IDENTITY PROVISIONING CONCEPT

Overview Identity Management and Provisioning

Identity management is often used as a generic term for the administrative processes and technical means used to administer user identities and permissions for different applications and services.

Provisioning is a part of the area of identity management, and is used to distribute identity and attribute information to relevant applications and services that have their own identity and authorization source.

Identity Provisioning

The Identity Provisioning (IP) Service synchronizes information across multiple Data Sources. Information can be synchronized across Data Sources in one enterprise. Information in an enterprise can also be synchronized with information in a cloud service or application.
Synchronization takes place through the migration of data from one Data Source to another. Data can be migrated to one Data Source or distributed to multiple data repositories simultaneously. Two-way provisioning is supported, so that a Data Source can be the source and target of identity information. Data flows can be saved in Policies and automated.

The IP Service consists of a server engine, Policy components, and an internal database. Policy components include Data Source objects, Schedulers, and Actions. Actions determine how data is gathered, modified, and distributed.

The IP Service works by constructing a virtual image of identity information integrated from one or more Data Sources. The virtual image and identity information can be modified by the Actions you configure.

The IP Service is developed in Java and can be installed on multiple operating system platforms. When installed, the IP Service can be started as a service on Windows or as a daemon process on other operating systems. This document aims to provide an overview and description of the functionality of the Identity Provisioning (IP) service and its architecture.

Architecture

IP's architecture consists of a server engine and components such as *Policies*, *Data Sources*, *Actions* and *Schedules*.
There is also an internal database, which is used to store configuration information and to handle transaction lines and time stamps.

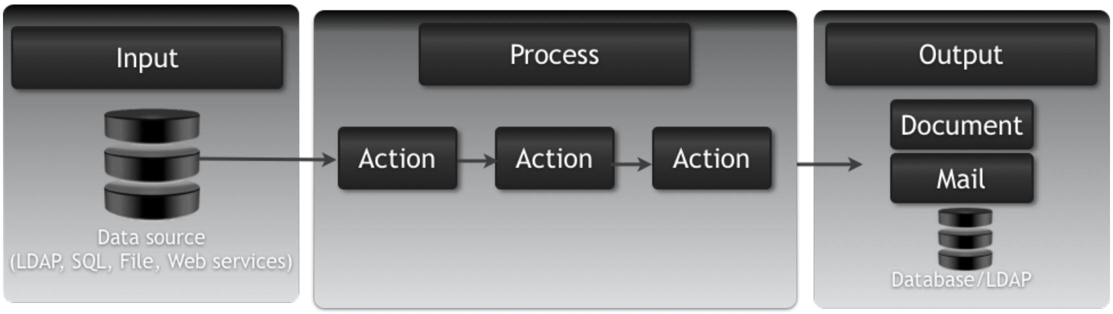
Policy Concept

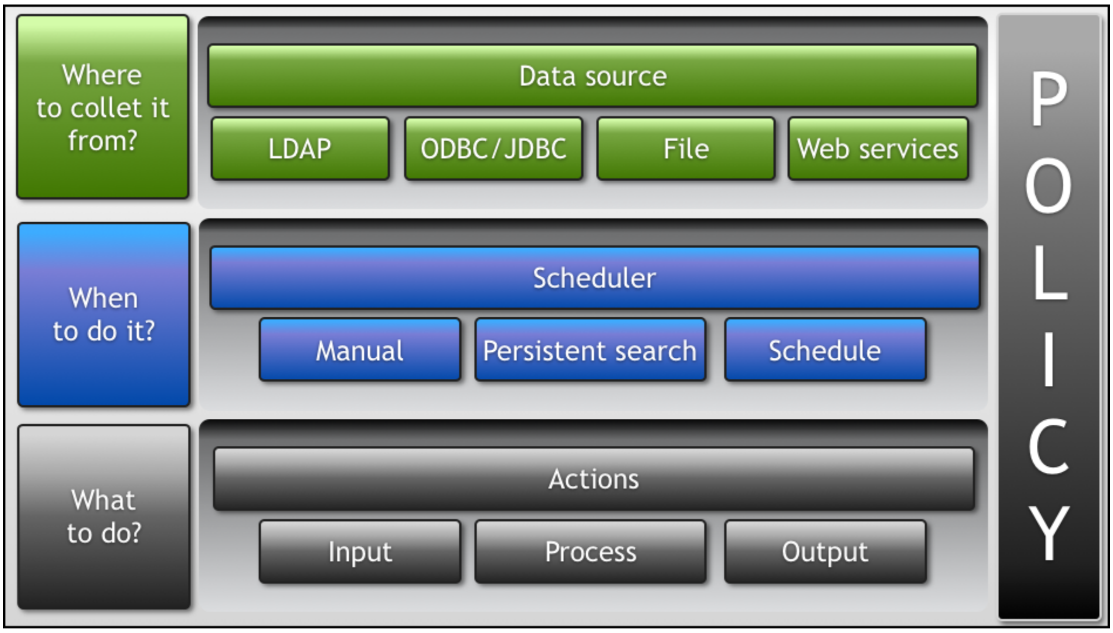
Policies require a Data Source, a Scheduler, and at least one Action.
Data Source — Where to collect the data
Scheduler — When to run the Policy
Action — What to do with the data

A policy has multiple functions and is the component that holds the logical concept by which policies are constructed:

- What data source connector and configuration to use for obtaining information from a specific data source to create session objects.
- Rules for how the session object should be created and processed.
  For example, the session object is created by performing searches or queries, manually or scheduled, in an LDAP directory, SQL database or any kind of text file (LDIF, CSV, Excel).

  Session objects can also be created when IP is notified of a change/event that has been carried out in an LDAP directory service that supports *Persistent Search* (see section Scheduler).
- A schedule is set to start and execute the desired process.
- Actions are defined in the policy and the order, in which these actions shall be executed, is set.





Picture: Shows the logical concept of a policy.

Data Sources

To gather data from a source, configure a Data Source connector in the IP Studio. Connectors are supported for the following databases and file formats:

- LDAP directory. Searches of the LDAP directory is performed by using the LDAP search filter syntax in RFC 2254.
- ODBC or JDBC database connection. SQL databases using SQL commands and syntax
- Imported LDIF or comma-separated files
- Web services interface
- Actions

Note: Supported LDAP directories include LDAP v3 Directory Services, Active Directory and Active Directory LDS, Novell eDirectory, Siemens DirX, and OpenDS.

Scheduler

The Scheduler defines when and how a Policy is started. There are three types of Schedulers. The type of Scheduler determines the type of Policy.

Manual — Manual Policies can only be executed in the administrative user interface or triggered by an Action configured in the administrative user interface.

Scheduled — Scheduled Policies are configured in the administrative user interface to be executed at a specified time or interval.

Persistent Search — Persistent Search Policies can be configured for an LDAP directory that supports Persistent Search or an Active Directory with DirSync control. Policies of this type start a separate thread that listens to the directory. When the thread notifies the Policy of specified events, the Policy automatically creates and updates Session Objects and Attributes according to rules defined in the Policy.

Actions

The Provisioning Service includes a menu of Actions that can be used when building the logic to be applied to the information in the Data Source. There are three types of Actions:
Input — Adds data from one or more Data Sources to the object virtual image by creating new Session Objects or Attributes.
Process — Updates existing Session Objects and their Attributes.
Output — Saves data from existing Session Objects and their Attributes by writing to one or more data repositories.

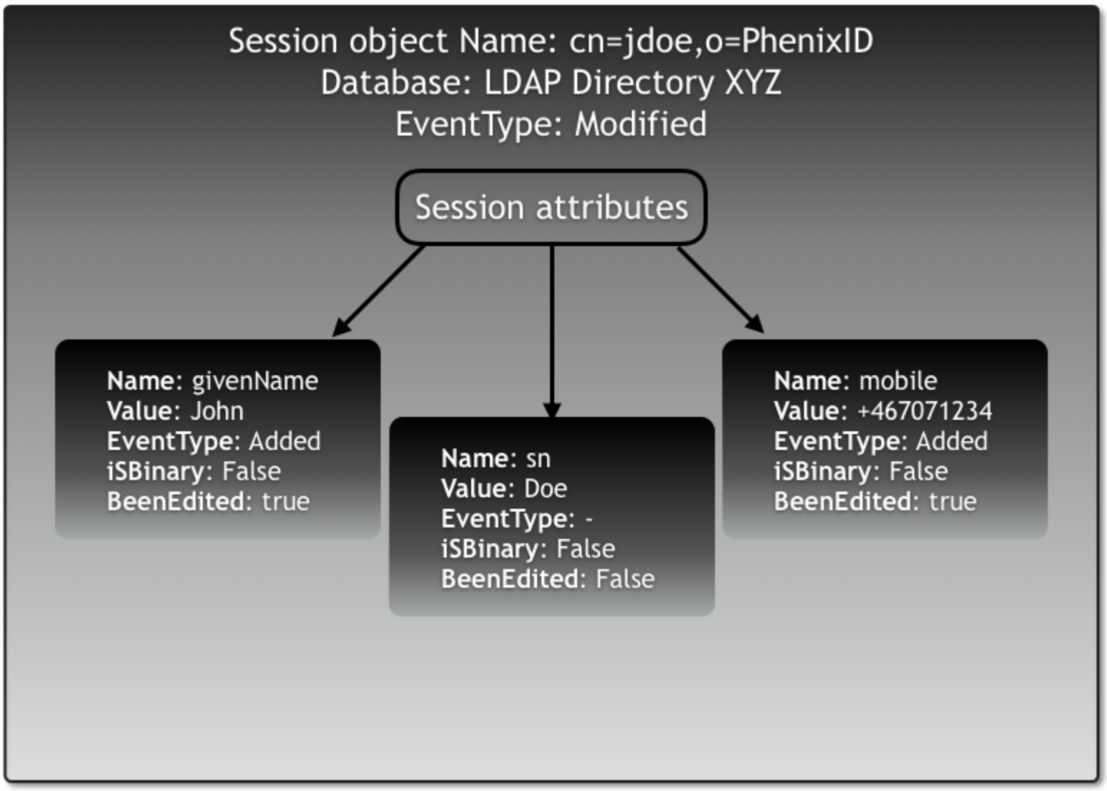
Actions contain definitions of what should be done in one or more session objects. The policy also states the order in which one or more Actions to be applied.
IP includes a number of accompanying Actions that can be used to build up the logic to be applied to the information received.

API to develop custom Actions

In addition, the IP Service includes an API that lets you develop custom Actions as needed in case the enclosed actions not are sufficient.

Session object and session attribute

All data entering the IP Service from a Data Source is converted to Session Objects. Session Objects are created when LDAP and SQL databases are searched or LDIF and CSV text files are parsed. Session Objects can be created and updated automatically by the IP Service when a change occurs in an LDAP directory that supports Persistent Search or Active Directory with DirSync control.
An IP Session Object contains information, such as the name of the database entry, the event type, and the Data Source. Session Objects have one or more Session Attributes. Attributes also contain information, such as a name, a value, an event type, and Boolean flags.



Picture: Session object

Communication security

Different types of security can be implemented to protect and encrypt communication between the IP service and external applications and systems. A connector of type LDAP, or Web service (XML) that uses HTTP can use certificate-based authentication and encryption by using LDAPS (SSL / TLS) or HTTPS.

Log handling

IP provides logging into several levels and can notify an interested part via several methods if any inaccuracies are detected. Logs can be redirected if required.