

Gabriel Magariño

Software Engineer

gabriel.magarino@gmail.com

www.javapassion.com/idm

Architecture Revisited

Disclaimer and Acknowledgments



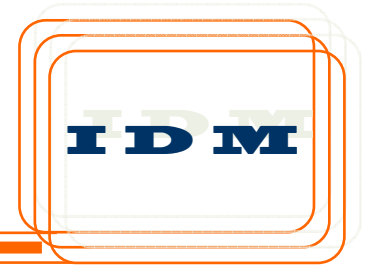
- ▶ The contents here are created as a own personal endeavor and thus does not reflect any official stance of Sun Microsystems on any particular technology
-

Identity Manager Components



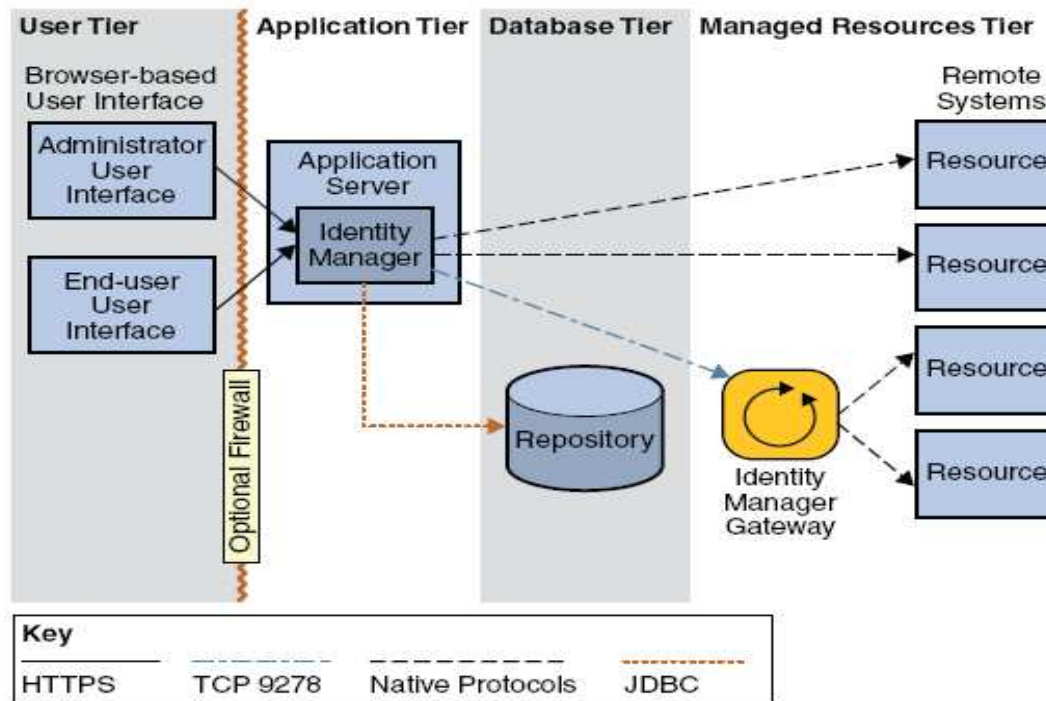
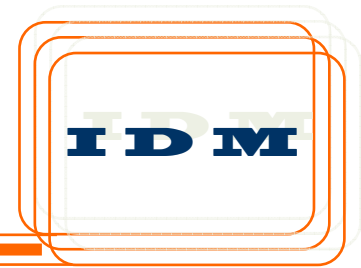
- ▶ Identity Manager is a Java 2 Platform, Enterprise Edition (J2EETM platform) web application.
 - ▶ The J2EE platform consists of a set of industry-standard services, APIs, and protocols that provide the functionality for developing multitiered, web-based, enterprise applications.
-

Identity Manager System Architecture



- ▶ The IdentityManager system architecture is distributed across four logical tiers
 - » The user tier
 - » The application tier
 - » The database tier
 - » The resources tier
-

Identity Manager System Architecture



User Tier



- ▶ The user tier consists of administrators and end users who interact with Identity Manager through one of the user interfaces.

 - ▶ The main user interface for the product is a web browser, which communicates with IdentityManager over HTTPS.

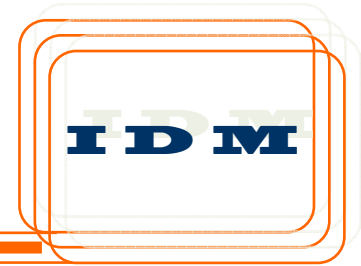
 - ▶ The two browser-based UIs, the *administrator user interface* and the *end-user interface*, primarily consist of HTML pages, although some features may use Java applets.
 - » Other user interfaces, however, are also located in the user tier.
 - These include the IVR telephone interface, the Identity Manager IDE, the SPML web services interface, and the Identity Manager console.
-

Application Tier



- ▶ Identity Manager (also known as the Identity Manager server) is installed in a J2EE web container inside an application server.
 - » **IdentityManager server consists of JSPTM files, HTML, images, and JavaTM classes.**
 - ▶ Adapters and connectors, which interface with other IT systems (also known as *resources*), are also located in Identity Manager on the application server.
 - ▶ Identity Manager is a web application, the user interface resides on the application server and pages are served to the user tier on a request-by-request basis.
-

Database Tier



- ▶ Identity Manager stores all of its provisioning and state information in the IdentityManager *repository*.

 - ▶ The repository is comprised of tables that store all the configuration data about Identity Manager.
 - » **It is a single point for IdentityManager to look up data and lock objects.**

 - ▶ The repository also contains an audit log, which is a history of actions taken in IdentityManager.
 - » **IdentityManager data is stored as XML.**
 - » **The repository can reside in local files or a relational database, although in production, a relational database is required.**
-

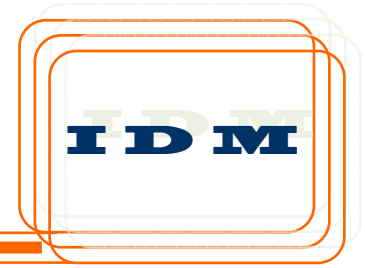
Database Tier...



- ▶ Identity Manager can connect to the repository over a direct JDBC connection, or it can use data source functionality made available by your application server.

 - ▶ The Identity Manager Service Provider feature requires an additional LDAP repository for storing user information.
-

Resource Tier



- ▶ The resource tier consists of the applications and IT systems to which you provision and deprovision user accounts.
 - » **It includes the Identity Manager Gateway, which is a helper application that allows Identity Manager to interact with certain resources.**

 - ▶ Adapters and connectors provide user management functions, including creating, updating, deleting, and reading user accounts, and performing password change management functionality.
 - » **Adapters and connectors can also extract account information from a remote system.**
-

Resource Tier ...



- ▶ Some common resources that require the use of the Sun IdentityManager Gateway include Microsoft Exchange, Windows Active Directory, Novell eDirectory (formerly Netware Directory Services), Lotus Domino, and several others.

 - ▶ The Gateway installs as a service in Windows and communicates with Identity Manager using TCP port 9278.
 - » **Communication is initiated from Identity Manager using a proprietary encrypted protocol.**

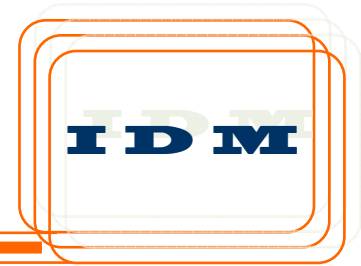
 - » **The Gateway then interfaces with managed resources using the resources native protocols.**
-

Resource Tier ...



- ▶ From an installation perspective, there are two type of adapters and connectors
 - » **Identity Manager adapters and connectors**
 - Identity Manager adapters and connectors are pre-installed in Identity Manager.
 - » **Custom adapters and connectors.**
 - Custom adapters and connectors, however, need to be copied to a designated directory in the Identity Manager installation directory located on the application server.
 - Custom adapters are easy to create using the Identity Manager *Resource Extension Facility (REF)* kit.
 - › The REF kit provides the API and a number of template adapters that companies can use to jump start the development process.
-

System Separation and Physical Proximity Guidelines



- ▶ Development environment
 - » In a development environment, the application server and database can reside on the same machine.

 - ▶ In testing and production environments
 - » Identity Manager instance should be installed on its own dedicated server.
 - The relational database also requires a dedicated server.

 - ▶ The Identity Manager Gateway, if required, must be installed on one or more Windows machines.
 - » The Gateway is a lightweight component and does not require a dedicated server.
 - » All Windows domains managed by a Gateway must be part of the same forest.
 - » Managing domains across forest boundaries is unsupported. If you have multiple forests, install at least one Gateway in each forest.
 - » In production the Gateway must be made highly available.
-

System Separation and Physical Proximity Guidelines...



- ▶ In a production environment, the highest amount of network traffic occurs between the database and application servers.
 - » These two environments must be on the same LAN with the shortest network hop possible.
 - » Gateway instances, as well as managed resources, do not need to be on the same network as Identity Manager.

 - ▶ If Identity Manager will be used for external users in a Service Provider configuration, a set of web servers should be setup in a DMZ.
-

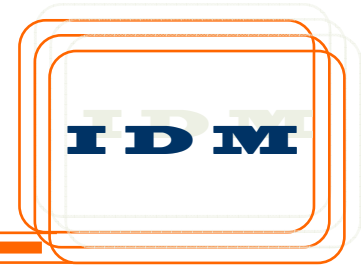
SPML and the Web Services System Architecture



- ▶ Service Provisioning Markup Language (SPML) and Identity Manager Web Services can be used to implement a custom front-end for Identity Manager.

 - ▶ Identity Manager sends and receives SPML messages and responses using the HTTPS protocol.
-

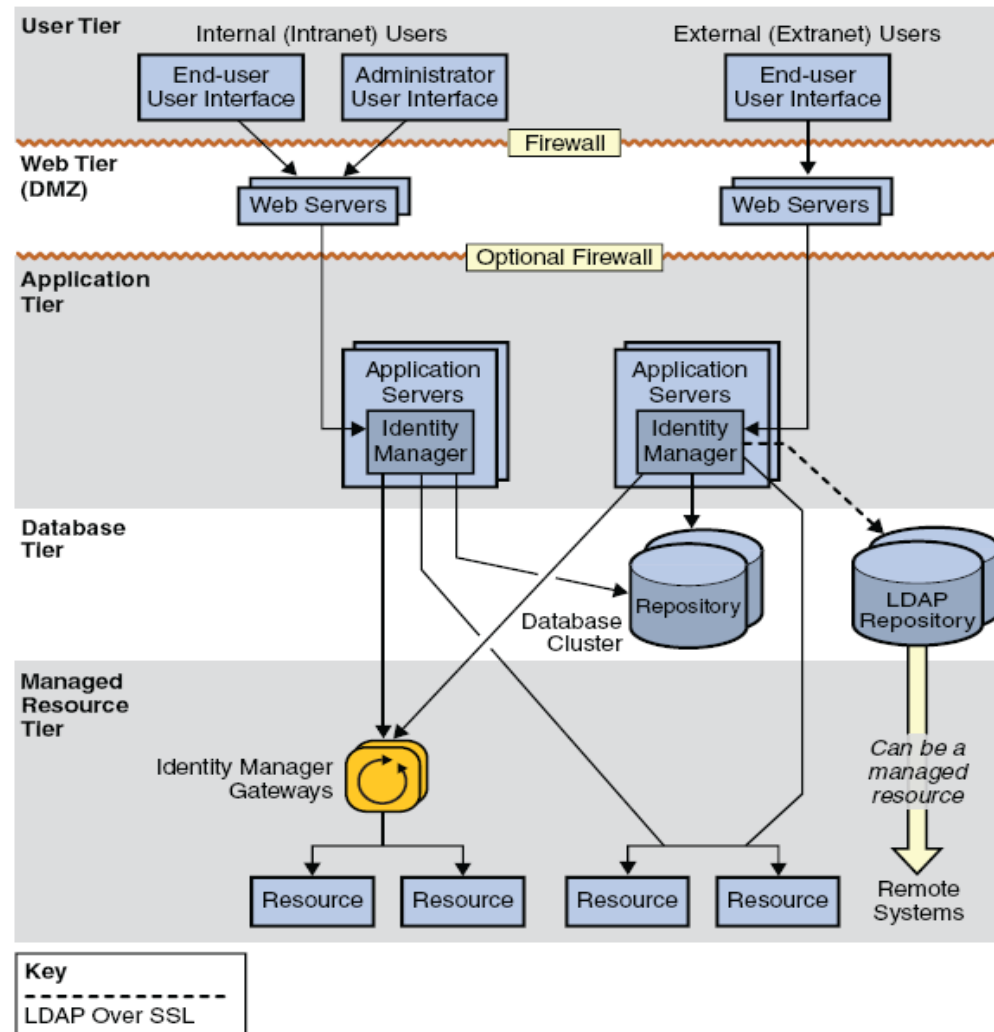
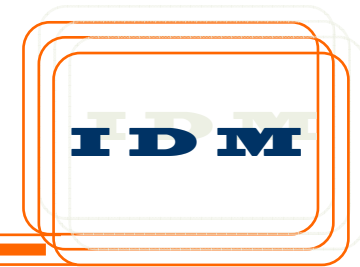
Identity Manager Service Provider System Architecture



- ▶ If the Identity Manager Service Provider feature is implemented, a fifth tier is required.
 - » **This tier is called the Web tier and it consists of one or more web servers located in a DMZ**
 - » **No Identity Manager components are installed in the web tier.**
 - Instead, the web servers in the DMZ support one or more application servers in the application tier by responding to web page requests.
 - Adding one or more web servers to the web tier provides enhanced scalability, and placing the web servers in a DMZ provides better network security.

 - ▶ The Service Provider feature also requires an LDAP repository. This repository resides in the database tier.
 - » **Because the LDAP repository can be a managed resource, the LDAP server can be understood as residing in the managed resource tier, as well.**
-

Identity Manager Service Provider System Architecture



Gabriel Magariño

Software Engineer

gabriel.magarino@gmail.com

www.javapassion.com/idm

Architecture Revisited