An Oracle White Paper
January 2010

The Identity Warehouse: Best Practices

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Table of Contents

1. Executive Summary

Enterprises are always in a state of flux. They are expanding their geographical footprint, shrinking their employee count, outsourcing non-core business or service areas, changing organizational structures, or engaging with third-party service providers who are privy to sensitive data. Business dynamics, therefore, demands that technology capture these ongoing changes and provide managers and decision makers with a macroscopic view of employees, both temporary and permanent, as well as the resources they have access to.

Oracle Identity Analytics, Oracle's comprehensive role management and identity compliance solution, is the technology that addresses the challenge of providing an enterprise-wide view of all users and their access to various target systems. The Oracle Identity Analytics Identity Warehouse is the central repository that contains all the important entitlement data for your organization. This white paper introduces the Identity Warehouse, provides best practices for building the warehouse, and describes how Identity Warehouse data supports other features that are available in Oracle Identity Analytics.

Business Challenges

Technology experts, information officers, security personnel, and IT administrators are often looking for an answer to the following questions:

- Is there an enterprise-wide view of both employees and temporary contractors across various applications and target systems? Is this information being replenished on a regular basis? Is the current information the most up-to-date?
- Are there any orphan accounts in the enterprise? Have they been removed?
- Where can glossaries, which explain cryptic entitlements to certifiers, be stored? How can they be updated and maintained?
- Can entitlements that are sensitive to the security of the organization be classified?
- Is there a central repository that stores and displays identity- and access-related information such as roles and policies?
- Can policies concerning Segregation of Duties be defined at the roles and policy level?

2. Elements of the Identity Warehouse

The Identity Warehouse is a central repository that contains user and user entitlement data. This data is imported from one or more databases within your organization on a scheduled basis. The Oracle Identity Analytics import engine supports complex entitlement feeds saved as either text files or XML. Extract, Transform, and Load (ETL) processing capabilities are also available. In addition, a seamless integration with market leading Identity Management and provisioning solutions such as Oracle Identity Manager is also available, to automatically seed the Identity Warehouse. A glossary entry for each entitlement can also be captured during the import process.

The following table lists and defines the elements of the Identity Warehouse:

Element	Description
User	A discrete, identifiable entity that has a business need to access or modify enterprise information assets. A user has either a manager or an application *approver* who is tasked with carrying out various user- and role-management functions on the user.
Resources and Resource Type	Resources are the applications and enterprise information assets that users need to do their jobs. In Oracle Identity Analytics, a resource is an instance of a resource *type*, which is a grouping of like resources. For example, multiple Oracle® database instances may make up a resource type named Oracle, whereas each database instance is a resource. Common resource types include platforms (Windows 2000, UNIX®, Mainframe) or business applications (such as, billing and accounts payable applications). Each resource has an owner who handles the various operations on the resource, such as reviewing user entitlements.
Application	In the Identity Warehouse, an application is a view across multiple resource types and resources.
Business Structure	A *business structure* is defined as a department or sub-department within an organization. An organization can be segregated into as many business structures, with as many levels of hierarchy as is required to represent teams and sub-teams within the organization.
Roles	A *role* represents a job function. Roles contain policies that describe the access that individuals have on a directory. Roles represent unique job functions performed by users in

	the domain. For example, a person can function as a manager, a developer, and a trainer. In this case, there are three roles that represent each job function because each requires different privileges and access to different *resources.* A role can be embedded inside a role as a nested role. Role hierarchies can be defined to any level required in an organization.
Policies	*Policies* define account attributes and privileges that users have on different platforms or applications. A policy has a specific privilege on a specific data resource. Policies are assigned to roles, and roles are assigned to users. Policies provide consistent directory permissions and user rights across and within the organization for all of the users in a role.
Orphan accounts	An *orphan account* is an account that belongs to a user who is no longer with the organization or controlling business unit. (The user may have left the organization or shifted departments, but the account was not deactivated when the user left or moved).
Glossary	The glossary contains user-friendly terms for cryptic entitlements.
Data owner	Data owners are the owners or stewards of an attribute value. They are responsible for the users who have access to high-privileged information.
Data Classification	Data classification is a business-level categorization of user entitlement data that can be used to create SoD rules. For example, Accounts Receivable and Accounts Payable are two classifications that have a set of entitlements within them. SoD rules can check data classification levels and prevent users from receiving both Accounts Receivable and Accounts Payable entitlements.
Accounts	An account is an entitlement or permission that enables a user to access a particular resource type.

3. The Lego Approach: Building the Identity Warehouse

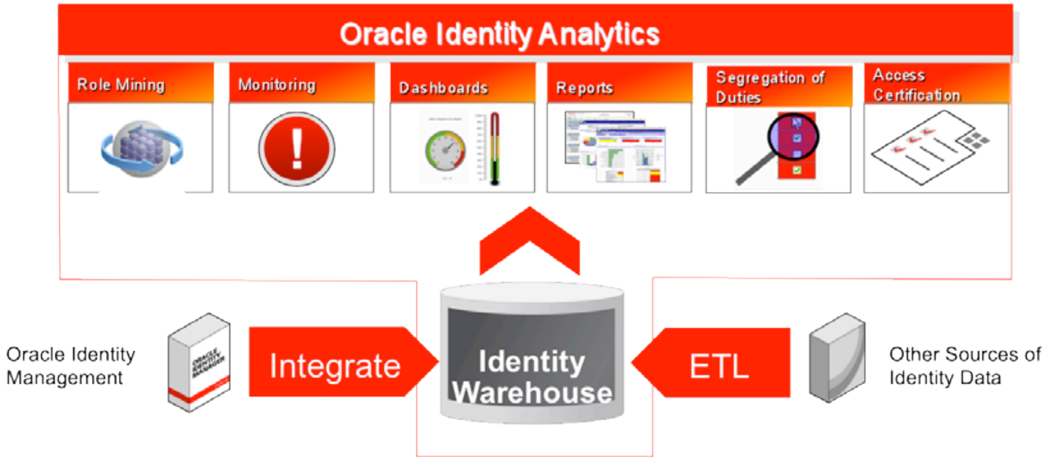


Figure 1.1: Components of Oracle Identity Analytics

As illustrated in figure 1.1, building the Identity Warehouse is the first step in working with Oracle Identity Analytics. The other modules (identity certification, identity audit, and role modeling and maintenance) are functional once the Identity Warehouse is populated.

This is a recommended step-by-step approach to building the Identity Warehouse:

1. **Import users:** Importing users is the preliminary step to seeding the warehouse. Ensure that you import the user set from an authoritative source and create a process for importing users on a nightly basis. Oracle Identity Analytics updates the changes and provides the most up-to-date view.

2. **Import user entitlements:** Importing user entitlements is the second step to building the Identity Warehouse. Oracle Identity Analytics supports the import of complex entitlements to display granular metadata information. This information can be leveraged during the certification process.
    a. **Perform data correlation:** Associating users with entitlements is a crucial step. If this step is not performed with caution, it can result in orphan accounts or users with no entitlements. Oracle Identity Analytics has the ability to support advance correlation rules as well.
    b. **Correlate Orphan accounts:** Importing user entitlements often results in orphan accounts. This is an opportunity for the owner of an asset or application to take one of the following actions:
        i. Assign the account to the user, a process called Claim-ID.
        ii. Deactivate these accounts and ensure that they no longer exist.

3. **Create business structures:** Business structures are logical groupings of users. They can reflect the current organizational structure and hierarchy. Business structures must be assigned to managers, who will be in charge of reviewing user access.
    a. **Create business structure rules:** A business structure rule directly assigns users to business structures based on a specified condition. Defining these rules will ensure that your business structures are also updated every time a new feed is imported.

4. **Import glossary:** Import the glossary, which explains cryptic entitlements to business managers in user-friendly terms. This information is vital for user managers when they are certifying user access.

5. **Build applications:** After the entitlements are imported, analyze the date and prioritize the entitlements. Create an application that groups users based on important entitlements. An application view can be across various resources and resource types. Drill down to the most granular level, if required.

6. **Manage Identity data:** Apart from storing data, the Identity Warehouse also enables data management. This is an essential aspect of maintaining the Warehouse. Make sure you do the following:
    a. Assign an owner: Assign owners to critical attribute values.
    b. Classify data: Label attribute values based on criteria critical to your organization. For example, data features can be classified as high risk, medium risk, or low risk.
    c. Identify high-privileged data.

4. Features of the Identity Warehouse

Once the Identity Warehouse has been built, customers can immediately start realizing some of the following benefits, including:

Feature	Benefit
Capturing user data	The identity warehouse captures comprehensive HR data for all users. This data can be leveraged during certification, role modeling, or identity audit.
Application view	Essential during the certification process, application view allows managers to sort and review access information based on applications.
Assigning data owner	Certifications can be launched based on data owners or attributes.
Creating data classification	Data classification can be used to define Segregation of Duties policies in an organization. This can be leveraged in the Identity Audit module.
Business Structures	All operations in Oracle Identity Analytics, such as identity auditing and identity certification, are performed on the basis of a business structure.
Roles view	Roles view provides a consolidated view of the roles created in the organization, including role history and version. This view also allows for the creation of ad-hoc roles, if required.
Policy view	Policy view provides a consolidated view of policies, including owners, history, version, and so on.
Glossary	Glossary view helps user managers understand what various entitlements mean. This enables them to make better decisions during the certification process.

Business Structure – User Rules	Business structure rules help keep business structures up-to-date based on changes in the user’s attributes. For example, if a user’s department is changed, this change is reflected in the Identity Warehouse as well.
Orphan account clean-up	The orphan accounts view captures important security-related information about users who have access, but who no longer exist or no longer need the access. This view provides an easy way to deactivate access or assign it to the right users.
Assigning account types to accounts	When importing accounts into the Warehouse, account types can also be imported. For example, account types such as provisioning accounts, system accounts, service accounts, test accounts, development accounts, and so on can be imported. This setting helps during the integration process with Identity Manager.
User view	The User view is the most important view in the Identity Warehouse. It provides a single view of all users and entitlements with n-level of hierarchies displayed across the enterprise.
Capturing the ‘nth’ level of hierarchy	Oracle Identity Analytics can capture entitlements at the most granular hierarchy level. These granular attributes can be viewed in the warehouse, certified, and evaluated during SoD or audit scans.
Out-of-the-box import process	Oracle Identity Analytics accepts CSV and XML files to import users, accounts, roles, policies, business structures, and glossaries. The simplicity of the import process is a huge benefit when onboarding a new application or target system.

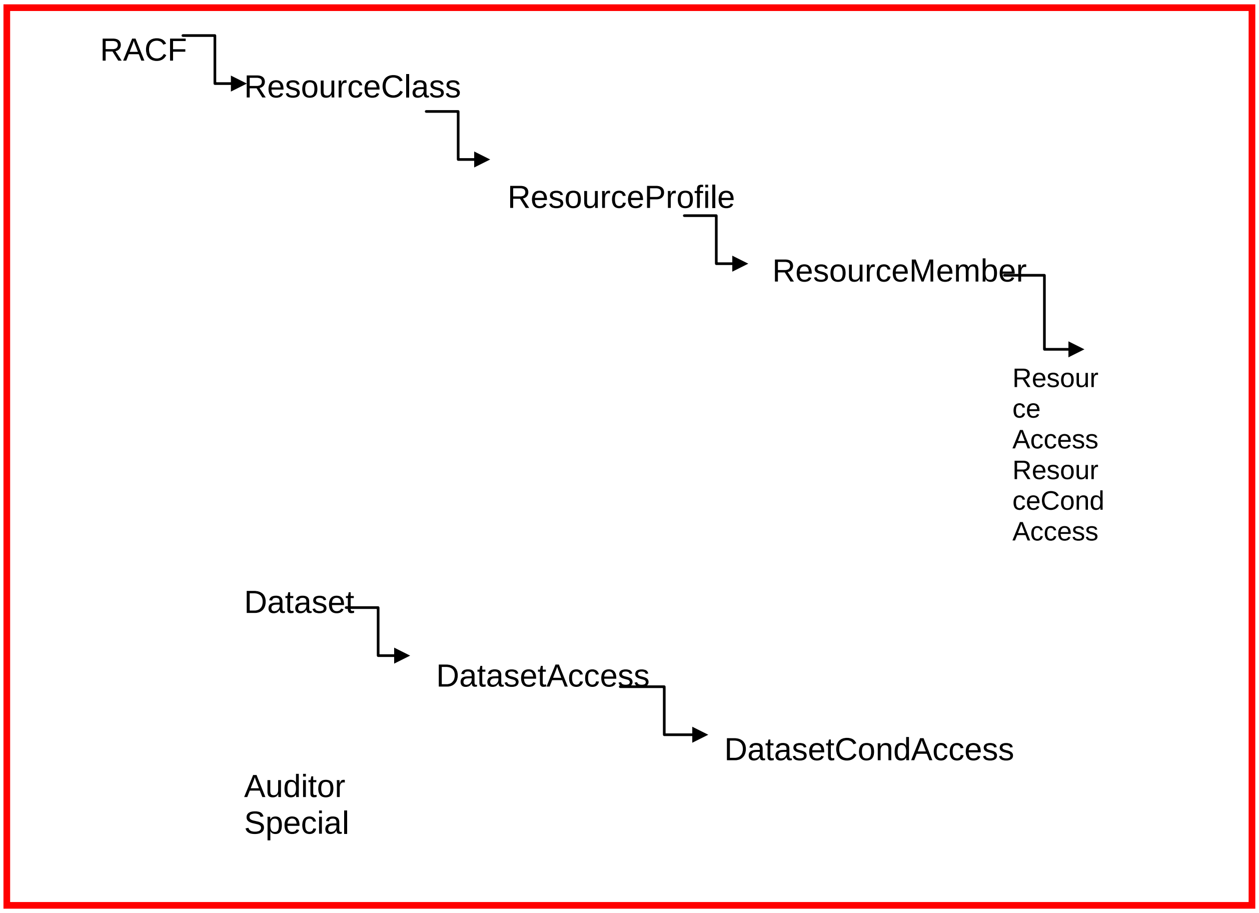
5. The Data Import Process

The import process is central to populating the Identity Warehouse. Application owners are involved in the process of importing the necessary elements to ensure that data is represented accurately in the user interface. Flexible import process schedules can be created to suit the requirements of your organization.
In Oracle Identity Analytics, you can import the following elements:

1. Users
2. Accounts
3. Roles
4. Policies
5. Business structures
6. Glossary items
7. Resource metadata
8. Resources

Resources and attributes are created when importing accounts that contain complex user entitlements. Oracle Identity Analytics can import CSV flat files or XML files. Flat files require a schema for the import process. XML files are recommended for accounts with multi-value attributes or n-level hierarchies.

For example, a mainframe system such as RACF has the following structure. This application can be imported using an XML file. As Oracle Identity Analytics can capture the nth level of hierarchy, entitlements can be imported down to the ‘ResourceAccess’ and ‘ResourceCondAccess’ level.



Maintaining the Warehouse is as important as building it. Flexible import schedules, regular imports of data, and constant validation will ensure that only current information is displayed. Providing a current view of users and their entitlements in your organization is the most important function of the Identity Warehouse.

Conclusion

To summarize, we introduced the problem most enterprises face today with providing a centralized view of their Identity & Access Management information, and then laid the foundation for the concepts behind a “recommended” Identity Warehouse and the “lego approach” to building a warehouse. We also talked about the benefits of a Warehouse, such as such as providing a centralized view of user entitlements across the enterprise, orphan account cleanup, modeling applications views with correlations to the users accessing them, business structure correlations to the users residing within these structures, capturing the nth level of entitlement hierarchies, providing a 360 degree view of user entitlement data via business glossaries, data owners, data classification and so on. Finally, the importance of maintaining the various components of the Identity Warehouse was also discussed.

Oracle Identity Analytics, Oracle’s comprehensive role management and identity compliance solution, is the technology that addresses the challenge of providing an enterprise-wide view of all users and their access to various target systems. The Oracle Identity Analytics Identity Warehouse is the central repository that contains all the important entitlement data for your organization.

The Identity Warehouse: Best Practices
January 2010
Author: Neil Gandhi
Contributing Authors: Viresh Garg

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com