's Guide:* A PDF manual for suppliers describing how to define and manage service offerings for applications that have been integrated with CT-MG.
- *Reseller's Guide:* A PDF manual for resellers describing how to prepare, offer, and sell services defined by suppliers.
- *Broker's Guide:* A PDF manual for brokers describing how to support suppliers in establishing relationships to customers by offering their services on a marketplace.
- *Marketplace Owner's Guide:* A PDF manual for marketplace owners describing how to administrate and customize marketplaces in CT-MG.
- *Developer's Guide:* A PDF manual for application developers describing the public Web services and application programming interfaces of CT-MG and how to integrate applications and external systems with CT-MG.
- *ServerView Resource Orchestrator Integration (GlassFish):* A PDF manual for operators describing how to offer and use virtual platforms and servers controlled by FUJITSU ServerView Resource Orchestrator through services in CT-MG.

- *Amazon Web Services Integration (GlassFish):* A PDF manual for operators describing how to offer and use virtual servers controlled by the Amazon Elastic Compute Cloud Web service through services in CT-MG.
- *OpenStack Integration (GlassFish):* A PDF manual for operators describing how to offer and use virtual systems controlled by OpenStack through services in CT-MG.
- *Trusted Public S5 Integration (GlassFish):* A PDF manual for operators describing how to offer and use virtual systems controlled by FUJITSU Cloud IaaS Trusted Public S5 through services in CT-MG.
- *VMware vSphere Integration (GlassFish):* A PDF manual for operators describing how to offer and use virtual machines provisioned on a VMware vSphere server through services in CT-MG.
- *Systemwalker Runbook Automation Integration Guide:* A PDF manual for operators describing how to offer and use automated operation processes of Systemwalker Runbook Automation through services in CT-MG.
- *IaaS Integration Guide:* A PDF manual for operators describing how to offer and use virtual systems on different platforms through services in CT-MG.
- Javadoc and YAML documentation for the public Web services and application programming interfaces of CT-MG and additional resources and utilities for application developers.

1 Introduction

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.

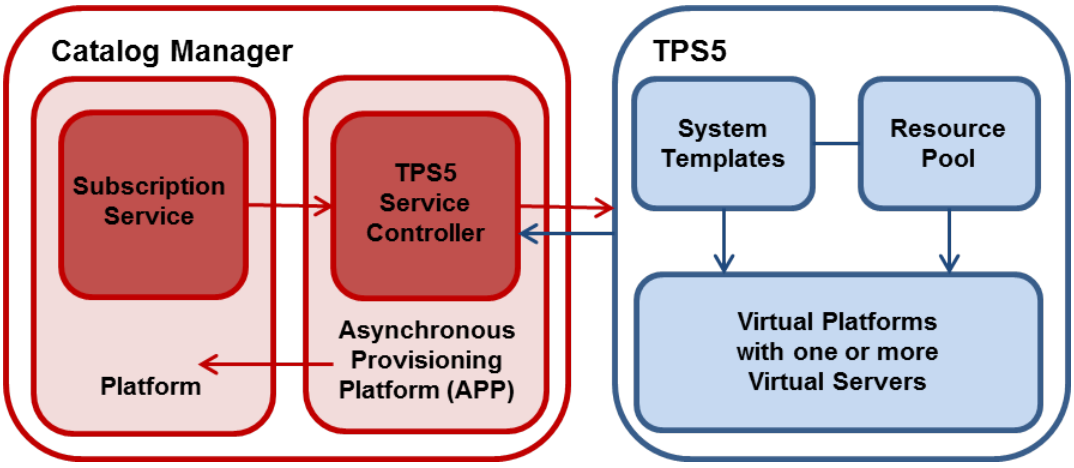
FUJITSU Cloud IaaS Trusted Public S5 (TPS5) gives you on-demand access to a shared pool of fully configured virtual server, storage, and network resources hosted in the FUJITSU global network of data centers. The provisioning of computing resources in the Cloud allows you to rapidly scale and flex your infrastructure to support new business initiatives or roll out services. On virtual platforms, 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 CT-MG and TPS5 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 platforms with one or more virtual servers in TPS5. The usage costs can be calculated and charged by means of the CT-MG billing and payment services.

The TPS5 integration package provided with CT-MG includes all the components required for connecting an existing CT-MG installation with TPS5. This manual describes how to deploy this package and how to create and use services for TPS5 on a CT-MG marketplace.

1.1 Components Involved in the TPS5 Integration

The following picture provides an overview of the main components involved in the integration of CT-MG and TPS5:



In CT-MG, customer subscriptions are managed by means of the **Subscription service**. When a customer creates, modifies, or terminates a subscription for a virtual platform in TPS5, the Subscription service asynchronously triggers the corresponding actions in TPS5 through the **Asynchronous Provisioning Platform (APP)** and the **TPS5 service controller**: Virtual platforms are created, modified, or deleted in TPS5.

APP is a framework which provides a provisioning service, an operation service, as well as functions, data persistence, and notification features which are required for integrating applications with CT-MG in asynchronous mode. The actual communication with the applications is carried out by service controllers. APP and the TPS5 service controller are the main components that make up the TPS5 integration software.

In TPS5, the basic configurations of virtual platforms for typical usage scenarios are defined by the TPS5 administrators in so-called **system templates**. Different system templates are available for small, medium, and large scale operation. Virtual images for provisioning the virtual servers on the virtual platforms are provided in a **resource pool**.

Each APP installation supports one TPS5 service controller. This limitation can be overcome by installing APP several times to different application server domains. The need for more than one service controller may arise because multiple TPS5 accounts or technology provider organizations have to be used.

1.2 Usage Scenarios

The CT-MG TPS5 integration supports the following usage scenarios:

- **Provisioning of a virtual platform**: When a customer subscribes to a corresponding service on a CT-MG marketplace, TPS5 is triggered to create a virtual platform with one or more virtual servers based on a specific system template.
- **Horizontal scale-up and scale-down**: By changing the corresponding parameters at an existing subscription, customers can trigger TPS5 to add a virtual server to their virtual platform. In the same way, they can request TPS5 to remove a virtual server from the platform.
- **Vertical scale-up and scale-down**: By changing the corresponding parameters at an existing subscription, customers can trigger TPS5 to add disks to each virtual server in their virtual platform. In the same way, they can request TPS5 to remove disks from the virtual servers.
- **Starting and stopping a virtual platform**: A customer can explicitly start and stop a virtual platform in TPS5 by executing a service operation at the corresponding subscription.
- **Deletion of a virtual platform**: When a customer terminates a subscription for a virtual platform, TPS5 is triggered to delete it. The subscription is terminated independent of whether the deletion is successful.

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

For more details on the usage scenarios, refer to *Using TPS5 Services in CT-MG* on page 24.

2 Installing the TPS5 Integration Software

The following sections describe how to install and configure the TPS5 integration software as well as the preparations you need to take beforehand.

Installing the TPS5 integration software consists of installing APP and registering the TPS5 service controller.

If you already have a working APP installation in your environment, proceed as described in *Installing the TPS5 Service Controller in an Existing APP Environment* on page 18.

2.1 Prerequisites and Preparation

The following sections describe the prerequisites that must be fulfilled and the preparations you need to take before installing and deploying the TPS5 integration software.

2.1.1 CT-MG and TPS5

- You must have access to a fully functional CT-MG installation. You can install the TPS5 integration software in the same environment or on a different server.
- You must have access to CT-MG as an administrator and as a technology manager of an organization that has at least the technology provider role.
- You must have access to the TPS5 platform.

  You have to register as a service subscriber in the Service Portal of your TPS5 region. As a registered service subscriber, you receive an Administrator ID and an initial password. With these credentials, you can log in to the Service Portal to download the client certificate that is needed for accessing the TPS5 platform. For details on the certificates, refer to the TPS5 documentation.

2.1.2 Hardware and Operating Systems

The TPS5 integration software as a Java application does not rely on specific hardware or operating systems. It can be deployed on any platform supported by the application server and the database management system.

2.1.3 Java and Ant

The TPS5 integration software requires a Java Development Kit (JDK), version 7, 64 bit. Deployment with JDK 7, Update 45 has been tested and is recommended.

Due to a CORBA library change which is incompatible with Oracle GlassFish Server version 3.1.2.2, deployment with JDK 7, Update 55 and higher is not supported.

In order to be able to execute the installation scripts, you need to install the Apache Ant 1.8 (or higher) open source software. In the subsequent sections, `<ANT_HOME>` is the installation directory of Apache Ant.

2.1.4 Application Server

The TPS5 integration software must be deployed on an application server compatible with Java EE version 6. The following application server is supported:

Oracle GlassFish Server, version 3.1.2.2.

You can deploy the TPS5 integration software on the application server you use for CT-MG. Alternatively, you can use a separate application server installation.

Note: Before installing GlassFish, make sure that the `JAVA_HOME` environment variable points to a Java Development Kit (JDK), version 7, 64 bit.

Proceed as follows:

1. Install the application server as described in its documentation, and configure it as required by your environment.

Note: Make sure that the path of the GlassFish installation directory does not contain blanks.

2. After you have configured GlassFish, make a backup copy of the GlassFish installation.
3. Make sure that GlassFish is running in a JDK 7 environment. Also, make sure that no other applications (e.g. Tomcat) are running on your GlassFish ports.

The installation of the TPS5 integration software creates the `app-domain` domain in your application server. If required, you can change the domain name in the `glassfish.properties` file before starting the installation.

In the subsequent sections, `<GLASSFISH_HOME>` is the installation directory of GlassFish.

2.1.5 Relational Database

The TPS5 integration software stores its data in a relational database. The following database management system (DBMS) is supported:

PostgreSQL, version 9.1.12.

Install the DBMS as described in its documentation.

If required, you can use a separate machine for the TPS5 integration database.

Setup and Configuration

Edit the file

`<postgres_dir>/data/postgresql.conf`

as follows (`<postgres_dir>` is the PostgreSQL installation directory):

1. Set the `max_prepared_transactions` property value to `50`.
2. Set the `max_connections` property value to `210`.

   This property determines the maximum number of concurrent connections to the database server.

   Note the following: This setting is used in combination with the JDBC pool size settings for the domains on your application server. If you change the JDBC pool size, you might need to adapt the `max_connections` setting. Refer to the CT-MG *Operator's Guide*, section *Tuning Performance*, for details.

3. Set the `listen_addresses` property value:

   Specify the IP addresses of all application servers on which the database server is to listen for connections from client applications. If you use the entry `'*'`, which corresponds to all available IP addresses, you must be aware of possible security holes.

4. Save the file.

If you use a server name in all configuration files instead of `localhost` during installation, edit the file

`<postgres_dir>/data/pg_hba.conf`

as follows (`<postgres_dir>` is the PostgreSQL installation directory):

1. Add the IP address of the application server that is to host the TPS5 integration software.

   For example:

   ```
   host all all 123.123.12.1/32 md5
   ```

   Also add the application server's IPv6 address.

   For example:

   ```
   host all all fe80::cdfb:b6ed:9b38:cf17/128 md5
   ```

   There are authentication methods other than `md5`. For details, refer to the PostgreSQL documentation.

2. Save the file.

Restart your PostgreSQL server for the changes to take effect.

2.1.6 Mail Server

To inform users about relevant issues, the TPS5 integration software requires a mail server in its environment. You can use any mail server that supports SMTP.

The settings for addressing the mail server are defined in the `glassfish.properties` file of the TPS5 integration package.

2.2 Installation

The installation of the TPS5 integration software consists of the following main steps:

- *Preparing the Software and Setup Utilities* on page 12
- *Configuring the TPS5 Integration* on page 13
- *Setting up the Database* on page 15
- *Setting up the Application Server Resources* on page 16
- *Exchanging Certificates* on page 17

2.2.1 Preparing the Software and Setup Utilities

The TPS5 integration software and setup utilities are provided in the TPS5 integration package, `oscm-tps5-install-pack.zip`. The contents of the package need to be made available in your environment as follows:

Extract the contents of the `oscm-tps5-install-pack.zip` package to a separate temporary directory on the system from where you want to install and deploy the TPS5 integration software.

In the following sections, this directory is referred to as `<install_pack_dir>`.

After extraction, the following directories are available:

- **`databases/app_db`**

  Configuration files for setting up the database used by the TPS5 integration software.

- **`doc`**

The *Trusted Public S5 Integration* guide (this manual).

- **`domains/app_domain`**
  - Configuration file (`glassfish.properties`) for setting up the application server resources for the domain to which the TPS5 integration software is to be deployed.
  - `applications`: The APP application (`oscm-app.ear`) and the TPS5 service controller (`oscm-app-tps5.ear`).
  - `applib`: Folder for the required TPS5 libraries. See below for details.
- **`install`**

  XML files that support you in setting up the database and the application server resources for APP.
- **`samples`**

  Technical service samples.

Adding the TPS5 libraries to the `applib` folder:

Specific libraries required for accessing TPS5 are not delivered in the TPS5 integration package, `oscm-tps5-install-pack.zip`. They must be downloaded from the TPS5 Service Portal:

1. Log in to the Service Portal of your TPS5 region.
2. Open the **Manual** menu and click **API Library** in the **Related Documents** section. This starts the download of the `OViSSSDK_*.zip` file containing the required libraries.
3. Extract the `.zip` file to a temporary directory.
4. Copy the content of the `OViSS_JAVASDK/lib` directory to the `applib` subdirectory of the `<install_pack_dir>/domains/app_domain` directory.

2.2.2 Configuring the TPS5 Integration

The TPS5 integration software and setup utilities require a number of settings. These settings are provided in the following subdirectories and files of `<install_pack_dir>`:

- **`databases/app_db`**
  - `db.properties`: Settings for the database setup and access.
  - `configsettings.properties`: Configuration settings for APP.

    The initial installation stores these settings in the `bssapp` database, where you can change them later, if required. An update installation only adds new settings to the database, but does not overwrite existing ones.
  - `configsettings_controller.properties`: Configuration settings for the TPS5 service controller.

    The initial installation stores these settings in the `bssapp` database. You can change them later using a graphical user interface.

    The `configsettings_controller.properties` file specifies the organization ID and user credentials for accessing CT-MG as well as the account settings for accessing the TPS5 platform. For security reasons, it is recommended that you delete the file as soon as you have successfully installed and configured the TPS5 integration software.
- **`domains/app_domain`**

  The configuration settings for setting up the application server domain to which APP is deployed are provided in the following file:

`glassfish.properties`

Additional configuration files contained in other subdirectories are used internally and must not be changed.

For details on the configuration settings, refer to *Configuration Settings* on page 32. For details on updating the configuration settings, refer to *Updating Configuration Settings* on page 28.

You need to adapt the settings in the files above to your environment. In particular, server names, ports, paths, user IDs, and passwords require adaptation.

Proceed as follows to view and adjust the configuration settings:

1. Open each of the configuration files listed above with an editor.
2. Check the settings in each file and adapt them to your environment.
3. Save the files to their original location in `<install_pack_dir>/<subdirectory>`. For future reference, it is a good idea to create a backup of the files.

Observe the following configuration issues:

- The specified ports are suggestions and work with the default settings used in the files.
- If you install everything on the local system, use either the server name or `localhost` in all configuration files for all URLs that need to be resolved by APP.

  The `APP_BASE_URL` setting in the `configsettings.properties` file for the `app-domain` domain must be resolved by clients. They always require that the server name be specified.

  Specify the `APP_BASE_URL` setting as follows:

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

  If you have changed the `glassfish.domain.portbase` setting in the `glassfish.properties` file, you must change the port here accordingly.

Configuration for SAML_SP authentication mode:

If the CT-MG installation you want to work with is configured for SAML_SP authentication mode, Web service calls to it are secured and authenticated by a Security Token Service (STS). This is a Web service that issues security tokens as defined in the WS-Security/WS-Trust specification. The STS is usually provided by the Identity Provider (IdP) system in use (for example Active Directory Federation Service, Cloudminder, or OpenAM).

To use an STS for Web service calls, you must perform the following steps before installing the TPS5 integration software:

1. From the 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 STS.
2. Save the metadata exchange file to the following file, overwriting the existing empty file:

   `<install_pack_dir>/domains/app_domain/wsit/STSService.xml`
3. Open the `STSService.xml` file and retrieve the value of `targetNamespace`, for example:

   `http://schemas.microsoft.com/ws/2008/06/identity/securitytokenservice`
4. Open the following file:

   `<install_pack_dir>/domains/app_domain/wsit/wsit-client.xml`
5. Replace the placeholder in the `namespace` tag of the `wsit-client.xml` file with the `targetNamespace` value copied from the `STSService.xml` file.
6. Close and save the `wsit-client.xml` file to its original location.

During the installation process, an `OSCM-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 `<install_pack_dir>/domains/app_domain/lib`.

7. Make sure that you enter correct values for the SAML_SP authentication mode in the `configsettings.properties` file in `<install_pack_dir>/databases/app_db`:
   - `BSS_AUTH_MODE=SAML_SP`
   - `BSS_STS_WEBSERVICE_URL=https://<server>:<port>/{SERVICE}/STS`
   - `BSS_STS_WEBSERVICE_WSDL_URL= https://<server>:<port>/oscm/v1.9/{SERVICE}/STS?wsdl`
   - `APP_KEYSTORE_PASSWORD=changeit`
   - `APP_TRUSTSTORE_PASSWORD=changeit`

2.2.3 Setting up the Database

The TPS5 integration software requires and stores its data in the `bssapp` PostgreSQL database.

The database is created by executing installation scripts. It is initialized with the appropriate schema and settings.

Proceed as follows:

1. Make sure that the database server is running.
2. Open the command prompt (Windows) or a terminal session (UNIX/Linux).
3. Set the following environment variable for your current session:

   `DB_INTERPRETER`: The absolute path and name of the `psql` executable of PostgreSQL. The executable is usually located in the `bin` subdirectory of the PostgreSQL installation directory.

   Example (Unix/Linux):

   ```
   export DB_INTERPRETER="/opt/PostgreSQL/9.1/bin/psql"
   ```

   Example (Windows):

   ```
   set DB_INTERPRETER="C:\Program Files\PostgreSQL\9.1\bin\psql"
   ```

4. Create the database by executing the `build-db.xml` file in `<install_pack_dir>/install` as follows:

   ```
   <ANT_HOME>/bin/ant -f build-db.xml initDB
   ```

   If you set an ID or password other than `postgres` for the PostgreSQL user account (`postgres`) when installing the database management system, you have to specify the ID or password with the call to the `build-db.xml` file as follows:

   ```
   <ANT_HOME>/bin/ant -f build-db.xml initDB
      -Ddb.admin.user=<user ID> -Ddb.admin.pwd=<password>
   ```

Note: It may be required to enclose the `-Ddb.admin.user=<user ID>` and `-Ddb.admin.pwd=<password>` in double or single quotes depending on the operating system.

If the setup of the database fails with errors, proceed as follows:

1. Check and correct the configuration files.
2. Execute the `build-db.xml` file in `<install_pack_dir>/install` as follows:

```
<ANT_HOME>/bin/ant -f build-db.xml DROP.dbsAndUsers
```

3. Repeat the setup.

2.2.4 Setting up the Application Server Resources

The TPS5 integration software requires specific settings and resources in the application server, such as mail settings or a data source.

Proceed as follows to create the resources and make the required settings in the application server:

1. Open the command prompt (Windows) or a terminal session (UNIX/Linux).
2. Execute the `build-glassfish.xml` file in `<install_pack_dir>/install` as follows:

```
<ANT_HOME>/bin/ant -f build-glassfish.xml SETUP
```

   This has the following results:

   - The `app-domain` domain is created and started.
   - The settings and resources for APP are created in the application server.
   - APP (`oscm-app.ear`) is deployed to the `app-domain` domain.
   - The TPS5 service controller (`oscm-app-tps5.ear`) is deployed to the `app-domain` domain.

3. Depending on your environment, it may be required to define a proxy server for the `app-domain` domain in the **JVM Options** of the application server. The TPS5 service controller can address the corresponding system via the proxy server.

   To define a proxy server, specify the following JVM options:

   - `-Dhttps.proxyHost`
   - `-Dhttps.proxyPort`

   If authentication is required, specify the following additional settings:

   - `-Dhttps.proxyUser`
   - `-Dhttps.proxyPassword`

   For all direct communication, you need to bypass the proxy server. Specify the hosts which are to be addressed directly and not through the proxy server in the following setting:

   - `-Dhttp.nonProxyHosts`

   For example, APP must not use the configured proxy for Web service calls to CT-MG:

   `-Dhttp.nonProxyHosts=localhost|127.0.0.1|myServer*`

   where `myServer` is the host on which CT-MG is running.

   In case several service controllers are to run in the same APP domain, and only one of them is to communicate via a proxy server, you need to exclude the target systems of the other service controllers, for example, as follows:

   `-Dhttps.proxyHost=proxy.intern.myserver.com`

   `-Dhttps.proxyPort=8081`

   `-Dhttp.nonProxyHosts=myServer.com|localhost|127.0.0.1|`

`http://10.140.18.112*|http://myServer.com:8880/templates/*|`
`https://ror-demo.myServer.com:8014/cfmgapi/endpoint*`

After having configured the proxy server, restart the `app-domain`.

If the setup of the application server domain fails with errors, proceed as follows:

1. Stop the `app-domain` domain.
2. Delete the `app-domain` domain.
3. Repeat the setup.

2.2.5 Exchanging Certificates

For secure communication of the TPS5 integration software with CT-MG, you need to exchange the corresponding certificates.

You need to:

- Import the certificates of CT-MG and TPS5 into the truststore of the `app-domain` application server domain of the TPS5 integration software.
- Export the certificate of the `app-domain` domain and import it into the `bes-domain` application server domain of CT-MG.

Proceed as follows:

1. Obtain a `.crt` file with the certificate of CT-MG from the CT-MG operator.

   The `.crt` file can be created, for example, by executing the following command at the command prompt (Windows) or in a terminal session (UNIX/Linux) on the application server where CT-MG is deployed:

```
<AppServerJRE>/bin/keytool -export -rfc -alias s1as
   -file ctmgbss.crt -storepass <password> -keystore
   <GLASSFISH_HOME>/glassfish/domains/bes-domain/config/keystore.jks
```

2. Obtain the valid TPS5 certificate by exporting it from the `cacerts.jks` file. The file is contained in the `OViSS_JAVASDK/bin/security` subdirectory of the temporary directory to which you extracted the `OViSSSDK_*.zip` file you downloaded from the TPS5 Service Portal. Refer to *Preparing the Software and Setup Utilities* on page 12 for details.

   For details on the certificates, refer to the TPS5 documentation.

3. Import the certificate of CT-MG and TPS5 into the truststore of the `app-domain` application server domain.

   To import the CT-MG certificate from the `.crt` file you created, you can use, for example, the following command at the command prompt (Windows) or in a terminal session (UNIX/Linux) on the application server:

```
<AppServerJRE>/bin/keytool -import -trustcacerts -alias <alias>
   -file <filename>.crt -storepass <password> -keystore
   <GLASSFISH_HOME>/glassfish/domains/app-domain/config/cacerts.jks
```

   To import the TPS5 certificate, you can use, for example, the following command at the command prompt (Windows) or in a terminal session (UNIX/Linux) on the application server:

```
<AppServerJRE>/bin/keytool -import -trustcacerts -alias <alias>
   -file <filename> -storepass <password> -keystore
   <GLASSFISH_HOME>/glassfish/domains/app-domain/config/cacerts.jks
```

4. Create a `.crt` file with the certificate of the `app-domain` domain in which you have deployed the TPS5 integration software.

   The `.crt` file can be created, for example, by executing the following command at the command prompt (Windows) or in a terminal session (UNIX/Linux) on the application server:

```
<AppServerJRE>/bin/keytool -export -rfc -alias s1as
   -file ctmgapp.crt -storepass <password> -keystore
   <GLASSFISH_HOME>/glassfish/domains/app-domain/config/keystore.jks
```

5. Import the certificate of the `app-domain` domain into the `bes-domain` application server domain of CT-MG.

   To do this, you can use, for example, the following command at the command prompt (Windows) or in a terminal session (UNIX/Linux) on the application server:

```
<AppServerJRE>/bin/keytool -import -trustcacerts -alias ctmgapp
   -file ctmgapp.crt -storepass <password> -keystore
   <GLASSFISH_HOME>/glassfish/domains/bes-domain/config/cacerts.jks
```

6. If the TPS5 integration software and CT-MG are configured for SAML_SP authentication mode, obtain the relevant certificates from the IdP system and import them into the truststore of the `app-domain` domain.

   For example, when using Microsoft Active Directory as the IdP, you need to obtain and import the service communications and token-signing certificates.

7. Stop and restart the `app-domain` and the `bes-domain` domains for the certificates to become effective.

2.3 Installing the TPS5 Service Controller in an Existing APP Environment

If you already have a working APP installation in your environment, you can use it for the TPS5 integration and simply register the TPS5 service controller in it. Proceed as follows:

1. Check the prerequisites described in *CT-MG and TPS5* on page 10.
2. Deploy the TPS5 service controller to the `app-domain` domain. To do this, you use the GlassFish administration console, for example:

   `http://127.0.0.1:8848/`

   The `oscm-app-tps5.ear` file of the service controller is located in `<install_pack_dir>/domains/app_domain/applications`
3. Register the TPS5 service controller as follows in APP:
   1. In a Web browser, access the base URL of APP, for example:
      `http://127.0.0.1:8880/oscm-app`
   2. Log in with the ID and password of the user and organization defined in the `configsettings.properties` file of APP (`BSS_USER_ID` and `BSS_USER_PWD`).
   3. Specify the controller ID (`ess.tps5`) and the technology provider organization responsible for the TPS5 service controller.
   4. Click **Save Configuration** to save the settings.
4. Configure the TPS5 service controller following the instructions in *Updating Configuration Settings* on page 28.

5. Import the certificate of TPS5 into the truststore of the `app-domain` application server domain of the TPS5 integration software:
   - Obtain the valid TPS5 certificate by exporting it from the `cacerts.jks` file. The file is contained in the `OViSS_JAVASDK/bin/security` subdirectory of the temporary directory to which you extracted the `OViSSSDK_*.zip` file you downloaded from the TPS5 Service Portal. Refer to *Preparing the Software and Setup Utilities* on page 12 for details.

     For details on the certificates, refer to the TPS5 documentation.
   - Import the TPS5 certificate, for example, by executing the following command at the command prompt (Windows) or in a terminal session (UNIX/Linux) on the application server:

```
<AppServerJRE>/bin/keytool -import -trustcacerts -alias <alias>
   -file <filename> -storepass <password> -keystore
   <GLASSFISH_HOME>/glassfish/domains/app-domain/config/cacerts.jks
```

6. Stop and restart the `app-domain` and the `bes-domain` domains for the certificate to become effective.

2.4 Update Installation

Before updating your installation of the TPS5 integration software, read the *Release Notes* of the new release. They contain information on compatibility issues, changes and enhancements, and known restrictions.

Preparing the Update

Before you start with the update installation, carry out the following steps:

1. Make sure that all provisioning operations are complete. Follow the steps as described in *Handling Problems in the Provisioning Process* on page 26.
2. In the `app-domain` application server domain, disable or undeploy the following applications:

   `oscm-app`

   `oscm-app-tps5`
3. Check for `.glassfishStaleFiles` files in the `app-domain` domain. If there are any, delete them. The files are located in

   `app-domain/applications/<application name>/.glassfishStaleFiles`

   For example:

   `app-domain/applications/oscm-app/.glassfishStaleFiles`
4. Set the following environment variable for your current session:

   `DB_INTERPRETER`: The absolute path and name of the `psql` executable of PostgreSQL. The executable is usually located in the `bin` subdirectory of the PostgreSQL installation directory.

   Example:

```
export DB_INTERPRETER="/opt/PostgreSQL/9.1/bin/psql"
```

5. Prepare the new TPS5 integration software and setup utilities and include the required TPS5 libraries. Proceed as described in *Preparing the Software and Setup Utilities* on page 12.

6. Execute the `patch-SSO.xml` file in `<install_pack_dir>/install` as follows:

```
<ANT_HOME>/bin/ant -f patch-SSO.xml
 patchController -Ddomain.dir=app_domain
```

Note: This command creates a backup of the initial `<install_pack_dir>/domains/app_domain/applications/oscm-app-tps5.ear` file in the following directory:

`<install_pack_dir>/domains/app_domain/tmp`

The initial file is overwritten with the one containing the TPS5 libraries.

Updating the Database

Proceed with updating the database as follows:

1. Check whether the file

   `postgresql-9.1-903.jdbc4.jar`

   is contained in the following directories of the application server:

   - `lib` directory of the `app-domain` domain
   - `<GLASSFISH_HOME>/mq/lib/ext`

   If it is not, copy the file from the `<install_pack_dir>/install/lib` directory to the location where it is missing.
2. Create a backup of the `bssapp` database using the standard PostgreSQL commands. The database backup must be compatible with PostgreSQL 9.1.12.
3. Update the following configuration files so that the settings match your current installation:
   - `db.properties`
   - `configsettings.properties`
   - `configsettings_controller.properties`
4. Update the schema and configuration settings of the `bssapp` database by executing the `build-db.xml` file in `<install_pack_dir>/install` as follows:

```
<ANT_HOME>/bin/ant -f build-db.xml updateDatabase
```

Note: Make sure that Ant runs in a Java 7 runtime environment when calling the `build-db.xml` file.

Updating the Application Server

After you have executed the preparation steps, redeploy or deploy the applications that make up the TPS5 integration software in the `app-domain` domain:

1. `oscm-app`
2. `oscm-app-tps5`

Restart the `app-domain` domain.

Updating the Configuration for SAML_SP Mode

If you are running CT-MG and the TPS5 integration software in SAML_SP mode, and if the IdP metadata of your SSO environment have changed, you need to update your WSIT files accordingly:

1. Extract the `OSCM-wsit.jar` file into a separate directory.

   The `.jar` file is located in

   `<GLASSFISH_HOME>/domains/app_domain/lib`

   The `OSCM-wsit.jar` file contains the following files:

   `wsit-client.xml`

   `STSService.xml`

2. Adapt the `.xml` files as required by your environment. For details, refer to *Configuring the TPS5 Integration* on page 13.
3. Recreate the `OSCM-wsit.jar` file with the modified contents.
4. Stop the `app-domain` domain.
5. Copy the adapted `OSCM-wsit.jar` to the following directory:

   `<GLASSFISH_HOME>/domains/app_domain/lib`

6. Restart the `app-domain` domain.

Note: If, for some reason, you recreate the `app-domain` domain, you also need to recreate the `OSCM-wsit.jar` in the `<GLASSFISH_HOME>/domains/app_domain/lib` directory.

3 Creating and Publishing Services

The following sections describe how to create and publish services in CT-MG by means of which customers can request and use virtual platforms in TPS5.

3.1 Prerequisites and Preparation

The following prerequisites must be fulfilled before you can create and publish services in CT-MG:

- To create technical services for the TPS5 integration in CT-MG, you must have access to CT-MG as a technology manager. You must be a member of the technology provider organization responsible for the TPS5 service controller as specified in the configuration settings for the installation.
- In TPS5, appropriate system templates for virtual platforms and images for virtual servers must exist, to which the technical services in CT-MG can be mapped. The TSP5 user specified in the configuration settings for the installation must have the necessary credentials to create and configure virtual platforms based on these templates and images.
- To create marketable services for the TPS5 integration in CT-MG, you must have access to CT-MG as a service manager of an organization with the supplier role. This may be the same organization as the technology provider organization or a different one.
- To publish your marketable services, you must have access to an appropriate marketplace in CT-MG in your service manager role.

3.2 Creating Technical Services

The first step in providing CT-MG services for TPS5 is to create one or more technical services.

Proceed as follows:

1. Define one or more technical services in an XML file.

   The TPS5 integration package, `oscm-tps5-install-pack.zip`, includes a technical service as a sample. Use the sample as a basis for defining your own technical services as required:

   `samples/TechnicalService_VirtualSystem.xml`

   In the technical service definition, be sure to specify:

   - The asynchronous provisioning type
   - The direct access type
   - Service parameters which represent the system templates and images defined in TPS5. For details on the supported service parameters, refer to *Service Parameters and Operations* on page 39.

Note:	Make sure that you do not specify the `baseUrl` attribute in the technical service definition XML file. It specifies an application's remote interface and is not needed for providing CT-MG services for TPS5.

2. Log in to the CT-MG administration portal with your technology manager account.
3. Import the technical services you created and appoint one or more supplier organizations for them.

For details on these steps, refer to the *Technology Provider's Guide* and to the online help of CT-MG.

3.3 Creating and Publishing Marketable Services

As soon as the technical services for the TPS5 integration exist in CT-MG, you can define and publish marketable services based on them. Your cost calculation for the services should include any external costs for operating the virtual platforms.

Proceed as follows:

1. Log in to the CT-MG administration portal with your service manager account.
2. Define one or more marketable services based on the technical services you created for TPS5.
3. Define price models for your marketable services.
4. Publish the services to a marketplace.

For details on these steps, refer to the *Supplier's Guide* and to the online help of CT-MG.

4 Using TPS5 Services in CT-MG

The following sections describe how users can subscribe to and work with the services you have created for TPS5 in CT-MG. You will find details of the supported usage scenarios outlined in *Usage Scenarios* on page 9.

4.1 Subscribing to Services

Users of customer organizations can subscribe to the services you have created for TPS5 on the marketplace where you have published them. This results in the provisioning of a virtual platform with one or more virtual servers in TPS5, as defined in the underlying technical service.

To enable the provisioning of a TPS5 instance, the customer has to enter a name for the virtual platform. The technical service may specify a prefix which is prepended to this name, as well as a pattern against which the name is checked before the provisioning operation is started.

The provisioning operations are carried out in asynchronous mode. As long as the provisioning is not complete, the status of the subscription is **pending**. The status changes to **ready** as soon as the provisioning has been finished successfully.

As soon as the provisioning is complete, the subscription and the virtual platform are ready to be used. The users assigned to the subscription can access the virtual servers on the virtual platform using the IP addresses and initial passwords indicated in the subscription details on the marketplace. The initial user ID for accessing the virtual servers is `Administrator` for Microsoft Windows systems, `root` for Linux systems. It is strongly recommended that the initial password is changed after the first login.

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

4.2 Modifying Subscription Parameters

By modifying the corresponding service parameters at their subscriptions, customers can change the virtual platforms provisioned in TPS5.

The following scenarios are supported by the TPS5 integration software:

- **Horizontal scale-up and scale-down**: By changing the corresponding service parameters, customers can trigger TPS5 to add a virtual server to their virtual platform. In the same way, they can request TPS5 to remove a virtual server from the platform.

  If a subscription is updated successfully, the subscription and the virtual platform are ready to be used with the changed parameters. The IP addresses of the virtual servers on the platform and the initial passwords for accessing them are output in the subscription details. The initial user ID is `Administrator` for Microsoft Windows systems, `root` for Linux systems. It is strongly recommended that the initial password is changed after the first login.

- **Vertical scale-up and scale-down**: By changing the corresponding service parameters, customers can trigger TPS5 to add disks to each virtual server in their virtual platform. In the same way, they can request TPS5 to remove disks from the virtual servers.

  If a subscription is updated successfully, the subscription and the virtual platform are ready to be used with the changed parameters.

The modifications are carried out in asynchronous mode. As long as the update is not complete, the status of the corresponding subscription is **pending update**. The status changes to **ready** as soon as the modification has been finished successfully.

Note:	If the subscription was **suspended** before starting the modification, its status changes to **suspended update** as long as the operation is not complete.

In the technical service definition, you can specify an address to which emails are to be sent that notify service users or administrators of customer organizations about a successful modification of a virtual platform.

Note:	If a customer changes an individual service parameter of a subscription, dependencies to other service parameters must be taken into account. If a request for a subscription update fails with an error, it is necessary to check the configuration of the virtual platform in TPS5. The specification of virtual servers, for example, may no longer match the specified firewall configuration.

4.3 Executing Service Operations

Customers can explicitly start and stop a virtual platform in TPS5 from CT-MG. To do this, they execute the appropriate service operation from the subscription for the virtual platform:

- **Start**: Starts the virtual platform if it was stopped.
- **Stop**: Stops the virtual platform if it was started.

4.4 Terminating Subscriptions

A customer can at any time terminate a subscription for a virtual platform in TPS5.

TPS5 is triggered to delete the virtual platform. The subscription is terminated independent of whether the deletion is successful. Note, however, that the virtual platform instance name cannot be re-used before the deletion has been completed in TPS5.

5 Administrating the TPS5 Integration

The following sections describe administration tasks you may need to perform in your role as an operator of the TPS5 integration software:

5.1 Controlling the Provisioning Process

The TPS5 integration provides you with the following feature for controlling the provisioning, modification, and deprovisioning of virtual platforms:

In the definition of the technical services for TPS5, you can specify the `MAIL_FOR_COMPLETION` parameter. This is an address to which emails are to be sent describing manual steps required to complete an operation.

If you specify this parameter, the TPS5 service controller interrupts the processing of each operation before its completion and waits for a notification about the execution of a manual action. This notification consists in opening the link given in the email.

Omit the `MAIL_FOR_COMPLETION` parameter if you do not want to interrupt the processing.

5.2 Handling Problems in the Provisioning Process

If the provisioning or modification of a virtual system fails on the TPS5 side or if there are problems in the communication between the participating systems, the corresponding subscription in CT-MG remains pending. The TPS5 service controller informs the technology managers of its responsible technology provider organization by email of any incomplete provisioning, modification, or delete operation in TPS5.

You can then take the appropriate actions to solve the problem in TPS5 or in the communication. For example, you could remove an incomplete virtual platform, or you could restore a missing connection.

After solving the problem, the TPS5 integration components 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 responsible for the TPS5 service controller.
2. Invoke the instance status interface of APP for the TPS5 service controller by opening the following URL in a Web browser:

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

   For example:

   `https://127.0.0.1:8881/oscm-app/controller/?cid=ess.tps5`

   The Web page shows all subscriptions for TPS5, including detailed information such as the customer organization, the ID of the related TPS5 instance, and the provisioning status.

3. Find the subscription for which you solved the problem in the most recent provisioning, modification, or delete operation.
4. In the **Action** column, select the action for the TPS5 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 TPS5 does not respond.
   - `UNLOCK` - to remove the lock for a TPS5 instance in APP.
   - `DELETE` - to terminate the subscription in CT-MG and remove the instance in APP, but keep the virtual platform in TPS5 for later use. The service manager role is required for this action.
   - `DEPROVISION` - to terminate the subscription in CT-MG, remove the instance in APP, and delete the virtual platform in TPS5. The service manager role is required for this action.
   - `ABORT_PENDING` - to abort a pending provisioning or modification operation in CT-MG. CT-MG is notified to roll back the changes made for the subscription and return it to its previous state. In TPS5, no actions are carried out.
   - `COMPLETE_PENDING` - to complete a pending provisioning or modification operation in CT-MG. CT-MG is notified to complete the changes for the subscription and set the subscription status to **ready** (or **suspended** if it was suspended before). This is possible only if the operations of the service controller are already completed.
5. Click **Execute** to invoke the selected action.

The instance status interface provides the following additional functionality that is useful for problem-solving purposes:

- You can display service instance details for each subscription by clicking the corresponding entry in the table. This displays all subscription-related information that is stored in the `bssapp` database.
- The **Run with timer** column indicates whether the timer for the interval at which APP polls the status of instances is running. You can reset the timer, if required. For details on the timer setting, refer to *Configuration Settings* on page 32.

5.3 Handling Communication Problems Between APP and CT-MG

When the communication between APP and CT-MG is no longer possible, for example, because 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 to make sure that CT-MG is up and running again correctly.

You then have the following possibilities to resume the processing of requests by APP:

1. Click the link provided in the email.
2. Log in to APP.

   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://127.0.0.1:8880/oscm-app`

2. Log in with the ID and password of the user and organization defined in the `configsettings.properties` file of APP (`BSS_USER_ID` and `BSS_USER_PWD`).

   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`.

5.4 Backup and Recovery

The TPS5 integration software does not offer integrated backup and recovery mechanisms. Use the standard file system, application server, and database mechanisms instead.

Backup

It is recommended that you create a regular backup of the following data according to the general guidelines of your organization:

- Database (`bssapp`). The frequency of database backups depends on the amount of changes and the availability of time slots with low load. PostgreSQL supports database backups without previous shutdown. For details, refer to the PostgreSQL documentation.
- Certificates contained in the truststore of the `app-domain` domain (`cacerts.jks` file).
- Configuration files.

Note: When preparing for an update installation of the current TPS5 integration software, always create a backup of the data mentioned above.

Recovery

If you need to recover your TPS5 integration installation, the recommended procedure is as follows:

1. Restore the `bssapp` database from the backup using the relevant PostgreSQL commands.
2. Stop the `app-domain` domain of the application server.
3. Restore the certificate truststore of the `app-domain` domain (`cacerts.jks` file) from the backup.
4. Start the `app-domain` domain.

5.5 Updating Configuration Settings

The TPS5 integration software and setup utilities require a number of settings. In the installation, you adapted the settings, in particular server names, ports, paths, and user IDs, to your environment.

The configuration settings are provided in the following subdirectories and files of `<install_pack_dir>`:

- **`databases/app_db`**
  - `db.properties`: Settings for the database setup and access.
  - `configsettings.properties`: Configuration settings for APP.

The initial installation stores these settings in the `bssapp` database, where you can change them later, if required. An update installation overwrites the settings. If you don't want existing settings to be overwritten, delete them from the properties file. In case that mandatory settings are missing in the properties file and not yet stored in the database, an exception will occur.

- `configsettings_controller.properties`: Configuration settings for the service controller.

  The initial installation stores these settings in the `bssapp` database. You can change them later using a graphical user interface.

- **`domains/app_domain`**

  The configuration settings for setting up the application server domain to which APP is deployed are provided in the following file:

  `glassfish.properties`

For details on the configuration settings, refer to *Configuration Settings* on page 32.

If you need to change the settings, proceed as described in the following sections.

To update the configuration settings for database access:

1. Log in to the administration console of the application server.
2. Adapt the settings as required.

To update the configuration settings for the application server:

1. Open the `glassfish.properties` file located in `<install_pack_dir>/domains/app_domain` with an editor.
2. Check the settings in the file and adapt them to your environment if required.
3. Save the file to its original location in `<install_pack_dir>/domains/app_domain`.
4. Update the settings and resources in the application server by executing the `build-glassfish.xml` file in `<install_pack_dir>/install` as follows:

```
<ANT_HOME>/bin/ant -f build-glassfish.xml
   SETUP.configureDomains
```

To update the configuration settings for APP:

1. Edit the content of the `configsettings.properties` file as required.
2. Execute the `build-db.xml` file in `<install_pack_dir>/install` as follows:

```
<ANT_HOME>/bin/ant -f build-db.xml
   UPDATE.configSettings
```

To update the configuration settings for the TPS5 service controller:

1. In a Web browser, access the URL of the TPS5 service controller, for example: `http://127.0.0.1:8880/oscm-app-tps5`.
2. Log in with the ID and password of the user specified in the configuration settings for the TPS5 service controller (`BSS_USER_ID` and `BSS_USER_PWD`) or as another technology manager registered for the same organization.
3. Enter the required settings.
4. Save the settings.

If you want to change the technology provider organization responsible for the TPS5 service controller, you can use the Web interface of APP:

1. In a Web browser, access the base URL of APP, for example:
   `http://127.0.0.1:8880/oscm-app`
2. Log in with the ID and password of the user specified for `BSS_USER_KEY` in the configuration settings for APP or as another administrator of the same organization.
3. Specify the technology provider organization for the TPS5 service controller, `ess.tps5`.
4. Save the settings.
5. Make sure that the configuration settings for the TPS5 service controller are updated.

   Any technology manager registered for the technology provider organization you specified can log in to the graphical user interface for updating the controller configuration settings (see above). At least the ID and password of the user to be used for accessing CT-MG must be changed in the controller configuration settings.

5.6 Adapting the Log Configuration

The TPS5 integration software records information and problems such as connection issues in the following log files on the application server:

- `<GLASSFISH_HOME>/domains/<DOMAIN_NAME>/logs/app-tps5.log`: Log of the TPS5 service controller
- `<GLASSFISH_HOME>/domains/<DOMAIN_NAME>/logs/app-core.log`: Log of the APP component

The logging is based on `log4j`. The default log level is `INFO`, which may not be sufficient depending on the circumstances. In such a case, you will need to adapt the log level in the configuration files. The following configuration files are of relevance:

- `<GLASSFISH_HOME>/domains/<DOMAIN_NAME>/config/log4j.ess.tps5.properties`: Log configuration of the TPS5 service controller
- `<GLASSFISH_HOME>/domains/<DOMAIN_NAME>/config/log4j.app.core.properties`: Log configuration of the APP component

Proceed as follows to adapt the log level:

1. Open the relevant configuration file.
2. Find the string `log4j.logger.org.oscm.app` in the configuration file.
3. Change the log level as desired to one of the following:
   - `ERROR` - designates error events that might still allow the application to continue running.
   - `WARN` - designates potentially harmful situations.
   - `INFO` - designates informational messages that highlight the progress of the application at coarse-grained level.
   - `DEBUG` - designates fine-grained informational events that are most useful to debug an application.

   Example:

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

Every 60 seconds, the TPS5 integration software checks for changes in the log configuration. There is no need to restart the application.

6 Uninstallation

If you want to uninstall the TPS5 integration software, take the following preparations:

- Back up resources and data you would like to keep. For details, refer to *Backup and Recovery* on page 28.
- In CT-MG, delete the marketable services and technical services related to TPS5.

To uninstall the TPS5 integration software:

1. Stop the `app-domain` domain in the application server.
2. Delete the `app-domain` domain.
3. Delete the `bssapp` database in the database management system.
4. Uninstall the database management system and the application server if you no longer need them for other purposes.

For details on how to proceed, refer to the documentation of the database management system and the application server.

Appendix A: Configuration Settings

The configuration settings for the TPS5 integration software are provided in the following files in subfolders of the directory to which you extracted the `oscm-tps5-install-pack.zip` file (`<install_pack_dir>`):

- `domains/app_domain/glassfish.properties`
- `databases/app_db/db.properties`
- `databases/app_db/configsettings.properties`
- `databases/app_db/configsettings_controller.properties`

This appendix describes the settings in detail.

A.1 GlassFish Configuration Settings

The `glassfish.properties` file located in `<install_pack_dir>/domains/app_domain` contains the configuration settings for the GlassFish application server. The settings are required for configuring the domain where APP is deployed.

Below you find a detailed description of the settings.

GLASSFISH_HOME

The absolute path and name of the GlassFish installation directory.

JDBC_DRIVER_JAR_NAME

The name of the PostgreSQL JDBC driver jar file as available after installation.

Example: `postgresql-9.1-903.jdbc4.jar`

MAIL_HOST

The host name or IP address of your mail server.

MAIL_RESPONSE_ADDRESS

The email address used by the server as the sender of emails.

Example: `saas@yourcompany.com`

MAIL_PORT

The port of your mail server.

Default: `25`

MAIL_USE_AUTHENTICATION

Optional. Defines whether mails can be sent only to users authenticated against the SMTP mail system.

Allowed values: `true`, `false`

Default: `false`

MAIL_USER

Mandatory if `MAIL_USE_AUTHENTICATION=true`. Specifies the name of the user to be used for authentication against the SMTP mail system.

MAIL_PWD

Mandatory if `MAIL_USE_AUTHENTICATION=true`. Specifies the password of the user to be used for authentication against the SMTP mail system.

MAIL_TIMEOUT

Optional. The time interval in milliseconds for sending email messages, i.e. until a socket I/O timeout occurs.

Allowed values: Any value between `0` and `4924967296`

Default: `30000`

MAIL_CONNECTIONTIMEOUT

Optional. The time interval in milliseconds for establishing the SMTP connection, i.e. until a socket connection timeout occurs.

Allowed values: Any value between `0` and `4924967296`

Default: `30000`

glassfish.domain.portbase

Mandatory. The base number for all ports used by the domain of the APP application.

Example: `8800`

glassfish.domain.portadmin

The administration port of the domain used for APP.

Example: `8848`

glassfish.domain.name

The name of the domain where APP is deployed.

Example: `app-domain`

glassfish.domain.admin.user

The user name of the APP domain administrator.

Default: `admin`

glassfish.domain.admin.pwd

The password of the APP domain administrator.

Default: `adminadmin`

glassfish.domain.admin.master.pwd

Mandatory. The master password required for accessing the keystore and truststore files of the application server domain.

Default: `changeit`

glassfish.domain.stop.waitSeconds

Mandatory. The time in seconds the application server waits until a stop domain operation is executed.

Default: `60`

glassfish.domain.start.maxWaitSeconds

Mandatory. The maximum time in seconds the application server waits until it checks whether a domain is started.

Default: `600`

A.2 Database Configuration Settings

The `db.properties` file located in `<install_pack_dir>/databases/app_db` contains the configuration settings for database access. This configuration is used for the initial setup and schema updates.

db.driver.class

The Java class of the JDBC driver.

Default: `org.postgresql.Driver`

db.host

The database host.

Default: `localhost`

db.port

The database port.

Default: `5432`

db.name

The name of the database.

Default: `bssapp`

db.user

The name of the user to connect to the database.

Default: `bssuser`

db.pwd

The password of the user to connect to the database.

Default: `bssuser`

db.type

The type of the database.

Default: `postgresql`

A.3 APP Configuration Settings

The `configsettings.properties` file located in `<install_pack_dir>/databases/app_db` contains the configuration settings for APP.

APP_BASE_URL

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

The URL used to access APP.

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 takes longer. If you decrease it, more load is put on the system. We strongly recommend that you do not set a value of more than 180000 milliseconds (3 minutes), although the maximum value is much higher (922337203685477580).

If you do not specify this setting at all, the default value used is 15000.

APP_MAIL_RESOURCE

`APP_MAIL_RESOURCE=mail/APPMail`

The JNDI name of the GlassFish mail resource used to send emails.

The resource `mail/APPMail` is created during setup with the parameters defined in the `glassfish.properties` file. This setting needs to be changed only if you want to use a different mail resource.

APP_ADMIN_MAIL_ADDRESS

`APP_ADMIN_MAIL_ADDRESS=admin@example.com`

The email address to which email notifications are sent.

APP_KEYSTORE_PASSWORD

`APP_KEYSTORE_PASSWORD=changeit`

The password required to access the keystore of the domain used for APP in the application server.

APP_TRUSTSTORE_PASSWORD

`APP_TRUSTSTORE_PASSWORD=changeit`

The password required to access the truststore of the domain used for APP in the application server.

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 single sign-on. The setting must be identical to the `AUTH_MODE` setting in CT-MG.

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

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

BSS_USER_KEY

`BSS_USER_KEY=<userKey>`

The user key for accessing CT-MG.

Replace `<userKey>` with the user key which you receive with the confirmation email for your user account.

The user specified here must have the administrator role for your organization in CT-MG. The user account is used for carrying out actions on behalf of APP in CT-MG. In addition, the user is allowed to register service controllers in APP.

BSS_USER_ID

`BSS_USER_ID=<userId>`

The identifier of the user specified in `BSS_USER_KEY` for accessing CT-MG.

Replace `<userId>` with the user ID.

BSS_USER_PWD

`BSS_USER_PWD=_crypt:<password>`

The password of the user specified in `BSS_USER_KEY` for accessing CT-MG.

Replace `<password>` with the plain text password. The password is encrypted when it is stored in the database.

BSS_WEBSERVICE_URL

`BSS_WEBSERVICE_URL=https://<server>:<port>/{SERVICE}/BASIC`

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

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 URL specifying the version of the CT-MG Web services to be used. The `{SERVICE}` placeholder must not be replaced.

BSS_STS_WEBSERVICE_URL

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

Mandatory when `BSS_AUTH_MODE` is set to `SAML_SP` and security token based authentication is used. The endpoint of the CT-MG Web services to be used. The `{SERVICE}` placeholder must not be replaced.

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 URL specifying the version of the CT-MG Web services to be used. The `{SERVICE}` placeholder must not be replaced.

A.4 Controller Configuration Settings

The `configsettings_controller.properties` file located in `<install_pack_dir>/databases/app_db` contains the configuration settings for the TPS5 service controller. This configuration is used for the initial setup and stored in the APP database.

CONTROLLER_ID

`CONTROLLER_ID=ess.tps5`

The identifier of the service controller.

BSS_ORGANIZATION_ID

`BSS_ORGANIZATION_ID=<organizationID>`

The ID of the organization in CT-MG which is responsible for the service controller. The organization must have the technology provider role.

BSS_USER_KEY

`BSS_USER_KEY=<userKey>`

The user key for accessing CT-MG.

Replace `<userKey>` with the user key which you receive with the confirmation email for your user account.

The user specified here must have the technology manager role in CT-MG and belong to the organization specified in the `BSS_ORGANIZATION_ID` setting.

It is recommended that the user account is used only for carrying out actions on behalf of the service controller in CT-MG.

BSS_USER_ID

`BSS_USER_ID=<userId>`

The identifier of the user specified in `BSS_USER_KEY` for accessing CT-MG.

Replace `<userId>` with the user ID.

BSS_USER_PWD

`BSS_USER_PWD=_crypt:<password>`

The password of the user specified in `BSS_USER_KEY` for accessing CT-MG.

Replace `<password>` with the plain text password. The password is encrypted when it is stored in the database.

IAAS_API_LOCALE

`IAAS_API_LOCALE=<locale>`

The locale to be used for communicating with TPS5.

Replace `<locale>` with the identifier of the desired locale, for example, `en` or `ja`.

IAAS_API_URI

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

The URL of the TPS5 API.

Replace `<TPS5 server>` and `<port>` with the host name and port of your TPS5 server.

IAAS_API_KEYSTORE_TYPE

```
IAAS_API_KEYSTORE_TYPE=<type>
```

The type of certificate used for accessing the TPS5 API.

Replace `<type>` with the identifier of the certificate type, for example, `pkcs12`.

IAAS_API_KEYSTORE_PASS

```
IAAS_API_KEYSTORE_PASS=_crypt:<password>
```

The password required for accessing the keystore used by the TPS5 API.

Replace `<password>` with the plain text password defined when creating the certificate for the user who accesses TPS5. The password is encrypted when it is stored in the database.

IAAS_API_KEYSTORE

```
IAAS_API_KEYSTORE=<path>
```

The path to the certificate file.

Replace `<path>` with the URL leading to the certificate file on the application server.

Appendix B: Service Parameters and Operations

The following sections describe the technical service parameters and service operations which are supported by the TPS5 service controller.

Service Parameters for Virtual Platform Provisioning and Scaling

The following parameters are required for provisioning a virtual platform with one or more virtual servers:

APP_CONTROLLER_ID

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

Default (must not be changed): `ess.tps5`

INSTANCENAME_PATTERN

Mandatory. A regular expression specifying a pattern for the virtual platform instance name entered by the users when they subscribe to a corresponding service. If the names do not match the pattern, the subscription is rejected.

Example: `tps5([a-z0-9]){2,25}`

INSTANCENAME_PREFIX

Optional. A string to be prepended to the virtual platform instance name entered by the users when they subscribe to a corresponding service.

Example: `tps5`

INSTANCENAME

Mandatory. The name of the virtual platform to be instantiated. 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`

MAIL_FOR_COMPLETION

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

Example: `info@company.com`

MAIL_FOR_NOTIFICATION

Optional. The address to which emails are to be sent that notify service users or administrators of customer organizations about a successful modification of a virtual platform. Such modifications result from changes in the configuration parameters at a corresponding subscription.

Example: `administrators@company.com`

SYSTEM_TEMPLATE_ID

Mandatory. The system ID of the TPS5 system template to be used for the virtual platform.

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 system template, have fixed parameter options for selection.

`SYSTEM_TEMPLATE_ID` must be a one-time parameter, since the modification of this parameter is not supported.

Example: `TPL_f36620_GNQ7WM8J7SOW`

Service Parameters for Additional Virtual Servers

The following parameters are required for instantiating additional virtual servers on a virtual platform:

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. The name of the virtual server specified in `VSERVER_<#>`.

Example: `WindowsT1`

VSERVER_<#>_NETWORK_ID

Mandatory 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 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. 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: `IMG0020_Cent64_64_EN_v1_NoSPT`

VSERVER_<#>_VSERVER_TYPE

Mandatory. 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: `10 GB`

Service Parameters for Firewalls

The following parameters are required for instantiating a firewall for a virtual platform:

FIREWALL_CONFIG

Optional. Configuration setting for managing the communication between the virtual platform 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:

```
FIREWALL_CONFIG=INTERNET(${SIP})>DMZ(:80,443)
FIREWALL_SIP=85.1.2.0/24:25
```

Service Operations for Virtual Platforms

The TPS5 service controller supports the service operations below for virtual platforms.

The `actionURL` for each operation is:

`https://<host>:<port>/OperationService/AsynchronousOperationProxy?wsdl`

`<host>` and `<port>` are the server and port of the `app-domain` domain where the TPS5 integration software is deployed.

Note:	If you provision a virtual platform that does not support start and stop operations, make sure that you remove the service operations from the technical service definition.

START_VIRTUAL_SYSTEM Starts a virtual platform in TPS5 if it was stopped.
STOP_VIRTUAL_SYSTEM Stops a virtual platform in TPS5 if it was started.

Glossary

Administrator

A privileged user role within an organization with the permission to manage the organization's account and subscriptions as well as its users and their roles. Each organization has at least one administrator.

Application

A software, including procedures and documentation, which performs productive tasks for users.

Billing System

A system responsible for calculating the charges for using a service. CT-MG comes with a native billing system, but can also be integrated with external ones.

Broker

An organization which supports suppliers in establishing relationships to customers by offering the suppliers' services on a marketplace, as well as a privileged user role within such an organization.

Cloud

A metaphor for the Internet and an abstraction of the underlying infrastructure it conceals.

Cloud Computing

The provisioning of dynamically scalable and often virtualized resources as a service over the Internet on a utility basis.

Customer

An organization which subscribes to one or more marketable services in CT-MG in order to use the underlying applications in the Cloud.

Infrastructure as a Service (IaaS)

The delivery of computer infrastructure (typically a platform virtualization environment) as a service.

Marketable Service

A service offering to customers in CT-MG, based on a technical service. A marketable service defines prices, conditions, and restrictions for using the underlying application.

Marketplace

A virtual platform for suppliers, brokers, and resellers in CT-MG to provide their services to customers.

Marketplace Owner

An organization which holds a marketplace in CT-MG, where one or more suppliers, brokers, or resellers can offer their marketable services.

Marketplace Manager

A privileged user role within a marketplace owner organization.

Operator

An organization or person responsible for maintaining and operating CT-MG.

Organization

An organization typically represents a company, but it may also stand for a department of a company or a single person. An organization has a unique account and ID, and is assigned one or more of the following roles: technology provider, supplier, customer, broker, reseller, marketplace owner, operator.

Organizational Unit

A set of one or more users within an organization representing, for example, a department in a company, an individual project, a cost center, or a single person. A user may be assigned to one or more organizational units.

OU Administrator

A privileged user role within an organization allowing a user to manage the organizational units for which he has been appointed as an administrator, and to create, modify, and terminate subscriptions for these units.

Payment Service Provider (PSP)

A company that offers suppliers or resellers online services for accepting electronic payments by a variety of payment methods including credit card or bank-based payments such as direct debit or bank transfer. Suppliers and resellers can use the services of a PSP for the creation of invoices and payment collection.

Payment Type

A specification of how a customer may pay for the usage of his subscriptions. The operator defines the payment types available in CT-MG; the supplier or reseller determines which payment types are offered to his customers, for example payment on receipt of invoice, direct debit, or credit card.

Platform as a Service (PaaS)

The delivery of a computing platform and solution stack as a service.

Price Model

A specification for a marketable service defining whether and how much customers subscribing to the service will be charged for the subscription as such, each user assigned to the subscription, specific events, or parameters and their options.

Reseller

An organization which offers services defined by suppliers to customers applying its own terms and conditions, as well as a privileged user role within such an organization.

Role

A collection of authorities that control which actions can be carried out by an organization or user to whom the role is assigned.

Seller

Collective term for supplier, broker, and reseller organizations.

Service

Generally, a discretely defined set of contiguous or autonomous business or technical functionality, for example an infrastructure or Web service. CT-MG distinguishes between technical services and marketable services, and uses the term "service" as a synonym for "marketable service".

Service Manager

A privileged user role within a supplier organization.

Standard User

A non-privileged user role within an organization.

Software as a Service (SaaS)

A model of software deployment where a provider licenses an application to customers for use as a service on demand.

Subscription

An agreement registered by a customer for a marketable service in CT-MG. By subscribing to a service, the customer is given access to the underlying application under the conditions defined in the marketable service.

Subscription Manager

A privileged user role within an organization with the permission to create and manage his own subscriptions.

Supplier

An organization which defines marketable services in CT-MG for offering applications provisioned by technology providers to customers.

Technical Service

The representation of an application in CT-MG. A technical service describes parameters and interfaces of the underlying application and is the basis for one or more marketable services.

Technology Manager

A privileged user role within a technology provider organization.

Technology Provider

An organization which provisions applications as technical services in CT-MG.