Best Practice
PIM 7 Installation (PIM, Audit Trail)

Version 1.0

Popa, Gabriel Adrian
IPS Technical Experts
Heiler Software GmbH (an Informatica Company)
Version management

1.1 Current Document

This document contains instructions and remarkable points how to achieve a clean PIM 7 installation.

1.2 Versions

<table>
<thead>
<tr>
<th>Version</th>
<th>Author</th>
<th>Comment</th>
<th>Released</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>A. Gabriel Adrian Popa</td>
<td>PIM 7 installation</td>
<td>No</td>
</tr>
<tr>
<td>1.0</td>
<td>M. Keck</td>
<td>Document reviewed and released</td>
<td>Yes</td>
</tr>
</tbody>
</table>
2 Summary

2.1 Short summary of this Best Practice

This document contains instructions and noteworthy points how to achieve an Informatica PIM 7 installation on a windows environment.

The goal is to define an action plan from the start until the end of a project.

2.2 What is Informatica PIM?

Informatica Product Information Management (PIM) is the central product information platform for e-commerce and multichannel commerce.

The solution provides distributors and manufacturers with a central solution for all product data in a central data source for the purpose of distribution in all communication channels and languages.

Key elements of the solution include the import (Onboarding) and central mastering of highly structured product data and the corresponding media assets (Informatica Media Manager).

This means that centrally managed product data can be adapted to suit the needs of various target systems (Multichannel), such as online shops or print systems, when it is exported in data formats on the basis of CSV or XML.

Informatica PIM comprises the following three functional areas that support Product Information Management along the supply chain from onboarding of product data to the multichannel export into various target systems:

2.3 Why the Best Practice was used

The Best Practice was used to help technical consultants to install PIM for our customers.

Different installations, each customer has another one, can be confusing. A standardized installation makes it much easier to find every installation location for analyzing (e.g. the customer reports a problem, and the person who did the installation is not here).
2.4 What are the benefits of this Best Practice

The benefit of this Best Practice is that you do not have to read the whole PIM installation manual, or asking a technical expert only to achieve a simple, working installation.

2.5 What problems/issues were associated with this Best Practice

An incorrect configured PIM can affect performance of the running processes.

2.6 Experience / Application used this Best Practice

The Best Practice is not used yes. Let’s see if it works in other PIM 7 projects.
3 Best Practice

The objective of this Best Practice is to help the reader to set up a clean Informatica PIM 7 installation. The result, which is a working installation, can be extended with increasing PIM knowledge.

3.1 Business description

3.1.1 General

This Best Practice shows how to achieve a clean PIM 7 installation.

3.1.2 Processes

To do this installation you’ll need estimated 1 day.

3.1.2.1 Predefined processes

There are no predefined processes. Each installation with configuration is unique on every customer system.

3.1.2.2 Flow

For a successful installation start it is very important that all necessary elements of the pre installation are met.

e.g.

- Access to the system
- Service user with full access rights
- No security issues

These are the four mandatory basic steps which have to be done.
3.2 Installation

3.2.1 Hardware and Software Requirements

The following requirements apply to all PIM 7 installation:

• Application Server

<table>
<thead>
<tr>
<th>Operating System (Supported Version, Chip Set, Specific patch set used in certification test environment, Binary Type)</th>
<th>Database/Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows Server 2012</td>
<td>C</td>
</tr>
<tr>
<td>Microsoft Windows Server 2008 R2 SP1, x64</td>
<td>S</td>
</tr>
</tbody>
</table>

• Database Server

<table>
<thead>
<tr>
<th>Operating System (Supported Version, Chip Set, Specific patch set used in certification test environment, Binary Type)</th>
<th>Database/Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows Server 2012</td>
<td>C</td>
</tr>
<tr>
<td>Microsoft Windows Server 2008 R2 SP1, x64</td>
<td>S</td>
</tr>
<tr>
<td>Novell SUSE Linux Enterprise Server 11 SP4, x86-64, SP4, 64-bit</td>
<td>C</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 5.x, x86-64, RHEL 5.03 2.6.18-128.el5 #1 SMP, 64-bit</td>
<td>S</td>
</tr>
</tbody>
</table>

• Desktop Clients

<table>
<thead>
<tr>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 7 SP1</td>
</tr>
<tr>
<td>Windows XP</td>
</tr>
</tbody>
</table>

• Browser Clients

<table>
<thead>
<tr>
<th>Browser / Version</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer 9</td>
<td>C</td>
</tr>
<tr>
<td>Firefox 16.x ... 19.x</td>
<td>C</td>
</tr>
<tr>
<td>Chrome 25.x</td>
<td>S</td>
</tr>
<tr>
<td>Safari 6</td>
<td>S</td>
</tr>
</tbody>
</table>

• Legend/Explanation

<table>
<thead>
<tr>
<th>Certification Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>Certified i.e. product has been tested on this specific platform combination</td>
</tr>
<tr>
<td>S</td>
<td>&quot;Supported but not certified&quot;. This means that even though a customer will be running on a non-certified platform, Informatica will still honor the SLA’s in their Support contract. This commitment can only be given by the Product Management team in consultation with Engineering and is only for the specific configurations described. (Certified platforms are the platforms on which QA completed acceptance testing.)</td>
</tr>
<tr>
<td>Not Applicable/Not Available/Not Supported</td>
<td>Not Applicable/Not Available/Not Supported</td>
</tr>
</tbody>
</table>
3.2.2 PIM Compatibility Matrix

<table>
<thead>
<tr>
<th>System Environment</th>
<th>PIM Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PIM Server (&quot;HPM&quot;)</td>
</tr>
<tr>
<td>Sever OS</td>
<td>7.0.05</td>
</tr>
<tr>
<td>PIM Rich Client OS</td>
<td>7.0.04</td>
</tr>
<tr>
<td>Browser Clients</td>
<td>7.0.05</td>
</tr>
<tr>
<td>MS SQL Server</td>
<td>7.0.02</td>
</tr>
<tr>
<td>[11g R2]</td>
<td>7.0.01</td>
</tr>
<tr>
<td>[11.2.0.3.0]</td>
<td>7.0.00</td>
</tr>
</tbody>
</table>

3.2.3 Pre-Installation Checklist

- **PIM Application Server**
  1. Install Operating System according the compatibility matrix.
  2. Create windows domain user for the PIM Windows service.
  3. Create windows users for remote access (RDP) with local administrator rights.
  4. Open Ports:
     - 1712 (used to connect PIM – Desktop with PIM Server)
     - 1501 (http port for integrated Jetty PIM Webserver)
     - 55555 (default Java Management Extension port, needed to attach troubleshooting and tuning)
     - 61616 (port for message queue connection)
     - 25 (port to send emails via smtp)
     - 445 and 139 (windows file share ports for media asset file communication)
  5. Test connection from PIM Application server to database server using the database administration tools was successful.

- **PIM Database**
  1. Installation of a database system according the compatibility matrix
  2. Creation of a database user with full Read-/Write permissions to the create PIM schemas, inclusive the right to create new tables
  3. Installation of the database administrations tools (MS SQL Server Management Studio / Oracle SQL Developer) on PIM Application Server and Database server
  4. Open ports:
     - **Port Database**
     - 1433 MSSQL
     - 1521 Oracle
  5. Test connection from PIM Application server to database server using the database administration tools

- **PIM - Web Search**
  1. **System Requirements**
     - **Memory Requirement**
       - PIM - Web Search and the underlying Solr Server needs much RAM memory, that is completely allocated at start time ensuring a fast search index build and a web search:
       - Minimum of 1.5 GByte is required
       - 2 GByte is recommended
Java
An actual java JDK7 64Bit version is required for the use of PIM - Web Search. It has to be ensured, that the system property JAVA_HOME is set.

2. OS User Permissions

Windows
- The users which installs the PIM - Web Search need to be in the local Administrators group.
- You need read/write permissions to the <PIM_WEBSEARCH_INSTALLATION_ROOT> directory.
- The windows service user which runs the PIM - Web Search, also needs read/write permissions to the <PIM_WEBSEARCH_INSTALLATION_ROOT> directory.

3. PIM - Web Search Default Ports

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>PIM Module / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>18090</td>
<td>http</td>
<td>PIM Search Server (Tomcat Application Server)</td>
</tr>
<tr>
<td>1501</td>
<td>http</td>
<td>PIM Core Service API</td>
</tr>
</tbody>
</table>

If this port is already in use in your installation, follow the instructions below to change the ports.

4. Change Application Server Ports

If you have another application running on your machine which is using the same ports that PIM Search uses by default, you may need to change the port which PIM Search will use. You need to modify the server port (default is 18095), the http nio connector port (default is 18090) and the ajp connector port (default is 18100) to ports that are free on your machine.

1) Open file <PIM_WEBSEARCH_INSTALLATION_ROOT>\configuration.properties
2) Change Property:
   - container.http.port: http nio connector port (default is 18090)
   - container.shutdown.port: server port (default is 18095)
   - container.ajp13connector.port: ajp connector port (default is 18100)

This has to be done before running the PIM - Web Search installation.
**Note:** netstat can be used to identify free ports on your machine

- PIM - Audit Trail

1. OS User Permissions
   Windows
   - The users which install the PIM - Audit Trail modules need to be in the local Administrators group.

2. PIM - Audit Trail Default Ports

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>PIM Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>61616</td>
<td>tcp</td>
<td>MessageQueue</td>
<td>This port is used for sending messages from PIM Core to PIM - Audit Trail server over MessageQueue.</td>
</tr>
<tr>
<td>2801</td>
<td>tcp</td>
<td>Audit Trail</td>
<td>This port is used for the communication between PIM - Desktop and PIM - Audit Trail server.</td>
</tr>
</tbody>
</table>
3.2.4 Database configuration hints

- **Microsoft SQL Server**
  - **Server Collation**
    - Latin1_General, Case Sensitive, Accent sensitive
  - **User Settings** - the user which installs the PIM database must have:
    - set the roles: dbcreator, public
    - default language: English
    - Enforce password policy disabled
  - **Memory**
    Take care to define a maximum fixed setting for the memory size. Take care that you leave enough memory for the operation system.
  - **Named-Instances**
    PIM support „Named Instances“. Take care that MS SQL Server network settings are correct. In section „IP ALL“ the TCP Port must set to a free port (default: 1433). Deactivate the option „TCP Dynamic Ports“

- **Oracle**
  - **User Settings**
    For the installation of the PIM database the SYSTEM user must be used.
  - **Server Settings:**
    - Enable at least the feature "Enterprise Manager Repository"
    - Set database character set to Unicode (AL32UTF8).
    - Set the national specific character set to AL16UTF16 - Unicode UTF-16 Universal character set.
    - Set standard increase redo-log file size to 1024 MB (each).
    - Set standard language to American.
    - Set the parameter open cursors to 3000
    - Set the parameter processes to 600
    - Create a tnsname.ora file at `<OracleDBInstanceFolder>/NETWORK/ADMIN` and map service names to the connect descriptors for the local naming method
    - (Optional) Disable password expiration
    - Specify pga_aggregate_target and sga_target due to system restrictions
  - **Initialization parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>db_block_size</td>
<td>9192</td>
</tr>
<tr>
<td>db_domain</td>
<td></td>
</tr>
<tr>
<td>db_file_multiblock_read_count</td>
<td>16</td>
</tr>
<tr>
<td>java_pool_size</td>
<td>0</td>
</tr>
<tr>
<td>job_queue_processes</td>
<td>10</td>
</tr>
<tr>
<td>nls_language</td>
<td>AMERICAN</td>
</tr>
<tr>
<td>nls_territory</td>
<td>AMERICA</td>
</tr>
<tr>
<td>open_cursors</td>
<td>3000</td>
</tr>
<tr>
<td>processes</td>
<td>600</td>
</tr>
<tr>
<td>remote_login_passwordfile</td>
<td>EXCLUSIVE</td>
</tr>
<tr>
<td>sessions</td>
<td>670</td>
</tr>
<tr>
<td>undo_management</td>
<td>AUTO</td>
</tr>
<tr>
<td>undo_tablespace</td>
<td>UNDOTBS1</td>
</tr>
<tr>
<td>TNS_LISTENER</td>
<td>TCP Protocol</td>
</tr>
</tbody>
</table>
3.2.5 Installing PIM Core Database

1. **Download the PIM Core zip**
   - Download PIM Core zip from PIM Software Download Area
   - Choose your Version and navigate to the Binaries Download area of the appropriate section then download PIM_<Version>_Core.zip.
   - The database setup archive is distributed within the PIM Core zip and has the following format PIM_<Version>_<Revision>_database.zip

2. **Extract the database setup archive**
   - Perform the following instructions to extract the database setup archive.
     - On the database server unzip the PIM_<Version>_<Revision>_database.zip to an installation root of your choice. (in our case <PIM_DATABASE_INSTALLATION ROOT> = C:\INFORMATICA\PIM )
     - Check if the following folder structure exists under the installation root afterwards

3. **Configure the database properties in the server.properties file**
   - Before running the database installation, some basic configuration needs to be done. The settings for the database connection are configured in the server.properties file. Templates for this file can be found in the database setup archive:

     `<PIM_DATABASE_INSTALLATION ROOT>\database\setup\server.properties.template.[DBMS]`

   - Perform the following steps to adjust the server.properties file:
     - Make a copy of the appropriate template file `<PIM_DATABASE_INSTALLATION ROOT>\database\setup\server.properties.template.[DBMS]`
     - Rename this copy to `server.properties`
     - Open this file in an editor and adjust the database properties to your needs.
     - Save the changes to this file.

   For the database installation the following aspects need special attention:

   - **General Settings:**
     - General Host and Directory Settings
       - `dest.host`: Hostname of the database server e.g. localhost
       - `dest.root.local`: database installation root directory e.g C:\INFORMATICA\PIM

   - **MSSQL Installation:**
     - Database settings
       - `db.default.port`: Port number of the database server default 1433
       - `db.default.user`: Database user which needs dbcreator and public permissions e.g. hpm
       - `db.default.password`: password for the above specified database user

   - **Oracle Installation:**
### Database settings

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>db.default.database</td>
<td>The oracle SID or Service Name of the oracle database e.g. HPM11g</td>
</tr>
<tr>
<td>db.default.port</td>
<td>Port number of the database server default 1521</td>
</tr>
<tr>
<td>db.default.password</td>
<td>password for the database users/schemas (MAIN, SUPPLIERS, MASTER)</td>
</tr>
</tbody>
</table>

4. **Creating/Updating databases**

Perform the following steps to finally create or update the databases/schemas:

- Make sure that the folders specified in the server.properties file in the section Database Settings exist on the database host.
- Open the folder `<PIM_DATABASE_INSTALLATION ROOT>/database/setup`.
- Start the PIM Core database setup with a double click on the setup.cmd file. A command-window will appear:

  - Enter "y" if you want to do a new installation. In the case you already have created schemas you will see this screen:

    - This means that there are already PIM Core schemas in the server. Enter "y" if you want to update the existing schemas.
    - After a successful creation of the schemas the command line output should look like this:

    - Check the log files (`<PIM_DATABASE_INSTALLATION ROOT>/database/setup/logs`) for any errors, also in case the build returned...
3.2.6 Installing PIM - Audit Trail Database

Audit Trail needs its own data storage. It is strongly recommended to deploy PIM Core database and Audit Trail database on different servers or at least on different storage. This is necessary because the Audit Trail database requires a lot of disk space and fast I/O.

1. Download the PIM - Audit Trail zip
   - Download PIM - Audit Trail from PIM Software Download Area
   - Choose your Version and navigate to the Binaries Download area of the appropriate section then download PIM_<Version>_AuditTrail.zip.

2. Extract the Audit Trail archive
   - Choose your <ARCH> version and unpack the corresponding audit trial server archive PIM_<Version>_<Revision>_atserver<ARCH>.zip to an installation root <PIM_AUDITTRAIL_INSTALLATION_ROOT> (for example C:\INFORMATICA\PIM\AuditTrail).

3. Configure the database properties

   **Note:** There should be no white space in the <PIM_AUDITTRAIL_INSTALLATION_ROOT> otherwise setup will fail.

   Before running the database installation, some basic configuration needs to be done:
   - Go to <PIM_AUDITTRAIL_INSTALLATION_ROOT>/configuration/audittrailserver/
   - Rename server.properties.template.MSSQL2008 or server.properties.template.ORAl1.g file to server.properties
   - Update database connection properties if necessary (defaults assume you have database instance running on localhost)

   **Database settings**
   
<table>
<thead>
<tr>
<th>Database settings</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>dest.host</td>
<td>Hostname of the database server</td>
</tr>
<tr>
<td>db.audittrail.port</td>
<td>Port number of the database server</td>
</tr>
<tr>
<td>db.audittrail.dir.local</td>
<td>Local directory at database server to store files which are</td>
</tr>
<tr>
<td></td>
<td>related to Audit Trail</td>
</tr>
<tr>
<td>db.audittrail.schema</td>
<td>Database/Schema name in capital letters</td>
</tr>
<tr>
<td>db.audittrail.user</td>
<td>Database username. For Oracle database users same as schema</td>
</tr>
<tr>
<td>db.audittrail.password</td>
<td>Password for the above specified database user</td>
</tr>
</tbody>
</table>

   **Note:** Configured directory (db.audittrail.dir.local) should exist otherwise database setup will fail.

   **Database settings (Oracle only)**
   
<table>
<thead>
<tr>
<th>Database settings</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>db.sys.password</td>
<td>Update password for SYS user that should be with SYSDBA role.</td>
</tr>
<tr>
<td></td>
<td>It's required for installation and can be removed after</td>
</tr>
<tr>
<td>db.audittrail.tns</td>
<td>The TNS name used by Oracle. Please verify that TNS is enabled at Oracle Database</td>
</tr>
</tbody>
</table>

4. Install database:
   - Go to <PIM_AUDITTRAIL_INSTALLATION_ROOT>/bin
   - Run setup_console.bat in folder <PIM_AUDITTRAIL_INSTALLATION_ROOT>/bin
   - A console with osgi> prompt pops up, press return after log4j message
   - Type dbInstall in console and confirm installation.
   - After installation check out <PIM_AUDITTRAIL_INSTALLATION_ROOT>/logs/dbsetup/*.log
     - If it was successful there will be all following log files without failures expect <databasename>_check.log.
3.2.7 PIM - Server Installation

1. **Setting up the installation root**
   Before you start with the installation, you must set up an installation root folder. Besides, you have to store the valid license to a folder accessible to the PIM - Server application server.

   - **Create the installation root**
     On the machine which will host the the application server create the installation root `<INSTALLATION_ROOT>` , e.g. C:\INFORMATICA\PIM.

   - **Copy the license file**
     Copy the license file to a folder accessible to the application server. It is recommended to store the license in a separate license folder `<INSTALLATION_ROOT>\license`, e.g. C:\INFORMATICA\PIM\license.

2. **Download the PIM Core zip**
   If you have not downloaded PIM Core zip already, please click on the link below to get to the

   - **PIM Software Download Area**
     Choose your **Version** and navigate to the Binaries Download area of the appropriate section then download `PIM_<Version>_Core.zip`.

   - **The application server archive is distributed within the PIM Core zip and has the following format** `PIM_<Version>_<Revision>_server_[ARCH].zip`

3. **Extracting the application server archive**
   Perform the following instructions to extract the application server archive to your installation root:

   - On the server on which you want to install the application server, unzip the application server archive `PIM_<Version>_<Revision>_server_[ARCH].zip` (e.g. `PIM_7.0.03.00_Rev-xxxxx_server_win64.zip`) to the installation root `<INSTALLATION_ROOT>`.

   - Check if the following folder structure exists within `<INSTALLATION_ROOT>\server`:

![Folder Structure](image)

4. **Configuration**
   Central configuration (server.properties)
   The settings for the database connection, license, folders, etc. are configured in the server.properties file which is located under:

   `<INSTALLATION_ROOT>\server\configuration\HPM\server.properties`

   Templates for this file can be found in the application server archive, which contains a template file for each supported DBMS.

   `<INSTALLATION_ROOT>\server\configuration\HPM\server.properties.template.[DBMS]`

   Perform the following steps to adjust the server.properties file:
1) Make a copy of the appropriate template file
<INSTALLATION_ROOT>\server\configuration\HPM\server.properties.template.[DBMS].
2) Rename this copy to server.properties.
3) Open this file in an editor and verify each property in this file and adjust the properties to your needs.
4) Save the changes to this file.

See the Configuration Manual for more information about all possible configuration parameters.

For a default installation the following aspects need special attention, all other properties have a default value:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dest.host</td>
<td>Server name of the application server's host (e.g. &quot;henriHost&quot;).</td>
</tr>
<tr>
<td>dest.root.local</td>
<td>Root folder of your installation &lt;INSTALLATION_ROOT&gt;, for example: C:\INFORMATICA\PIM</td>
</tr>
<tr>
<td></td>
<td>Note that in property files, backslashes must be escaped by duplication (\). Alternatively you can specify paths by using a slash (/)</td>
</tr>
<tr>
<td>license.customer.file.local</td>
<td>Local path to the license file. Please contact the Informatica PIM Partner Management to obtain a license file. e.g. &lt;INSTALLATION_ROOT&gt;\license</td>
</tr>
<tr>
<td>license.customer.key</td>
<td>Appropriate customer key (in case of multiline keys, use backslash at the end of the line)</td>
</tr>
</tbody>
</table>

Client/Server communication (NetworkSettings.xml)

Open the <INSTALLATION_ROOT>\server\configuration\HPM\NetworkSettings.xml file to adjust the communication protocol settings. In order that the client can resolve the server name correctly, you have to specify the fully qualified domain name of the server in the host attribute of the HLR-TCP tag. In our example the host name is hpm-server and it is located in the domain henri.com. Optionally you can also adjust the port attribute to the port to be used by the server.

```xml
...<PROTOCOL ...
<HLR-TCP port="1712" host="hpm-server.henri.com"/>
</PROTOCOL>
...```

Note: The default setting for the host attribute 127.0.0.1 (local host) will not work, unless the client is on the same machine!

5. **Startup parameters**

This chapter will explain how to configure the startup parameters such as the memory settings.

This is done in the configuration file <INSTALLATION_ROOT>\server\_environment.conf.

Perform the following steps:

1) Open the configuration file _environment.conf.
2) Change the set.MEM_MAX parameter to the maximum heap space for the Java VM. Never configure more than the physically available memory of the machine.
   (The normal rule is: Physical memory - 1 GB for the OS = maximum heap space.)
3) Change the set.MEM_NEW parameter to the amount of heap memory reserved for the "new generation" in the Java VM. Usually this should be about half the size of the set.MEM_MAX parameter, in case you have a lot of memory, you can reduce this to 1/3 of the maximum heap

PIM 7 Installation (PIM, Audit Trail) 15/26
4) Change the set.GC_THREADS parameter to the maximum number of concurrent garbage collection threads. You should not configure more than about 75 % of the number of available CPUs.
5) Optionally, you can change the PIM Core service name using the set.NAME_SHORT and set.NAME_LONG parameters.
6) Optionally define a different port for the java management extensions (JMX) using the set.JMX_PORT parameter.
7) Save the changes to this file.

6. Media asset provider
In order to work with multimedia documents such as images, videos, etc. the PIM Core module needs a media asset provider. If not configured otherwise, the core module is pre-configured with it's build-in provider (aka Classic Provider, HLR). The build-in provider is merely a simple directory based storage for multimedia documents with limited capabilities regarding image processing etc. If the customer needs a richer set of functionality, please consider using the PIM - Media Manager module.

7. Classic Provider
GraphicsMagick for Classic Provider

The Classic Provider uses GraphicsMagick for processing preview images. This 3rd party tool which is located on the 3rd party archive cd must be installed separately. Classic Provider works with Version GraphicsMagick 1.3.14-Q16 (32 bit for Windows) (other Versions are not tested and are not recommended to be used!). You can find the needed version (GraphicsMagick-1.3.14-Q16(32 bit for windows) ) on the 3rd party archive cd, install it according to it's own installation instructions. See the Configuration Manual for more information about all possible configuration parameters.

8. PIM Web Server Configuration
PIM - Web is part of the PIM - Server since PIM7 and hence must not be installed separately. It uses the integrated Jetty web server, which is configured in:

<PIM_SERVER_INSTALLATION_ROOT>/server/configuration/HPM/server.properties.

<table>
<thead>
<tr>
<th>HTTP Server Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>http.enabled</td>
<td>Enables/disables the integrated web server. In case of false, the file transfer mode 'http' is not available, also the web-services and PIM - Web will not work (default is true)</td>
</tr>
<tr>
<td>http.port</td>
<td>The default port for the web-server (default is 1501)</td>
</tr>
</tbody>
</table>

By default, the application is reachable via the following url:

http://localhost:1501/pim/webaccess
### 3.2.8 MessageQueue Installation

PIM - Audit Trail feature is using Apache ActiveMQ JMS server and one of its features called virtual topics. The idea of virtual topics is to create a message routing from JMS topic to JMS queue. The main difference between topic and queue is communication model: queue is point-to-point and topic is publish-subscriber. In other words it is possible once to read a message from a queue and it is possible to read same message multiple time from topic. You can read more about it here.

In PIM - Audit Trail the Informatica PIM - server is writing messages to a topic but PIM - Audit Trail server is reading topic from a queue. In order to route messages from topic to queue we relay on ActiveMQ virtual topics. No extra configuration in JMS server is required to setup that routing rather ActiveMQ uses a naming convention for topic and queues. Thus is it important to correctly configure topic and queue in PIM - server and PIM - Audit Trail server respectively. See notes in server.properies and audittrail.properties file and note blocks in the document.

#### 3.2.8.1 Installing the Apache Message Queue 5.5.1

The procedure for setting up the Apache Message Queue 5.5.1 for Windows is as follows:

1. Uncompress `PIM_7.0.03_ThirdPartySoftware.zip` from your PIM 7 distribution to your local computer
2. Navigate to the directory `\ActiveMQ 5.5.1`.
3. Unpack the file `MessageQueue.zip` to `C:`.
4. Launch the application using the script `C:\MessageQueue\startup.bat`.
5. To manage the Message Queue use the following link: `http://localhost:8161/admin/`
6. For checking the entries use the following link: `http://localhost:8161/admin/queues.jsp`

To change the connection URL open `C:\MessageQueue\conf\activemq.xml` and modify this entry:

```xml
<transportConnectors>
  <transportConnector name="openwire" uri="tcp://localhost:61616"/>
</transportConnectors>
```

#### 3.2.8.2 Run Apache Message Queue 5.5.1 as a service

1. Call `InstallService.bat` in directory `C:\MessageQueue\activemq\bin\win32`.
2. Open the Microsoft service administration.
3. Open the properties of the "Informatica PIM ActiveMQ" service.
4. On the "General" tab set the startup type to "Automatic".
5. Click on OK.
6. Start the service.

**Note:** With `UninstallService.bat` the service can be deleted.

#### 3.2.8.3 Security (optional)

You can use `SimpleAuthenticationPlugin`. With this plugin you can define users and groups directly in the broker’s XML configuration (`conf/activemq.xml` by default). Take a look at the following snippet for example:

```xml
<plugins>
  <!-- Configure authentication; Username, passwords and groups -->
  <simpleAuthenticationPlugin>
    <users>
      <authenticationUser username="system" password="$\{activemq.password\}"
        groups="users,admins"/>
      <authenticationUser username="user" password="$\{guest.password\}"
        groups="users"/>
      <authenticationUser username="atcsreader" password="arpass"
        groups="atreaders,users"/>
      <authenticationUser username="atcswriter" password="awpass"
        groups="awriters,users"/>
      <authenticationUser username="guest" password="$\{guest.password\}"
        groups="guests"/>
    </users>
  </simpleAuthenticationPlugin>
</plugins>
```

PIM 7 Installation (PIM, Audit Trail) 17/26
Note: Adding the **SimpleAuthenticationConfiguration** into the broker's xml the elements need to be alphabetically sorted: plugins (letter p) has to be inserted after persistenceAdapter and before transportConnectors (letter t).

This snippet should be added in `<broker>` tag. Most of it is default configuration from example. These lines define users used by PIM - AuditTrail:

```xml
<authenticationUser username="atcsreader" password="arpass" groups="atreaders,users"/>
<authenticationUser username="atcswriter" password="awpass" groups="atwriters,users"/>
```

Passwords should be changed. Remember to change them in server.properties files also. These lines grant those users needed access rights:

```xml
<authorizationEntry topic="VirtualTopic.ATCS.ALL" read="atreaders,atwriters" write="atwriters" admin="atwriters"/>
<authorizationEntry queue="Consumer.ATCS.VirtualTopic.ATCS.ALL" read="atreaders" admin="atreaders"/>
```

### 3.2.9 Install PIM - Audit Trail storage server

1. **Download the PIM - Audit Trail zip**
   1) download PIM - Audit Trail from PIM Software Download Area
   2) choose your Version and navigate to the **Binaries Download area** of the appropriate section then download `PIM_<Version>_AuditTrail.zip`.

2. **Extract the Audit Trail archive**
   Choose your `<ARCH>` version and unpack the corresponding audit trial server archive `PIM_<Version>_<Revision>_atserver<ARCH>.zip` to an installation root `<PIM_AUDITTRAIL_INSTALLATION_ROOT>` (for example `C:\INFORMATICA\PIMAuditTrail`).
   Update configuration settings you can copy the properties you already configured while setup the database.

3. **Configure the server connections**
   Following steps will configure the JMS consumer settings.
   1) Go to `<PIM_AUDITTRAIL_INSTALLATION_ROOT>/configuration/audittrailserver/server.properties`
   2) Configure the MessageQueue connection

<table>
<thead>
<tr>
<th>JMS settings</th>
<th>tcp://&lt;host&gt;;&lt;port&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>JMS settings</td>
<td>It has to match the audittrail.properties configuration in PIM - Server. Default: tcp://localhost:61616</td>
</tr>
<tr>
<td>JMS settings</td>
<td>&lt;queue name&gt;</td>
</tr>
<tr>
<td>JMS settings</td>
<td>JMS subscription queue name. The consumer is using VirtualTopic Queue, so queue name should match Consumer.<em>.VirtualTopic.</em> pattern. Default: Consumer.ATCS.VirtualTopic.ATCS.ALL</td>
</tr>
</tbody>
</table>
Optional

<table>
<thead>
<tr>
<th>jms.connection.username</th>
<th>JMS consumer username. It has to match the MessageQueue activemq.xml authenticationUser. Default: atcsreader</th>
</tr>
</thead>
<tbody>
<tr>
<td>jms.connection.password</td>
<td>JMS consumer password. It has to match the MessageQueue activemq.xml authenticationUser. Default: arpass</td>
</tr>
</tbody>
</table>

Note that JMS consumer is using VirtualTopic queue. It means that the queue name should match the following pattern Consumer. <consumerUniqueName>.VirtualTopic.<rest of the topic name> where consumerUniqueName is a name of the consumer and can be what ever you want and "rest of the topic name" is a topic name defined in the PIM Core audittrail.properties file.

3) Configure Audit Trail Server remote access. Those settings should match to PIM Core configuration audittrail.properties(audittrail.persistence.server.*)

<table>
<thead>
<tr>
<th>Remote access</th>
<th></th>
</tr>
</thead>
</table>
| server.communication.host | Audit Trail server host  
 Default: localhost                                                                 |
| server.communication.port | Audit Trail server port  
 Default: 2801                                                                 |
| server.authentification.enabled | Turn authentification on/off  
 Default: true                                                  |

4) Optional: Only necessary if Audit Trail server security is activated
   - run <PIM_AUDITTRAIL_INSTALLATION_ROOT>/bin/setup_console.bat (a console with osgi> prompt pops up)
   - update remote access username/password for default user using userSetPassword command in console.

4. Start Audit Trail server
   1) run <PIM_AUDITTRAIL_INSTALLATION_ROOT>/bin/console.bat or install as system service <AUDITTRAIL_INSTALLATION_ROOT>/bin/serviceInstall.bat
   2) Check <PIM_AUDITTRAIL_INSTALLATION_ROOT>/configuration/*.log and <PIM_AUDITTRAIL_INSTALLATION_ROOT>/logs/.error.log if server does not start.

3.2.10 Install PIM Audit Trail feature in PIM - Server

PIM - Audit Trail feature can simple installed by coping content of the PIM_<Version>_._<Revision>_audittrailHpmServer.zip package into PIM - Server installation root <PIM_SERVER_INSTALLATION_ROOT>/iserver (into features and plugins folders respectively).

PIM - Audit Trail feature can be configured by setting the following properties in <PIM_SERVER_INSTALLATION_ROOT>/configuration/HPM/audittrail.properties file:

1. Enable PIM - Audit Trail

<table>
<thead>
<tr>
<th>General settings</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>audittrail.enabled</td>
<td>Enable or disable Audit Trail functionality. If Audit Trail is disabled there will be no performance overhead.</td>
</tr>
</tbody>
</table>

2. JMS connection configuration

ATCSs (Audit Trail change sets) are sent to JMS so a connection URL and topic name should be specified. Username and password should be specified if JMS server is configured to accept only authenticated connections.

<table>
<thead>
<tr>
<th>JMS settings</th>
<th></th>
</tr>
</thead>
</table>
| audittrail.jmsconsumer.jms.topic | JMS topic where Audit Trail Change Sets will be sent to.  
 Default: VirtualTopic.ATCS.ALL |
The topic name should start with VirtualTopic prefix because ActiveMQ maps such topics to queues internally by a convention. In the Audit Trail storage server configuration corresponding queues have to be named Consumer.*.VirtualTopic.<rest of the topic name> where part of the queue name marked by asterisk should be different for each consumer.

Example:

```
audittrail.jmsconsumer.jms.topic = VirtualTopic.ATCS.ALL (in PIM Core audittrail.properties file)
```

```
jms.queue.name = Consumer.ATCS.VirtualTopic.ATCS.ALL (in the Audit Trail server server.properties file)
```

- `audittrail.jmsconsumer.jms.persisted`: Default: false

If messages are not persisted then they will be lost if JMS server crashes or is restarted but JMS server can become a performace bottle neck if messages are persisted (SSD or raid can help). You can see if JMS server is a bottle neck in JMX bean `com.heileurer.ppm/auditTrail/auditTrailJmsStatisticsWaitingThreadsCount` attribute. Ideally it should be 0. The JMS server is definitly a bottle neck if `WaitingThreadsCount` equals `SessionPoolSize` or `auditTrailProcessorStatisticsPoolSize`.

3. **ATCS local storage configuration**

If JMS server temporary is not accessible then audit trail processor attempts to save ATCS records locally. Saved messages are sent to JMS as soon as JMS server become accessible.

One can configure different types of local storage:

**Storage types:**

1. `file` - each message is serialized to file - recomendend
2. `discard` - messages discarded (ATCS records will be lost)
3. `jdbm` - storage based on JDBM (fast but not stable on large volumes)
4. `memory` - stores messages in memory

<table>
<thead>
<tr>
<th>ATCS storage configuration</th>
<th>&lt;storage type&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>audittrail.jmsconsumer.storage.type</code></td>
<td><code>&lt;storage type&gt;</code></td>
</tr>
<tr>
<td>Default: file</td>
<td></td>
</tr>
</tbody>
</table>

4. **Audit Trail server configuration (for client)**

Default Audit Trail server configuration is transferred to PIM - Desktop. It is used to search in Audit Trail (AT) storage from the client.

<table>
<thead>
<tr>
<th>Audit Trail server connection settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>audittrail.persistence.server.host</code></td>
<td>Audit Trail server host</td>
</tr>
<tr>
<td>Default: localhost</td>
<td></td>
</tr>
<tr>
<td><code>audittrail.persistence.server.port</code></td>
<td>Audit Trail server port</td>
</tr>
<tr>
<td>Default: 2801</td>
<td></td>
</tr>
<tr>
<td><code>audittrail.persistence.server.username</code></td>
<td>Audit Trail server connection credential - username</td>
</tr>
<tr>
<td>Default: Administrator</td>
<td></td>
</tr>
<tr>
<td><code>audittrail.persistence.server.password</code></td>
<td>Audit Trail server connection credential - password</td>
</tr>
<tr>
<td>Default: Administrator</td>
<td></td>
</tr>
</tbody>
</table>

5. **ATCS configuration**

<table>
<thead>
<tr>
<th>ATCS configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>audittrail.atcsbuilder.locale</code></td>
<td>Locale for object labels and entity names (Audit Trail saves object labels only in one language). If not defined then HPM server locale is used. Default: en_US</td>
</tr>
</tbody>
</table>
### 6. Start PIM - Server

In case of successful Audit Trail startup you should see the following log messages:

- Initialize audit trail
- audit trail is enabled
- registering default audit trail processor
- Initialize audit trail completed (Duration: 29.9680 ms)

### 3.2.11 PIM - Audit Trail activation in repository

Audit Trail can be activated for any root entity in the repository.

1. Open the repository editor,
2. Go to Custom section and select a root entity
3. Set Supports Audit trail flag to true in order to activate Audit Trail for this entity

**Note:** Audit Trail can be activated and deactivated any time.

### 3.2.12 PIM - Desktop Installation

1. **Download the PIM Core zip**
   - If you have not downloaded PIM Core zip already, please click on the link below to get to the
     1) PIM Software Download Area
     2) choose your Version and navigate to the Binaries Download area of the appropriate section then download `PIM_<Version>_Core.zip`.
     3) The client archive is distributed within the PIM Core zip and has the following format `PIM_<Version>_<Revision>_client_win32.msi`

2. **Installing the client with MSI file**
   - This chapter describes how to install the client by means of a MSI file which is a Microsoft Installer executable providing a wizard like installation procedure.
   - **Note:** there's a limitation of the MSI package: PIM Web permissions cannot be configured when using a MSI based installation. Please use the zipped client installation package instead to setup PIM Web permissions.

   Perform the following steps:
   1) Execute the installer file `PIM_<Version>_<Revision>_client_win32.msi` (e.g. `PIM_7.0.03.00_Rev-28944_client_win32.msi`).
   2) Click on Next.
3) Choose a destination folder to which Informatica PIM - Desktop will be extracted and click on **Next**.

4) Click on **Install**.

5) The **Informatica PIM - Desktop** will be extracted to the destination directory.

6) Confirm the signature warning dialog (only Windows Vista and Windows 7).

7) Click on **Finish** to exit the Setup Wizard.

**Note:** In case you have a customized client, you might not have the MSI installation package, but the zipped archive **PIM_<Version>_<Revision>_client_<ARCH>.zip**. The client's installation is really nothing more than unpacking the zip file to a folder of your choice in which you have modify permissions. The uninstall is done by deleting the directory in which you unzipped the client.
3.2.13 Install PIM Audit Trail feature in PIM - Desktop

PIM - Audit Trail feature can simple installed by coping content of the PIM_<Version>_<Revision>_audittrailHpmClient.zip package into PIM - Desktop installation root <PIM_DESKTOP_INSTALLATION_ROOT> (into features and plugins folders respectively).

PIM - Audit Trail permission must be granted in order to search and browse audit trail data.

3.2.14 Starting the PIM server as service (only Windows)

The following instructions describe how the server can be started as a service. Perform the following steps:

1. Open Start > All Programs > Administrative Tools > Computer Management > Local Users and Groups > Users > New User ...

2. Create a new user account for the PIM service (e.g. PIM).
   In case the PIM - Server Application Server Host is part of a domain, we recommend to use a special domain user for the following steps, rather then creating your own local user.
   Note: Please contact your network administration department so they create this service user for you.

3. In the Windows Explorer, go to the <INSTALLATION_ROOT> directory.
4. Give the PIM user “modify” permissions to this directory. This can be reached by right click 'Properties', Tab 'Security', 'Edit'
5. Open Start > All Programs > Administrative Tools > Local Security Policy > Local Policies > User Rights Assignment.
6. Assign the "Lock pages in memory" privilege to the PIM user.

7. Log on with the PIM account.
8. Check the user specific TEMP and TMP environment variables.
   It is necessary that they have no whitespaces in them (take care about the %USERPROFILE% variable - it might contain whitespaces).

9. In the Windows Explorer, start the <INSTALLATION_ROOT>\server\console.cmd file to ensure that your configuration is correct. If the server starts successfully, you can proceed.
10. Stop the server again by pressing CTRL+C in the command line window.
11. Execute the <INSTALLATION_ROOT>\server\install.cmd command file which will register the PIM - Server as a service. (The <INSTALLATION_ROOT>\server\uninstall.cmd removes the service registration again).
12. Open Start > All Programs > Administrative Tools > Services.
13. Modify the service's properties so that it uses the PIM user.
14. Optionally, you can change the "Startup Type" to "Automatic".
15. Check the correct registration.

16. Start the PIM - Server service. The start of the service can require nearly 2 minutes!
   You can watch the start activity at the file `<INSTALLATION_ROOT>\server\logs\out.log`
   (Tools like Tail for Win32 or Log Viewer (both work like the well known tail command in unix)
   are quite handy for this). In case you want to have a short test of your system setup it is also
   possible to startup the server in console mode with the following batch
   file `<INSTALLATION_ROOT>\server\console_debug.cmd`
17. Check the correct start by opening the
   file `<INSTALLATION_ROOT>\server\logs\out.log` and checking for errors.

Tip: If you have special environment configuration needs, you can adjust the default settings
in the `<INSTALLATION_ROOT>\server\service\wrapper.conf` file.
Note: Usually there is absolutely no need to modify any of these settings. Contact the Informatica PIM
Support department if you think you absolutely need to modify it.

3.2.15 Starting the client

Perform the following steps:

1. Run the Informatica PIM - Desktop by double clicking the "Informatica PIM Desktop" shortcut on
   your desktop or in your start menu.
2. While starting, the Informatica PIM - Desktop tries to connect to its corresponding Informatica
   PIM - Server.
   In case the client cannot find the server with the default connection settings, it will prompt for
   alternative connection settings.

3. Enter the server name and port of the Informatica PIM - Server and click OK.
4. In case your local windows user is not (yet) known to the Informatica PIM, or the Single-Sign-
   On feature is disabled, you will be prompted with a login screen.
5. Enter your user name and password here and confirm with OK. For a very first login you can use the default Administrator account with the credentials Administrator/Administrator to create an initial set of users.

Note: If you don't want to use the default connection settings or you want to login as another user than the local windows user, you can change the server connection settings and the user login when you keep the CTRL key pressed during startup.