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.
EXECUTIVE SUMMARY

Today’s enterprises are under increasing pressure to be more competitive and compliant. As a key business enabler, corporate IT must protect mission-critical applications and sensitive business data, while reducing operational cost. Since mission-critical applications and sensitive business data reside within the operating system (OS), effective management and enforcement of OS access is of paramount importance. Unfortunately, a Forrester survey of 77 server security decision-makers identified ensuring appropriate access control/administration rights\(^1\) as their top challenge.

For authentication and user management, Unix and Linux systems provide native local account management capability that is very costly to administer and lack consistency across systems. While Network Information Service (NIS) provides a centralized approach for user management and authentication, it has its own significant security issues, and is still a silo from enterprise identity management framework. Some LDAP products provide pluggable authentication module (PAM) support, however most organizations find that existing solutions are difficult to deploy, lack key platform integration, and require extensive LDAP knowledge for Unix administrators.

Oracle Authentication Services for Operating Systems enables enterprises to centralize the management of Unix and Linux authentication, user accounts, password policies, and sudo authorization policies using Oracle Internet Directory (OID). Based on open standards interfaces, Oracle Authentication Services for Operating Systems provides full automation of client configuration and user migration.

Centralized management and auditing using Oracle Authentication Services for Operating Systems ensures strong security and consistent policies across platforms, and facilitates compliance. With the automation tools, Oracle Authentication Services for Operating Systems significantly reduces administration cost and accelerates deployment. In addition, as a component of Oracle Identity Management suite, the solution can be an integral part of a comprehensive enterprise identity management deployment.

---

\(^1\) Operating System Vendors: Do More To Help Users With Vendor Security, Forrester Research, April 2007
BUSINESS CHALLENGES

IT departments are under consistent pressure to reduce cost, enhance security, and improve compliance to support ever-competitive business. Unix and Linux servers are critical IT assets that must be secured to protect corporate sensitive data that resides in it. Unfortunately, as indicated in the figure below, a recent Forrester survey identified controlling access to operating system servers as enterprise’s top security challenge.2

<table>
<thead>
<tr>
<th>Please rank the most challenging aspects of securing your servers.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Most challenging</td>
</tr>
<tr>
<td>1. Ensuring appropriate access control/administration rights</td>
</tr>
<tr>
<td>2. Complexity of deciding which patches to apply</td>
</tr>
<tr>
<td>3. Tracking servers’ patch levels</td>
</tr>
<tr>
<td>4. Downtime due to security upgrades (planned downtime)</td>
</tr>
<tr>
<td>5. Hiring appropriate staff</td>
</tr>
<tr>
<td>6. No automatic patching service</td>
</tr>
<tr>
<td>7. Downtime due to errors or attack (unplanned downtime)</td>
</tr>
<tr>
<td>8. Keeping out rogue servers</td>
</tr>
</tbody>
</table>

Least challenging

Base: 77 decision-makers responsible for server security

Source: Forrester Research, Inc.

Managing authentication, user accounts, password policies, and sudo authorization policies across heterogeneous Unix and Linux platforms is extremely challenging due to co-ordination and technical complexity. Let’s take a look at some of these challenges.

High cost of local account management

While Unix/Linux systems provide some level of native operating system security functions, there are security gaps and administrative concerns with its authentication and account management.

Using native Unix/Linux security, user account, password policies, and sudo authorization policies are managed for each user on each machine. Redundant administration cost is high, and the cost increases significantly as the user population and the number of servers increase. In addition, different Unix and Linux platforms have different levels of security functionality and different ways to perform similar tasks. As a result, managing accounts locally becomes a complex and error prone task in large heterogeneous environments. Furthermore, consistent policies, such as password policies, are difficult to apply and enforce across systems, if at all possible.

Security concerns over NIS

Some enterprises have deployed Network Information Service (NIS) to manage Unix and Linux authentication and accounts. NIS provides a centralized approach for Unix and Linux account management. However it has its own significant security shortcomings, which include limited data protection and an inefficient data replication model that relies on one master and multiple replica servers.

---

When using NIS for centralized user management, one of the security limitations is that once the account is enabled, this user has access to all hosts in that NIS domain without granular access control. In addition, account data is not secure, since queries against the NIS servers are only protected by IP address, and no strong encryption is available. These security gaps may result in un-authorized retrieval of Unix and Linux user information residing in NIS server, and granting excessive access rights to arbitrary hosts.

For large organizations with geographically distributed data centers, it is critical to quickly adopt security changes across data centers, but NIS single master replication is not up to enterprise standard.

**Complexity with existing directory based solutions**

A good approach to address local account management issues or NIS security concerns is to implement directory based solutions. Unix and Linux support LDAP directories for user management and authentication through standard PAM_LDAP interface.

Some LDAP directory vendors offer PAM_LDAP module to integrate their directories with Unix and Linux. However, there are several challenges with existing solutions:

- Implementing these solutions requires OS administrators to have intimate knowledge of LDAP. Furthermore, the client configurations and user migration are platform specific, so deployments are very difficult in a heterogeneous enterprise environment. For example, to secure a deployment, OS clients should be configured to use SSL for connections with the LDAP server. However the daunting task of SSL setup for different platforms forces many companies to give up and live with insecure deployments.

- These solutions may only support a subset of OS platforms within a heterogeneous environment

- The limitation of scalability, availability, manageability, and security of the directory itself.

These challenges result in high cost to deploy and maintain the solutions and potentially weak security.
ORACLE AUTHENTICATION SERVICES FOR OPERATING SYSTEMS

Overview

Oracle Authentication Services for Operating Systems provides centralized authentication and account management for Unix and Linux platforms. The solution consists of Oracle Internet Directory (OID), integrated with major Unix and Linux operating systems using open standards including PAM_LDAP, NSS_LDAP, and sudo LDAP, configuration automation tools, and user migration tools. Oracle Authentication Services for Operating Systems is designed to address the Unix and Linux authentication and account management challenges outlined above.

Automated configuration

Oracle Authentication Services for OS (as part of Oracle Fusion Middleware 11g R1) provides the required automation tools to seamlessly integrate and configure Unix and Linux clients to work with Oracle Internet Directory for user authentication and account management. The automation tools consist of configuration scripts for both SSL and non-SSL configurations across major Unix and Linux platforms (see Oracle Fusion Middleware Supported System Configurations). The configuration scripts can be pushed to the client and then executed. They configure the client to connect and authenticate to OID via SSL or non-SSL without further administrator intervention.

User migration

Migration of existing user information to OID is a key deployment step. There are three scenarios for user migration: migrate local user accounts to OID, migrate NIS user accounts to OID, and migrate user accounts from other directories to OID. Tools are available either through third party or through Oracle Authentication Services for OS to facilitate user migration for above scenarios.

Migrating account information from local files or NIS to OID can be achieved via a number of free tools available in the public domain. These tools export existing information and generate files in the LDAP Data Interchange Format (LDIF). For small data sets the standard ‘ldapadd tool’ can be used to load the
information into Oracle Internet Directory. For large LDIF files Oracle provides a bulk load utility which checks data consistency and then loads the data directly into the Oracle database that stores OID data. Furthermore, Oracle has validated the process of migrating data using the LDAP migration tools available at PADL Software Limited (www.padl.com).

Directory server migration, without proper tools, can easily become a time consuming task. Directory migration typically happens in two phases, and Oracle Authentication Services for OS provides tools for both phases. Phase one is schema (metadata) migration. Oracle Authentication Services provides a tool to compare and reconcile the schema of the third party directory (e.g. Redhat Directory Server) with Oracle Internet Directory. Phase two is the data migration, during which another automation tool is provided to convert, verify and synchronize the user data.

Centralized Management of Password Policies
Oracle Internet Directory provides password policy management and enforcement capabilities including password composition policies (e.g. how many character a password must have), password state policies (e.g. a user has to change the password every 30 days), and account lockout policies (e.g. account lock out after three failed logins). Oracle Internet Directory supports multiple password policies per realm. These policies can be applied to any subtree within that realm. So, if multiple organizational units are managed in OID, each one can have separate policies down to the level that even user specific password policies are possible.

Oracle Authentication Services for OS leverages OID’s flexible password policies to enforce enterprise wide strong passwords across server platforms, a feature not available in NIS or OS local authentication.

Centralized Sudo Policy Management
Once a user or administrator is being authenticated to a server, it is important to manage and audit authorization for privileged users to execute programs or batch jobs.

Privileged user management via sudo (‘superuser do’) is widely used with Unix and Linux to restrict program and data access. Traditionally, sudo policies are managed and stored locally on the machine, which results in similar challenges as locally managed accounts – high administration cost and inconsistent policies. The latest sudo version supports LDAP directories as data storage, however they have to be configured first. Oracle Authentication Services for Operating Systems provides the required sudo directory schema support out of the box to enable centralized sudo policy management and consistent authorization policies across heterogeneous enterprise.

High scalability, availability, and security
Oracle Authentication Services for Operating Systems leverages OID as the key solution component and inherits all OID scalability, availability, and security features:

- Oracle Internet Directory is a high available and scalable directory based on the Oracle database. An OID benchmark testing two billion entries delivered the unmatched performance of over 100,000 operations per second with average latency of 2.5 ms.
Oracle Internet Directory provides multiple layers of security to protect sensitive data. The first layer of security is the built-in access control framework in the LDAP protocol that protects sensitive data like passwords. The next layer of protection is the integration with Oracle Database Vault whereby identity data in the database is protected from being read or modified by database administrators. The third security layer involves applying Transparent Data Encryption to the database thus securing the physical data from unauthorized access, in case a backup media gets lost.

Oracle Enterprise Manager can be leveraged for enterprise-wide monitoring and administration for enterprise-wide of OID, database and servers. Thus providing a one-stop system management center.

CONCLUSION
Access to operating systems should be centrally managed and audited due to its sensitive nature. Oracle Authentication Services for Operating Systems enables cross-platform storage, management, and authentication of users using open standards, simplifies deployment, and enhances operating system security. Additionally, operating system identity management should be an integral part of enterprise identity management framework, not a separate silo. Oracle Authentication Services for Operating Systems is a component of Oracle Identity Management suite, the industry-leading identity management suite that delivers a total identity management and access control solution for enterprises with lower total cost of ownership (TCO). Oracle Authentication Services for Operating Systems can be used with other Oracle Identity Management components for more comprehensive deployment. For example, Oracle Identity Manager complements the solution by provisioning Unix/Linux users to the directory with workflows and approval process.