ORACLE ACCESS MANAGER 11G

SINGLE SIGN-ON SIMPLIFIED

KEY FEATURES

- AppSecure Control Center
- Single Sign-On Security Zones
- Session Management
- Centralized Policy Administration
- Simplified Application Integration

KEY BENEFITS

- Create and manage agents and run diagnostics from a central administration console to simplify ongoing security administration
- Scopes encryption keys for data passed been WebGates and the Oracle Access Manager Access Server to an application enforcement point, creating security zones that prevent unauthorized access from spreading to multiple applications
- Provides high performance access to distributed security session data allowing centralized control over user sessions by enforcing constraints such as a single session per user
- Gives end users the ability to create and reset their password without assistance to dramatically reduce help desk costs and helps to keep users productive
- Simplifies administration through a unique set of tools that provide remote application registration, policy simulation, and test-to-production migration
- Provides built-in and seamless integration to Oracle Fusion Middleware applications

Oracle Access Manager helps enterprises create greater levels of business agility, ensures smooth application integration, and enables regulatory compliance. Through an innovative modular architecture Oracle Access Manager combines access control, session management, and system management services to provide centralized authentication, policy-based authorization, identity propagation, session controls, system diagnostics, agent management, and auditing. Protecting resources at the point of access and propagating the authenticated identity downstream, Oracle Access Manager secures enterprise applications while reducing cost, complexity and administrative burdens.

Introduction

Oracle Access Manager is an enterprise level solution that centralizes critical access control services to provide an integrated solution that delivers authentication, authorization, web single sign-on, policy administration, enforcement agent management, session control, systems monitoring, reporting, logging, and auditing. Oracle Access Manager's key features include the AppSecure Control Center, Single Sign-On Security Zones, and Centralized Policy Administration and Session Management, which combine powerful security controls with an easy-to-use and intuitive interface to dramatically simplify how enterprises manage application security. Oracle Access Manager excels in complex, heterogeneous enterprise environments and integrates out-of-the-box with market leading directory servers, application servers, web servers, and enterprise applications.

AppSecure Control Center

Oracle Access Manager's AppSecure Control Center provides a powerful administration that coordinates all aspects of agent management including basic diagnostics, real-time monitoring of operational metrics, and a utility that can be executed remotely to perform agent registration. The AppSecure Control Center registers Oracle Access Manager agents using a simple and intuitive user interface. In addition, the agent registration process gives administrators the option to automatically create policy objects, eliminating unneeded complexity and simplifying how applications are secured. The AppSecure Control Center extrapolates the information from the registration process to provide all policy objects necessary to secure the application the registered agent is intended to protect.

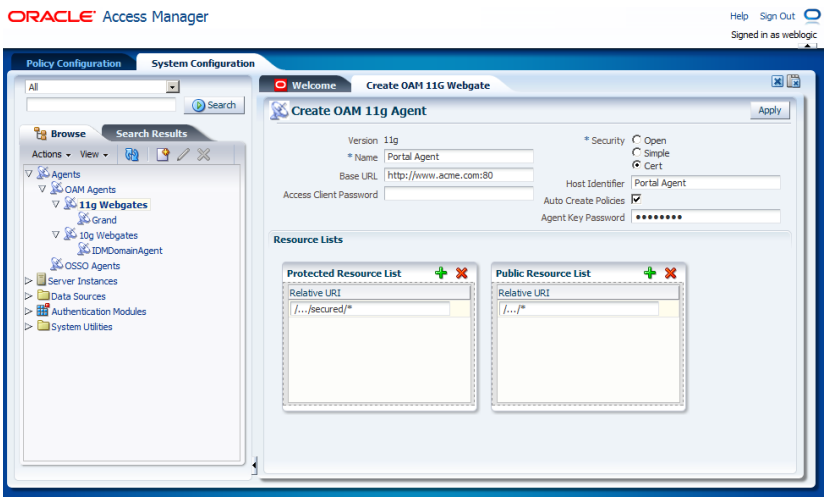

Figure 1. Registration of agents using AppSecure Control Center

The AppSecure Control Center simplifies the operations of an enterprise security administrator by providing simple out-of-the-box monitoring of the Oracle Access Manager components including server and agent operational metrics. The operational metrics provide administrators a better view of the security environment and its operational status.

Single Sign-On Security Zones

A common concern of security administrators is the containment of a security compromise. Oracle Access Manager's Single Sign-On (SSO) Security Zones address this concern by ensuring the compartmentalization of policy enforcement point (PEP) agents such that any compromise to individual PEP agents will not spread to other enforcement points. SSO Security Zones scope encryption keys used to secure data communications to individual PEP agents ensuring access to only the applications protected by that PEP agent and preventing unauthorized access to other protected applications unless explicitly granted by Oracle Access Manager's Access Server.

Session Management

Oracle Access Manager gives security administrators complete control over real-time distributed user session data. It enforces constraints against any user's session including limiting the number of concurrent sessions an individual user can have at any given time. Furthermore, Oracle Access Manager allows security administrators to search for and terminate specific sessions providing enterprises unprecedented visibility and control over users and their security sessions.

The core of Oracle Access Manager's Session Management functionality is a high performance distributed caching system that enables Oracle Access Manager to propagate creation and modifications to user session across the various distributed runtime servers. The nature of the distributed cache system implicitly supports site affinity such that any runtime servers have access to the same set sessions when serving access requests that may have bounced through multiple servers. An additional option to utilize a persistent session store makes it possible to recover from mass failures in the security environment and maintain the same user sessions once the failures are resolved.

ORACLE IDENTITY MANAGEMENT

Oracle Access Manager delivers access control, single sign-on, and session management to a heterogeneous application environment.

RELATED PRODUCTS

Oracle Adaptive Access Manager provides superior protection for businesses and their customers through strong yet easy-to-deploy multifactor authentication and proactive, real-time fraud prevention.

Oracle Entitlements Server externalizes and centralizes fine-grained authorization for enterprise applications and web services via comprehensive, reusable, and auditable authorization policies and a simple, easy-to-use administration model.

Oracle Identity Federation enables cross-domain single sign-on with an identity federation server that is completely self-contained and ready to run out-of-the-box.

Oracle Web Services Manager is a comprehensive solution for adding policy-driven security and management capabilities web services.

Oracle Identity Manager is a powerful and flexible enterprise identity provisioning and compliance solution that automates the creation, updating, and removal of users from enterprise systems.

Oracle Identity Analytics empowers customers with rich analytics and dashboards to allow monitoring, analyzing and governing user access in order to mitigate risk and satisfy compliance mandates.

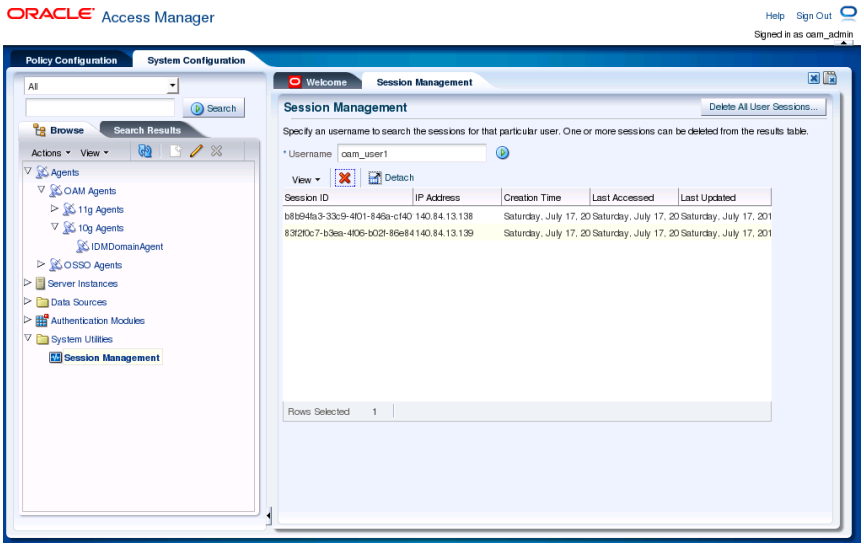

Figure 2. Searching for user sessions by user identifier

Self-Service Password Management

Giving end users the ability to create and reset their password without assistance dramatically reduces help desk costs and helps to keep users productive. Exposing such sensitive flows on the intranet and extranet requires advanced security measures to protect them from exploitation by criminals however. Oracle Access Manager 11g now has out of the box integrations with Oracle Identity Manager 11g and Oracle Adaptive Access Manager 11g to provide real-time risk analytics and risk-based challenge mechanisms including knowledge based authentication and OTP Anywhere. These integrations dramatically strengthen security while maximizing usability which makes for a truly enterprise class security solution.

Centralized Policy Administration

Oracle Access Manager simplifies the process of creating, managing and propagating security policies through a centralized, intuitive, and easy-to-use administration console. These centrally managed policies are seamlessly and automatically propagated in real-time across Oracle Access Manager's distributed runtime servers within an organization's environment. The propagation ensures that policy enforcement is aligned and consistent throughout the environment at any given point of time.

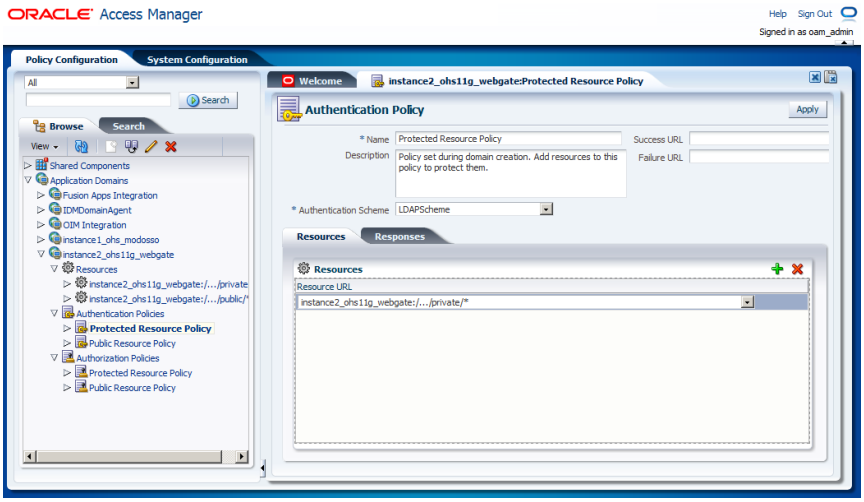

Figure 3. Managing an authentication policy through the administration console

Authentication Extensibility Framework

With the ever changing security landscape that enterprises face today, the ability to extend and customize authentication flows above and beyond the out-of-the-box capabilities is crucial. Oracle Access Manager 11g provides a set of API interfaces for security developers to develop customized authentication modules that are tailored to a specific customer's authentication process. These authentication modules can then be plugged into Oracle Access Manager 11g by security administrators and orchestrated to form a customized authentication flow.

Bottom Line

Oracle Access Manager is the industry's most comprehensive access management solution with single sign-on, authentication and authorization enforcement, session management, centralized policy administration, built-in monitoring tools, and extensibility framework. Oracle Access Manager already supports a wide variety of authentication mechanism, such as HTML Forms, X.509 certificates, and Kerberos authentication, and has an intuitive and centralized administration framework for creating and managing access control policies as well as system configuration. Authentication control and policy enforcement is provided out of the box for a wide variety of web servers, application servers, and packaged enterprise applications running on nearly any flavor of operating system, including Windows, SUSE Linux, RedHat Linux, Oracle Enterprise Linux, Solaris, AIX, and HP-UX. Oracle Access Manager is the choice for complex, heterogeneous, highly distributed, or massively scaled environments, and has been consistently recognized as the leading web access management solution by the industry's most important analysts.

Contact Us

For more information about Oracle Access Manager, visit www.oracle.com/identity or call +1.800.ORACLE1 to speak to an Oracle representative.

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

SOFTWARE. HARDWARE. COMPLETE.

ORACLE