

PRODUCT FLASH

IBM's Tivoli Identity Manager v5.1 with Integrated Operational Roles Management

Sally Hudson

IN THIS PRODUCT FLASH

This IDC Flash looks at IBM's latest upgrade to its Tivoli Identity Manager (TIM), and examines it in the context of market demand for enterprise compliance and security. TIM v5.1 is designed to reduce costs, manage risks, and enable secure collaboration as part of IBM's overall Dynamic Infrastructure initiative.

SITUATION OVERVIEW

IBM Tivoli was the worldwide IAM revenue market leader in 2006 and 2007, and once again it leads the list in license and maintenance revenue for IAM software suites in 2008. The company offers enterprise customers a full suite of IAM products, with Tivoli Identity Manager (TIM), Tivoli Access Manager (TAM), and Resource Access Control Facility (RACF) successfully deployed in many large and medium-sized IT organizations worldwide. IBM products are available on a wide range of platforms and operating systems, including PCs, Unix, and mainframes.

The latest release of TIM, 5.1, is designed to help organizations administer, secure, monitor, and certify user identities and their access to applications, information, and systems. Release 5.1 provides customers with operational role management capabilities to assist with a deeper and more granular level of user access management as well as greater visibility and control over their access rights.

Features of TIM 5.1 include:

- ☒ **Role management:** Simplifies user administration through the use of an enterprise role structure that governs user access to resources
- ☒ **Group management:** Simplifies and reduces the cost of user administration
- ☒ **Separation of duties:** Helps in preventative and detective analysis of role and permission conflicts
- ☒ **Access certification:** Provides ongoing review and validation of user access

These capabilities add to the integrity of the risk management profile of the organization while significantly enabling the ability to meet ever-increasing regulatory and compliance requirements. Roles have become more sophisticated in terms of both their capabilities and their deployment, and entitlement management can be used to further reduce the complexity of the roles definition process. TIM v5.1 should increase the level of manageability while increasing security by extending more control around access rights within enterprise organizations. IBM rounds out its offerings in the identity space with entitlement management capabilities within Tivoli Security Policy Manager, and privileged identity management (PIM) is provided by Tivoli Compliance Insight Manager (TCIM). TCIM is integrated with TIM and included in the Tivoli Identity and Access Assurance solution, along with TIM and other solution elements. In addition, IBM ISS does have a privileged identity management services offering that is based on TIM. IDC believes that a significant portion of the insider threat problem can be alleviated by utilizing a privileged identity management platform within an overall IAM solution. Enterprise organizations must look at PIM as an essential step in achieving and maintaining overall health in governance, risk, and compliance (GRC), as well as an integral source of the security of the internal organization on a continual basis.

FUTURE OUTLOOK

Compliance is the driving factor for up to 85% of all IAM purchases in 2008, and we see this trend continuing in 2009. There is now a universal demand for corporate compliance. In light of the banking, financial, and manufacturing crisis, we believe that compliance regulations will increase, not decrease, over the next several years. The ability to track user rights and privileges as well as combat authorization drift is an integral part of a strong compliance program.

Organizations must move from a reactive compliance stance to proactive, cost-effective information protection and control. This means that enterprises must go beyond the minimum requirements of regulatory compliance to internal policy compliance at a higher level of assurance. The ability to perform automated checks in advance of auditing, to report on a regular basis, and to monitor employees and discern behavior patterns to stop malicious and noncompliant actions before they occur requires that steps be taken to achieve proactive and effective cost management.

IBM has underscored its commitment to IAM and GRC, with announcements for closed loop identity and access management as well as the v5.1 enhancements to its current product line.

Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or Web rights. Visit us on the Web at www.idc.com. To view a list of IDC offices worldwide, visit www.idc.com/offices.

Copyright 2009 IDC. Reproduction is forbidden unless authorized. All rights reserved.

Filing Information: July 2009, IDC #219175, Volume: 1, Tab: Vendors

Security Products: Product Flash