

IBM Tivoli Access Manager for Operating Systems

Highlights

- Defend against the top security threats that enterprises face: malicious and fraudulent behavior by internal users and employees
- Help achieve the safety of fine-grained authorization for UNIX and Linux systems, for both administrators and users
- Streamline management of heterogeneous UNIX and Linux systems with integrated, delegated administration
- Use extensible, configurable auditing capabilities to document compliance with government regulations, corporate policy and other security mandates
- Leverage best-practice security policy templates to help minimize implementation effort and time
- Take advantage of mainframe-class security and auditing in a lightweight, easy-to-use product

Meet today's security challenges

Employees — not hackers or viruses — present the greatest threat to IT security. Internal users account for the majority of cyber-theft and malicious damage to corporate systems. They know where the most valuable data resides and the times at which it is most vulnerable.

Well-meaning UNIX® and Linux® administrators can accidentally make your systems and business-critical applications vulnerable.

These administrators will often create back-door access routes that hackers frequently exploit.

Secure boundary defenses alone cannot provide adequate protection for your critical business systems. Attacks come in many forms, often exploiting weaknesses in applications and other high-level protocols. A common goal of these attacks is to obtain unrestricted “super-user” rights on the target systems.

To defend your systems and business-critical applications from these internal and external threats, your company needs a fine-grained, policy-driven security solution. Securing your server infrastructure with IBM Tivoli® Access Manager for Operating Systems is a critical step toward facilitating compliance with corporate security policy and regulatory requirements. It can provide fine-grained authorization — to file system resources, local and remote network services, login services, changes of user and group identity, and more. As important as it is to secure systems, it is equally important to audit compliance with security policy. Not only is auditing required by federal regulations and corporate best practices, auditing helps identify loopholes in the security policy. For example, by using Tivoli Access Manager for Operating Systems, auditors can determine if administrators are using their privileges appropriately. If there is any inappropriate activity, Tivoli Access Manager for Operating Systems allows security policy to be further restricted.

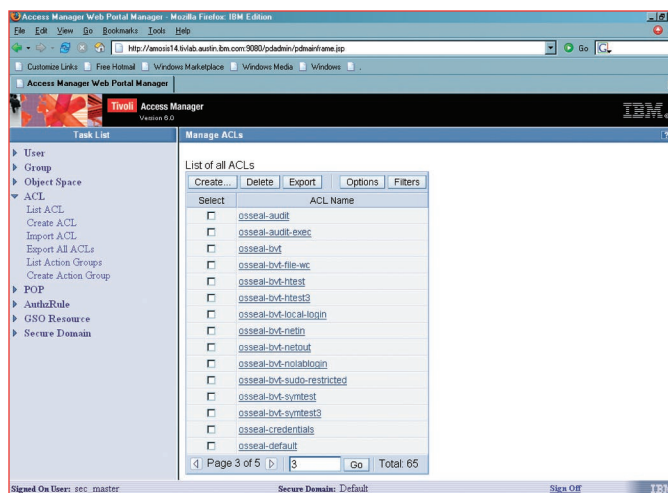
Address security consistently across the enterprise

IBM Tivoli software includes a comprehensive portfolio of identity and security management solutions. An integral component of this enterprise suite, Tivoli Access Manager for Operating Systems brings granular, user identity-based access control and auditing services to the UNIX and Linux operating system environments.

Shared components across the Tivoli security management portfolio provide consistent user interfaces and security models that an organization can use to help secure the varied resources within the enterprise. Consistent policy administration makes it easier for security administrators to define accurate and more comprehensive identity-based policies, and reduces errors that create security holes hackers and malware can target.

Tivoli security management software also leverages the innovative IBM Tivoli Common Auditing and Reporting Service to help simplify compliance with corporate policies and regulatory requirements. This common platform includes:

- Centralized audit data collection.
- Audit log management.
- Reporting features.



Tivoli Access Manager for Operating Systems provides an intuitive administrative user interface to help you define consistent, accurate security policy.

Help simplify security administration by using flexible tools

Tivoli Access Manager for Operating Systems includes Web Portal Manager, a GUI-based, Web-accessible management tool. This tool lets you manage security policy in a point-and-click format. Command line interfaces, script accommodation and APIs for C and Java™ provide UNIX and Linux experts with tools they can use to streamline and automate various management tasks.

Additionally, Web Portal Manager gives your security managers the flexibility to delegate limited authority for routine or emergency matters to local subdomain administrators or business units — without sacrificing control. In the case of network interruption, for instance, you can delegate control to local subdomain administrators without

granting them excessive access or access to other subdomains.

Tivoli Access Manager for Operating Systems also helps simplify administration by allowing you to group together UNIX and Linux systems that share specific security needs. You can then manage that set of resources as a group instead of managing each system individually.

Furthermore, the multidimensional policy management capabilities in Tivoli Access Manager for Operating Systems allow administrators to define access policy based on several different attributes of a resource. The result is that administrators can expend significantly less effort when dealing with similar resources and no longer need to manually synchronize policies across those resources.

Quickly establish best-practices security policy

When your enterprise is ready to quickly ramp up to effective security, you can use the Fast Track Policy Modules of Tivoli Access Manager for Operating Systems to ease customization. These prewritten, best-practice security policies come in application-specific versions to make it easy to tailor security policy for specific missions. What's more, you can use the Web Portal Manager to customize the best-practice policy templates to fit your unique needs.

For example, you might seek to enhance Web security or defend customer relationship management applications, enterprise resource planning applications, other applications and databases. Fast Track Policy Modules help you match your security policy to your business goals.

Flexibly audit security-related events

To facilitate compliance with your auditing requirements, Tivoli Access Manager for Operating Systems provides powerful, flexible auditing tools. You can use the software to maintain secure 24x7 audit logs on users, programs, files, ports, resources and systems. Administrators can use centralized reports of security events to review how and when certain users accessed resources.

The screenshot displays three overlapping windows from the Tivoli Access Manager for Operating Systems interface:

- General Audit Event History:** A summary window showing report details.

Report Date	08/11/2008
Report Time	01:41:06
Date Range	System Default
Begin Time(UTC)	08/11/2008 - 01:00:00
End Time(UTC)	08/11/2008 - 01:00:00
Maximum Number of Events	100
Event Type	All
Product Selected	All
Sort By	Timestamp

General Statistics
Total number of audit events: 100
- Audit Events By Event Type:** A summary table showing the count of events for each type.

Event Type	Number of Audit Events
audit_admin	61
audit_admin	41
- Event Log Table:** A detailed table listing individual audit events.

Event Type	Timestamp (UTC)	User	Process	Outcome	Event Reference ID
audit_admin	07/11/2008 01:00:00	root	sshd[sshd]	successful	751_151
audit_admin	07/11/2008 01:00:00	root	sshd[sshd]	successful	751_152
audit_admin	07/11/2008 01:00:00	root	sshd[sshd]	successful	751_153
audit_admin	07/11/2008 01:00:00	root	sshd[sshd]	successful	751_154
audit_admin	07/11/2008 01:00:00	root	sshd[sshd]	successful	751_155
audit_admin	07/11/2008 01:00:00	root	sshd[sshd]	successful	751_156
audit_admin	07/11/2008 01:00:00	root	sshd[sshd]	successful	751_157
audit_admin	07/11/2008 01:00:00	root	sshd[sshd]	successful	751_158
audit_admin	07/11/2008 01:00:00	root	sshd[sshd]	successful	751_159
audit_admin	07/11/2008 01:00:00	root	sshd[sshd]	successful	751_160
audit_admin	07/11/2008 01:00:00	root	sshd[sshd]	successful	751_161
audit_admin	07/11/2008 01:00:00	root	sshd[sshd]	successful	751_162
audit_admin	07/11/2008 01:00:00	root	sshd[sshd]	successful	751_163
audit_admin	07/11/2008 01:00:00	root	sshd[sshd]	successful	751_164
audit_admin	07/11/2008 01:00:00	root	sshd[sshd]	successful	751_165
audit_admin	07/11/2008 01:00:00	root	sshd[sshd]	successful	751_166
audit_admin	07/11/2008 01:00:00	root	sshd[sshd]	successful	751_167
audit_admin	07/11/2008 01:00:00	root	sshd[sshd]	successful	751_168
audit_admin	07/11/2008 01:00:00	root	sshd[sshd]	successful	751_169
audit_admin	07/11/2008 01:00:00	root	sshd[sshd]	successful	751_170

Tivoli Access Manager for Operating Systems allows auditors to easily customize and run reports across domains and even on privileged root users.

The secure collection and management of audit data is also critical to easing compliance with corporate security policy and regulatory requirements. Consequently, Tivoli Access Manager for Operating Systems integrates with the Tivoli Common Auditing and Reporting Service. When audit log data is collected from a variety of sources, it is easier to manage and report on audit data.

Bring identity management to super-user accounts

Unmonitored super-user (or “root”) accounts are notorious for opening the door to misuse. The shared use of root accounts by multiple people exacerbates vulnerability and accountability problems inherent in UNIX and Linux systems. Tivoli Access Manager for

Operating Systems responds to this threat by offering user-based controls for UNIX and Linux super-user accounts that help prevent the accidental or deliberate misuse of applications and data.

The software tracks and logs the activities of the individual users who use these root accounts. Because even a super user cannot modify the software’s audit logs to remove traces of their actions, your organization can reliably record and monitor the activities of the privileged users in your environment.

Unlike competitive offerings, Tivoli Access Manager for Operating Systems provides these controls without adding the administrative burden of changing your business processes.



Administrators can continue to perform their duties without changing their operational procedures. Protection applies whether users access the system resources directly through the operating system or through a command shell or application. The multithreaded design of Tivoli Access Manager for Operating Systems adds this rigorous security without impeding applications or impacting the user experience.

For customers who require complete awareness of changes to certain critical programs, Tivoli Access Manager for Operating Systems provides the ability to define them as being part of a trusted computing base (TCB). Files that are members of the TCB are monitored for changes to the file's signature. If Tivoli Access Manager for Operating Systems detects that the integrity of a program defined in the TCB is compromised, it records that the program is "untrusted" and does not allow an "untrusted" program to be executed until an administrator explicitly retrusts it.

About Tivoli software from IBM

Tivoli software from IBM helps organizations efficiently and effectively manage information technology (IT) resources, tasks and processes in order to meet ever-shifting business requirements and deliver flexible and responsive IT service management, while helping to reduce costs. The Tivoli portfolio spans software for security, compliance, storage, performance, availability, configuration, operations and IT life-cycle management, and is backed by world-class IBM services, support and research.

For more information

To learn more about Tivoli security management solutions and integrated solutions from IBM, contact your IBM sales representative or IBM Business Partner, or visit ibm.com/tivoli/solutions/security

© Copyright IBM Corporation 2006

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

Produced in the United States of America
4-06
All Rights Reserved

IBM, the IBM logo and Tivoli are trademarks of International Business Machines Corporation in the United States, other countries or both.

Linux is a trademark of Linus Torvalds in the United States, other countries or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries or both.

Other company, product and service names may be trademarks or service marks of others.