IMPROVING COMPLIANCE AND EFFICIENCY WITH SUN IDENTITY AUDITING

and Other Sun Identity Management Capabilities

Sun-on-Sun Case Study
January 2008

Abstract

Faced with increasing compliance requirements and related challenges since the passage of the Sarbanes-Oxley Act of 2002 and other regulations governing data integrity and privacy, Sun and its alliance partner Deloitte & Touche LLP (Deloitte & Touche) deployed Sun Java™ System Identity Manager and Java System Identity Auditor software to improve Sun's processes related to user account management and access controls and to achieve operational efficiencies. This paper recounts the process from solution criteria and selection through planning and deployment, and describes the benefits that have resulted for both Sun and its customers.

Table of Contents

Executive Summary **1**

Challenges: Regulatory Compliance and Operational Efficiency **2**

Regulatory compliance 2

Operational efficiency 3

Solution Criteria and Selection **4**

Suitability of Sun identity management for the project 4

The Implementation Process: Planning and Deployment **6**

Planning 6

Deployment 7

Results and Benefits to Sun and Sun Customers **11**

Sun end users and management 11

Sun customers and prospective customers 11

Conclusion **13**

About Sun 13

Chapter 1

Executive Summary

Like any public company operating today, Sun must comply with the Sarbanes-Oxley Act of 2002 on an ongoing basis, including having sufficient controls on the monitoring and enforcement of user access to critical business applications and systems. These expectations include enforcement of segregation of duties, minimizing the distribution of superuser privileges, and having managers conduct periodic access reviews of user entitlements. These requirements are a must-have for complying with Sarbanes-Oxley, in addition to bringing value to the organization through improved operational efficiency, decreased risk for fraud, and cost reductions that can result from streamlined management of user entitlements.

Sun Microsystems, in coordination with systems integrator Deloitte & Touche, deployed products from the Sun identity management portfolio to address Sarbanes-Oxley compliance, specifically with regard to reducing excessive access and enforcing segregation of duties among end users. The goal was threefold: to prevent conflicts of interest, to protect the security and privacy of sensitive application information, and to maintain the integrity of transactions.

Today, this deployment of Java System Identity Manager and Java System Identity Auditor software enables Sun to manage 50,000 user identities in 160 countries and plays an important role in Sun's compliance with Sarbanes-Oxley. In addition, the deployment successfully addresses costly inefficiency issues associated with provisioning resources for Sun users.

This paper provides an in-depth discussion of the:

- Challenges driving the decision to deploy an identity management solution
- Criteria for selecting Java System Identity Manager to address the challenges
- Planning and deployment processes associated with the project, including the role of Deloitte & Touche as Sun's system integrator
- Results for Sun — and for Sun customers who will benefit from Sun's experience

Chapter 2

Challenges: Regulatory Compliance and Operational Efficiency

Sun uses a number of Oracle E-Business Suite modules to handle business processes, including: GL, AP, AP, PO, Inventory, WIP, Project Accounting, and System Administration.

It's not unusual for a large enterprise to have multiple enterprise systems in place to carry out various operational functions, and Sun is no exception. To address Sun's initial focus of Sarbanes-Oxley compliance, the first phase of Sun's identity management deployment was focused on supporting the company's human resources (HR) systems as well as Oracle 10.7 and Oracle 11i-based systems, which handle key business processes. These systems support a significant portion of Sun's financial reporting processes, so they were key to addressing the company's Sarbanes-Oxley objectives. Subsequent implementation phases will extend this deployment to address other elements of Sun's information technology environment.

With the passage of Sarbanes-Oxley and the explosion of network usage in the early 2000s, having multiple enterprise systems created a twofold challenge for Sun: ensuring that user-access privileges across systems complied with Sarbanes-Oxley, and getting users of the systems provisioned quickly and efficiently.

Regulatory compliance

Prior to implementing Java System Identity Manager software, Sun relied on manual quarterly auditing processes to detect excessive or inappropriate access to resources. This created several potential risks for the company, including the possibility that inappropriate access would remain undetected until the next quarterly audit, or that some managers might not complete their quarterly audits. The manual approach also made remediation more time consuming and less likely to be completed. Sun realized that to have a sustainable approach to compliance, the organization needed a control system that would provide efficiency, auditability and repeatability.

To address the situation, Sun first needed a single source of user provisioning and access control functionality. A single view of access privileges for each user would provide insight into the privileges within each system, allowing for efficient cross-application checking to detect potential segregation-of-duties problems across the user's entire access profile. Second, the company needed to automate provisioning and access control processes so that potential violations could be detected and appropriate action taken automatically and immediately.

Operational efficiency

Slow, inefficient provisioning processes presented an operational challenge for Sun. Not only did it take time to detect excessive or inappropriate access, it also took time for provisioning and access changes to take effect. This was because whenever a user's role changed, updates from HR to the enterprise directory had to be done in batch process — which meant that the entire data set had to be read to determine what had changed in comparison to the last time the update process had been completed. This approach required a number of ad hoc, nonstandard processes, and forced users to wait longer than necessary to get the access they needed to start making productive contributions in their new roles.

Sun needed to find a way to compress the time and effort required to change a user's account access in response to a change in the user's roles. Automating the processes associated with creating, updating, and deleting user accounts would accomplish this goal. To further increase efficiency, the company also needed a single system that could do this across applications.

Chapter 3

Solution Criteria and Selection

To manage regulatory compliance and improve operational efficiency, Sun defined the following parameters for a technology solution. The solution had to:

- Accelerate the processes for provisioning users (for example, adding new access and removing access) when their roles within the organization change. This would reduce the potential risk for excessive or inappropriate access and enable greater operational efficiencies.
- Establish a single, centralized point of control over user access to resources, and provide a single view into that access to facilitate compliance.
- Be operable across disparate systems, to enable extending the solution to support additional systems.
- Offer ease of deployment into the Oracle 10.7 system and other legacy systems with no system reconfiguration, new APIs, or additional software. This would minimize the investment and time required to implement the solution.
- Enable managers and application owners to conduct periodic access and certification reviews.
- Be able to automate the process of remediation, collaboration, and escalation to resolve potential segregation-of-duties conflicts.
- Perform checks proactively for potential segregation-of-duties conflicts and excessive superuser access.
- Provide reports for managers, administrators, and executives.

Suitability of Java System Identity Manager for the project

Java System Identity Manager and Java System Identity Auditor software modules were chosen for the following reasons:

Required functionality

Sun determined that the comprehensive portfolio of Sun identity management products delivered all the functionality to serve as the system of record for multiple systems. Java System Identity Manager functionality includes user provisioning, authorization, and authentication, with extensive identity auditing capabilities for preventing, detecting, and remediating inappropriate access.

Automated operations

Java System Identity Manager uses automation to speed provisioning processes, eliminating potential lag time between the occurrence of a potential violation and its detection. The automation of provisioning, auditing, and other functions also eliminates the need for manual processes, which are slower and less efficient than automated processes.

Centralized control and visibility

All user-access processes — from provisioning to identity auditing — are managed from a single central point. This dashboard delivers a summary view of compliance metrics and displays violations, exceptions, and anomalies.

Interoperability

Java System Identity Manager is a standards-based, cross-platform product that operates with leading operating systems, enterprise applications, databases, message platforms, and other key business resources. This facilitates expansion of the identity management system to support user-entitlement management for virtually any platform in the Sun organization.

Noninvasive architecture

Java System Identity Manager includes more than 60 resource adapters that can be used to connect to external resources (applications, operating systems, and more) without deploying additional software on these resources. This noninvasive, agentless approach to connecting with resources significantly reduce the effort required to roll out the identity management solution.

Even though more than 60 resource adapters are available, when older legacy systems are involved, it's not unusual for a new one to need to be developed. Once developed, the new resource adapter is added to the existing set for use by other organizations. In this deployment, a resource adapter was needed for the legacy Oracle 10.7 system. This was included in the scope of work for the project.

Market leadership

In addition to meeting all the functional requirements of the organization, Java System Identity Manager came with a long track record of successful implementations in large enterprise environments. In addition, Java System Identity Manager — specifically, its provisioning capabilities — had been singled out as industry-leading by a number of analysts and observers, including Forrester Research and Gartner.

Chapter 4

The Implementation Process: Planning and Deployment

Planning

There were four major steps involved in planning for the implementation of Java System Identity Manager software.

Step 1. Formalize project requirements.

The first step in planning the implementation was to establish the high-level requirements for addressing compliance and operational efficiency:

- Real-time, nonbatch provisioning of user accounts from HR to Sun's enterprise directory
- Automated provisioning, auditing, and reporting
- Automated checking for inappropriate access, particularly access with implications for potential segregation of duties
- Periodic access review processes by presenting a user entitlement report to appropriate managers

Step 2. Choose a system integrator.

Because of its previous experience with customers, Sun understood the importance of working with a system integrator. Given the complexity of identity management deployments, an experienced systems integrator can bring extensive deployment expertise and value-added services to bear to improve the potential for project success.

Based on numerous successful teaming experiences implementing Sun's identity management technology in complex Fortune 500 environments, Sun selected Deloitte & Touche as the system integrator for this deployment. In addition to addressing the requirements outlined above, Deloitte & Touche provided:

- A business-driven approach with its Identity and Access Management methodology (IAMethods), which establishes strategies to facilitate provisioning process reengineering, data-quality analysis and clean-up, project management, and organizational change management
- Strong technical implementation skills, including previous experience working with Sun to deploy new resource adapters, as reflected in Deloitte & Touche's extensive team of professionals experienced with Sun's identity management solutions
- A robust quality assurance and oversight framework, which is leveraged by all of Deloitte & Touche's project teams to enable successful deployments

Step 3. Define measurable points to ensure that project stays on target.

The most important consideration at this stage is project sizing. To define a realistic target time frame for completion, it's critical to take into account any factors that could significantly affect the timing and costs of the project. In this case, the complicating factor was the development of a new resource adapter for connectivity with the Oracle 10.7 system. For other companies, it could be anything from the need for custom integration points for resources to the existence of highly complex business rules or workflows.

Step 4: Plan for development, testing, and implementation of new resource adapter.

Because Sun identity management products have a large number of readily available resource adapters, most deployments don't find it necessary to develop an entirely new resource adapter from scratch. However, with Sun's identity management deployment, it made more sense to keep the existing Oracle 10.7 legacy system in place and create a new resource adapter for this system to minimize business disruption. The alternative was to replace the Oracle 10.7 system and upgrade to a more recent Oracle release that had a readily available resource adapter.

This same approach could also be used by organizations that have an internally developed, enterprise-specific application or resource whose functions can't be duplicated by a more widely available system. Rather than sacrifice important functionality by replacing the custom system, an organization in this position can instead simply have Sun or the system integrator create a new resource adapter to support such custom or legacy systems.

Deployment

To facilitate this deployment, Deloitte & Touche's utilized its IAMethods deployment methodology. IAMethods is based on Deloitte & Touche's long history of successful implementations of identity management solutions.

Deployment activities set out in the IAMethods methodology include:

- Inception
  - Defining the project scope to clarify current state and desired future state
- Elaboration
  - Analyzing the requirements to develop them into complete sustainable statements
  - Designing the solution architecture and developing a strategy to implement it efficiently

- Construction
  - Configuring the solution and installing it in development and test environments
  - Verifying that the system is operating as required
- Transition
  - Deploying the system into the production environment
  - Transferring control from the deployment team to the operational support team

Project roles

Following the approach established in Deloitte & Touche's IAMethods methodology, Sun assigned the following personnel to the project:

- *Project manager*, responsible for day-to-day project decisions in collaboration with the systems integrator's project manager
- *Project sponsor*, responsible for setting business objectives for the project, overseeing change requests, and serving as the escalation point for project delays or issues
- *Executive sponsor*, responsible for overall project authorization and for making financial commitments
- *Identity management technical lead*, responsible for understanding the technical implementation objectives and providing the system integrator's technical specialists with access to subject matter experts within Sun
- *Technical administrator*, responsible for maintaining the implementation according to the product documentation
- *Change management lead*, responsible for integrating the project with Sun's existing change control processes to improve quality and mitigate risk from design through transfer into production

In addition to the core members described above, the team included end users who would ultimately be users of, and affected by, the system. Their experiences were critical in the inception and elaboration stages of implementation, when key decisions were made about how provisioning and deprovisioning would occur. Also, because the development of a new resource adapter would be an important part of the project, the engineering team that originally created the resource adapters for the Sun identity management portfolio were engaged to take advantage of their special expertise.

Proof of concept

To show that Sun identity management could be up and running quickly, and that it would provide a workable solution, a proof of concept was done early in the implementation process to demonstrate connectivity between HR identity information and the enterprise directory. This established credibility for the project early on and smoothed the way for procuring funding.

Major challenges

There were three major challenges associated with the construction and transition stages of the implementation.

- *Creating the custom resource adapter* for the legacy Oracle 10.7 system was one of the greatest challenges of the implementation, largely because the system was so old and required extensive research and analysis to make decisions about how best to connect to it. Time was built into the implementation schedule to define and figure out how to resolve any problems that might be associated with development of the new adapter.
- *Testing of the resource adapter* turned out to be an even greater challenge than development. This was primarily due to a lack of clarity about who was responsible for what aspects of testing — the system integrator or Sun. The experience underscored the importance of developing a scope of work that contains sufficient detail about division of responsibilities.
- *Validating the automated segregation-of-duties check* within Java System Identity Auditor for use with Oracle 11i. Deloitte & Touche's experienced Oracle engineers provided deep technical insight into Oracle's forms-level access rights.

Project turnaround

The turnaround for the project was longer than many of the same type due to the Oracle 10.7 resource adapter development aspect of the process, which required strong collaboration between Deloitte & Touche developers, Sun business users, and Sun product engineers. Once this custom development effort was completed, adding resources took less than a month.

The project was deployed in phases, with more resources added three months after the internal rollout and another set of resources added one month after that to complete the implementation. As of the time of publication of this paper, Sun had ten Oracle resources deployed using resource adapters for Oracle 10.7, 11i, and 11.03 applications.

Project architecture

The following diagram illustrates Sun's implementation of Java System Identity Manager and Sun Java System Identity Auditor software. Provisioning requests for Oracle 11i and Oracle 10.7 resources coming in from multiple sources are automatically checked for potential segregation-of-duties conflicts before the requests are granted. HR identity information is updated in near real-time instead of in batch process, dramatically improving the speed and efficiency with which provisioning requests can be granted.

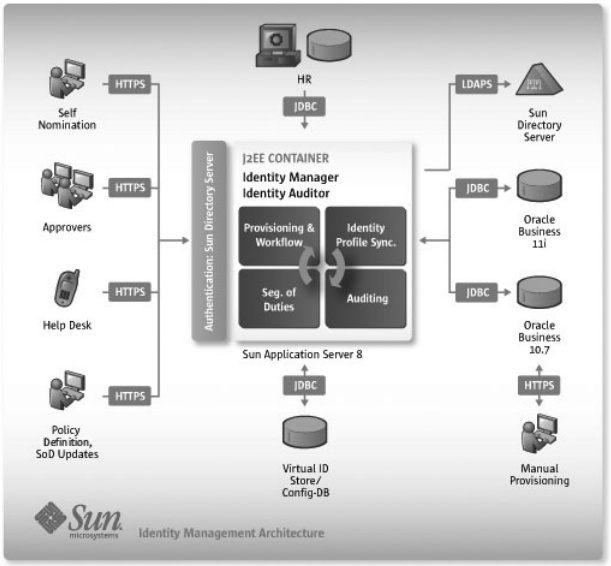

Figure 1. Sun identity auditing and other identity management capabilities

Chapter 5
Results and Benefits to Sun and Sun Customers

Sun end users and management

With this deployment of Java System Identity Manager and Sun Java System Identity Auditor software for provisioning and auditing, Sun achieved its goals for compliance and efficiency.

Compliance

Java System Identity Manager is now making it possible to easily prevent and detect compliance violations among end users — violations that could have been overlooked if provisioning and auditing processes continued to be conducted manually. Now, the person responsible for approving a provisioning request immediately receives a full analysis that shows whether approval will violate segregation-of-duties controls. This is the result of the identity management solution providing comprehensive visibility into user access privileges whenever access requests are submitted. Users are also automatically deprovisioned from the Oracle applications whenever their employment terminates or if they fail to use the application within any six-month period.

Efficiency

Sun is now seeing faster update cycles when changes are made to end users' identity data. Changes take effect in the enterprise directory in 10 to 20 minutes — and frequently in less time. For those who are responsible for reviewing and approving access requests, the process takes two or three minutes instead of 15 minutes. The implementation also enables greater efficiency, enabling employees to get up and running with new responsibilities more quickly. And it greatly reduces the risk of human error in the process.

Sun customers and prospective customers

Post-project review is a formal part of Deloitte & Touche's IAMethods methodology. After all deliverables have been completed, Deloitte & Touche and Sun personnel involved with the deployment took stock to determine lessons learned and to capture best practices resulting from this deployment. This practice can result in significant benefits for current and future customers.

In this case, the post-project review identified the following insights:

Improving compliance-related processes

Sun is hardly unique in the need to comply with Sarbanes-Oxley. To help customers improve their compliance processes, lessons learned from this implementation have now been built into the production environment for Sun's customers. For example, it became increasingly apparent that provisioning users and auditing their access were closely related processes, suggesting it could be extremely advantageous to integrate these two distinct capabilities. As a result, Sun now offers these capabilities together in one product rather than as two separate identity management offerings.

Enabling easy connectivity with Oracle 10.7

Even though Oracle 10.7 is a relatively old version of the Oracle E-Business Suite, it's still widely used in many enterprises. Now, customers who want to establish connectivity from Java System Identity Manager to Oracle 10.7-based systems have a resource adapter available to provide them with connectivity right out of the box. This resource adapter joins the more than 60 others that are already available for connecting with a variety of operating systems, applications, and other enterprise resources.

Chapter 6

Conclusion

Sun has demonstrated through its own experience that Sun Java System Identity Manager can:

- Enable enterprises to create a more efficient and compliance-friendly environment for provisioning and auditing
- Adapt easily to legacy systems, so that organizations can achieve compliance and efficiency goals without the expense and disruption of switching to new systems
- Be deployed in a timely fashion with the assistance of expert and experienced Sun system integrators such as Deloitte & Touche

Sun Java System Identity Manager has proven to be an outstanding choice for improving compliance and increasing efficiency in its own operations, and one that will benefit other organizations that face similar challenges.

About Sun

A singular vision, The Network is the Computer™, drives Sun in delivering industry-leading technologies that focus on the whole system — where hardware, software, and services combine. With a proven history of sharing, building communities, and innovation, Sun creates opportunities, both social and economic, around the world. You can learn more about Sun at sun.com.

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA **Phone** 1-650-960-1300 or 1-800-555-9SUN (9786) **Web** sun.com

SunWIN# 502178 Lit.# SWWP12615-1 01/08