ORACLE PRIVILEGED ACCOUNT MANAGER 11g

KEY FEATURES

- Secure password vault for privileged accounts
- User Session Management and Recording
- Extensible Java based framework to build custom solutions
- Easy to use user interface for OPAM administrators and users
- Auditing and reporting of privileged account activities
- RESTful and command line interface provides standardized access to OPAM functionality and allows custom integrations
- Rich set of target connectors for Databases, UNIX/Linux and Directories including Oracle Exadata and Oracle Exalogic
- Integrated governance solution with Oracle Identity Manager and Oracle Identity Analytics
- Complements existing Oracle solutions: DB Vault, DB Enterprise User Security and Authentication Services for Operating Systems

KEY BENEFITS

- Monitoring and recording of user sessions enables individual accountability through session transcripts
- Enforce internal security policies and eliminate potential security threats from privileged users
- Cost-effectively enforce and attest to regulatory requirements
- Reduce IT costs through efficient self service and common security infrastructure
- Centralized auditing and customizable audit reports through BI Publisher
- Enables custom built solutions, for example Ticketing System integration, through Java plug-ins

Oracle Privileged Account Manager (OPAM) is a secure password management solution designed to generate, provision, and manage access to passwords for privileged accounts like Linux/Unix "root" or Oracle database "sys" accounts. It enables auditing and establishes accountability for users who normally share privileged account credentials, and additional user Session Management and Recording. OPAM's integration with the Oracle Identity Governance platform provides central governance for both regular users and privileged users, complete auditing, reporting and certification of user's regular accounts and shared accounts, and lifecycle management from request, approval, to certification and usage tracking. OPAM greatly enhances security and significantly improves compliance.

Oracle Privileged Account Manager

OPAM manages privileged account passwords on target systems. Privileged account credentials are centrally managed and the OPAM administrators define policies governing who (user, role or group) can access certain privileged account credentials.

When a user needs to access a target system using the privileged account, the user must authenticate to OPAM and retrieve (checkout) the credential, upon successful authorization. The credential access is audited, and exclusive usage for a time period can be enforced.

In addition OPAM's user Session Management Recording enables individual accountability through session transcripts.

Users and OPAM administrators interact with OPAM through the same web-based console. The web console supports role-based access to determine if it is a user retrieving a password or session, or an OPAM administrator to manage OPAM. Users check-in/check-out the privileged accounts passwords or sessions, and OPAM administrators manage targets, accounts, grantees, usage and password policies. OPAM console access can be secured by Oracle Access Manager and Oracle Adaptive Access Manager for strong authentication and single sign-on (SSO).

All OPAM user and administrator interactions are audited and stored in a central audit database. At any given time the OPAM administrator can see which accounts are checked out.

OPAM leverages the Oracle Integrated Connector Framework (ICF) to provide connectors that link OPAM with target systems such as user directories, database servers, and operating systems. The OPAM server exposes a RESTful API used by OPAM client applications including the OPAM console and the OPAM command-line. Customers can build custom integrations using OPAM's public RESTful API or the flexible Java based plug-in framework. Privileged accounts can be auto discovered and identified through connectors. Passwords

managed by OPAM are encrypted and persisted in an Oracle DB credential store. When passwords are stored in an Oracle database, customers can leverage Oracle Database Vault and Transparent Data Encryption (TDE) for additional security.

OPAM integration with Oracle's Identity Governance Platform

OPAM can be used as a standalone component, although, a key benefit is its integration into the Oracle Identity Governance platform. Oracle Identity Governance platform provides a complete governance solution which supports lifecycle management of both regular and privileged accounts, as well as the support of exclusive and shared accounts to meet enterprise compliance requirements. Integration includes, user provisioning into the OPAM identity store using policy- and role-based provisioning, and delegating access to privileged accounts through self-service delegation functionality. Administrators can request privileged account access via the OIM catalog, or make “break-the-glass” (emergency) requests, to access accounts they are normally not entitled to. Other areas leverage risk-based certification and closed-loop remediation.

OPAM Complements Oracle Solutions

Oracle Database Vault enables fine-grained authorization and separation of duties to prevent DBAs from unauthorized access to application data stored in the database. Database Enterprise User Security enables centralized management of database users (except privileged DB accounts like “sys”) and enterprise roles in a directory. Oracle Authentication Services for Operating Systems (OAS4OS) enables enterprises to centralize the management of Unix and Linux account. OPAM complements these solutions through management of privileged database, directory and operating system accounts and users to ensure accountability, auditability, enhanced security and compliance.

Summary

Oracle Privileged Account Manager (OPAM) provides a versatile and integrated solution that allows organizations to manage their privileged account passwords and audit privileged activities. Additionally OPAM’s user Session Management Recording enables individual accountability through session transcripts. OPAM can operate as a standalone solution, but delivers more value when used in conjunction with other Oracle Identity Management components. Oracle Identity Governance platform provides a complete governance solution supporting lifecycle management of both regular and privileged accounts and users’ individual and shared accounts to meet enterprise compliance requirements

Contact Us

For more information about Oracle Privileged Account Manager, visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.

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

Hardware and Software, Engineered to Work Together