

Gabriel Magariño

Software Engineer

gabriel.magarino@gmail.com

www.javapassion.com/idm

Overview 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
-



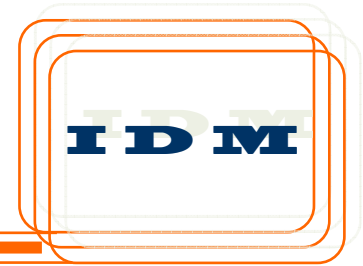
What is IdentityManager?

- ▶ Sun IdentityManager makes it possible to automate the process of creating, updating, and deleting user accounts across multiple IT systems.

 - ▶ This process is known as *provisioning* (that is, creating and updating user accounts) and *deprovisioning* (deleting user accounts).

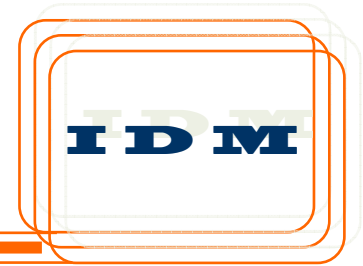
 - ▶ IdentityManager can also enforce audit policies on an ongoing basis.
 - » **An *audit policy* specifies what types of access a user may or may not have.**
-

Identity Manager Interface With Other IT Systems



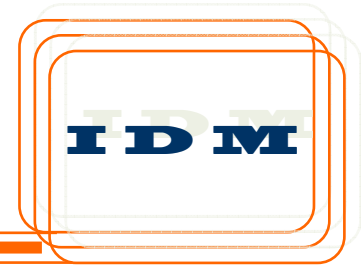
- ▶ In IdentityManager, managed applications and other IT systems are called *resources*.
 - » **Identity Manager uses either *adapters* or *connectors* to interface with resources.**
 - ▶ Adapters and connectors are installed on the Identity Manager server.
 - » **IdentityManager does not require special software (called *agents*) to be installed on target resources.**
 - ▶ Dozens of Identity Manager adapters and connectors are available, and new ones can be created to communicate with almost any resource using standard protocols or known application programming interfaces (APIs).
-

Identity Manager Interface With Other IT Systems

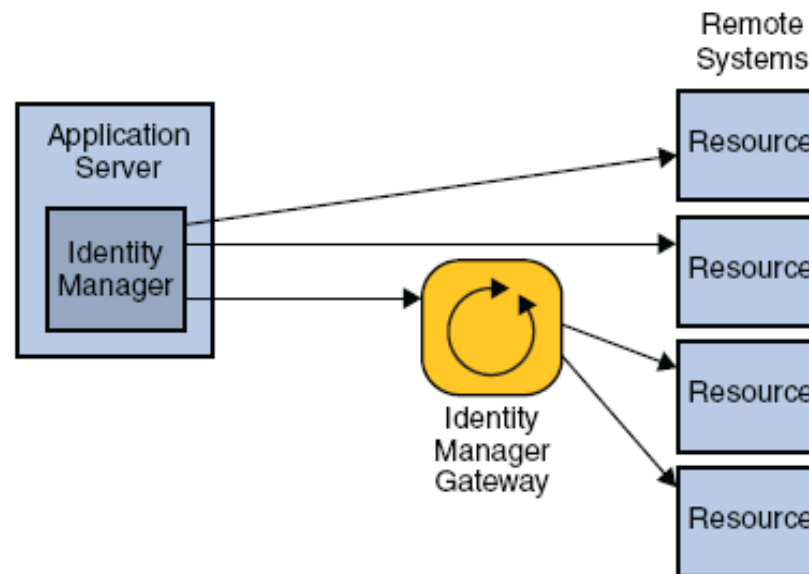


- ▶ Some resources cannot be communicated with directly and require the use of the Sun Identity Manager Gateway.
 - » **Examples of resources that require the Gateway include Microsoft products, such as Exchange and Windows Active Directory, Novell products, such as eDirectory (formerly Netware Directory Services), and several others.**
 - » Identity Manager communicates directly with the Gateway and the Gateway interfaces with the resource.
-

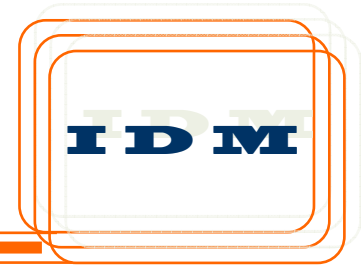
Identity Manager Interface With Other IT Systems



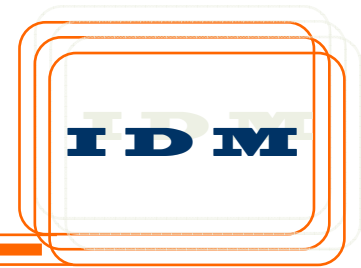
- ▶ IdentityManager Interfaces with Some Resources Directly, While Other Resources Require the IdentityManager Gateway



Users Connected to Identity Manager

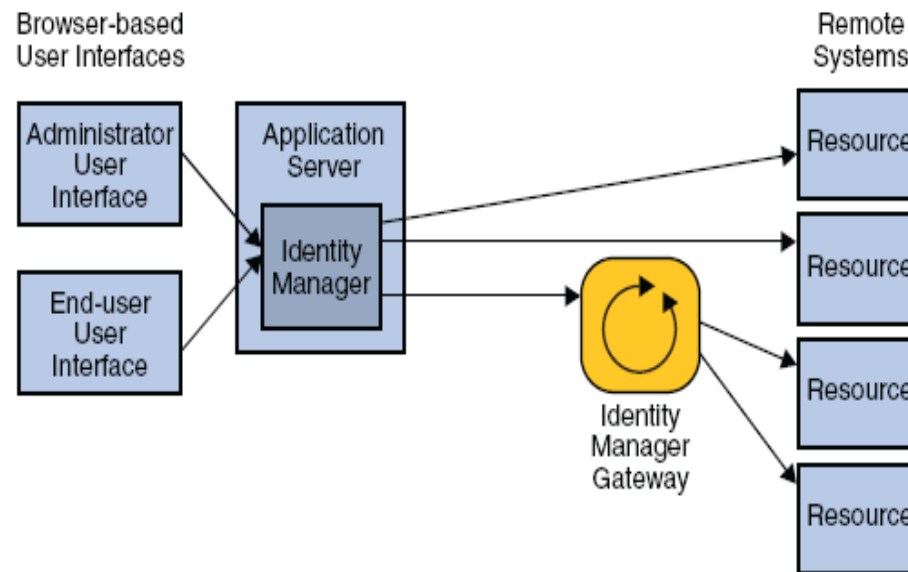


- ▶ IdentityManager has a user interface (UI) for administrators, and a separate interface for end users.
 - » To use IdentityManager, administrators and end users use a web browser to log on to IdentityManager.
 - » Administrators use the *administrator interface* to manage users, set up and assign resources, define rights and access levels, establish audit policies, manage compliance, and perform other business administrator and system administrator functions.
 - » End users use the *end-user interface* to perform a range of self-service tasks, such as changing passwords, setting answers to authentication questions, requesting access to IT systems, and managing delegated assignments.
-



Users Connected to Identity Manager...

- ▶ Users Can Connect to Identity Manager Using the Administrator Interface and the End-User Interface



Users Connected to Identity Manager...



- ▶ Companies can also use SPML (Service Provisioning Markup Language) to either create their own user interface, or integrate an existing front-end system with Identity Manager.

 - ▶ **Other IdentityManager interfaces include the following:**
 - » The IVR (Interactive Voice Response) telephone interface, which enables end users to perform IdentityManager functions using a telephone
 - » The IdentityManager IDE (Integrated Development Environment), which is used by software developers to customize IdentityManager
 - » The IdentityManager console, which is a command-line interface available to administrators
-

Identity Manager Service Provider



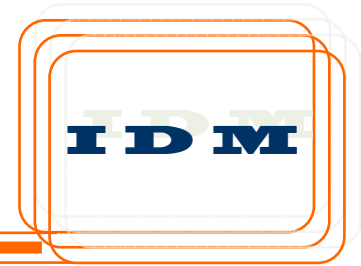
- ▶ Identity Manager Service Provider is a highly scalable, extranet-focused identity management feature that is capable of provisioning and maintaining millions of end user accounts that are stored on an LDAP directory server.
 - ▶ The Service Provider feature uses a subset of the features and functionality available in Identity Manager. For example, auditing functionality is not available because it is less useful in an extranet environment.
-

Sun's Other Identity Management Products



- ▶ In addition to Identity Manager, Sun's other identity management solutions include Sun Java™ System Directory Server Enterprise Edition, Sun OpenSSO Enterprise, and Sun Role Manager.
 - ▶ These products complement IdentityManager, and, in the case of Role Manager, can extend the capabilities of Identity Manager.
-

Sun's Other Identity Management Products...



▶ Sun Java System Directory Server Enterprise Edition

- » Sun Java System Directory Server Enterprise Edition is a scalable, high-performance LDAP data store for identity information.
- » Directory Server Enterprise Edition provides core directory services, as well as other complementary data services.

▶ OpenSSO Enterprise

- » Sun OpenSSO Enterprise (formerly Sun Java System Access Manager and Sun Java System Federation Manager) centralizes and enforces a comprehensive security policy for internal and external applications and web services.
- » It provides secure and centralized access control and single sign-on (SSO) functionality.
- » It allows for federated identity management, which makes it possible to share applications with companies that have different directory services, security, and authentication technologies.
 - Federated partners trust each other to authenticate their respective users and vouch for their right to access services.

▶ Sun Role Manager

- » Sun RoleManager (formerly Vaau RBACx) simplifies access control compliance by managing access based on a user's roles within a company and not on an individual, user-by-user basis.
 - » By creating roles based on usage and enterprise policies, companies can gain greater visibility into access and manage it in a more efficient, secure, and compliant manner.
-

Gabriel Magariño

Software Engineer

gabriel.magarino@gmail.com

www.javapassion.com/idm

Overview Revisited