ORACLE

FUSION MIDDLEWARE
ACCESS MANAGEMENT

An Oracle White Paper
December 2013

Access Manager for Oracle Access Management 11gR2 PS2

Introduction

Access management is critical to any effective identity and security strategy, but the complex nature of access management continues to challenge IT departments that are struggling to balance demands for total access control with shrinking IT budgets.

Oracle recognized the need for comprehensive access management and has delivered a solution that addresses the broadest set of access management capabilities ranging from Web Single Sign-On (SSO), identity federation and a Security Token Service (STS) to mobile security, social identity and fraud prevention under a single umbrella. Oracle's truly unique access management platform provides comprehensive and Internet scale access management in a single product, with innovative new services and simplified deployment and management.

Access Manager is the service component at the foundation of Oracle Access Management that provides the core functionality of Web SSO, authentication, authorization, centralized policy administration and agent management, real-time session management and auditing. In addition to key functionality that it provides, Access Manager is extremely scalable to handle Internet scale deployments, proven with a 250-million user benchmark that provides thousands of logins per second with a single server. Multi-data-center load balancing and failover capability enables enterprises to build a 24x7 access infrastructure to support their business. Access Manager works with existing heterogeneous environments in the enterprise with agents certified on hundreds of web servers and application servers as well as applications.

Access Manager provides rich functionality, extreme scalability and high availability thereby increasing security, improving user experience and productivity and enhancing compliance while reducing total cost of ownership. This white paper provides a technical introduction to the features of Oracle Access Management. To learn more about the entire Oracle Access Management platform, please refer to the "Complete and Scalable Access" white paper.

Access Manager Overview

As enterprises deploy Web applications to meet their internal and market needs, they need an access management solution that will allow users to access those applications in a secure manner. If every application builds its own security infrastructure, it will lead to proliferation of independent security silos thereby multiplying administration points and increasing development and maintenance costs. This also introduces huge security risks due to the lack of enforcement of consistent security policies across the enterprise. Finally, it is cumbersome for end users to have to remember and enter different credentials for every application they are trying to access.

Access Manager addresses these problems by providing a single, secure point of entry where the user's identity can be verified and access to enterprise resources can be managed.

Figure 1 provides a simple overview of Access Manager, the industry-leading Web Access Management (WAM) solution. The enforcement of access policies at runtime is achieved by deployment of WebGates (also called "agents") on Web servers. These WebGates, which act as Policy Enforcement Points (PEPs), front-end protected enterprise resources. WebGates intercept site traffic and verify that the user is authenticated and authorized to access the resource. The first time the user tries to access a resource, if the user isn't yet authenticated, the WebGate redirects the user to a login page. The login page then validates the user's credentials against a user repository, such as a corporate directory service. If successfully authenticated, a session gets established on the Access Manager server and a cookie gets created in the user's browser that facilitates access for all subsequent requests in that session.

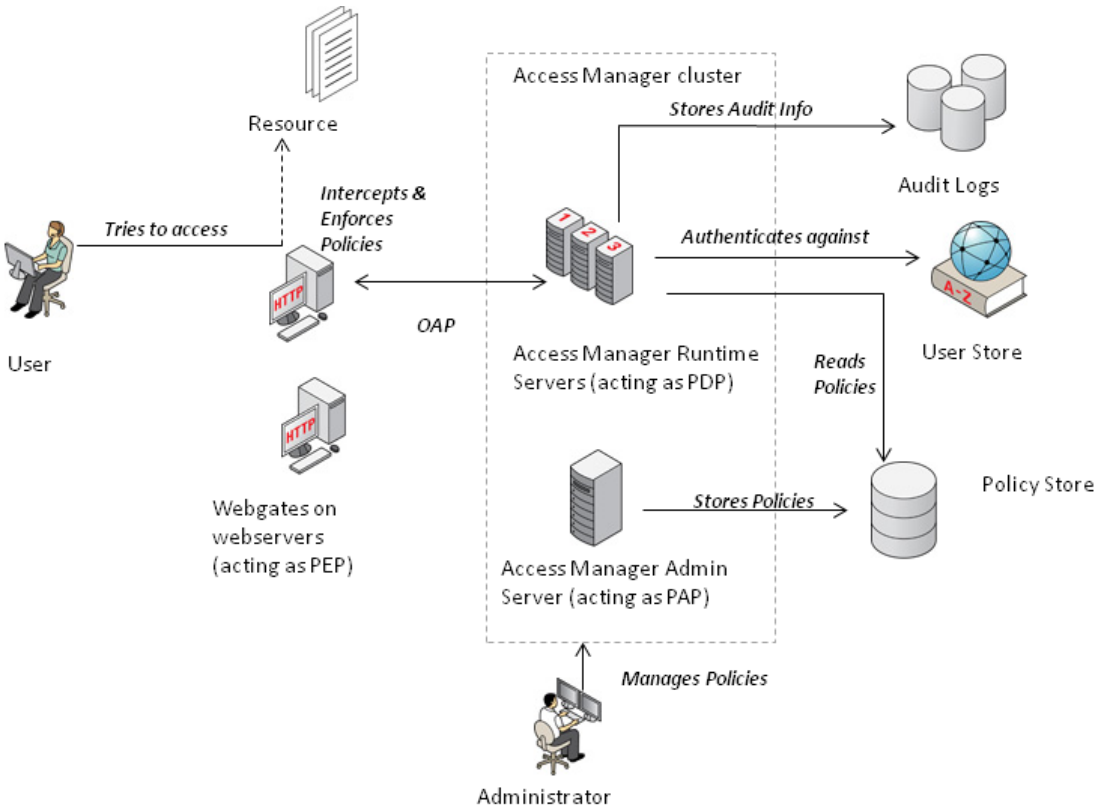

Figure 1. Web SSO using Access Manager

The WebGates communicate with the Access Manager server using the secure Oracle Access Protocol (OAP). Policies are created and maintained by administrators through the Oracle Access Management console, which acts as the central Policy Administration Point (PAP). These policies are stored in the Policy Store, using an Oracle database.

As an authenticated user tries to access different applications and resources, the runtime Access Manager server acts as Policy Decision Point (PDP) evaluating whether the user is authorized to access a particular resource. It then conveys that information back to the WebGate for enforcement. Every action gets logged for audit purposes.

Key Capabilities

This section covers key capabilities provided by Access Manager.

Simplified Web SSO

As explained in the previous section, Web SSO is a key capability that Access Manager provides. It facilitates administrators to easily create and manage access policies at a central location and then enforces these policies thorough Access Manager run-time servers and WebGates deployed across the enterprise. Access Manager thus provides a seamless SSO experience to all users while ensuring access policies are consistently applied across the enterprise. Web SSO improves user productivity and reduces security risks since users do not have to remember multiple passwords or note them down.

Authentication

Authentication is the process of proving that a user is who he or she claims to be. Authenticating a user's identity with Access Manager refers to running a pre-defined set of processes to verify the digital identity of the user. In its simplest form, authentication is the process where a user provides a username and password and the system validates these credentials against a user registry, such as a corporate directory. In real-world use, authentication can take various forms, including Windows Native Authentication using Kerberos, X.509 digital certificates, and federated tokens such as in the Security Assertion Markup Language (SAML) standard. Access Manager also supports Multi-Factor Authentication (MFA), which requires a user to provide a second factor for authentication, such as a dynamic key or PIN, before accessing a resource.

Using Access Manager, a resource or group of resources can be protected by an Authentication Policy. One or several Authentication Policies can uses a specific authentication process known as an Authentication Scheme. An Authentication Scheme helps provide a layer of abstraction for the actual authentication process. For example, one would use LDAPScheme for all resources that need to be protected by credential validation against an LDAP whereas for resources that needs user credentials to be validated using X.509 digital certificates one would use the X.509 scheme and so on. Access Manager provides a number of authentication schemes out-of-the-box, simplifying the set up for administrators.

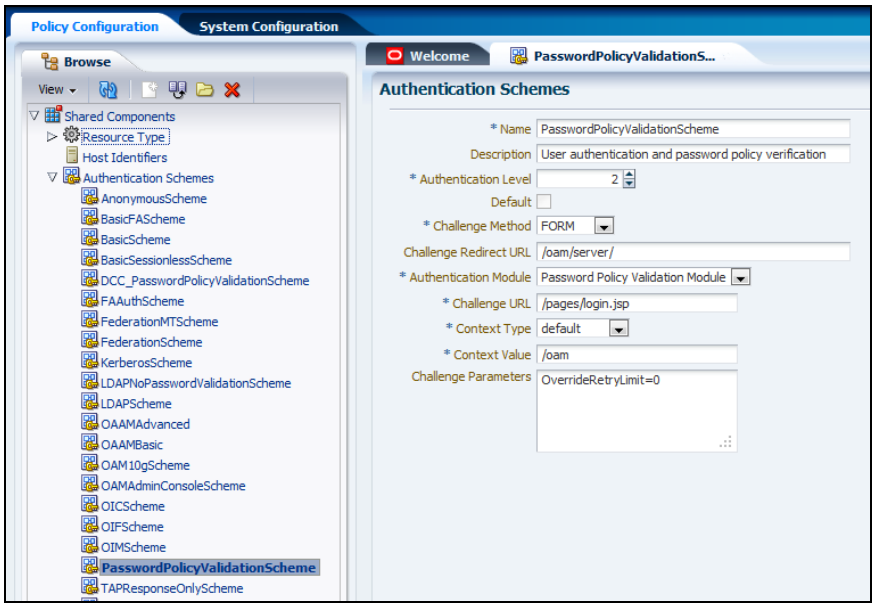

Figure 2. Interface to define an Authentication Scheme

Administrators can also define Authentication Levels against every Authentication Scheme that determines the strength of authentication needed for the group of resources protected by that scheme. More sensitive applications will be protected by schemes with higher authentication levels that will be enforced as step-up authentication during run time. For example, an enterprise may have standard authentication at Level 2 for their intranet portal but require a step-up authentication with a second factor of authentication if a user tries to access his payroll application, which may be configured at Level 4. It should be noted here, that Authentication Levels are a mechanism for administrators to define relative strengths of authentication for internal purposes and are not correlated to NIST standards for authentication levels.

Access Manager also provides a Multi-Step Authentication Framework that uses a custom authentication plug-in to transmit information between the user and the authentication scheme during the multi-step authentication flow. The multiple steps can be orchestrated in the console, with every step based on the outcome of the step before. For example, if user provides username and password and the credential validation is successful, then prompt the user for a dynamic key and so on.

Further, Access Manager also provides the ability to specify advanced pre and post-authentication rules to dynamically switch the authentication scheme or throw a second factor of authentication based on certain conditions. Figure 3 below shows how you can configure these advanced rules to challenge user for a one time PIN (OTP) if he is trying to access from outside the VPN.

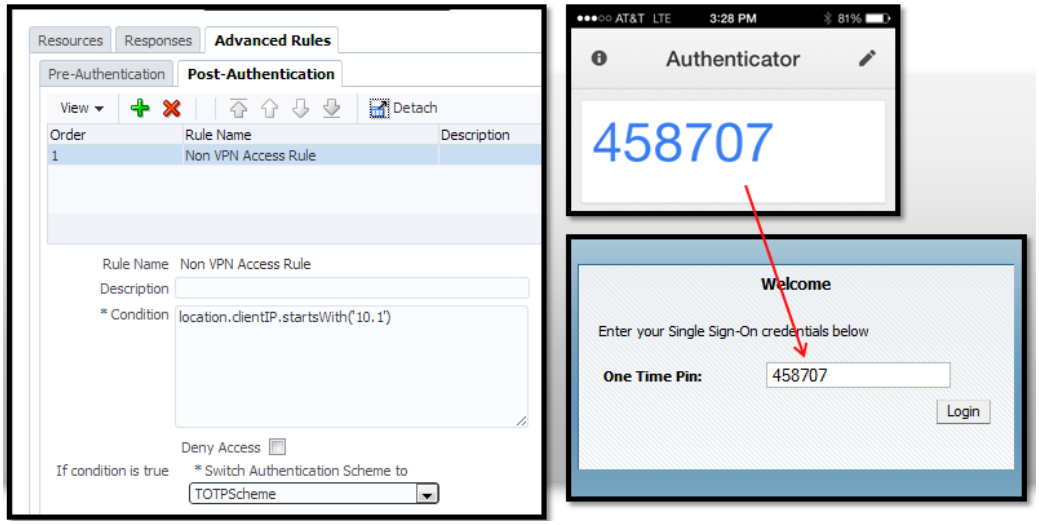

Figure 3. Advanced Rule to challenge for OTP

Finally, when used in conjunction with Oracle Adaptive Access Manager (OAAM), Authentication is integrated with platform risk analytics, which determines when additional authentication is required, based on increased levels of risk. Please refer to the OAAM white paper for more details.

For deployments that are not as sensitive to security, Administrators can choose to enable a persistent login capability to improve user experience. In this case, after the first time login the user does not have to enter credentials from that particular browser/device. This is facilitated via a persistent cookie which can be configured for a specific period of time.

Coarse Grained Authorization

After authenticating a user, Access Manager determines whether the user is authorized to access the requested resource. The conditions that need to be evaluated to determine whether a user should be allowed or denied access to a particular resource is encapsulated in an Authorization Policy. Access Manager provides coarse-grained authorization capability where access is controlled at the level of a particular web resource or URL. Each Authorization Policy has one or more conditions that need to be satisfied in order to provide the user access to the requested resource. For example, an Authorization Policy could restrict access to the HR Admin application only to users that are part of the HR Admin group in the corporate directory.

Centralized Policy Administration

Access Manager simplifies the process of creating and managing access policies through a centralized, intuitive, and easy-to-use administration console. The Oracle Access Management console provides policy administrators a rich interface to create complex policies using simple, step-by-step screens.

Figure 4 below provides an overview of the various elements in the Access Manager policy model. Resources are logically grouped together under Application Domains. Policies are created by administrators for specific resources within an Application Domain. The policy engine allows the use of a number of wildcard characters (*, ? , [ ] etc) for defining resources thereby providing administrators with a lot of flexibility. Extensive validation at the time of policy creation ensures that every resource is protected by a single Authorization policy to avoid ambiguity on policy decisions.

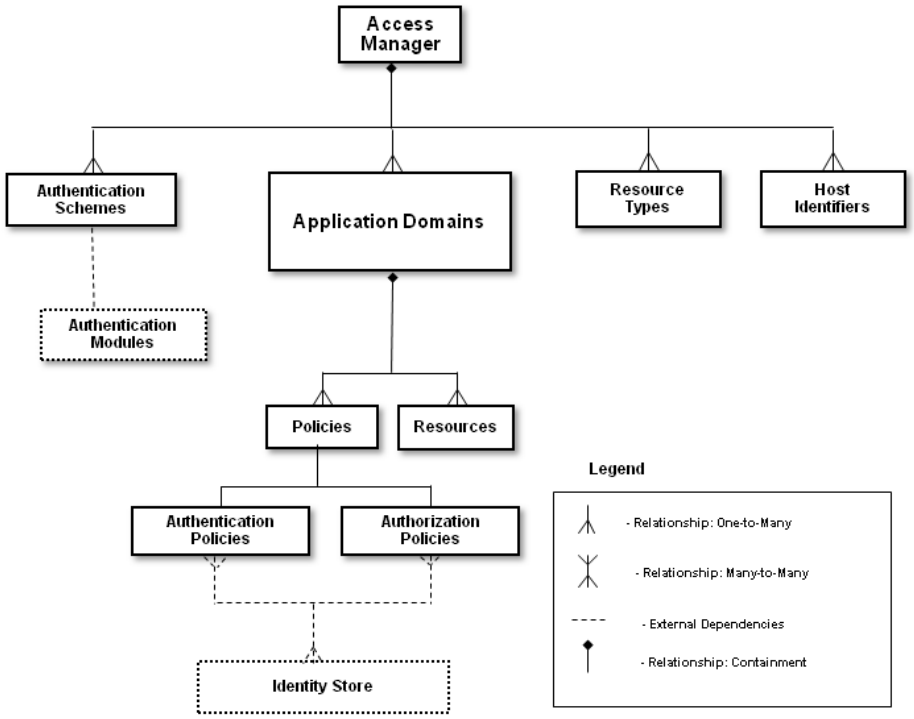

Figure 4. Policy Model for Access Manager

At runtime, when policies get picked up by the Policy Engine, by default it uses a best match algorithm to determine the order in which these policies are picked up for evaluation. This would typically suffice most use-cases. But this behavior can be optionally overridden in a given Application Domain by specifying a custom order for policy evaluation.

The policy model facilitates the creation of coarse-grained Authorization Policies based on a number of different conditions including

- Identity-based condition (if User is John Doe or User belongs to HR group in LDAP)
- Temporal condition (if current day is a weekday or current time is between 8 am and 5 pm)
- IP Range condition (if requesting user's IP address is between certain pre-defined ranges) or
- Attribute based condition, which could check the value of any User Attribute, Request Attribute or Session Attribute against a pre-defined value.

The identity-based condition even provides the flexibility of specifying an LDAP query filter (if the postal code LDAP attribute of the requesting user is so-and-so) instead of specifying a specific group name. Administrators can leverage this feature to dynamically query the LDAP repository at run-time while evaluating policies instead of pre-creating static groups as long as the resulting latency is acceptable.

Finally, an Authorization Policy can also have multiple conditions joined by operators like AND, OR, NOT, etc. to create complex expressions that will be evaluated at runtime. For example,

> Allow access if User X belongs to the HR group in the LDAP directory and value of the "hasPrivilege" session attribute is true but not if he is trying to access on a weekend

Access Manager provides a rich, flexible model to define coarse-grained authorization policies to resources or URLs. Further, if an organization needs to define more fine-grained authorization policies like a particular field in a form should be editable only for specific users or what data should be returned by a web-service based on the requesting user's privileges, Oracle Access Management 11gR2 platform includes an Oracle Entitlements Server (OES) that can be leveraged

for this purpose. Please refer to the OES white paper for more details. It should be noted that Access Manager internally leverages the same OES engine for facilitating coarse-grained authorization to resources.

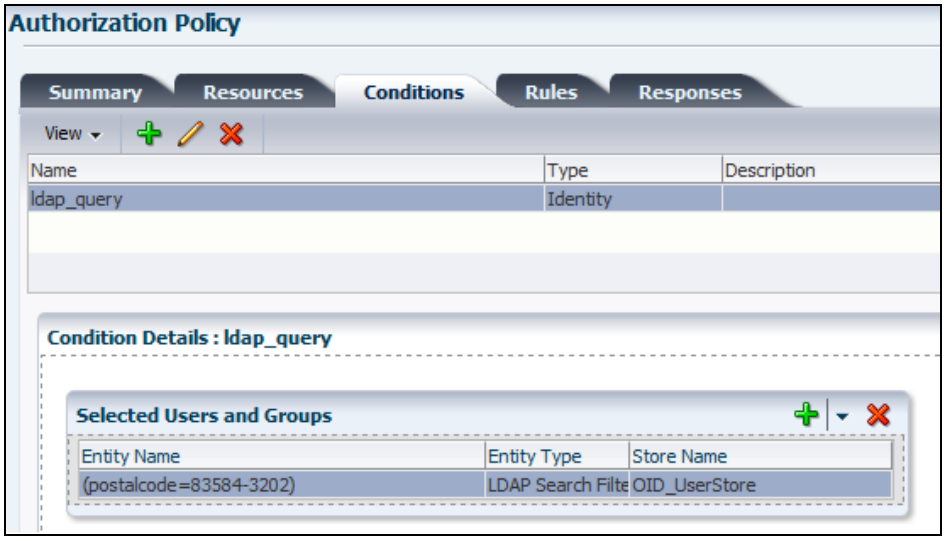

Figure 5. LDAP filter based condition for Authorization Policy

The Authorization policies centrally defined in the console are seamlessly and automatically propagated in real-time across the Access Manager distributed runtime servers within an organization's environment. This ensures that access policies are consistently applied across the enterprise at runtime and administrators have complete control on who can access what at any point of time.

Delegated Policy Administration

Though policies are centrally managed, Access Manager provides the ability to delegate the policy administration privileges for specific Application Domains to the respective business owners. These Application Domain Administrators have full privileges on their own Application Domains but cannot see other Application Domains in the console. They can also register new applications.

Advanced Session Management

Access Manager provides advanced session management capabilities giving administrators complete visibility and control over real-time distributed user session data. It allows administrators to enforce a number of constraints on user sessions including Session Lifetime, Idle Timeout and the maximum number of concurrent sessions an individual user can have. The Oracle Access Management console also allows administrators the ability to monitor all user sessions from a single point. Further, it also provides them the ability to search and terminate a specific or all sessions of a user with immediate effect. This is a powerful capability required in enterprises to lock out or de-provision a specific user immediately. Figure 6 below shows the session management interface in the console.

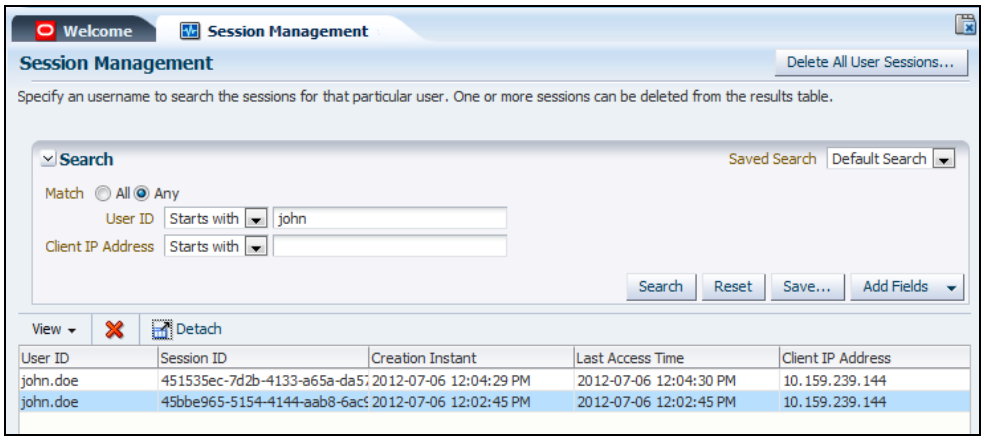

Figure 6. Session management interface in the console

Session Lifetime defines the total lifetime of a session after which it automatically expires forcing the user to re-authenticate and establish a new session. An active session becomes idle when the user does not access any protected content for the Idle Timeout period defined by the administrator. This forces the user to re-authenticate but it preserves the session attribute values. For example, an organization could define Session Lifetime as 24 hours and Idle Timeout as 15 minutes.

Further, Access Manager also allows individual Application Domains to specify an Idle Timeout that is less than the global Idle Timeout value if the applications are sensitive. For example, the global Idle Timeout may be 15 minutes but the Idle Timeout for PayRoll application may be set to 5 minutes.

The Session Management Engine (SME) of Access Manager internally uses Oracle Coherence, a high performance distributed caching system, to enable the monitoring and management of millions of user sessions across the enterprise in real time. Oracle Coherence replicates and distributes session data across all Access Manager run-time servers in the cluster and also communicates changes from the console to the run-time servers. The location of a session is transparent to the client. All Oracle Coherence traffic is automatically encrypted and it also performs automatic failover and reconciliation. For example, if one of the nodes in a cluster fails, Oracle Coherence automatically distributes data from the failed node to the distributed in-memory caches of the other nodes in the cluster.

Apart from in-memory caches, Oracle Coherence also provides the option to configure a database as an SME session store to persist session data.

Centralized and Streamlined Agent Management

The Oracle Access Management console provides a simple interface to centrally manage and control all the Policy Enforcement Points or WebGates deployed across the enterprise. Figure 6 below shows the console interface to look up and modify agents. Configuration changes on a specific WebGate can be done centrally through the console and propagated to the WebGate without the need to directly access the WebGate or restart the web server. This centralized agent management is really powerful especially for large deployments with thousands of WebGates spread across the enterprise.

Oracle Access Management11gR2 provides Agent Compatibility in order to allow enterprises currently using legacy access management platforms like OAM10g, OSSO, OpenSSO 8.0 or Sun Access Manager 7.1 to continue using their existing WebGates and agents while upgrading their server infrastructure to the new 11gR2 platform. A Protocol Compatibility Framework allows the Access Manager server to communicate with different type of legacy agents like OAM10g WebGates, OSSO agents, as well as OpenSSO 2.2 and 3.0 agents the same way it can communicate with a new 11g WebGate.

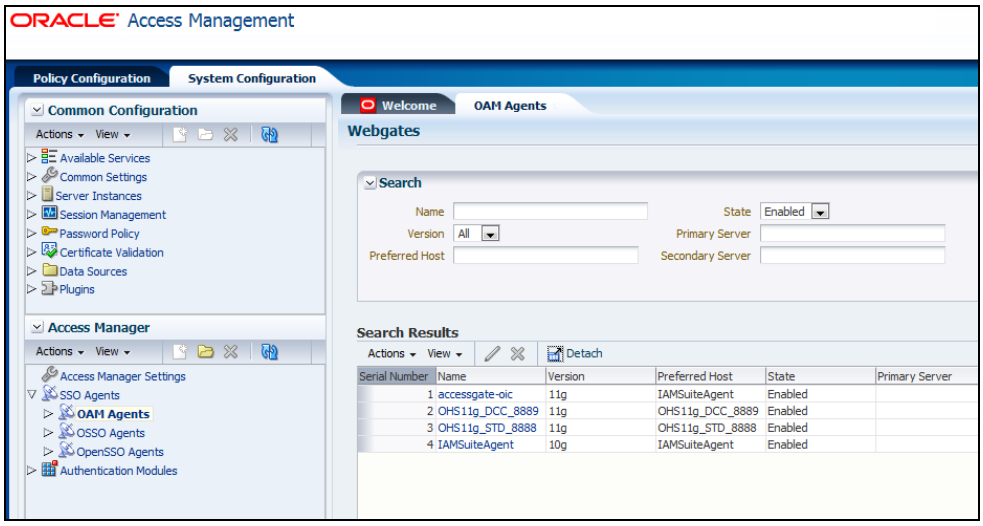

Figure 6. Interface to search and manage agents in console

These WebGates communicate with the server using the secure Oracle Access Protocol. This communication can also be SSL encrypted using a private key along with a global pass-phrase. Before a WebGate can start communicating with an Access Manager server, an administrator has to register the WebGate against the server (sometimes referred to as Partner Registration). This registration of agents can either be done at the Oracle Access Management console using a step-by-step wizard or using a command line Remote Registration tool.

Oracle Access Management 11gR2 also provides a portable, stand-alone Java application called Access Tester which can simulate a WebGate behavior allowing administrators as well as developers to test connectivity and responsiveness of the Access Manager server as well as results of specific policy changes. Apart from a graphical user interface, the Access Tester also provides a command-line interface which enables automated stress testing of the access infrastructure.

Native Password Management

As a part of the Oracle Identity and Access Management platform, Access Manager provides out of the box integration with Oracle Identity Manager, a component of the Oracle Identity Governance Suite for all password management capabilities. This is the recommended approach since Oracle Identity Governance Suite provides organizations with the complete set of capabilities required for identity governance, provisioning and role management. However, for organizations that have relatively simple password management needs, Access Manager also offers a built-in native password management capability.

The Oracle Access Management console provides administrators with an interface to define a global password policy. This includes password composition rules like minimum or maximum number of alphabets/numbers in the password, minimum and maximum permissible password length, whether special characters are allowed etc as well as other aspects of password policy like after how many days does the password expire, after how many days should it warn the user, after how many incorrect attempts should it lock the account and so on. This allows administrators to control the password policy for the organization. Figure 7 below, depicts the interface provided by the console for password management.

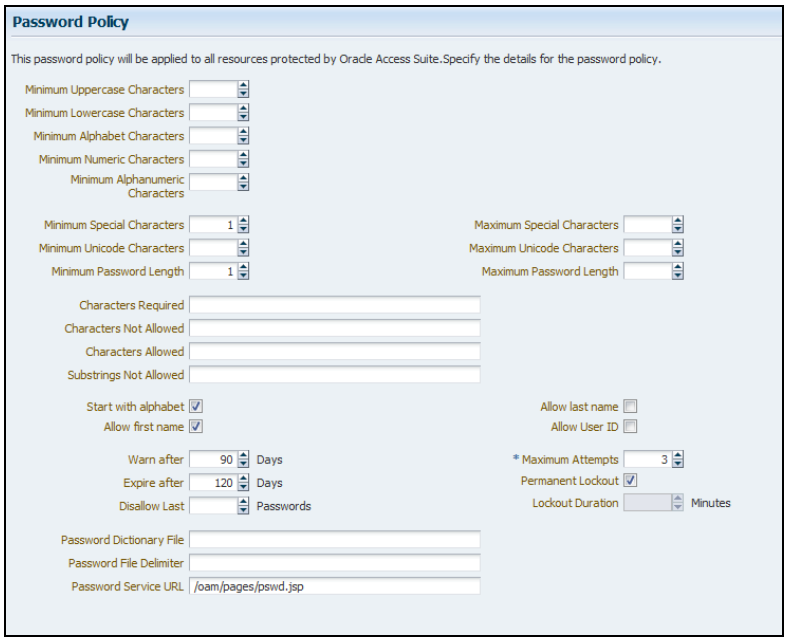

Figure 7. Interface to define password policy in console

Windows Native Authentication

Access Manager enables Microsoft Internet Explorer users to automatically authenticate to their Web-based single sign-on applications using their desktop credentials. This is known as Windows Native Authentication (WNA). Access Manager supports WNA with the underlying Windows Active Directory configured in Multi-Domain and Multi-Forest topologies.

Access Manager interoperates with Windows Native Authentication (WNA), which uses Kerberos credentials obtained when the user logs in to a Windows Domain. This cross-platform authentication is achieved by emulating the negotiate behavior of native Windows-to-Windows authentication services that use the Kerberos protocol. When Access Manager is configured for WNA, a user that has logged into his desktop can simply navigate to a protected resource without another challenge for credentials. This is because a Kerberos session ticket, which includes the user's credentials, is passed through the browser to the Access Manager server which then validates the credentials against the Key Distribution Center server (KDC server) on the Windows domain server. This whole interaction is completely transparent to the end user providing him with a seamless SSO experience.

For configuring WNA, all resources in Access Manager should be protected by a Kerberos Authentication Scheme with the WNA as the Challenge Method and the credentials are stored in Active Directory which is configured as a user store in Access Manager.

Comprehensive Auditing & Logging

In access management, auditing refers to the process of collecting specific information related to administrative, authentication, and run-time events that would help evaluate compliance to organizational polices, user access controls and risk management procedures. Audit data can be used to create dashboards, compile historical data, and assess risks allowing compliance officers to perform periodic reviews of adherence to compliance policies.

Access Manager leverages the underlying Oracle Fusion Middleware Common Audit Framework to capture comprehensive and detailed audit logs. This framework provides uniform logging and exception handling and diagnostics for all audit events and uses a database store to provide scalability and high-availability for the audit framework. Further, administrators can control and specify certain auditing parameters to meet the compliance requirements of their organization.

Reports can be generated from audit data by using Oracle Business Intelligence (OBI) Publisher. OBI Publisher allows auditors to generate reports based on various criteria, such as user name, time range, application type etc. Organizations can also leverage Oracle Business Intelligence Publisher to create custom audit reports based on requirements.

Logging is the mechanism by which various components of Access Manager write messages to flat files that can be used by administrators to diagnose and troubleshoot. Log levels can be specified to control the amount of details to be captured in the logs. By default, the log level for all Oracle Access Management components is set as Notification level. Logging at the Error level produces a small amount of output while other log levels can result in voluminous logging output, which can impact performance. In production environments, logging is usually either disabled or the log level is set to a level that results in a small volume of logging output unless administrators need to specifically troubleshoot an issue.

Architecture & Deployment

Internal Architecture

Access Manager has a well-designed internal architecture that enables it to provide the rich functionality described in the previous sections while ensuring superior performance and the ability to scale for large deployments.

Figure 8 below provides a visual representation of the various layers and components of Access Manager. User identities and credentials are stored in the directory while the policies are stored in an RDBMS like Oracle Database. The Oracle Platform Security Services (OPSS) and Oracle Coherence layers provide the platform security and caching services required for Access Manager. The configuration and policy services allow administrators to manage configuration and define policies.

Various run-time components like Authentication service, Authorization service, Session Management engine, Credential Collector etc provide run-time services. A protocol compatibility framework ensures that various policy enforcements points including legacy agents and SDK-based Access Clients can access this central server infrastructure.

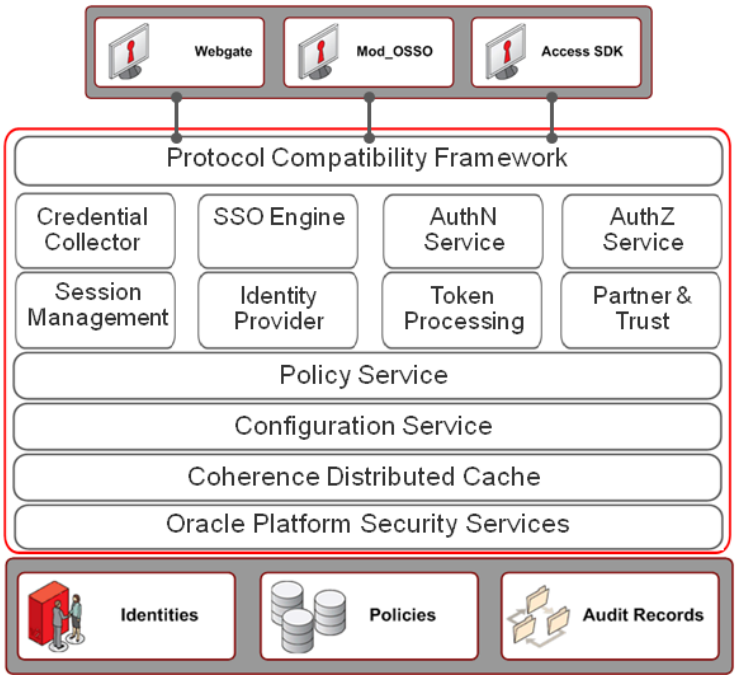

Figure 8. Internal Architecture of Access Manager

Detached Credential Collector

Credential Collection refers to the process of collecting the end user's credentials through a login page. If the WebGate intercepts a request and detects that the user is not authenticated yet, it redirects the user to this login page. In case of Access Manager, this login page on the server referred to as the Embedded Credential Collector (ECC) since the page is embedded in the server.

In Oracle Access Management 11gR2, a new concept of a Detached Credential Collector (DCC) has been introduced where a specific WebGate can be extended to provide credential collection capability. The DCC uses secure Oracle Access Protocol (OAP) to communicate with the back end Access Manager server while using the HTTPS to talk to the end user for obtaining credentials.

The DCC offers a number of benefits from a security as well as flexibility point of view. Since the DCC is completely decoupled from the Access Manager server, it provides the flexibility of being deployed anywhere in the area between an organization's trusted internal network and an untrusted, external network such as the Internet: sometimes known as a subnet, perimeter network, or DMZ. Since all the unsecure end user HTTP requests get terminated in the DMZ and all communication between the DCC and the Access Manager server uses the secure Oracle Access Protocol (OAP), it offers a complete isolation of the server from the establishment of any unauthenticated network connection.

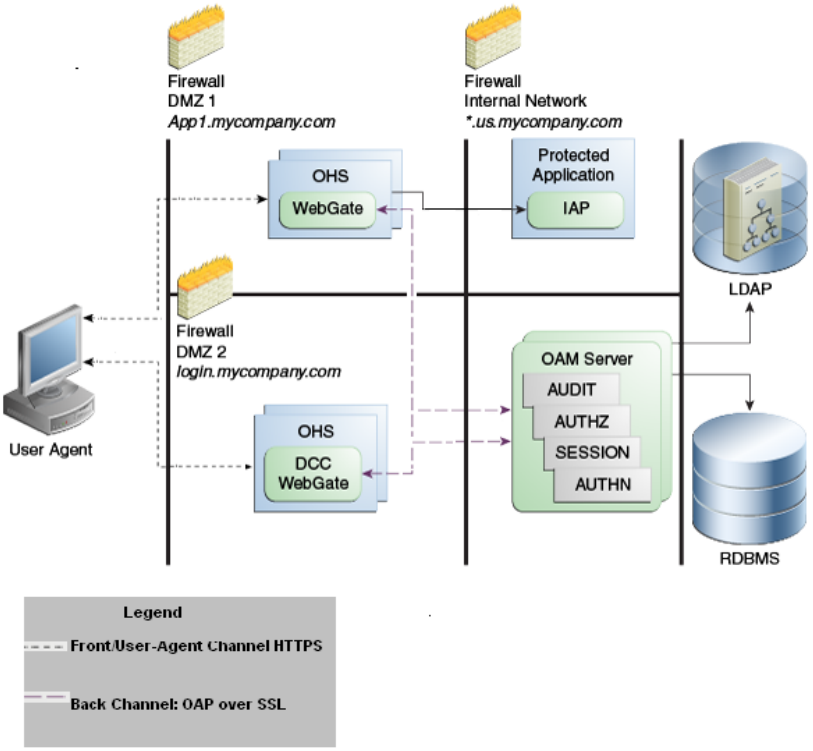

Figure 9. Sample Deployment using Detached Credential Collector

Figure 9 above shows a sample deployment of a Detached Credential Collector. When user tries to access a resource, the WebGate intercepts the request and communicates back to the server. Since credential collection is configured to use a DCC WebGate, server sends the request to the DCC which throws the login page to the user. When the user provides his credentials, the DCC communicates with the server to authenticate the user and a session gets established. The rest of the flow is similar to what would happen if an ECC would be used. The WebGate lets the user though to access the resource.

Scalable Deployment Model

Access Manager is designed for extreme scalability and high availability. The server is built as a 100% Java solution that can leverage the inherent scalability and clustering capability of the underlying Oracle WebLogic platform. While the Oracle Access Management console is deployed on the Admin server of the Oracle WebLogic cluster, the run-time Access servers are deployed on the managed nodes of the cluster. The WebGates are configured such that for every WebGate one of the Access Manager nodes is configured as a primary, another one as a secondary if it cannot contact the primary, a third one as a tertiary if both the primary and secondary are down and so on. At run-time, as millions of users try to access various resources, the load of handling the access requests gets distributed across these managed nodes ensuring high performance. The WebLogic cluster also ensures high availability wherein if one of the nodes of the cluster goes down, the user sessions seamlessly fail over to the other nodes. High performance caching provided by the Oracle Coherence layer ensures that all the user session data is in sync across all nodes at run time and user sessions can fail over from one node to the other without any impact to the end user. As the access requirements in the organization grow, additional nodes can be easily added to the cluster allowing the access management infrastructure to scale horizontally.

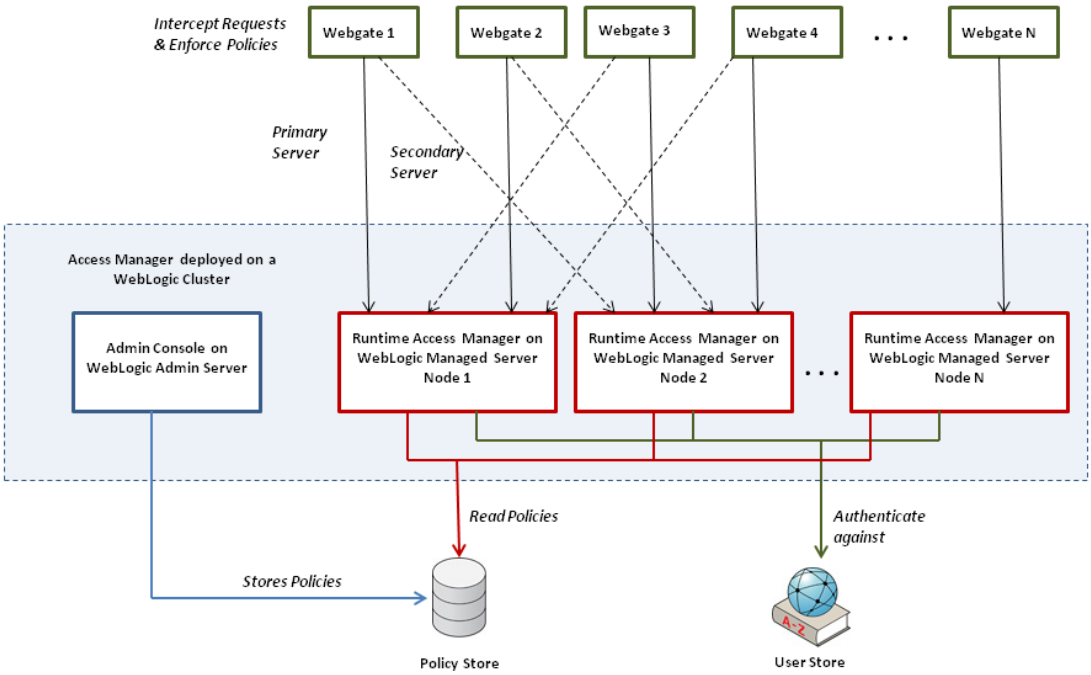

Figure 10. Horizontal Scalability through WebLogic Clustering

Figure 10 above shows how Access Manager achieves horizontal scalability through WebLogic clustering. Access Manager has been benchmarked for a 250-million user environment and has proven that it can scale extremely well to meet varying access loads.

Support for Multi-Data Center Deployment

Access Manager provides an extremely scalable deployment model not only via clustering multiple nodes within a single data center but also supporting clusters across multiple data centers. This provides load balancing across multiple data centers as well as failover capabilities in case one data center goes down.

Access Manager can support multi-data center deployment in different modes:

- Active-Active, where both datacenters are active at the same time catering to different sets of users
- Active-Passive, where one of the data centers is passive and can be brought up within a reasonable time in case the primary data center fails
- Active–Hot Standby, where one of the data centers is in a hot standby mode though it is not actively catering to users till the other data center goes down

Figure 11 below depicts an Active-Active data center set up where a global load balancer automatically directs users from different geographical locations to the appropriate data center based on affinity. The browser cookie keeps track of which data center the user is tied to.

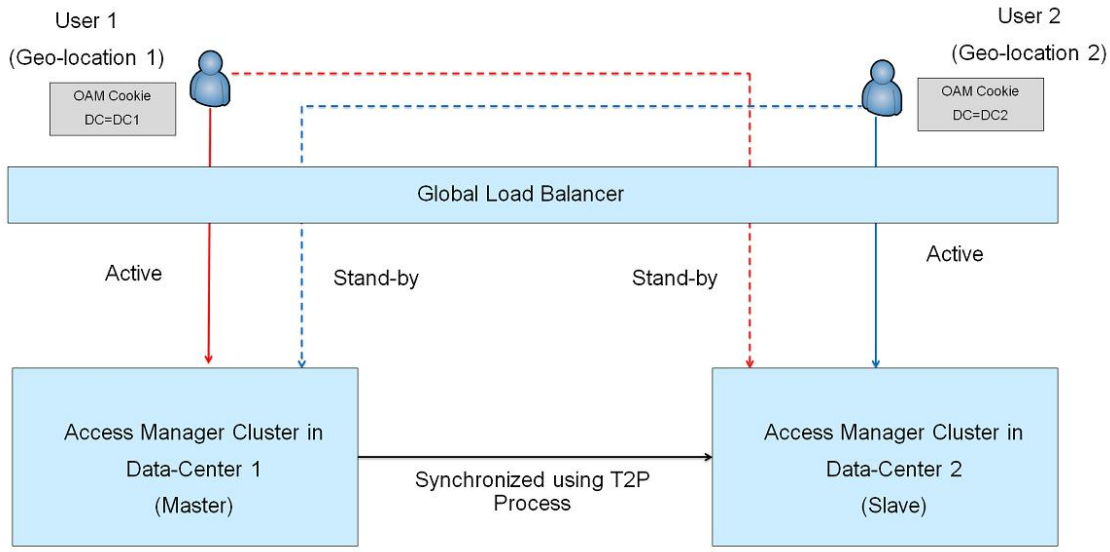

Figure 11. Active-Active multi-data center set up

In case a user from one data center gets moved to a different data center mid-way during a session either for load balancing or due to failure of one of the data centers, the multi-data center set up can be configured to either force the user to re-authenticate and re-establish a session or replicate the session transparently by invoking backend OAP calls to retrieve the user's session data from the remote data center as long as it is accessible.

For a multi-data center deployment, the Access Manager cluster in each data center has to be configured to be identical. This is done by configuring one of the data centers as a Master where all policy and configuration changes are implemented. The other Clone data centers are set up using Test-to-Production (T2P) tools the first time. A replication agreement is set up between the Master and Clone data centers so the Clone data centers can periodically poll the Master and synchronize policies and configuration.

Extensibility & Integration

Oracle & Third Party Integrations

Oracle Access Management 11g is part of the Oracle Fusion Middleware (FMW) stack and therefore provides out of the box integration with not only products and components of the Oracle FMW stack but also Oracle Fusion Applications. As part of the Oracle Identity & Access Management platform, Access Manager is tightly integrated with Oracle Identity Manager and other components of Oracle Identity Governance. It is also certified to work with Oracle E-business Suite, PeopleSoft, Siebel, JD Edwards and other ERP/CRM offerings from Oracle.

Further, Access Manager also provides simple, out of the box integration with a number of third party products including Microsoft SharePoint 2010, RSA Authentication Manager 7.1 and JBoss 5.1.0.

REST-based Policy Admin APIs

Access Manager provides a Policy Administration API that enables Create, Read, Update, and Delete (CRUD) operations on its policy objects. The Policy Administration API supports representational state transfer (REST) interfaces for administering Access Manager policy objects as RESTful resources. Operations performed by REST clients through Policy Admin APIs are subject to the same Access Manager policy administration rules that are enforced through the console. These REST-based Policy Admin APIs provide organizations with the powerful capability to create tools to automate policy management wherever appropriate instead of using the console.

Customization with Java SDK

While WebGates act as Policy Enforcement Points for standard points of web access like web servers, enterprises would sometimes want to build their own custom Policy Enforcement Point that can leverage the central access infrastructure and policy definitions.

Access Manager provides a comprehensive Java Software Development Kit (SDK) that allows developers to build custom Policy Enforcement Points referred to as Access Clients. Access Clients can be built to perform a number of functions like authenticating users to create a session on the Access Manager server, checking for authorization to access a particular resource, validating session tokens presented by user, saving or retrieving session attributes etc.

Benefits

To summarize, here are the key benefits that Access Manager has to offer:

- Centralized policy management and auditing reduces cost and improves compliance.
- Support for access management in a complex, heterogeneous environment reduces total cost of ownership and accelerates deployment.
- Flexible and powerful policy model allow organizations to meet complex access management needs.
- Scalable deployment model supports most demanding, internet scale deployments.
- Extensible architecture enables easy customization to meet organization specific requirements.

Conclusion

In conclusion, Oracle Access Management 11gR2 provides one of the most complete and scalable access management platforms for the enterprise. It provides a comprehensive set of capabilities to address current and future access management needs of the enterprise while ensuring simplified deployment and management. Using a platform approach,

Oracle Access Management11gR2 solution reduces the total cost of ownership, improves management efficiency and ensures security and compliance.

Oracle Access Management 11g
December 2013
Author: Venu Shastri
Contributing Authors: Svetlana Kolomeskaya

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

SOFTWARE. HARDWARE. COMPLETE.