IBM Proventia® Management SiteProtector™

Scalability Guidelines
Version 2.0, Service Pack 7.0

Trademarks and disclaimer

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. ADDME, Ahead of the threat, BlackICE, Internet Scanner, Proventia, RealSecure, SecurePartner, SecurityFusion, SiteProtector, System Scanner, Virtual Patch, X-Force and X-Press Update are trademarks or registered trademarks of Internet Security Systems, Inc. in the United States, other countries, or both. Internet Security Systems, Inc. is a wholly-owned subsidiary of International Business Machines Corporation.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

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

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

Disclaimer: The information contained in this document may change without notice, and may have been altered or changed if you have received it from a source other than IBM Internet Security Systems (IBM ISS). Use of this information constitutes acceptance for use in an "AS IS" condition, without warranties of any kind, and any use of this information is at the user's own risk. IBM Internet Security Systems disclaims all warranties, either expressed or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall IBM ISS be liable for any damages whatsoever, including direct, indirect, incidental, consequential or special damages, arising from the use or dissemination hereof, even if IBM Internet Security Systems has been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages, so the foregoing limitation may not apply.

Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by IBM Internet Security Systems. The views and opinions of authors expressed herein do not necessarily state or reflect those of IBM Internet Security Systems, and shall not be used for advertising or product endorsement purposes.

Links and addresses to Internet resources are inspected thoroughly prior to release, but the ever-changing nature of the Internet prevents IBM Internet Security Systems, Inc. from guaranteeing the content or existence of the resource. When possible, the reference contains alternate sites or keywords that could be used to acquire the information by other methods. If you find a broken or inappropriate link, please send an e-mail with the topic name, link, and its behavior to mailto://support@iss.net.

Contents

Overview

This document provides hardware and software recommendations for deploying SiteProtector 2.0, Service Pack 7.0.

Purpose

Use this document to assist you when planning an initial deployment of SiteProtector or when expanding an existing configuration to meet increased performance demands.

Related documentation

Refer to other SiteProtector documentation, as follows:

- For minimum system requirements, see the *SiteProtector System Requirements*.
- For installation instructions, see the *SiteProtector Installation Guide*.

Topics

Recommendations

This topic gives recommendations for hardware, software, and free disk space. The recommendations are based on typical customer environments and may not apply to your specific environment.

Important: This document provides sizing criteria for events and heartbeats. Do not exceed the average events per day or the maximum heartbeats per day regardless of the number of sensors in your configuration.

Hardware and software

Hardware and software recommendations are based on the following items:

Item	Description
Maximum events per day for the site	This number represents the maximum number of events processed per day throughout the entire site. The recommendations in this guide assume that the total number of events per day in your entire site will not consistently exceed the number in this column.
Maximum heartbeats per day	This number represents the maximum number of heartbeats the database processes per day throughout your entire site. The recommendations in this guide assume that the total number of events per day in your entire site will not consistently exceed the number in this column.

Free hard disk space

Free hard disk space recommendations are based on the following:

- expected event volume
- space required to store event data for 30 days
- space required to perform periodic database maintenance

Database layout

For information about the layout of your database files, go to the Microsoft SQL Web site:

http://www.microsoft.com/sql/

Performance considerations

If the average events per day and the maximum heartbeats per day in your site are consistently higher than the following guidelines, your site may experience performance problems regardless of the number of agents you are using. Potential problems include the following:

- The console may become slow or unresponsive.
- The database may become temporarily unable to accept new events until the activity drops to within the constraints for your configuration.
- The database may process events at a very slow rate until the activity drops to within the constraints for your configuration.

If the activity in your environment exceeds the constraints for your deployment size, consider using the following guidelines to scale your deployment.

Factors that impact performance

Several factors can impact the overall performance and responsiveness of SiteProtector:

- multiple console operations
- long-running analysis queries
- report generation
- fusion analysis
- attack patterns
- maintenance operations

Event Collector and Agent Manager setup

For medium and large deployments, IBM ISS recommends that you install Events Collectors and Agent Managers on the same computer. The system requirements for installing the Agent Manager on a dedicated system also apply to Event Collector and Agent Managers that share the same computer. For more information about Agent Manager requirements, refer to the *SiteProtector System Requirements*.

When to use multiple Agent Managers and Event Collectors

Multiple Event Collector and Agent Manager pairs are required to accommodate the increased bandwidth that is needed during agent updates, including providing redundancy. However, increasing the number of Agent Manager or Event Collectors does not increase the event and heartbeat limits stated in this document.

For Medium and Large Deployments

To optimize performance, the Event Collector installed on the database server should only be used for redundancy purposes. This allows for server resources to be dedicated to the database service, which may improve performance.

To optimize performance, the Agent Manager on the application server should only be used for redundancy purposes. This allows for server resources to be dedicated to the application server services, which may improve performance.

Microsoft Virtual Server 2005

Testing found that the allocation of resources when using Microsoft® Virtual Server 2005 affects the overall performance of SiteProtector™ more so than instances not using Virtual Server 2005. For example, on a single processor unit where the base OS and a single virtual instance was running, SiteProtector performed much slower than it on a hardware instance meeting the specifications of only the virtual instance. Therefore, consider providing additional resources when using Virtual Server 2005.

Update Servers for Proventia Desktop 9.0

Version 9.0 of Proventia Desktop includes signature-based antivirus and anti-spyware scanning, which requires frequent updates to virus definitions. To ensure that you can accommodate these updates, see the knowledge base article *How many Update Servers will I need to support Proventia Desktop 9.0 Agents?* (Answer ID 3830) at http://iss.custhelp.com/cgi-bin/iss.cfg/php/enduser/std_adp.php?p_faqid=3830.

Small deployment

A small deployment of SiteProtector can be installed on a single computer.

Environment

A small deployment is appropriate in the following environment:

Deployment Type	Maximum Events Per Day	Maximum Heartbeats Per Day	Recommended Number of Event Collectors and Agent Managers
Small	50,000	1,000[a]	1[b]

a. Assumes no more than 500 Proventia Desktop or RealSecure Desktop Agents.
b. See When to Use Multiple Agent Managers and Event Collectors section under Performance Consider

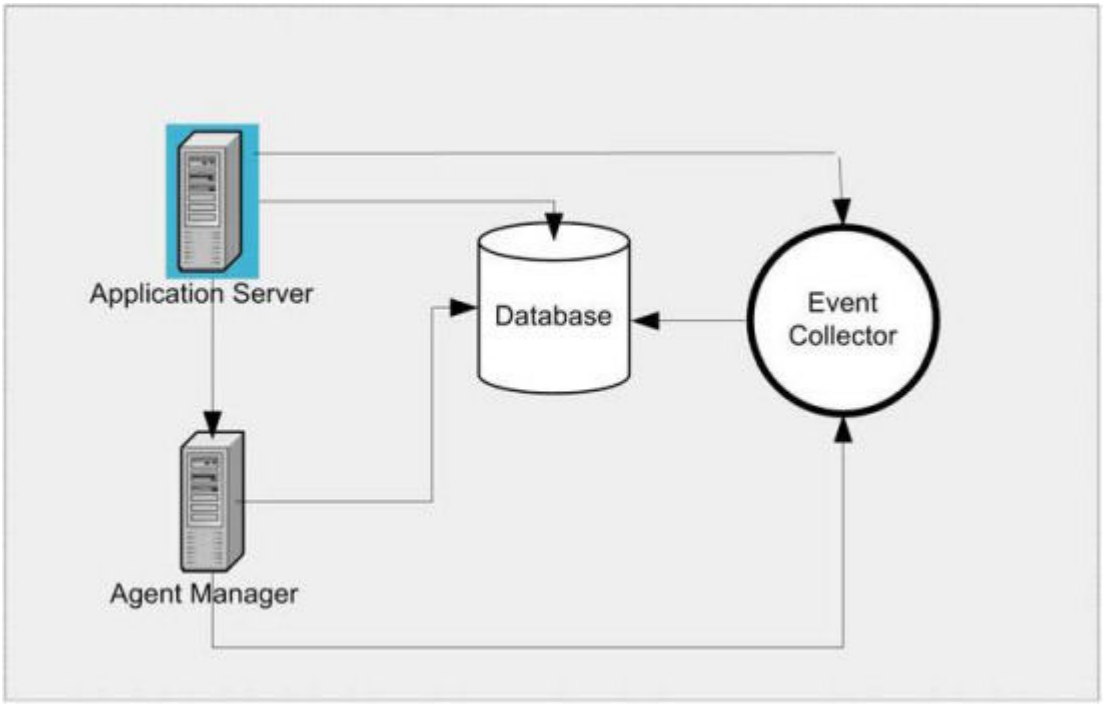
Hardware and software

The following table gives hardware and software recommendations for a small deployment:

Item	Recommendation
processor	(2) 2.4 GHz Xeon
operating system	Windows 2000 Server
	Windows 2003 Server
SQL Server	2000 Standard Edition
RAM	2 GB
free hard disk space	36-73 GB

Diagram

The following figure illustrates the small deployment diagram:



Medium deployment

A medium deployment of SiteProtector can be installed on four or more computers as follows:

Computer	Components
1	Application Server
2	Database
3 and 4	Event Collector
	Agent Manager

Environment

A medium deployment is appropriate in the following environment:

Deployment Type	Maximum Events Per Day	Maximum Heartbeats Per Day	Recommended Number of Event Collectors and Agent Managers
Medium	2,500,000	100,000[a]	2[b]

a. Assumes no more than 15,000 Proventia Desktop Agents or 10,000 RealSecure Desktop Agents.
b. See When to Use Multiple Agent Managers and Event Collectors section under Performance Consider

Hardware and software

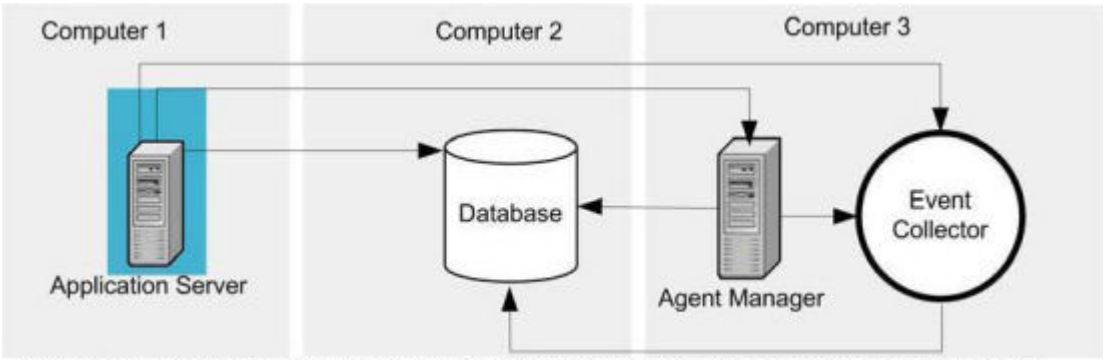
The following table gives hardware and software recommendations for the medium deployment:

Computer	Item	Recommendation
1 (Application Server)	processor	(1) 2.4 GHz Xeon
	operating system	Windows 2000 Server
		Windows Server 2003
	RAM	2 GB
	free hard disk space	36 GB
2 (Database)	processor	(2) 3.0 GHz Xeon
	operating system	Windows 2000 Server
		Windows Server 2003
	SQL Server	SQL Server 2000, Standard Edition
	RAM	4 GB
	free hard disk space	73 to 438 GB as follows: • 15K RPM SCSI disk • RAID configuration • multiple controllers

Computer	Item	Recommendation
3 and 4 (Event Collector/Agent Manager)	processor	2.4 GHz Xeon Intel Pentium 4
	operating system	Windows 2000 Server (with SP4) or later
		Windows 2000 Advanced Server (with SP4) or later
		Windows Server 2003
		Windows Enterprise Server 2003
	RAM	1 GB
	free hard disk space	36 GB

Diagram

The following illustrates the medium deployment diagram:



Note: More Agent Managers and Event Collectors can be added to the deployment as needed.

Large deployment

A large deployment of SiteProtector can be installed on five or more computers as follows:

Computer	Components
1	Application Server
2	Database
3, 4, and 5	Event Collector
	Agent Manager

Environment

A large deployment is appropriate in the following environment:

Deployment Type	Maximum Events Per Day	Maximum Heartbeats Per Day	Recommended Number of Event Collectors and Agent Managers
Large	5,000,000	300,000[a]	5[b]

a. Assumes no more than 50,000 Proventia Desktop or 25,000 RealSecure Desktop Agents.
b. See When to Use Multiple Agent Managers and Event Collectors section under Performance Consider

Hardware and software

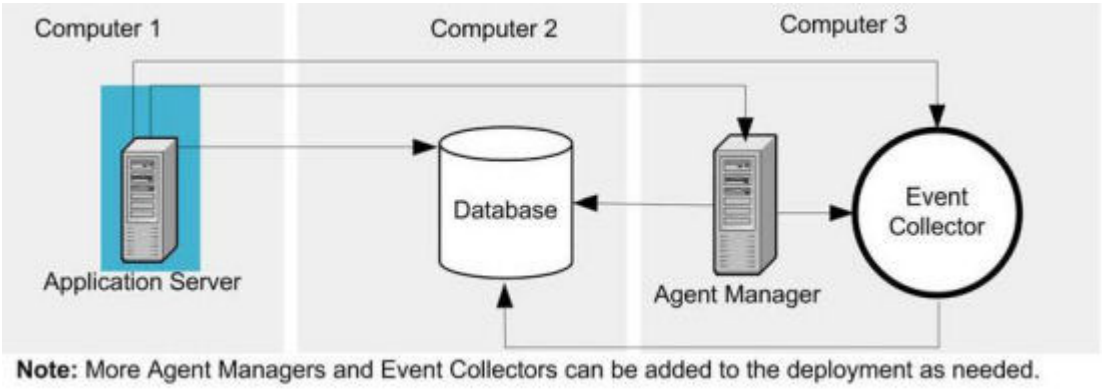
The following table gives hardware and software recommendations for the large deployment:

Computer	Item	Recommendation
1 (Application Server)	processor	(2) 3.2Ghz Xeon with 2 MB cache
	operating system	Windows 2000 Server (with SP4) or later
		Windows Server 2003
	RAM	2 GB
	free hard disk space	36 GB
2 (Database)	processor	(4) 3.2Ghz Xeon with 2 MB cache
	operating system	Windows 2000 Advanced Server (with SP4) or later
		Windows 2003 Server, Enterprise Edition
	SQL Server version	2000 Enterprise Edition
	RAM	8 GB
	free hard disk space	143-730 GB with the following specifications: • 15K RPM SCSI disk • RAID configuration • multiple controllers

Computer	Item	Recommendation
3, 4, and 5 (Event Collector/Agent Manager)	processor	2.4 GHz Xeon Intel Pentium 4
	operating system	Windows 2000 Server (with SP4) or later
		Windows 2000 Advanced Server (SP4) or later
		Windows Server 2003
		Windows Enterprise Server 2003
	RAM	1 GB
	free hard disk space	36 GB

Diagram

The following illustrates the large deployment diagram:



Multiple-site deployment

If your current configuration is too large, consider dividing it into several smaller sites. Use the guidelines and requirements for the small, medium, and large deployments described in this topic to help you choose the best deployment for each site.

The multiple-site deployment consists of several large deployments that report to a Site Summary instance. Use the multiple-site deployment if the following applies:

- the sizing criteria for your configuration exceeds the numbers specified in the large deployment
- your configuration is distributed over a large geographic area

Printed in USA