Oracle Access Manager

An Oracle White Paper

NOTE:

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.

INTRODUCTION

As the internet has become the primary medium for disseminating information, companies and government agencies are increasingly faced with the challenge of opening their IT infrastructure to grant customers and partners access to resources such as product support data. These organizations also need to regulate employee access to various corporate data, keeping track of who has access to what. Leading organizations increasingly rely on identity management solutions to increase regulatory compliance, cut operational costs and improve application security and usability. A strong identity management strategy requires integrated technology for managing user lifecycles, securely storing and administering user profile data, and controlling application access based on these profiles.

Oracle Access Manager is the only policy-based access management solution that not only provides heterogeneous platform support but is also pre-integrated with Oracle Fusion Applications and Middleware.

Oracle Access Manager is deployed at many of the largest companies in the Global 1000, and powers many of the most heavily trafficked portals in the world. Companies rely on Oracle Access Manager to bring security, administrative control, user self-service, delegated administration and increased visibility to portals, extranets and intranets deployed on multiple vendor products and platforms. This paper describes the main components and functions of Oracle Access Manager such as Identity Administration, Authentication, Authorization, and Auditing, which provide end-to-end security infrastructure to heterogeneous applications.

ORACLE ACCESS MANAGER OVERVIEW

Oracle Access Manager is the only product in the market that couples a strong access management system with a best-in-class identity administration system.

Oracle Access Manager is Oracle Identity Management's solution for web access management and user identity administration. Oracle Access Manager is designed to support complex, heterogeneous enterprise environments. As a key component of Oracle Fusion Middleware, it ensures ready support for Oracle's current and future ERP, CRM and Collaboration suite applications.

Oracle Access Manager consists of the Access System, and the Identity System. The Access System secures applications by providing centralized authentication, authorization and auditing to enable single sign-on and secure access control across enterprise resources. The Identity System manages information about individuals, groups and organizations. It enables delegated administration of users, as well as self-registration interfaces with approval workflows. These systems integrate seamlessly and may be deployed together or individually.

The backend repository for the Access Manager is an LDAP-based directory service that can be a combination of a multiple directory servers, which is leveraged for two main purposes:

- As the store for policy, configuration and workflow related data, which is used and managed by the Access and Identity Systems
- As the identity store, containing the user, group and organization data that is managed through the Identity System and is used by the Access System to evaluate access policies.

ACCESS MANAGEMENT

Oracle Access Manager's Access System provides centralized authentication, authorization, and auditing to enable single sign-on and secure access across enterprise resources such as web and J2EE resources(JSP,servlets, EJBs, etc.) and legacy systems. The Access System is an extensible solution that can be leveraged to protect any kind of resources through policies. Legacy or custom applications can leverage its broad set of APIs to externalize authentication, authorization and auditing from their applications, and be able to enforce centrally managed access policies in their distributed applications or system.

Authentication

The Access system provides a centralized means to authenticate users and systems attempting to access resources protected by Oracle Access Manager. The Access system supports the following authentication methods:

- Basic username/password
- X.509 Certificates
- Smart Cards
- Two factor tokens
- Form-based
- Custom authentications via Authentication APIs

Oracle Access Manager provides centralized policy-based authentication, authorization and auditing services to Web and J2EE resources.

The Access System allows customers to define policies that determine hierarchies of authentication levels, which can be used in conjunction to meet business requirements. For instance, customers may protect an employee portal system with username and password, but for the more sensitive HR self-service application that deal with sensitive data, users may be require to authenticate using an RSA SecurID token, thus providing a higher level of security to more sensitive resources or applications.

Additionally, the policy-based authentication model allows customers to define authentication flows or steps, which allow handling of various user types or backend authentication repositories, for example, a flow may require username and password and try to authenticate the user against an LDAP directory using these

credentials, however, if this authentication fails, the Access System may try to authenticate against a Windows domain. And this flow is transparent to the end user. The authentication flexibility allow customers to seamlessly migrate and integrate various backend authentication systems, without exposing this complexity to their end users.

Access Manager provides an authentication API for integrating a variety of authentication methods and devices. Support for smart cards such as SecurID is included out of the box. With the authentication API, customers can extend Access Manager to support nearly any form of authentication including biometrics and two-factor authentication.

Once a user is authenticated, the Access system creates a single sign-on session for the user that prevents the user from having to sign-on again to access other resources within that policy domain.

Authorization

By default, The Access system provides centralized policy-based authorization services to secure access to web and J2EE resources. Authorization is governed by a policy domain that includes an authorization expression among a set of default rules that specify how resources for this domain are protected. Administrators work with the Policy Manager console – a browser-based administrative system - to define policies that restrict access to specific resources by user, role, group membership (static, nested or dynamic), time of the day, day of the week and IP address.

In addition, the Access System provides an Authorization API can be used to build custom authorization plug-ins to allow incorporating custom authorization logic into the access management policies, which can extend the available range of authorization options available out-of-the-box. In many cases, the authorization plug-ins are leveraged to incorporate existing authorization logic or systems that customers want to either continue using or migrate from while deploying the Access System.

Centralized authorization greatly reduces development costs by allowing developers to focus on the application business logic, not on enforcing security policies.

Auditing

The Auditing services provide detailed and flexible logging, of events monitored by Oracle Access Manager. These events include authentication success or failure as well as authorization success or failure. The audit trail may include configurable identity information from the actor (i.e. end user) as well as contextual information (i.e. time of day, originating IP address, host identifier for the web server or web server farm, etc.)

The Access Manager provides a policy-based auditing model where administrators can define a default or "blanket" auditing policy that applies to all monitored events, but exceptions to this policy can be configure at a more granular level, such as by application, or even by resources (i.e. URLs or J2EE resources), as needed. This allows administrators to also manage the amount of auditing information needed according to the sensitivity or the importance of the particular application or resource. For example, the default policy may only capture the user's login name in addition to the operation and resource, whereas for the HR self-service application, the auditing policy would also include the employee number and cost center, along with the IP address where the user accessed the application and which specific web server identifier handled the transaction.

The auditing process enable administrators to perform threat and intrusion detection, security monitoring, and business-level reporting by integrating with third-party products. Audit logs can be written either to a flat file or to a Database (Oracle RDBMS 10g, SQL Server), and can be then harvested by any 3rd party reporting tool such as Oracle Reports or Business Objects to produce comprehensive auditing reports, such as authentication failures in a given period or for a given application, access history per user, authorization failures per user or per application, and so forth.

ACCESS SYSTEM COMPONENTS

The Access system includes the WebGate or web server client, the AccessGate or API-based client, Access Server, and the Policy Manager. The backend store for both policy and configuration data as well as identity data is an LDAP-based directory server. The functionalities of each of these components are described below.

In the Access System: WebGates and AccessGates are Policy Enforcement Points or PEPs, te Access Server is the Policy Decision Point or PDP and the Policy Manager is the Policy Management Authority.

WebGate

WebGate is an out-of-the-box access client for enforcing access policy on HTTP-based resources, hence it is the Access System's web Policy Enforcement Point or PEP. The WebGate client runs as a plugin or module on top of most popular web servers, and intercepts HTTP requests for web resources and forwards them to the Access Server where access control policies are applied. WebGates are optimized to work on web server environments, as are streamlined for the HTTP protocol, and understand URLs, session cookies, HTTP redirects, secure sessions (HTTPS); and also implement policy caches that improve WebGate's performance and allow for scalability in highly trafficked sites.

AccessGate

The AccessGate is the term used for any other Access System client that is not a WebGate, so it is the Access System's non-web PEP. Typically it is the implementation of a client using the Access API. AccessGates are leveraged to build the J2EE application server and portal connectors that are available within

the Access System, which include BEA WebLogic, IBM WebSphere, and Oracle OC4J. In addition, customers can implement their own Access System clients and develop enforcement points to their custom applications or systems.

Access Server

Access Manager's Access Server is a standalone software server that enforces access policies on web and non-web resources, so it is the Access System's Policy Decision Point or PDP. The Access Server can be deployed in a single instance, or as part of a clustered implementation to support load balancing and failover. Load-balancing and failover of the Access Server is built in and does not require the deployment of external load-balancers. The Access Server provides dynamic policy evaluation as users access resources, as well as authentication, authorization, and auditing services. The Access System is a scalable server, which provides configurable caching of both user and policy information to significantly improve the performance of access policy evaluation.

Policy Manager and Access System Console

Access Manager's Policy Manager is a browser-based graphical tool for configuring resources to be protected and well as creating and managing access policies, so it is the Access System's Policy Management Authority or PMA The Policy Manager provides the login interface for the Access System, communicates with the directory server to manage policy data, and communicates with the Access Server over the Oracle Access Protocol to update the Access Server cache when policies are modified. A screen shot of the policy administration interface of the Policy Manager is shown in figure 1. Master Access Administrators and Delegated Access Administrators use the Policy Manager to:

- Create and manage policy domains that consist of:
  - Resource types to protect
  - Authentication, authorization, and audit rules
  - Policies (exceptions)
  - Administrative rights
- Add resources to policy domains
- Test access policy enforcement

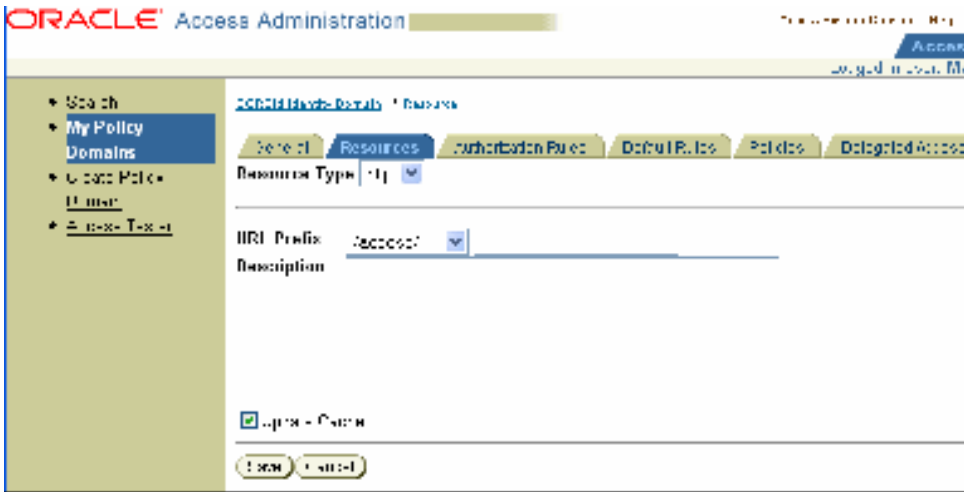

Figure 1. Policy and resource definition using Policy Manager

The Policy Manager provides web-based central console for policy administration. The Access System Console is a web-based administrative interface that is used for management and configuration of the Access System components.

The Access System console enables administrators to manage and administer the Access System. The administrators can add, change and remove Access Clients and Access Servers, configure authentication and authorization schemes, configure master audit settings, and configure host identifiers, revoke specific users', manage shared secret keys used for encryption, monitor the status of the system, and also define new type of resources that will be protected by a policy managed through the Policy Manager. The Access System Console is shown in figure 2.

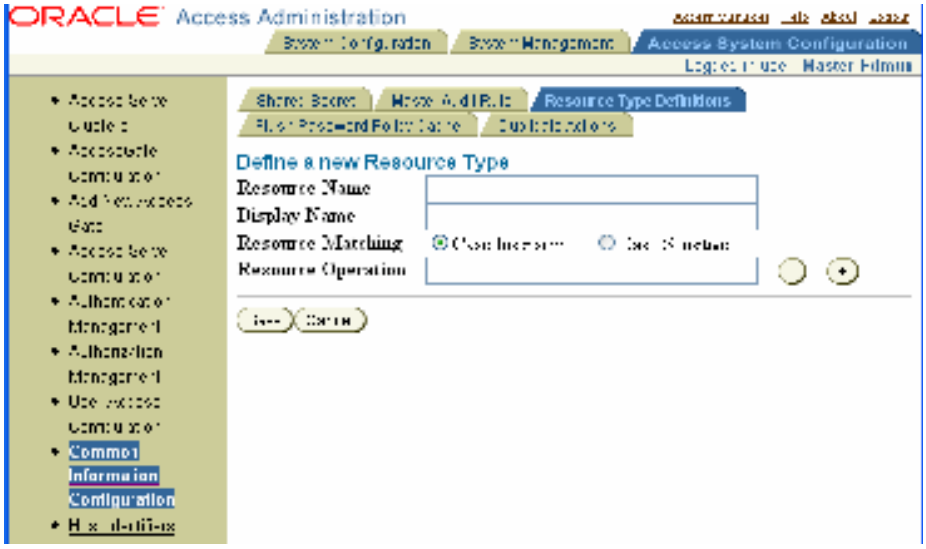

Figure 2. System Administration using the Access System Console

ACCESS SYSTEM ARCHITECTURE

An overview of the Access System architecture is depicted in figure 1. It illustrates the Access System deployed with 3 main components – WebGate, Access Server and the Policy Manager, as well as the backend Directory Server which is used as both the policy store and the identity repository. The Oracle Access Protocol (formerly known as the NetPoint or COREid Access Protocol) enables secure communication between Access System components during user authentication and authorization.

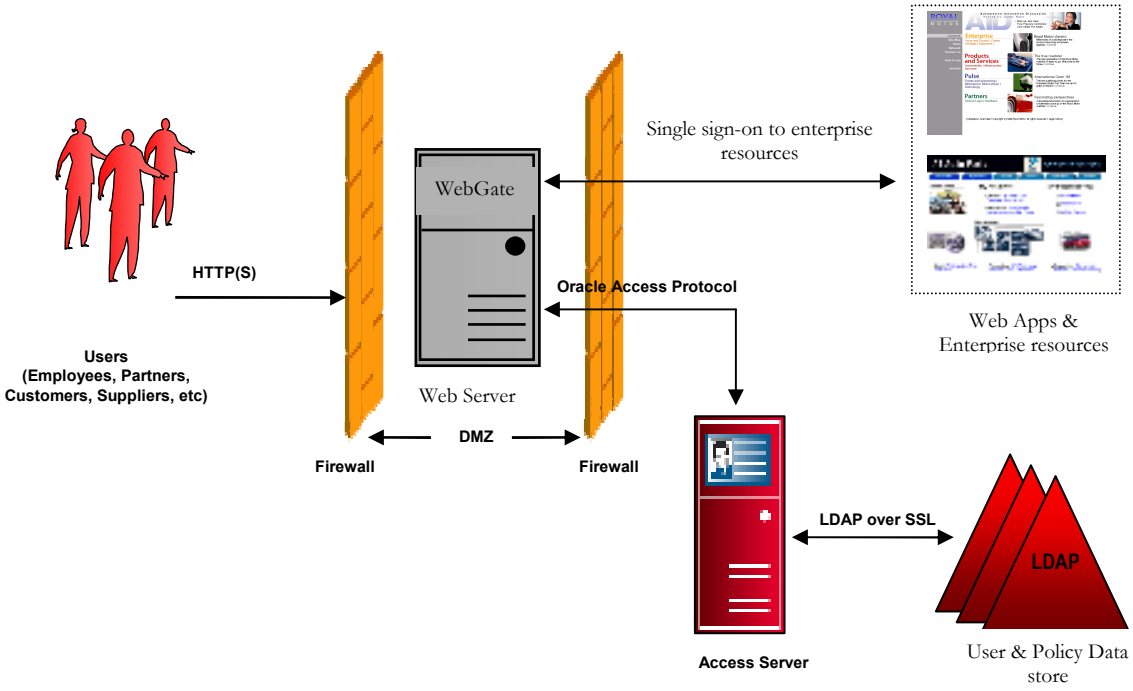

Figure 3. Access System architecture overview

When a user tries to access a protected enterprise resource, the WebGate and the Access Server execute the following sequence of steps.

1. The WebGate, which is typically deployed in the DMZ, intercepts the user request and checks with the Access Server whether the resource being accessed is protected
2. If the resource is protected, the WebGate challenges the user for credentials and forwards those credentials to the Access Server for validation
3. The Access Server validates the submitted user credentials against the backend directory server

4. The result of this validation is sent back to the WebGate. If the authentication is successful, the WebGate sets a cookie in the user's browser and checks with the Access Server whether the user has permissions to access the protected resource.
5. The Access Server fetches the policies from the directory and evaluates whether the user has access to the protected resource. The result is sent back to the WebGate.
6. If the user is authorized, he gets access to the secured resource.

IDENTITY ADMINISTRATION

Access Manager's Identity System delivers key identity administration functionality to administrators and end users, necessary for the effective administration of access control. In practice, the Identity System becomes the identity administration entity for the identities whose access is controlled by access policies managed by the Access System. This synergy of access management and identity administration is a unique differentiator for Oracle Access Manager.

The components of the Identity System include the Identity Server, and WebPass web server plug-in. The Identity Server is a stand-alone server that manages identity information about users, groups, organizations, and other objects, as well as providing a workflow engine specialized in identity management flows. The WebPass plug-in passes information between a web server and one or more Identity Server instances. This architecture provides a high degree of scalability, allowing more Identity Servers to be deployed as required by administrative demands.

Efficient, cost effective administration of portal environments requires administrative support for features such as delegated administration, dynamic group management, and user self-service and self-registration. Access Manager's Identity System provides these functionalities as a customizable, out-of-the-box console, as portal inserts embedded in a portal application, or as a custom interfaces integrated through web services. These Access Manager Identity System functionalities are described below.

Delegated Administration

Oracle Access Manager's Identity System delivers delegated administration, essential for managing large user populations.

When a portal deployment supports thousands or millions of users, it becomes a challenge for a centralized administration team to manage the constant changes to user profiles. Delegated administration makes efficient administration of such environments possible by "pushing" the responsibility for managing various user populations to group administrators. For example, if a manufacturer operates a supplier portal for a thousand suppliers, the manufacturer might delegate responsibility for user management in each supplier firm to a designated set of administrators at each supplier. The result is distributed work, more accurate data, and administrative scalability.

Oracle Access Manager provides the most flexible and scalable delegated administration functionality in the market today, proven in production in many of the largest portals in the world.

Oracle Access Manager includes powerful and flexible authorization features such as dynamic groups and attribute-level access control.

Dynamic Group Management

A very useful and common identity management need is the ability to assign users to groups, for better access control and administrative simplification. Groups are one of the most commonly used representations of roles, and are well understood by most mainstream applications, such as portals, application servers and collaboration and messaging systems.

Groups can be implemented staticly, where users are explicitly added to the group as members, or dynamicly, where the group is defined by a rule or filter that is evaluated at run time to determine who is a member. In real deployments, assigning large numbers of users to static groups does not scale well and typically impose challenges for administrators who have to manually manage groups of thousands of individual members. A better approach is to use dynamic groups based on user attributes. The following example serves to illustrate the value of dynamic groups.

In a wireless phone company's customer portal with millions of users, a dynamic group might be called "SMS users" containing all customers who currently have SMS messaging activated for their accounts. Users in this group would be automatically granted access to additional support web pages. Since customers may continually activate and deactivate SMS messaging, it would be impractical to assign users to this group manually, and in addition the potentially large amount of data that the group represents, can pose challenges for the backend directory, not only in terms of storage size, but also in terms of replication and integrity bookkeeping. In this case, an approach based on dynamic groups, leveraging the Access Manager's group management functionality can be used to assign and de-assign users to the "SMS users" group automatically based on profile attributes. The group is defined during setup with the appropriate filter in place; the group itself does not require large storage space and rarely changes. As a customer activates SMS messages in her account, a flag would be activated in her directory profile, and Access Manager would instantly include this customer in the group.

User Self-Service/Self-Registration

Allowing users to manage their own profiles also enhances administrative scalability. Oracle Access Manager's out-of-the-box self registration screens enable users to add themselves to a directory without administrative intervention. Self-registration can use Access Manager's workflow capability to ensure that controls and processes are enforced as users add their profiles. It also allows users to change their attributes, within the access levels granted. For example, some users may be allowed to update their own phone numbers but not their titles. Managers of these employees may change titles but not their department, and so on. Access

Manager supports unlimited access control flexibility for user attributes, and also links workflow to these changes. The result is increased user power and flexibility, all under the desired level of administrative control.

Lost Password Management

Lost password management enables users to reset their passwords if they forget them. When lost password management is enabled, a link appears on the Identity System login page or another page configured by the administrator. Selecting the link routes the users to a Web page where they must respond to one or more pre-configured, and personalized challenge questions. After providing the correct response, the user can set a new password online in real time. Thus allowing the user to go back and continue interacting with the system or application he/she intended to

To enable lost password management, the directory administrator defines a set attribute pairs named, for example, Challenge X and Response X (where X represents that the could be multiple pairs). From the Identity System Console, an administrator assigns the Challenge and Response semantic types to these attributes as well as configures the number of challenge questions to be presented randomly to the user at run time (typically a subset of the total configured). The Administrator can choose to prepropulate these value pairs during user creation, or require that users themselves enter these values during self-registration for instance. In many case, the list of allowed questions could be pre-defined so that end users can only choose from the pre-defined list of questions.. The Identity System encrypts these values using a strong encryption scheme licensed from RSA.

IDENTITY SYSTEM COMPONENTS

The Identity system includes the WebPass client, Identity Server, and the Policy Manager's Identity System Console. The functionalities of each of these components are described below.

WebPass

The WebPass is the presentation tier of the Identity System, it provides both an HTML interface to browser, and a SOAP-based Web Service interface to provide identity administration functionality in a SOA environment

A WebPass is a web server plug-in that passes information back and forth between the web server and the Identity Server over the Oracle Identity Protocol (formerly Netpoint or COREid Identity Protocol). Hence, WebPass is the presentation tier of the Identity System. By default, WebPass renders its content as HTML so that it can be accessed through a browser. But in addition, it provides a Web Service interface, known as IdentityXML, which SOAP-based clients can leverage to programmatically interact with the Identity System. The idea behind IdentityXML is that it allows the integration of business logic governing identity administration process to be available and easily integrated with existing applications in a SOA environment.

Identity Server

The Identity Server manages identity information about users, groups, organizations, and other objects. The Identity Server performs three main functions:

- Reads and writes to your LDAP directory server across a network connection
- Stores user information on a directory server and keeps the directory current
- Processes all requests related to user, group, and organization identification

To provide these functions, the Identity Server implements a very granular attribute-level access control functionality, that allows it to both define and enforce access rules to identity information at an attribute value level. This is one of the most distinctive strengths of the Identity System, in that this allows it to meet complex delegation, privacy and self-service business requirements. In addition, the Identity System provides a patent-protected workflow engine, which specializes on identity administration functions, such as creation, self-registration, request/approval changes, deactivation and deletion of identity information.

The Identity Server's workflow engine also provides an API, which allows it to invoke custom login on an event driven basis. This API supports bi-direction flow of information, such that data that is being managed by the Identity Server can be used in evaluating custom logic or additional data can be injected for the Identity Server to use in downstream steps in the workflow. A common use case is during self-registration, an end user may enter a customer ID number in the initial steps, and a custom plug-in built using the Event API validates that the customer ID is valid so the user can be allowed to register, in addition, during the validation process, the custom plugin can retrieve the user's mailing address, which can be injected to the workflow so that the user can verify it in the next step of the workflow.

The Identity Administration console of the Oracle Access Manager includes user self-service, delegated administration, personalization and audit capabilities.

Identity System Console

The Identity System Console provides web-based configuration and management of the Identity System components (WebPass and Identity Server) and the User Manager, Group Manager and Organization Manager applications of the Identity system.

IDENTITY SYSTEM ARCHITECTURE

The Identity System consists of 3 main components – WebPass, the Identity server and the Identity System Console.

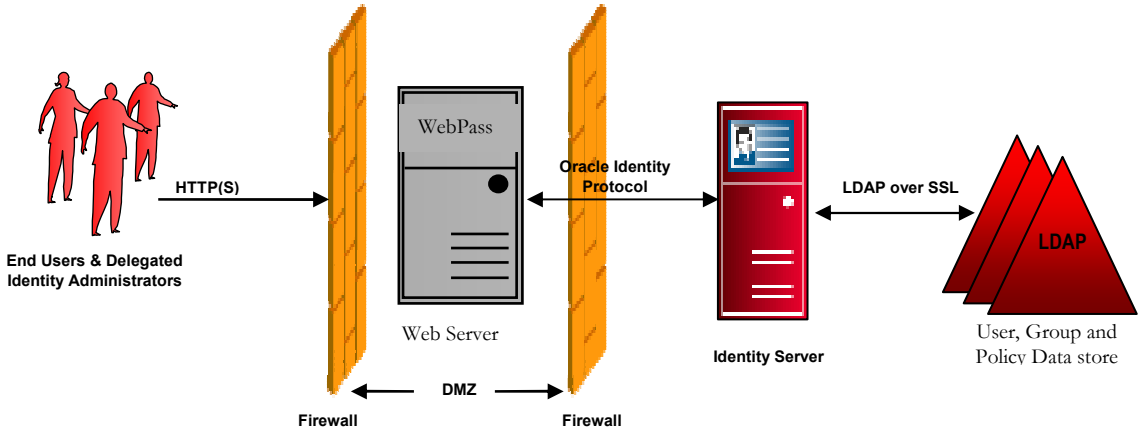

Figure 4. Identity System architecture overview

Figure 2 illustrates the basic Identity System components in a simple environment, as well as transport security between components over the Oracle Identity Protocol (formerly known as the NetPoint or COREid Identity Protocol). The end users and Administrators are typically separated from components by a Firewall. The web server with WebPass installed resides in the DMZ. The Identity Server and directory server reside behind the second firewall. The Oracle Identity Protocol facilitates communication between the Identity Server and the associated WebPass instances.

AUDITING

Oracle Access Manager can support compliance efforts by logging security and profile management activity to a centralized auditing database.

For audit reporting, Oracle Access Manager supports a reporting framework, so that all security and profile management activity can be logged to a centralized relational database, and reports can be built through any 3rd party reporting tool. Auditors now demand significant proof of compliance with regulations and internal policies, and administrators also wish to analyze security and identity operations for holes. Some of the most common audit reports include:

- Authentication statistics (success/failed rates across all Access Servers)
- Authorization statistics (success/failed rates across all Access Servers)
- Failed authorizations (by user)
- Failed authorizations (by resource)
- Access testing
- Group history (all changes to all group profiles)
- Identity history (by user)
- Locked-out users
- Password changes (in a particular interval of time)
- Users created/deactivated/reactivated/deleted

- User profile modification history (for all users)
- Deactivated users report
- Workflow execution time

HETEROGENEOUS SUPPORT

Oracle Access Manager integrates seamlessly with a number of third party web servers, application servers, directory servers and packaged applications.

Oracle Access Manager includes integration agents for managing and securing applications running on a variety of platforms. These integration components include out-of-the-box agents for leading web servers, application servers, and portal servers, running on multiple platforms. This enables customers, who have already invested in third-party technologies, to seamlessly deploy Oracle Access Manager in their environments, thereby increasing their return on investment (ROI).

Oracle Access Manager WebGate and AccessGate components plug into third party and custom infrastructure products to intercept requests and apply access policies. No other identity management vendor provides this breadth of support, covering multiple versions, products, and operating systems to protect real-world production environments.

INTEROPERABILITY WITH ORACLE SINGLE SIGN-ON

Oracle Access Manager is fully interoperable with OracleAS Single Sign-On, providing Oracle customers with single sign-on to all their enterprise applications.

Oracle Access Manager is fully interoperable with OracleAS Single Sign-On, Oracle's built-in authentication service for Oracle applications. This means that Oracle customers using Oracle Portal, Oracle Collaboration Suite, Oracle E-Business Suite Release 11*i*, or other Oracle applications can deploy Oracle Access Manager to provide a single point of access control, and user single sign-on, to all of their enterprise applications.

CONCLUSION

Oracle Access Manager is the industry's most comprehensive solution for access control and user identity administration. Access Manager's Access System provides web single sign-on for users, support for multiple authentication methods, and centralized policy evaluation and enforcement. Access Manager's Identity System provides scalable administration of identity information including delegated administration, workflow, dynamic group support and user self-service/self-registration. Together, they provide a key component of Oracle's identity management solution for the enterprise.

ORACLE FUSION MIDDLEWARE

Introduction to Oracle Access Manager

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