An Oracle White Paper
January 2014

Oracle Identity Manager – Business Overview

ORACLE

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.

Executive Overview

With the explosive growth in networked communications and ever increasing collaboration and mobile computing needs, today's enterprises struggle to determine which users have access to what resources and what they are doing with that access. A comprehensive awareness of access and enforcing governance controls is essential to reduce the risk that an employee, contractor, or malicious third party with inappropriately assigned access will take advantage of that access. It is also critical to comply with regulations that mandate access controls; without it companies have no way to provide meaningful evidence to auditors that explains how and why access was assigned within their environment.

For many enterprises, enforcing all such governance controls has been an ongoing challenge that is increasingly difficult to master. Business users are getting more involved in driving the whole governance initiative, like requesting access or delegated administration activities, which once was considered to be an IT function. A simplified and more business user-friendly experience that is easily customizable becomes critical for the overall success of an enterprise's governance initiatives. In addition to this, in the past enterprises were also challenged by the lack of a unified governance suite offered by a single vendor. Provisioning, Privileged Access management, Role management and Compliance products evolved independent of each other that led to customers implementing multiple products from multiple vendors as point solutions to address these needs. As regulatory and provisioning requirements continue to grow and change, such multi-vendor solutions only increased the complexity and costs of managing and integrating these products. As a result, enterprises are in an inevitable position of having to rely heavily on each of these vendors for support and also committing significant resources to governance efforts for integration and manual processes with little assurance that they will prove successful. Recent research also has made it evident that organizations can save up to 48% in overall costs deploying a single vendor platform solution when compared to deploying multi-vendor point solutions.

Introduction

Oracle Identity Governance Suite enables organizations to simplify access grants and review access by consolidating the key strengths of its industry leading and best-in-class provisioning (Oracle Identity Manager), newly released privileged access (Oracle Privileged Access Manager), role, policy and risk management (Oracle Identity Analytics) into a common, consistent and unified governance suite. With a single, converged platform, Oracle Identity Governance suite can provide benefits like:

- Increased end-user productivity - consistent and intuitive user interfaces, common business glossary, immediate access to key applications, role lifecycle management

- Reduced risk - guaranteed access revocation, detect and manage orphaned accounts, proactive and reactive IT audit policies detection and enforcement, fine grained authorization controlling who can do what, periodic re-certifications, continuous policy and role based access re-evaluation

- Increased operational efficiency - risk based identity certification reducing overall time to certify, automated repeatable user administration tasks, role consolidation, ease of deployment

- Reduced total cost - single vendor platform for governance, flexible and simplified customization framework, easily attest to regulatory requirements, common connector, standards based technology.

This overall unified solution is depicted in Figure 1.

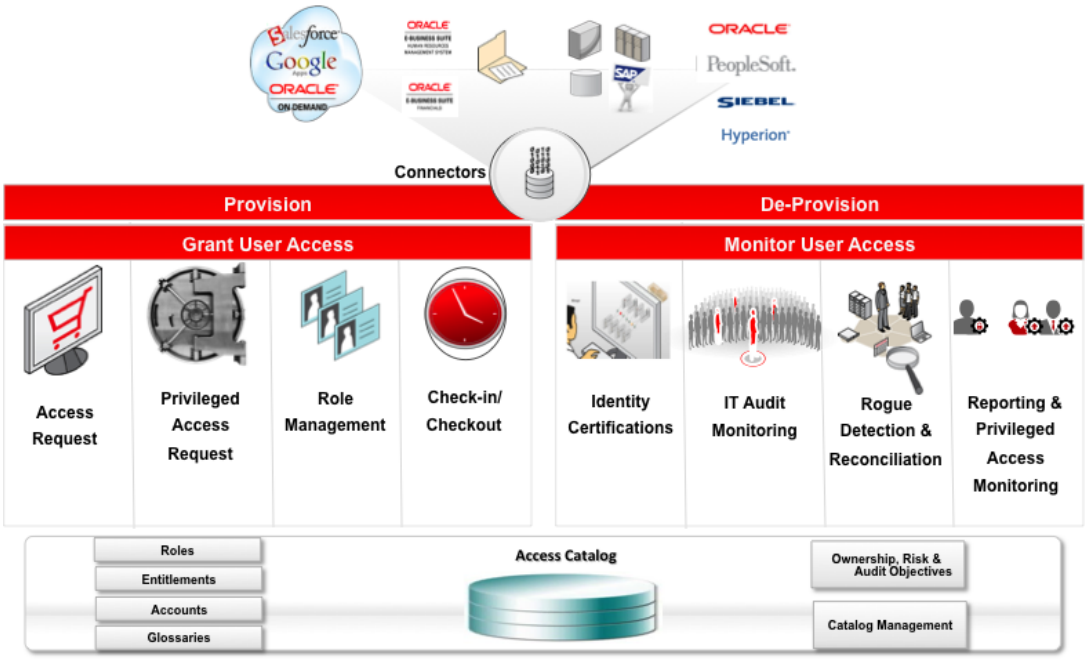

Figure 1: Oracle Identity Governance Suite – Core Solution Components

This whitepaper focuses on detailing the key features of Oracle Identity Manager providing an insight into its flexible, secure and scalable architecture to address every enterprise identity management need.

Oracle Identity Manager (OIM) automates the administration of user access privileges across a company's resources, throughout the entire identity management life cycle—from initial on-boarding to final de-provisioning of an identity. OIM helps to answer critical compliance questions like "who has access to what resources and when? How did users get access to resources and why?" and enables access re-certifications at periodic intervals.

Figure 2: Oracle Identity Manager 11g Overview

Figure 2 depicts the overall functions of Oracle Identity Manager. Its flexible architecture can orchestrate complex IT and business processes without requiring invasive changes to application infrastructure, policies or procedures. This hallmark flexibility is derived from the product's architecture, which distills core identity administration and provisioning functions into discrete layers. Changes to workflow, policy, data flow, or integration technology are isolated within the respective functional layers, minimizing impact to applications. In addition, Oracle Identity Manager is flexible because all configurations are done via its web interface, while also providing a powerful extensibility framework that allows the interface and its behavior to be tailored to the needs of the business. Its wide range of business-user friendly self-service functions that include a "shopping cart" like experience, allows business users to easily manage profiles and access using a personalize-able and extensible user interface.

Oracle Identity Manager can be used both in enterprise-centric (intranet) environments, and customer/partner-centric (extranet) environments. In extranet environments, Oracle Identity Manager's superior scalability allows enterprises to manage millions of the company's resources. In this case, customers/partners that need access, OIM provides centralized on-boarding and a combined self-registration interface to multiple enterprise applications, improving a company's operational efficiency and the ability to address increasing compliance and privacy regulations through centralized management of external users and partners.

These are some of the many reasons why OIM is considered the most advanced enterprise identity management solution available. For more details on Oracle Identity Manager, please visit www.oracle.com/identity.

Key Features

Simplified Self Service

OIM offers a wide range of self-service functions enabling business users to register for an account, manage their own profiles and credentials. These self-service capabilities easily pay for it many times over through reduced help desk calls and administrative costs.

Self Registration

OIM provides a configurable interface where end users (typically in an extranet environment) can submit a request for an account for themselves in the enterprise. A configurable workflow allows such requests to be approved before actually granting and notifying the account details to the user.

Profile Management

Using OIM's self-service interface, users can easily manage their own mutable profile data like changing their email ID, postal address, telephone number, emergency contact info, their password recovery questions and answers or set up a proxy/delegate user to act on their behalf for a specified time period.

Password Management

OIM's self-service interface enables users to manage their enterprise password that is used in single sign-on (SSO). OIM then synchronizes this password across all target resources provisioned to the user. OIM enforces compliance of this password with enterprise password policies, which may be authored in OIM itself. For the recovery of forgotten passwords, OIM employs the security challenge questions set during the user's first login or captured during self-registration. OIM also provides random password generation capabilities that may be invoked during registration or administrator-based password reset. The randomly generated password is compliant with password policies and may be sent to the user using various notification mechanisms including email, text message, or other means. Additionally, OIM's password management features are integrated with all login and password related flows in Oracle Access Manager (OAM) and Oracle Adaptive Access Manager (OAAM). Integration with OAAM includes password recovery mechanism using knowledge-based authentication (KBA) or one time password (OTP) based challenge questions and responses. The integration serves as a platform for advanced user and administrator authentication for scenarios requiring stronger authentication.

Request Catalog

OIM provides a centralized catalog of access rights, including enterprise and application roles, application accounts, and entitlements.

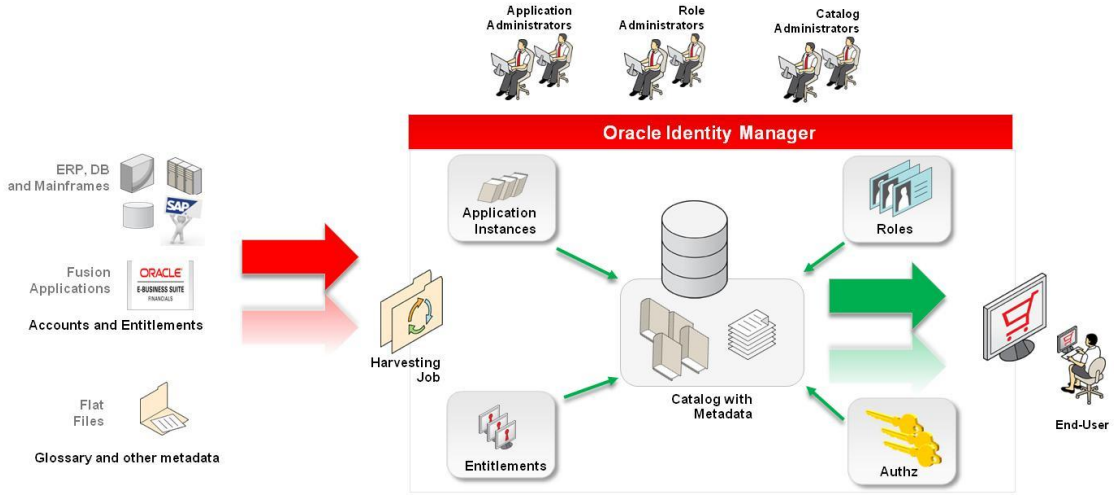

Figure 3: Oracle Identity Manager - Request Catalog

As shown in Figure 3, OIM automatically harvests privileges into the request catalog when new definitions of entitlements are detected in a target application or when the roles are defined or modified using the role administration features built in the product. Catalog administrators then enrich the harvested data to make it friendly for the business users. In particular, for each role and entitlement in the catalog, administrators can author business friendly descriptions, list the audit objectives, and set a risk level. While the catalog management system automatically populates a set of search tags based on names and descriptions of the catalog entities, catalog administrators can also seed keyword tags by which business users can find the roles and entitlements in various search results. Additionally, administrators can provide metadata for the catalog items. For example, they can specify the users or roles that will be involved in approval, certification or manual provisioning fulfillment activities related to the corresponding roles, accounts or entitlements. Once configured, catalog information is available across the identity governance processes including request creation, request tracking, approval, request history, manual provisioning, and certification.

Self-Service Access Request

OIM provides a browser-based tool to request access. The access request experience is similar to the "shopping cart" metaphor used on commercial websites, so users are able to request access without training on the tool and with only a basic understanding the organization's roles and entitlements. End users simply search for the roles and entitlements they require by entering keywords. They can further refine and filter search results by using the tool's automated suggestions. Users can also view detailed information about a particular entitlement granted to users. Once users find the entitlements they need, they simply place the appropriate entitlements in a cart and submit the request. OIM enables customers to create multiple views of the request catalog, like catalog by location, by department, or a hierarchical catalog showing all applications along with associated entitlements etc, tailored to their needs

OIM also supports delegated access request, meaning a user may request access on behalf of another person. A request can be as simple as a self-service request for access to a single application or as complex as multiple requested entities—including roles, accounts and entitlements—for multiple beneficiaries and can also include additional request information for each of the item requested.

OIM enables users to save their cart for future submission or bundle frequently requested privileges (called request profiles in OIM) that can be shared across other users. For example, managers who need to submit multiple, similar requests for their direct reports on an ongoing basis can save a request cart for the first request, and use the saved request profile to submit subsequent requests for other employees that require the same access (e.g., bank branch manager creates a "teller" cart).

Tracking a Request

Users and helpdesk administrators can track the progress of their requests online through OIM's tracking tool. The tracking tool graphically displays the current state of the request approval in the provisioning workflow. An image displays what steps are complete and what steps remain to fulfill the request. Using this tool, users can then help ensure their requests are handled in a timely fashion.

Handling Requests – Complex Workflows

OIM allows approvers to take various actions on an access request without significant difficulty. In addition to approving or denying the request, the approver may delegate the approval step to another person or role. As approvals may get critical in the overall user productivity, the system also supports configurable approval reminders and escalations. The approver may change the requested access information before approval. The approver may also upload various documents as attachments as part of the approval step. Approvers also have the capability to approve or reject directly from their email without needing to log in to the self-service interface. Once the request is approved, OIM initiates the provisioning actions. Some of the provisioning actions may be automated if a provisioning connector is deployed for the specific target system and others may be completed manually. In the case of a manual fulfillment, an administrator will be assigned a provisioning task, make the appropriate changes in the target system, and then mark the task "completed" in OIM. As approval needs can change over the period of time, policy owners can change the approval routing logic using a web interface.

Extensible User Interface

While OIM out of the box includes a complete self-service access request capability that is business user friendly, organizations may want to customize the tool to cater to their organization specific user interface standards and principles.

Global Customizations

OIM supports customizations that range from simple branding/logo/style-sheet changes to changing the layout of the page or changing the labels of various widgets on the page. Some of the advanced customizations may involve extending the out-of-box definition of various entities like users, roles, organizations, catalog entities by defining additional attributes on them and deciding various UI pages where the new attributes should appear. The new attributes may be added to search criteria, search results, various forms and other UI screens. The system also provides a sandbox environment to

perform, test, commit or rollback all such customizations without impacting other users. Once the customizations are made final, they can then be easily moved from one environment to the other.

Personalization

OIM provides a powerful personalization framework as part of its business user interface. When using OIM, each user sees a home page with multiple regions for the most commonly used features and information. Business users can personalize the layout of the home page by rearranging or hiding regions. Additionally, some of the non-technical users like helpdesk administrators or delegated administrators may perform the same query over and over again on various entities. Rather than entering the query criteria again and again, users can save their searches and reuse them across sessions. Business end users can also personalize how various UI widgets are rendered to them, for example, they can decide which columns they want to see in the tables, set sort preferences and they can also personalize how much real estate should be given to each column in the table. The system remembers any changes a user makes to the view, stores the changes, and applies these preferences at the user's next login.

Durability of UI Customizations

UI customizations in OIM can be performed by drag-and-drop editing in a web browser, without any complex programming or proprietary scripting. The UI customizations are stored in a specialized and reserved namespace in OIM's metadata repository to ensure that they are durable and that they survive patching and upgrades. After patching and upgrades, customers are not required to reapply their customizations which eliminating merge and testing cycles making it easier for customers to keep their deployments current.

Advanced Identity, Role and Application Administration

Users' access rights are managed in OIM throughout the identity lifecycle. When new users are on-boarded, they receive a set of accounts and entitlements based on any applicable "birthright provisioning" policies. Account and entitlement assignments may change as users' identity attributes change in the enterprise as a result of promotions, transfers, or other organizational changes. OIM automatically provisions these changes in the target systems. Users may also get additional access by requesting roles, accounts, or entitlements using OIM's self-service capabilities. When a user's employment is terminated, OIM ensures that all of their accounts are disabled or de-provisioned, according to enterprise policies configured in OIM. Automatic assignment and provisioning of accounts and entitlements increases employee productivity by eliminating long manual cycles typically required to provision accounts manually. Similarly, automatic de-provisioning of accounts and entitlements ensures compliance to key regulatory requirements by ensuring that terminated employees are not able to access key corporate applications after termination.

OIM Data Warehouse

The core of OIM is its centralized identity warehouse. The identity warehouse contains three key types of data:

Identities: Users' identities may be created based on authoritative systems or directly in OIM using self-service or delegated administration features. OIM can create user accounts and reconcile attributes and access based on data from any number of authoritative systems such as Oracle E-Business HRMS, PeopleSoft HRMS etc. OIM ships with a default set of attributes for user profiles, but customers can change the composition of user profiles by adding, modifying, or removing the default attributes. User identities are stored in OIM's database, but OIM can synchronize the database with any number of LDAP directories. Many customers synchronize the identities created in OIM into an LDAP to setup an enterprise LDAP that may be wired to various authentication and authorization systems that may need access to user's identity attributes.

Accounts: OIM reconciles users' account attributes and provisioned entitlements from various target systems, and stores any associated account information with users' profiles.

Access Catalog: Catalog data includes all the entitlement and role definitions with their associated keywords and metadata to support catalog searches and access requests. Entitlements metadata can also include detailed information on what an entitlement maps to in a target system. For example, e-Business role or responsibility (entitlement) can have additional metadata on which set of menu/button privileges would be granted to a user in e-Business.

Advanced Delegated Administration

OIM employs a sophisticated delegated administration system that uses logical organizations to control the visibility of data to the delegated administrators. User membership to these logical organizations can be static or dynamic (rule driven). Logical organizations control the scope of the delegated administration functions of a user in an organizational hierarchy and ensure that only users can view and manage other users and entities they are authorized to view and manage.

All managed entities including roles, entitlements, application or target instances are published to a set of logical organizations and are only available for request by the users of that organization. Such a secure delineation of entities is mandatory if an enterprise wants to limit what each user can see and request.

In a typical extranet deployment, an enterprise can define delegated administrators for say Suppliers, Partners and Customer organizations that can perform different sets of operations. In OIM, each of these can be modeled as logical organizations and each one can have a set of delegated administrators who can perform specific operations on the entities that belong to that organization. For example, a user in the Supplier organization can be delegated as a User administrator and Role administrator which would enable the user to perform all User and Role management functions but within the boundaries of the Supplier organization. At any instance, the system ensures that a supplier delegated administrator or a supplier user will never see users or data belonging to say Partner organization unless they have view privileges on the Partner organization. Such a flexible delegated administration enables customers to address the ever-growing need for fine grained access controls for delegated administration functions.

Role Administration

Enterprise roles evolve over time and so require a robust administration and audit process. OIM can also provide advanced role management capabilities. Upon detection of new roles, OIM can require administrative review and approval of associated entitlement updates. The solution also can perform real-time impact analysis for role consolidation before changes are applied in a live environment. The integration also supports versioning, which creates an offline copy of a role without disturbing the "live" version, and provides capabilities to revert to any previous version of a role. This improves the overall organizational flexibility by making it easy to change access based on business needs and also improves the alignment between IT and business organizations. This role lifecycle management features full audits all changes made to role definitions including role assignment rules and entitlement mapping policies.

Accelerated Application On-boarding

There may be systems in an enterprise that may not provide integration libraries and hence may require an administrator to manually provision access to users. Even for systems that do provide integration libraries, enterprises may prefer to perform manual provisioning and later move onto a completely automated and connected model. OIM provides a web based interface that enables business administrators to easily onboard such systems within a matter of minutes without writing any code or relying on developers. Once the provisioning is done, the target system administrators can flag the manual provisioning task as complete in OIM. As and when needed, such disconnected systems can then be easily converted to a connected provisioning solution using any of the above-mentioned connectors.

Application Integration / Service-Oriented Security

OIM supports easy integration and can be consumed as a service. OIM enables Oracle Fusion Middleware, Fusion Applications, and custom applications to externalize their identity administration services through an XSD profile or an SPML web service. Additionally, OIM supports integration with LDAP repositories for managing users, roles, and role assignments. Applications can therefore use the SPML web service to achieve LDAP integration. OIM also provides a range of identity services. For example, applications can use OIM's web services to generate a username or a random password for the user, or reserve a username in LDAP while user registration is going through approval. Applications that are pre-integrated with OIM's web services benefit from the innovation in OIM on day 1. Additionally, Fusion Middleware and Fusion Applications customers looking for enterprise provisioning solutions face a much shorter and smoother learning curve, given that they are already well versed with provisioning technology powering their applications.

OIM also provides simplified identity administration for all Oracle Applications Unlimited products including Oracle E-Business Suite, PeopleSoft, Siebel and JD Edwards products. These applications typically are deployed in an identity ecosystem involving SSO solutions, LDAP directories, GRC IT Audit Policy application, and one or more internal user repositories. For example, Oracle E-Business Suite is usually deployed with Oracle SSO, Oracle Internet Directory, Oracle Application Access Controls Governor, and FND, TCA, HRMS store. OIM abstracts the identity administration challenges of managing user accounts and entitlements in such a deployment by providing provisioning

orchestration across the entire ecosystem. Customer's total cost of ownership associated with securing their Applications Unlimited products is greatly reduced.

Connectors

OIM's Connector Framework eliminates the complexity associated with creating and maintaining connections to proprietary interfaces in business applications. The connector framework separates connector code (integration libraries specific and optimized for the target system) from connector meta-data (data models, forms, connectivity information and process). This separation makes extending, maintaining, and upgrading connectors a manageable and straightforward process. This also enables custom logic to be more easily pluggable through custom extensions that can hinder upgrading to improved versions of the connector code.

OIM provides the following integration technologies for the connector development:

Adapter Factory®: The Adapter Factory enables customers to create new integrations or modify existing integrations using a graphical user interface, without programming or scripting. Once connectors have been created, their definitions are maintained within the OIM repository, creating self-documenting views. These views make extending, maintaining and upgrading connectors a manageable and straightforward process.

Generic Technology Connector: The Generic Technology Connector framework provides a complimentary solution for data flows to applications that accept file formats. It is a framework with basic building blocks that allows system administrators to design custom connectors quickly and easily. Generic Technology Connector can communicate with any target resource by using standard protocols such as HTTP, SMTP, FTP, and Web Services combined with generic message formats such as CSV, SPML, and LDIF.

Identity Connector Framework: The Identity Connector Framework (ICF) separates connector code (integration libraries specific and optimized for the target system) from connector meta-data (data models, forms, connectivity information and process). The framework provides many common features that developers would otherwise need to implement on their own. For example, the framework can provide connection pooling, buffering, timeouts, and filtering. An ICF connector need not always be deployed in the application consuming it. It can potentially be deployed on another box/platform. ICF provides Connector Servers which enables remote execution of the Identity Connector. Connector servers are available for both Java and .NET. An ICF compliant converged connector is a connector that can be commonly used for both Oracle Identity Manager and Oracle Waveset.

For the most popular commercial applications and interface technologies, OIM offers an extensive and rapidly expanding library of pre-configured connectors for on-premise and cloud applications. With these connectors, an enterprise can get a head start on application integration. Each connector supports a wide range of identity management functions and uses the most appropriate integration technology recommended for the target resource, whether it's proprietary or based on open standards. These connectors enable out-of-the-box integration, but can be enhanced to work with each enterprise's unique integration requirements. To name a few, OIM provides out-of-the-box feature rich connectors for cloud applications like Google Apps, business applications like Oracle Fusion Applications, Oracle E-Business, PeopleSoft, JD Edwards, Siebel and SAP, LDAP directories

like Oracle Internet Directory, Oracle DSEE, Oracle Unified Directory, Active Directory and e-Directory, Security systems like RACF, Top Secret and ACF2, operating systems like Unix, AS/400 and Windows, ticketing systems like BMC Remedy. It also provides generic LDAP and Database connectors that can be easily integrated with COTS or in-house built applications.

Comprehensive Audit and Compliance Management

Identity Certifications

As the number of applications to which employees have access increases, certifying access becomes imperative, especially for larger enterprise organizations. In order to efficiently scale and sustain, these processes need to be both automated and resilient. With advanced, risk-based analytics and easy to navigate dashboards, Oracle Identity Governance offers a robust set of identity certification features that streamline the review and approval processes to effectively manage risk on an ongoing basis. Beyond understanding "who has access to what", in depth analytics can provide detailed metatdata about entitlements during certification, graphical and actionable business context, as well as 360-degree views on how such access was granted and highlights outliers for individuals versus their roles. In addition, Identity Certifications promote business user friendliness via innovative capabilities such as the ability for reviewers to complete certifications offline. In addition, workflow capabilities that allow both Business and IT teams to collaborate on a single Identity Certification campaign are also included. Finally, the solution offers closed loop remediation, which provides an automated way for reviewers to revoke improper access across target systems and includes alerts should remediation fail.

Account Reconciliation

Account reconciliation is a key control objective for regulatory compliance, as it allows administrators to detect changes in access privileges originating outside the identity management system. These account changes are potentially rogue activities, and therefore trigger various remediation activities through OIM including exception approvals, certification cycles, and de-provisioning of entitlements or disabling accounts.

Accounts are linked to users' identities based on the correlation rules defined in OIM. If the correlation rules are unable to link an account to an existing identity, administrators can map accounts manually. Typically this happens for some of the older accounts that were created before a strict user ID generation policy was in place. After manual linking there may still be accounts that may not be linkable to any user identities. These accounts are typically either recognized as specialized privileged or service accounts or orphaned accounts. Accounts may become orphaned because they were created at a given point of time for some special purpose and may not be required anymore. Orphaned accounts can be de-provisioned directly from OIM. The process of automatic and manual linking, identifying accounts, and remediating orphaned accounts is typically part of data cleansing that is done as first phase of on-boarding a new application with OIM. But periodic reconciliation can also help with detecting any orphaned accounts created.

Rogue/Orphan Account Management

A rogue account is an account created "out of process" or outside of the provisioning system's control. An orphan account is an operational account without a valid user. These accounts represent serious

security risks to an enterprise. Oracle Identity Manager can provide continuous monitoring of rogue and orphan accounts. By combining denial access policies, workflows and reconciliation, an enterprise can execute the requisite corrective actions when such accounts are discovered, in accordance with security and governance policies. With a seamless integration with Oracle Privileged Access Management, Oracle Identity Manager can also manage the lifecycle of special service accounts, also known as administrator accounts, which have special life cycle requirements that extend beyond the lifecycle of an assigned user and across the lifecycles of multiple assigned users. Proper management of service accounts can help to eliminate another source of potential orphan accounts.

IT Audit Policy Enforcement

As the engine controlling the assignment of entitlements to users, Oracle Identity Manager has to ensure that users get assigned those privileges that they should, and don't end up in a situation where they can commit fraud. Increasingly, access to these critical business applications is being governed through IT Audit policies.

IT Audit Policy can be broadly defined as a way of preventing a user from acquiring a set of entitlements that are not in conformance with applicable business policies. This set of entitlements, also referred as "toxic" combination in some literature, could allow a user to potentially perform fraudulent or undesirable activities by circumventing certain commonly established checks and controls (e.g., generate and approve payment to themselves). IT Audit Policy checks thus ensure that a single individual is not given enough authority to perpetrate a fraud on his/her own.

Enterprises thus need Oracle Identity Manager's provisioning actions to be IT Audit Policy compliant. OIM achieves this compliance through a pre-provisioning, real-time validation with the IT Audit policy engine managing the Audit policies for the relevant application. This is done through an integration framework that allows the business to plug Oracle Identity Manager into leading IT Audit policy engines such as Oracle Application Access Controls Governor and SAP GRC Access Controls.

Reporting and Auditing

Oracle Identity Manager reports on both the history and the current state of the provisioning environment. The system captures all necessary data to answer the question "Who has access to What, When, How, and Why?" Some of the identity data captured includes user identity profile history, user group membership history, user resource access and fine-grained entitlement history. When combined with the transaction data generated and captured by OIM's workflow, policy, and reconciliation engines, an enterprise has all the required data to address any identity and access related audit inquiry. Oracle Identity Manager's reporting and auditing capabilities enable an enterprise to cost effectively cope with ever increasingly stringent regulatory requirements, such as Sarbanes-Oxley, 21 CFR Part 11, Gramm-Leach-Bliley, HIPAA, and HSPD-12.

Diagnostics

Oracle Identity Manager introduces a new operational console in Oracle Enterprise Manager that enables administrators to get a complete view of all the defined OIM operations, out-of-the-box and customer defined event handlers, child processes, workflow processes their state and error information without requiring to mine different server logs. This tool does not replace the larger IDM management

pack in Enterprise Manager that provides a suite wide monitoring capability but serves as a useful diagnostic tool specifically for OIM.

Conclusion

Oracle Identity Manager is the most flexible and scalable enterprise identity administration and user provisioning application available on the market. With its innovative and advanced feature set, OIM helps an enterprise to reduce security risk, reduce the cost of compliance, and greatly improve service level and end-user experience. Its flexibility to integrate with Oracle and 3rd party applications and being a part of the Oracle Identity Governance Suite makes it an ideal choice to start or compliment an existing identity management deployment as an enterprise advances to reach its identity and access governance goals.

Oracle Identity Manager – Business Overview
January 2014

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

Oracle is committed to developing practices and products that help protect the environment

Hardware and Software, Engineered to Work Together