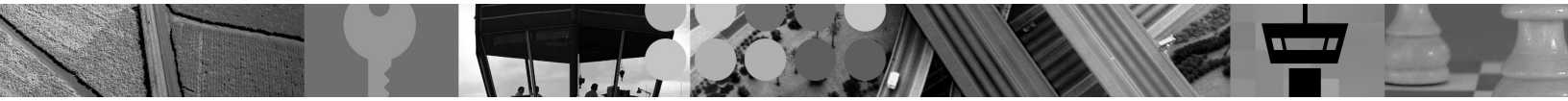
Security solutions
White paper

Tivoli® software

Succeeding with automated identity management implementations.



March 2007

Contents

Overview

Properly managing access to information has become a priority for today's corporations and a growing challenge. Many corporations require detailed auditing and reporting that shows exactly who accessed what, how and when, as well as who approved or granted user access. At the same time, IT organizations face increased pressure to contain costs and become more productive. And corporate mergers, acquisitions and other significant changes in the business can multiply these problems overnight.

To address these challenges, IBM Tivoli® Identity Manager provides a security-rich, automated, policy-based user management solution to help support security and compliance efforts, reduce IT administration costs, and increase user and IT efficiency.

When implementing an enterprise identity management solution, organizations should develop their implementation plan based on industry best practices in order to support two goals: a strategic, efficient process and an end result that meets the organization's needs. This white paper highlights best practices suggested by IBM and two IBM Business Partners, NetworkingPS and SecurIT, both with extensive histories of implementing successful solutions using Tivoli Identity Manager.

Understand how Tivoli Identity Manager addresses security challenges

In today's information-driven economy, ensuring that the right people have the right information at the right time is a key factor for business success. However, controlling access to this information through proper identity management is an ever-increasing challenge.

Highlights

Many corporations require detailed auditing and reporting that show exactly who accessed what, how and when, as well as who granted or approved the access. Furthermore, the costs and complexity of securely and efficiently managing access for a growing number of employees, customers, business associates and suppliers across multiple environments continue to climb.

This means that IT organizations – already stretched to the limit in terms of budget and resources – have to constantly find new ways to streamline operations and increase productivity through automation. And all of these problems can be multiplied overnight by corporate mergers, acquisitions and other changes in the organization.

A key element of IBM security management solutions, Tivoli Identity Manager is a security-rich, automated, policy-based user management solution

To address these challenges, IBM provides Tivoli Identity Manager, a security-rich, automated, policy-based user management solution. Designed as a key element of IBM security management solutions, Tivoli Identity Manager can help organizations:

- **Address policy compliance requirements** through centralized, policy-based access control, reports and audit trails across key information systems. The closed-loop automated user provisioning and reconciliation features of Tivoli identity Manager help ensure that accounts are set up properly and that updates are made according to the organization's security policy.
- **Reduce IT administration costs** by providing Web self-care interfaces to decrease help-desk calls; centralize control; provide local autonomy; and automatically manage accounts, credentials and access rights throughout the user life cycle.
- **Increase user and IT efficiency** by helping reduce turn-on time for new accounts and decreasing errors by automating user submission and approval requests.

Customers choose Tivoli Identity Manager to solve their enterprise identity management challenges because of the following attributes:

- **Proven scalability and performance —** Tivoli Identity Manager supports millions of users and has numerous customer success stories where high availability and performance are the keys to a successful identity management solution.
- **Out-of-the-box adapters —** IBM provides an extensive collection of full function adapters. IBM adapters adhere to a rigorous practice of supporting all pertinent user attributes on managed systems.
- **Easily customizable —** Quickly and easily extend Tivoli Identity Manager access to sources of identity data as well as downstream provisioning targets, by using the bundled IBM Tivoli Directory Integrator.
- **Supporting toolset —** Further extend your Tivoli Identity Manager product by using tools from IBM Tivoli Open Process Automation Library (OPAL). This online library contains product extensions (automation packages, integration adapters, monitoring solutions and development tools) developed by IBM and IBM Business Partners and is frequently updated with new tools from the field.
- **Policy simulation —** The Tivoli Identity Manager policy preview simulates the effect of policy changes on your environment before they are enacted, highlighting unintended policy changes or potential problems, and enabling these to be resolved before they affect live operations.
- **Closed-loop policy compliance —** IBM helps organizations ensure that user access privileges on managed systems remain compliant with enterprise security policy. If changes do not comply with policy, Tivoli Identity Manager can automatically instruct the managed system to roll back the changes or notify an administrator.

Requirements for a successful implementation

Identity management is a vital and complex technology issue that touches everyone in an organization, either directly or indirectly. Often the business processes and priorities, along with the owners of the information systems

and the user attributes that drive user identity and access information, are different across the organization. Furthermore, every organization is unique in its technology and business goals.

Integrating existing environments that are diverse and complex is no trivial task. But experience has shown that a realistic assessment of needs, resources and goals is the first step toward a successful implementation. Based on this assessment, a strategic plan can be deployed in a controlled manner and backed by the support of experienced deployment professionals, where required.

IBM and its partners' methodology for delivering integrated identity management solutions is tried and tested, based on industry standards, and built and refined through experience gained from hundreds of successful identity management implementations. It applies consistent, effective, sound security principles for developing complex enterprise solutions that address both business and technical requirements.

Recommendations gleaned from experience

IBM and two of its Business Partners, NetworkingPS and SecurIT, offer the following recommendations – based on recent Tivoli Identity Manager implementations. These recommendations represent a valuable, "real-world" perspective on identity management strategies, procedures and processes.

Ensure that all relevant department heads are fully engaged

Engage management across the organization, including human resources, the IT department and line-of-business application owners. Engagement across the organization usually requires a mix of education, cooperation and reassurance. The involvement of management can be critical for validating business drivers and requirements, as well as for mobilizing the organization for change.

Highlights

Senior managers must understand the necessity of the implementation, so they can lend their support, communicate the importance of the project and explain to their departments that the implementation is a requirement, not an option.

As you navigate the corporate terrain with this initiative, it will serve you well to understand the intricacies of corporate security and compliance office processes.

Explain the business case

To help encourage buy-in and foster the cultural adoption of new business processes, everyone should have at least a basic understanding of the business case for identity management. Potential benefits should be clearly articulated, including:

- Operational cost reductions for security and IT administration.
- Reduced cycle times to grant or remove access.
- Assistance with policy compliance requirements, including audit record capture.

Tivoli Identity Manager automates low-level administrative tasks, freeing IT professionals to address more strategic projects

Tivoli Identity Manager can automate mundane, low-level administrative tasks such as creating access rights – leaving IT professionals free to tackle more strategic projects that make better use of their talents and skill sets.

Set expectations throughout the project

From the very first project meeting, everyone should understand his or her role and the level of time and effort required to support that role. These roles should be reassessed regularly and often. Setting expectations in terms of results and timelines throughout the project helps everyone plan accordingly and avoid being blindsided by unexpected demands.

Assess specific user account needs

Planners need to ask specific questions regarding every stage of the user account life cycle. To show improvement in provisioning, how long does it take to provision access for users? Is user access configured correctly to every resource? Once provisioned, can users efficiently gain access to valid resources? Can administrators ensure that appropriate accounts are retired and that all remaining user accounts on each resource are valid? What are the various types of accounts a user needs? What account attributes need to be configured?

Once an organization has answers or objectives for these questions, it is important to show the results back to the sponsoring organization – to verify that they represent the correct goals for the identity management system.

After the requirements have been established clearly, businesses can leverage Tivoli Identity Manager to help enforce these types of policies, including handling reconciliation to ensure that system administrators have not changed any accounts that would be against the corporate policy. This feature is particularly useful when addressing requests that originate from audit and compliance initiatives.

Consider and weigh the implications of different approaches

Organizations can approach automated identity management in different ways depending on the priorities of the business. For example, some organizations cannot afford compromises in terms of operations, availability or performance,

while others can afford inconveniences more than they can afford high implementation costs. Here are two approaches to consider.

- **Focused approach:** provides deep coverage on a single application. This approach involves higher per-user and per-platform implementation costs, but it typically has a low impact on operational and maintenance resources while providing a showcase for future implementations.
- **Broad-based approach:** involves password management implemented for a large number of users. This approach can have greater impact initially on system owners and others, but the benefits are visible at an earlier stage to the organization.

Realistically, both approaches should be considered and even combined where appropriate, since each approach addresses different needs. Remember to focus on the business problem to be solved and its priority.

Start with a limited deployment that will provide an early return on investment

Due to the complexity, duration and cost of identity management initiatives, it can be politically and financially important to provide an early return on investment.

Help-desk cost reduction is an area where many organizations are focused. One opportunity for an early success is to leverage Tivoli Identity Manager for its user self-service capabilities. Allowing users to manage their own passwords and provide account request capabilities can significantly reduce end-user calls to your help desk, leading to early savings and improved end-user satisfaction. This quick win can help establish the importance and credibility of your identity management initiative.

Another valuable way to limit the scope of the initial deployment – but still see significant initial value at the beginning – is to implement identity management on existing tools and business processes rather than using a new application that requires training. For example, administrators may be more familiar with IBM Resource Access Control Facility (RACF®), or end users

Highlights

might make password updates that would be desirable when integrated into a central identity and access management repository. Tivoli Identity Manager adapters or password caching modules should be considered to help deploy a solution that can be used most effectively by end users and administrators.

Do not implement your identity management solution on all applications or business lines at one time — start with five or six top applications and become familiar with the process

Do not try to implement your identity management solution on all applications or business lines at one time. You should start with perhaps five or six top applications to gain rapid initial value from Tivoli Identity Manager and become familiar with the processes involved with centralizing and automating identity management. Then, add more applications as needed.

Take advantage of password synchronization

Leverage out-of-the-box Tivoli Identity Manager adapters for password synchronization from the Tivoli Identity Manager Lightweight Directory Access Protocol (LDAP) repository. This shows an immediate ROI and can set a positive tone with the organization as you attempt to increase the scope of your identity management project. It will serve as a strong foundation towards solving more complex identity and access management issues.

Document and examine existing processes to determine the potential impact of reengineering

In order to accurately assess the success of an identity management implementation, you must be able to compare the "before and after" scenarios in a real and meaningful way. To do this requires accurate and documented processes.

In addition, an identity management project provides a great opportunity for an IT organization to optimize and streamline its processes before they become automated. Are they efficient and effective? Do they require some level of reengineering? Automating a poorly designed process will lead to failure in terms of business value. Take this opportunity to examine your existing processes. Determine if they need reengineering before they become part of an automated solution.

Conclusion

While an organization might be tempted to cut corners to advance quickly, when it comes to identity management implementations, a "forklift change" can lead to problems that will undermine the overall initiative. An incremental approach – based on an understanding of the entire project scope – is typically best. Then you can build on your early successes.

This recommendation along with others described in this paper can help an organization:

- Develop a strategic identity management program that is considered a success by corporate management and end users.
- Foster and maintain support from a high-level management sponsor throughout.
- Contain the risk of cost overruns, missed deadlines and the need for rework.
- Provide a strong foundation for the future growth and evolution of security solutions.

For more information

To learn more about Tivoli identity Manager and other IBM security solutions, contact your IBM representative or IBM Business Partner, or visit **ibm.com**/software/tivoli/solutions/security

About NetworkingPS

Based in Piscataway, New Jersey, NetworkingPS is a professional services firm that specializes in planning, designing, assessing, implementing and supporting systems, applications and networks in multivendor environments. For more information, visit www.networkingps.com

About SecurIT

Since its inception in 1999, SecurIT has built a track record of successful identity and access management implementations throughout Europe. A qualified IBM Business Partner for Tivoli security solutions, SecurIT has developed a suite of software products that complements the strength of IBM Tivoli Access Manager and Tivoli Identity Manager. For more information, visit www.securit.biz

About Tivoli software from IBM

Tivoli software provides a comprehensive set of offerings and capabilities in support of IBM Service Management, a scalable, modular approach used to deliver more efficient and effective services to your business. Tivoli software enables you to deliver service excellence in support of your business objectives through integration and automation of processes, workflows and tasks. The security-rich, open standards–based Tivoli service management platform is complemented by proactive operational management solutions that provide end-to-end visibility and control. It is also backed by world-class IBM Services, IBM Support and an active ecosystem of IBM Business Partners. Tivoli customers 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
3-07

TAKE BACK CONTROL WITH **Tivoli.**

TIW10295-USEN-00