Tivoli software

# IBM Tivoli Access Manager for Operating Systems

## Highlights

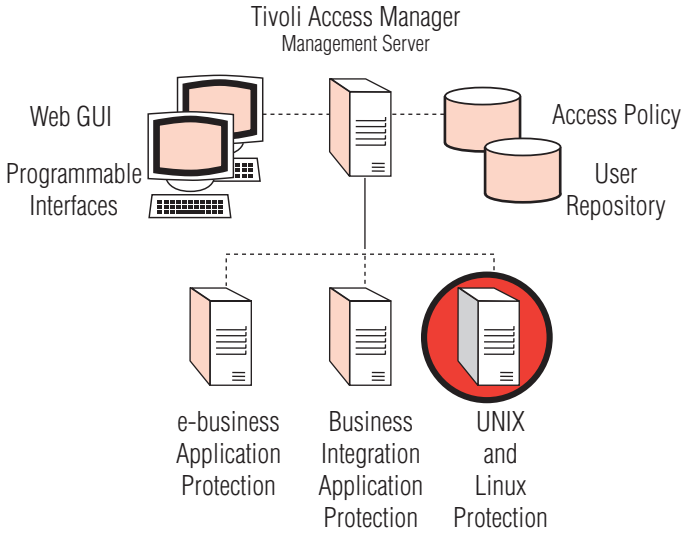
- ***Provides mainframe-style security for UNIX and Linux systems in a low-overhead design***
- ***Provides access control to a variety of resources for all user levels, including root***
- ***Enhances auditing of security-related events***
- ***Promotes consistent security policy across multiple UNIX and Linux platforms***
- ***Integrates with other Tivoli applications from IBM, sharing data and user interfaces***

### A comprehensive and centralized solution

IBM® Tivoli® Access Manager for Operating Systems provides a centrally administered solution to help prevent unauthorized access to your UNIX® and Linux® systems. With a single solution, you can help increase the integrity of your systems and improve the efficiency of your access management. You can also avoid the cost of implementing different techniques for operating systems from different vendors. Easy integration with IBM Tivoli Access Manager for e-business and IBM Tivoli Access Manager for Business Integration also helps you provide a consistent policy management model based on a single user repository.

### Maximize access control

Tivoli Access Manager for Operating Systems helps you prevent security violations that can occur during everyday usage of UNIX and Linux systems, especially issues that arise from "root" or other privileged users. Use of the root ID is required for many administration tasks, which can lead to either accidental or deliberate misuse and abuse. Organizations also might allow multiple people to use the root ID, which reduces accountability. By implementing access control lists on resources on a per-user or per-group basis with Tivoli Access Manager for Operating Systems, you can compartmentalize access to application and operating system resources, regardless of a user's privilege status. You can also track the login process and apply policies that improve login security, such as defining the number of permitted failed login attempts before a user is locked out.




*Tivoli Access Manager for Operating Systems employs a centralized management server that provides Web-based, delegatable administration of policy and can be used with other Tivoli Access Manager products. User credentials, administration management and policy maintenance are then consistent whether protecting Web applications, WebSphere MQ applications or UNIX and Linux resources.*

**Enhance auditing of security-related events**

Tivoli Access Manager for Operating Systems provides flexible auditing capabilities, including auditing of specific resources. It also provides a unique audit trail for protected resources, tracking access by every user. You can track significant access attempts, provide security-related information on activity (including a policy-warning mode) and even send events to IBM Tivoli Enterprise Console® and IBM Tivoli Risk Manager. This secure logging of security events helps you verify the stability of your access policy.

**Cross-platform security management**

Tivoli Access Manager for Operating Systems can help you resolve the problems of managing disparate security models and can make the differences between IBM AIX®, Sun™ Solaris™, Hewlett-Packard HP-UX and Linux transparent to administrators. It can help you consistently enforce security policies across both geographic and platform boundaries.

The solution also can help improve productivity with its consistent user interface and the subscription of managed systems to sets of configuration data. Tivoli Access Manager for Operating Systems includes a sophisticated security engine that has many parallels to the IBM RACF® Security Server used on IBM OS/390® and IBM z/OS™.

**Reduce administration costs**

Tivoli Access Manager for Operating Systems can help reduce administration costs through Web-based delegated administration. This capability can be used to delegate selected management capabilities to authorized partners or business units. Administration also can be simplified by grouping similar UNIX and Linux systems that use a specific security configuration. Security management can then be performed on the group of resources instead of each individual system. Standardized sets of predefined best-practices policy definitions can be used to speed implementation. These policy definitions can be tailored for your specific environment.

**Unobtrusive authorization**

Unlike many tools that claim to solve the root administrator problem, Tivoli Access Manager for Operating Systems operates using a seamless layer of protection that does not require a change to administrative practices. Protections apply whether accesses are made through command shells or through applications. A multithreaded design with advanced caching adds significant authorization control while avoiding noticeable overhead.

**Integrates to extend your management capabilities**

Optional integration with IBM Tivoli Identity Manager extends UNIX management and provisioning and integrates it with multiple platforms including Microsoft® Windows®, IBM AS/400®, the OS/390 Security Server (RACF) and many other directory systems and applications.

**Integration with other Tivoli Access Manager products**

Tivoli Access Manager for Operating Systems shares a common set of services with the other Tivoli Access Manager products. These products include Tivoli Access Manager for e-business (provides single sign-on and authorization services for Web resources) and Tivoli Access Manager for Business Integration (provides security for WebSphere MQ applications). All three products use and ship the same set of shared services including a central security policy manager, a central credential directory and a Web-based administration tool. A single instance of these shared services can support the installation of all three products, allowing you to consolidate the administration and management of security policy across WebSphere MQ queues, Web resources and UNIX and Linux resources.

**Integrated identity management**

Tivoli Access Manager for Operating Systems is an integrated component of the IBM identity management solution that can help you get users, systems and applications online and productive fast, reduce costs and maximize return on investment. IBM identity management provides identity lifecycle management (user self-care, enrollment and provisioning), identity control (access and privacy control, single sign-on and auditing), identity federation (sharing user authentication and attribute information between trusted Web services applications) and identity foundation (directory and workflow) to effectively manage internal users as well as an increasing number of customers and partners through the Internet.

**Integrated security event management**

Tivoli Access Manager audit events can be sent to IBM Tivoli Risk Manager, which can store those events in the Tivoli Enterprise™ Data Warehouse. Tivoli Risk Manager can correlate and evaluate these and other enterprise events and then automate responses. New reporting capabilities can be used to leverage the information in the data warehouse.

**No prerequisites**

Tivoli Access Manager for Operating Systems can exploit and interoperate with many Tivoli security products from IBM and has no prerequisites. It is based on the Tivoli Access Manager architecture and includes the components required for implementation.

**To learn more**

For information about Tivoli Access Manager for Operating Systems and integrated solutions from IBM, visit **tivoli.com**/security

**Tivoli software from IBM**

An integral part of the comprehensive IBM e-business infrastructure solution, Tivoli technology management software helps traditional enterprises, emerging e-businesses and Internet businesses worldwide maximize their existing and future technology investments. Backed by world-class IBM services, support and research, Tivoli software provides a seamlessly integrated and flexible e-business infrastructure management solution that uses robust security to connect employees, business partners and customers.

## Supported platforms

| **Tivoli Access Manager management server supports:** |
|---|
| AIX, HP-UX, Solaris, SuSE Linux Enterprise Server 7 and Windows |
| **Tivoli Access Manager for Operating Systems secured platform support continues to expand. The current release includes:** |
| AIX 4.3.3 and 5.1 |
| HP-UX 11 and 11i |
| Solaris 2.7 and 2.8 |
| Red Hat Linux 7.1, 7.2, and 7.3 (x86) |
| Red Hat Linux 7.2 for IBM S/390® (31-bit) |
| SuSE Linux 7.3 and 8.0 (x86) |
| SuSE Linux Enterprise Server 7 for S/390 and IBM zSeries™ (31-bit) |
| SuSE Linux Enterprise Server 7 for zSeries (64/31-bit) |



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

10-02



The Tivoli home page on the Internet can be found at **ibm.com/tivoli**

The IBM home page on the Internet can be found at **ibm.com**

e business software

G325-6788-01