Service management
White paper

Tivoli® software

Manage access control effectively across the enterprise with IBM solutions.

July 2008

Contents

Overview

This white paper discusses current requirements and new products for developing access control solutions that can help demonstrate compliance, provide proper information access and enhance security across today's heterogeneous environments.

The discussion covers recent trends in single sign-on (SSO) solutions and today's requirements for application security, including identity management, message-level security and protection against both external threats and internal user activities. In addition, the paper will explore how IBM Tivoli® Access Manager software and other IBM offerings can help organizations securely manage access to business-critical applications and data while giving users proper access to the information they need.

Understand today's requirements for developing effective access control

To help demonstrate compliance, organizations face a number of critical requirements for access control. First of all, disclosure rules should be implemented and enforced consistently across the enterprise to help protect data and applications access policies. This can be particularly challenging since today's IT infrastructures invariably support a number of heterogeneous applications, data sources and operating systems.

At the same time, access control solutions should demonstrate, report and audit the effectiveness of IT security controls in terms of the following questions:

- Who has access to applications and databases?
- What data — both structured and unstructured — resides in files, databases and other data stores?
- Who actually needs access to that data?
- What access controls should be established as a result?

Highlights

Finally, an access control solution should address all stages of the user identity life cycle, including correct access permissions, the enforcement of access control policies, the ability to correct any attempts to modify security policies or user permissions, and final account retirement.

Identify current trends in SSO solutions

To address the rigorous requirements of access control, organizations have introduced password protection for applications. However, each application often requires its own password and user name. For users, trying to remember and manually enter these passwords and user names – many of which need to be changed on a regular basis – can lead to frustration, lost productivity and even compromised security when passwords are not kept in a secure location.

Organizations are now implementing enterprise-wide, modular SSO at the desktop, across the Internet, across heterogeneous environments and among federated entities as an integral part of their access control solutions

As a result, organizations are now implementing enterprise-wide, modular SSO at the desktop, across the Internet, across heterogeneous environments and among federated entities as an integral part of their access control solutions.

With SSO solutions such as IBM Tivoli Access Manager for e-business, users only need to authenticate once for access to most applications, improving the service experience. Tivoli Access Manager for e-business can also contain help-desk costs by lowering the number of password reset calls and reducing the time lost by users who are locked out of systems.

With Web SSO solutions such as Tivoli Access Manager for e-business, employees, contractors and external users need to authenticate only once for access to most applications, helping to improve productivity and to authorize their access to business-critical applications. IBM Tivoli Access Manager for Enterprise Single Sign-On helps end users simplify their password management and provides desktop SSO to Web and non-Web applications. The IBM solution can also contain help-desk costs by helping to lower the number of password reset calls and to reduce the time lost by users who are locked out of systems. Applications supporting sensitive information can also deploy strong authentication mechanisms such as biometrics and smart tokens.

Highlights

Tivoli Federated Identity Manager is an application security software that offers modular federated SSO and Web services/SOA identity mediation services designed to simplify application integration using many forms of user credentials and facilitate the secure sharing of information between trusted parties, such as business partners or separately managed divisions within an organization operating in an SOA environment

Many SSO solutions are limited to one or two environments. However, IBM solutions support integrated SSO across multiple environments such as Java™, Microsoft® .NET and mainframe. These solutions can also provide federated identity management that allows a user from one federation partner to seamlessly access resources from another federation partner in a secure and trustworthy manner.

As one example, IBM Tivoli Federated Identity Manager delivers cross-domain or federated SSO as well as identity propagation in service oriented architecture (SOA) and Web services environments. The result is a flexible yet powerful solution that enables trusted and auditable partner interactions while helping to address key compliance concerns related to partner access from other domains.

Review recent developments in application security

Application security is another requirement for effective access control, and today's solutions address this requirement at a number of levels.

The first level is upfront filtering and identity management – in essence, "letting the good guys (and services) in and keeping the bad guys out." Tivoli Access Manager for e-business lets organizations manage user entitlements in alignment with their corporate security policy. To enforce compliance with these policies, access policy can be designed to manage user entitlements to specific services or applications. In addition, IBM Managed Protection Services provide a wide range of firewall, intrusion prevention, anti-virus, anti-spam, content security and virtual private network (VPN) capabilities.

Proper identity management also includes the activities of privileged or "super users," many of whom have unlimited access to critical legacy and business application environments. IBM Tivoli Access Manager for Operating Systems provides fine-grained authorization management of UNIX® and Linux® root accounts, helping organizations address system vulnerabilities surrounding privileged users.

Highlights

WebSphere DataPower SOA appliances are purpose-built, easy-to-deploy network devices that can simplify, help secure and accelerate XML and Web services deployments, and extend the SOA infrastructure

Message-level security is another critical requirement for securing applications. IBM WebSphere® DataPower® SOA appliances are purpose-built, easy-to-deploy network devices that can simplify, help secure and accelerate XML and Web services deployments, and extend the SOA infrastructure. These appliances offer an innovative, pragmatic approach to harness the power of SOA while simultaneously enabling organizations to leverage the value of existing application, security and networking infrastructure investments. In addition, WebSphere DataPower SOA appliances can be fully integrated with a wide range of other IBM offerings, such as Tivoli Federated Identity Manager.

Explore entitlement management and context-based access control for improved compliance and Web 2.0 and SOA adoptions

For today's businesses, an increased focus on compliance and the need to secure access to information have resulted in a number of critical goals for application owners and IT security operations. These include establishing tighter access control, developing governance around the process of issuing and managing entitlements (what a user can specifically do with his or her access), and consistently enforcing roles-, rules- and attributes-based access to business-critical applications. Emerging standards — such as eXtensible Access Control Markup Language (XACML) — must be evaluated to implement a consistent application- and data-entitlement management solution.

Similarly, Web 2.0 technology enables and accelerates service delivery and collaboration within the enterprise and across the extended supply chain. SOA supports Web 2.0 activities and information sharing by loosely coupling applications and consolidating them into services.

The ability to implement context-based access control becomes more important with the increasing adoption of Web 2.0 composite applications (mashups) and software as a service (SaaS). Mashups are social, role-based, network-centric applications that combine information and services from multiple sources. They are essential to all knowledge-based networks, models and businesses. They can also dramatically enhance customer experience to drive productivity growth, support innovation and achieve fundamental advancements in knowledge-based competitiveness.

Highlights

Securing access to mashups, other new types of applications and SaaS can be improved by using additional user context for access control. Authorization and entitlement decisions should be managed by attributes such as data tags, as well as by rules- and roles-based evaluations of the user request.

Security will likely remain a critical issue for SOA environments as Web 2.0 continues to grow. According to the Burton Group, organizations wishing to secure their SOA environments should maintain access control through:

- Authorization to allow or deny transactions based on predefined policies.
- Authentication and integrity to help ensure that transactions originate from the correct SOA end point.
- Transformation to maintain a user's identity throughout the entire transaction.*

In the years ahead, Web 2.0 and SOA will continue to converge as the two most important organizing principles for enterprise software development. Organizations should develop flexible access control solutions that fully leverage the openness of Web 2.0 and SOA while helping to ensure security, compliance and proper governance.

Recognize additional, end-to-end security solutions from IBM

IBM can help organizations develop a fully integrated framework for security and compliance that can be expanded incrementally and strategically

IBM provides a portfolio of security solutions that is unsurpassed in the industry. With IBM, organizations can develop a fully integrated framework for security and compliance that can be easily expanded in an incremental, strategic manner as their needs evolve.

Solutions relevant to access control include:

IBM Tivoli Identity Manager, a security-rich, automated and policy-based user management solution to help effectively manage user accounts – along with access permissions and passwords – from creation to termination across the IT environment. Tivoli Identity Manager integrates with the Tivoli Access Manager family of products to provide effective identity and access management life-cycle capabilities.

IBM Rational® AppScan, a suite of automated Web application security solutions that scan and test for common Web application vulnerabilities. Rational AppScan provides intelligent fix recommendations and advanced remediation capabilities, such as comprehensive task lists necessary to fix vulnerabilities uncovered during the scan and improve an organization's overall security posture.

IBM Tivoli Security Information and Event Manager, a comprehensive solution that provides centralized log management, event correlation, a policy compliance dashboard and a reporting engine. Tivoli Security Information and Event Manager can also help protect intellectual property and privacy by auditing the behavior of all users – privileged and nonprivileged.

IBM Tivoli zSecure suite, a comprehensive solution for improving the productivity of mainframe security management, including administration, enforcement and auditing. With the Tivoli zSecure product family, organizations can establish effective processes to automate and simplify user administration, audit their environment's configurations and settings, and monitor changes and events. These capabilities can help maximize IT resources, reduce errors, improve quality of services and demonstrate compliance efforts.

IBM Classification Module, a part of IBM Enterprise Content Management (ECM) that automates the categorization of content through full-text analysis. With Classification Module, organizations can manage and control access to unstructured data such as e-mail, documents, presentations and graphics.

Conclusion

With Tivoli Access Manager software and other IBM offerings, organizations can leverage integrated, comprehensive access control solutions designed to:

- Enhance security with automatic password generation and password policy support.
- Support simple, consistent authentication across all systems, services and applications.
- Extend flexible SSO to Web-based applications spanning multiple sites or domains.
- Eliminate help-desk calls and other security problems associated with multiple passwords.
- Define and manage centralized authentication, access and audit policies for a broad range of business initiatives.
- Strengthen security through powerful password encryption and the elimination of poor end-user password behavior.
- Provide messaging security that protects information communicated across systems.
- Effectively audit application and platform activity to defend against malicious or fraudulent behavior by internal users and employees.

For more information

To learn more about Tivoli Access Manager and other IBM solutions for enhancing access control, contact your IBM representative or IBM Business Partner, or visit **ibm.com**/tivoli

About Tivoli software from IBM

Tivoli software offers a service management platform for organizations to deliver quality service by providing visibility, control and automation – visibility to see and understand the workings of their business; control to effectively manage their business, and help minimize risk and protect their brand; and automation to help optimize their business, reduce the cost of operations and deliver new services more rapidly. Unlike IT-centric service management, Tivoli software delivers a common foundation for managing, integrating and aligning both business and technology requirements. Tivoli software is designed to quickly address an organization's most pressing service management needs and help proactively respond to changing business demands. The Tivoli portfolio is backed by world-class IBM Services, IBM Support and an active ecosystem of IBM Business Partners. Tivoli clients and Business Partners can also leverage each other's best practices by participating in independently run IBM Tivoli User Groups around the world – visit www.tivoli-ug.org

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
July 2008

*Diodati, Mark. "Web Access Management Market 2007: Expanding the Boundaries," Burton Group, May 30, 2007

TAKE BACK CONTROL WITH Tivoli®

TIW14009-USEN-00