Provide an early warning system to identify security policy violations and potential security vulnerabilities

Tivoli software

IBM Tivoli Security Compliance Manager

Highlights

- ***Automate security scans of servers and desktop systems to help minimize costs and time***
- ***Provide a fast, simple, proactive and cost-effective solution to protect business IT infrastructure by helping identify software security vulnerabilities prior to damage being done***
- ***Leverage included best-practice policies and reports to optimize startup speed and time to value***
- ***Offer an effective way to assess and monitor enterprise-wide security policy compliance***

The need for enhancing and verifying security growth

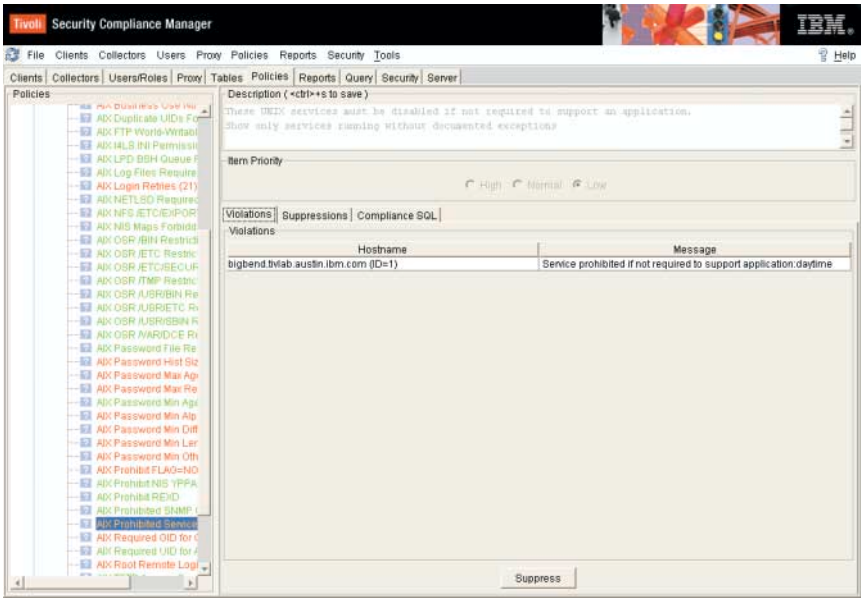
In recent years, IT and security administrators have seen the number of attacks by viruses and worms skyrocket. Many come from outside the enterprise. Others come from inside, often through human error and innocent negligence. Regardless of their source, any breach in an enterprise's security can cause lost time, corrupt or destroyed data, damaged credibility, embarrassment and even litigation.

As many as 90 percent of security incidents can be avoided by implementing and enforcing consistent enterprise-wide security policies. IBM Tivoli® Security Compliance Manager acts as an early warning system, helping small, medium and large businesses identify security policy violations and potential system vulnerabilities before a security incident occurs. It offers businesses a quick, cost-efficient and proactive way to gather and manage information about the security posture and health of their organizations.

Increasingly, businesses must also address compliance with corporate policies created in response to a growing number of government regulations aimed at maintaining data protection and integrity. A system should be in place to verify compliance with corporate policies.

Automation streamlines a tedious process

Manual security compliance checks can be tedious and costly, often taking days to accomplish. Unfortunately, they also can be prone to human error and inconsistency. Tivoli Security Compliance Manager is built around on demand automation, which is at the core of IBM's highly respected and enduring software strategies. Automated centralized security compliance checks generally can be completed in a matter of minutes. This in turn can free administrators from time-consuming routine functions—helping maximize efficiency, save money and minimize the risk of human error.



Tivoli Security Compliance Manager provides security policies as templates for getting started quickly. Customers can easily modify these security policies or create new ones to meet the needs of their organization.

Best-practice policies — part of the Tivoli Security Compliance Manager package

Best-practice out-of-the-box security policies and canned reports ship with Tivoli Security Compliance Manager. Built on flexible, scalable Java™, the product allows users to customize existing templates to build highly tuned and meaningful security policies. Using the GUI interface, a security administrator can efficiently take policy "snapshots" to determine compliance across the enterprise, detect security violations and alert owners of noncompliance — and provide steps for remediation. The software uses a color-coded red, yellow, green stoplight-style warning to indicate the detection of a violation. The administrator knows at a glance which systems across the enterprise have passwords incorrectly set, out-of-date anti-virus signature files, down-level operating system hotfixes, dangerous or unnecessary services and so forth. Follow-up security policy compliance checking provides a picture that verifies how and where violations have been corrected and checks that policies are being followed.

Minimizing complex and costly processes while optimizing productivity

Shipping security policy templates helps minimize the complex, time-consuming and costly processes usually associated with creating a set of compliance procedures. These ready-made security policies provide a framework for a security administrator to begin with, avoiding the "start-from-scratch" syndrome that can be so daunting at a project's onset.

Tivoli Security Compliance Manager accomplishes on demand automation by moving from costly and tedious manual security server checking to automated security policy checking. As compliance assessments become automated, the time needed to manage

security policies, compliance and security audits can decrease. Additional savings can also occur as potential security exposures across IBM AIX®, Solaris, HP-UX, Microsoft® Windows®, Linux and Linux on zSeries® are identified before a costly security breach can occur.

Tivoli Security Compliance Manager features autonomic functionality, including a "heartbeat" capability that automatically sends periodic pulses from the managed end points to the central server, letting the system know that systems remain updated and running properly. This autonomic functionality enables the software to self-manage and automatically update relevant Java-based end points. Part of IBM's on demand initiative, this automated approach to security policy compliance includes helping our customers become resilient and adaptive to threats.

Integrates with IBM Tivoli automated security management products

Tivoli Security Compliance Manager sends information related to security violations or noncompliance into Tivoli automated security management tools to help mediate security policy violations and risks. By integrating and working with other Tivoli software, such as IBM Tivoli Risk Manager, IBM Tivoli Enterprise Console® and IBM Tivoli Configuration Manager, businesses can take action to help prevent damage from being done and assist in fixing policy violations. Tivoli Security Compliance Manager can work in tandem with these Tivoli solutions to stop unneeded services, change permissions, upgrade software or deploy patches.

For more information

To learn more about Tivoli Security Compliance Manager and integrated solutions from IBM, contact your IBM sales representative or visit **ibm.com**/tivoli/products/security-compliance-mgr

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.

Hardware requirements

Processor and memory requirements for Tivoli Security Compliance Manager server

Type of Tivoli Security Compliance Manager deployment	Processor	Memory requirements
Small (1-500 clients)	1	512MB RAM
Medium (501-2,500 clients)	2	512MB RAM
Large (2,501-10,000 clients)	2-4	2-4GB RAM

You need 5MB of disk space to install the server package.

Disk and memory requirement for client and collectors

Disk and memory requirements for Tivoli Security Compliance Manager client

Client platform	Disk requirements for installation directory	Disk requirements for temporary directory	Memory requirements
AIX	64MB	45MB	75MB RAM
HP-UX	64MB	6MB	75MB RAM
Linux	64MB	46MB	75MB RAM
Solaris	64MB	65MB	75MB RAM
Windows	64MB	44MB	75MB RAM

Note: The HP-UX platform values in the table are much smaller than the other platform values because the Java Runtime Environment is not packaged with the HP-UX client.

Disk and memory requirement for administration utilities

Disk and memory requirements for Tivoli Security Compliance Manager administration console

Administration console platform	Disk requirements for installation directory	Disk requirements for temporary directory	Memory requirements
Windows	64MB	42MB	128MB RAM minimum, 256MB RAM recommended

Software requirements

Tivoli Security Compliance Manager requires:

IBM DB2 Universal Database™, Version 7.2 or Version 8.1 (Tivoli Security Compliance Manager 5.1 product package includes DB2 Universal Database, Version 8.1.)

Supported operating systems

The following tables list the supported operating systems for the Tivoli Security Compliance Manager server, client and administration console.

Tivoli Security Compliance Manager server

Operating system	Level	Patch/maintenance level
AIX	5.1, 5.2	No fix pack required
Windows 2000	Server	Latest fix pack level
Solaris	2.8, 2.9	Latest fix pack level
SUSE Linux Enterprise Server	8	Latest fix pack level

Tivoli Security Compliance Manager client

Operating system	Level	Patch/maintenance level
AIX	5.1, 5.2	Latest cumulative patches
HP-UX	11.0, 11i	Latest cumulative patches
Red Hat Linux	6.2, 7.0, 7.1, 7.2, 7.3, 8.0, 9.0	Latest cumulative patches
Solaris	2.6, 2.7, 2.8. 2.9	Latest cumulative patches
Windows NT®	4.0 Server, 4.0 Workstation	Latest service pack and security roll up package
Windows 2000	Server, Advanced Server, Professional	Latest service pack and security roll up package
Windows XP	Professional	Latest service pack and security roll up package
Windows 2003	Server Standard Edition, Enterprise Edition	Latest cumulative patches
Red Hat Enterprise Linux	2.1	Latest cumulative patches
Red Hat Enterprise Linux Advanced Server	3.0 (see note below)	Latest cumulative patches
Red Hat Enterprise Linux for zSeries	3.0	Latest cumulative patches
Red Hat Enterprise Linux for iSeries® or pSeries®	3.0	Latest cumulative patches
Red Hat Enterprise Linux for zSeries	7.2	Latest cumulative patches
Red Hat Enterprise Linux Advanced Server	2.1	Latest cumulative patches
SUSE Linux	7.0	Latest cumulative patches
SUSE Linux Enterprise Server	8	Latest cumulative patches
SUSE Linux Enterprise Server for zSeries	8	Latest cumulative patches
SUSE Linux Enterprise Server for iSeries or pSeries	8	Latest cumulative patches

Tivoli Security Compliance Manager administration console

Operating system	Level	Patch/maintenance level
Windows 2000	Professional	Latest service pack and security roll up package
Windows XP	Professional	Latest service pack and security roll up package

Note: Unless otherwise noted for Linux systems, only Intel® IA32 is supported.

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

06-04