Symantec™ Data Loss Prevention Endpoint Server Scalability on VMware

Version 11.1

Symantec™ Data Loss Prevention Endpoint Server Scalability on VMware

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version: 11.1, June 15, 2011

Legal Notice

Copyright © 2011 Symantec Corporation. All rights reserved.

Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the *Third-Party License Agreements* document accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrades protection
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level

- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Managed Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Education Services	Education Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about enterprise services, please visit our web site at the following URL:

www.symantec.com/business/services/

Select your country or language from the site index.

Contents

Chapter 1

Overview of Endpoint Server Scalability on VMware

This chapter includes the following topics:

About Endpoint Server scalability on VMware

As of version 11.1 of Symantec Data Loss Prevention, Symantec supports the deployment of Endpoint Servers on the VMware ESX platform. This document describes scalability testing where the Endpoint Server is deployed on VMware ESX. The test results and recommendations that are presented in this document can help you understand and plan your Symantec Data Loss Prevention deployment.

The tests examined the following operations:

- The effect of adding Agents to an Endpoint Server
- The effect of restarting the Endpoint Server
- The effect of Agents connecting and disconnecting from the network
- Policy updates

Other Endpoint scalability documents

The following documents, available from the Symantec Data Loss Prevention Knowledge Base, also discuss Endpoint scalability:

- Symantec Data Loss Prevention Endpoint Server Scalability (https://kb-vontu.altiris.com/article.asp?article=54542&p=4)
- Symantec Data Loss Prevention Endpoint Scalability on Citrix XenApp (https://kb-vontu.altiris.com/article.asp?article=54540&p=4)

Chapter 2

Testing methodology

This chapter includes the following topics:

Product setup and configuration

The scalability tests used typical customer environments and configurations to measure the performance of a Symantec Data Loss Prevention deployment under load.

Table 2-1 describes the environments and configurations that were used for the tests.

Table 2-1 Test environment for Endpoint Server scalability on VMware

Setup or Configuration	Description
Enforce Server hardware and software configuration	Enforce Server and Oracle database: ■ 2 x 3.0 GHz dual-core CPU ■ 8 GB RAM ■ Microsoft Windows 2003 Enterprise SP2 (x86) ■ Oracle 10g, version 10.2.0.4 ■ Symantec Data Loss Prevention version 11.1 The Enforce Server and Oracle database were deployed on a hardware computer. Virtualization was not used.

Table 2-1 Test environment for Endpoint Server scalability on VMware *(continued)*

Setup or Configuration	Description
Endpoint Server hardware and software configuration	The Endpoint Server was deployed in a container that was hosted on a VMware ESX server, version 4.0.0. The ESX server was configured with the following hardware: ■ Intel x7460 Xeon 2.66 GHz CPU ■ Processor speed: 2.7 GHz ■ Processor sockets: 4 ■ Cores per socket: 6 ■ Logical processors: 24 ■ 128 GB RAM ■ 134.75 GB local storage ■ 1,400 GB external storage (NetApp) ■ Broadcom netXtreme II Network card, 100 Mbps The Endpoint Server was deployed in a virtual container on this ESX server in the following two configurations for the tests: Configuration 1: ■ 2 x Intel x7460 Xeon 2.66 GHz CPU ■ 8 GB RAM ■ Microsoft Windows 2008 Enterprise R2 (x64) ■ Symantec Data Loss Prevention version 11.1 Configuration 2: ■ 4x Intel x7460 Xeon 2.66 GHz CPU ■ 16 GB RAM ■ Microsoft Windows 2008 Enterprise R2 (x64) ■ Symantec Data Loss Prevention version 11.1

Table 2-1 Test environment for Endpoint Server scalability on VMware *(continued)*

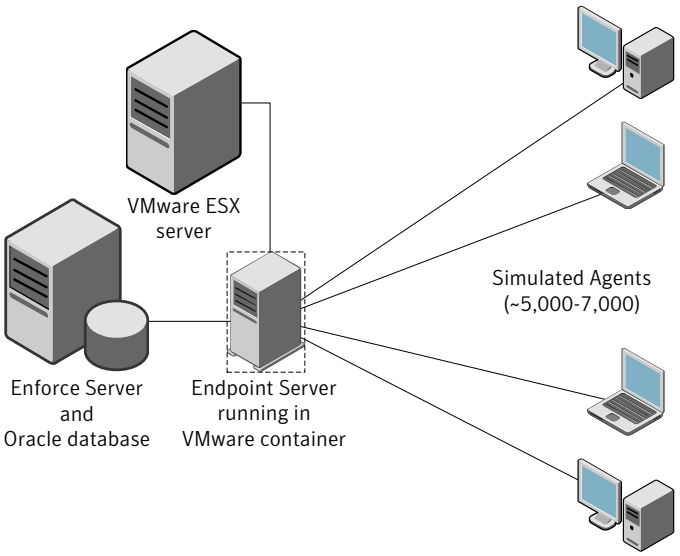
Setup or Configuration	Description

Policies	Polices were chosen that were of sufficient size and complexity. The policies were derived from actual production environments and represent the types of policies that most customers use.
	
	The polices used the following configurations:
	
	■ Types of Detection rules used:
	  ■ Described Content Matching for Keyword and Data Identifier
	  ■ File Properties for Message Attachment or File Size
	■ The policies used 14 detection rules
	■ The policies used 15 exceptions
	■ The size of the policy (as it was saved in the Agent database) was 2 MB

Network setup	The tests were carried out in a well-controlled laboratory environment where systems were connected on a local area network that had 100-Mbps Ethernet connectivity. Although the tests were performed in a controlled environment, the network was not isolated. Other systems that were not related to this test were connected and communicating but these systems were not performing any network-intensive activity. This design was intentional and the aim was to simulate real-time load on the network while the tests were in progress.
Incidents generated during testing	The simulated Agents sent one removable storage incident per hour per Agent.
Events sent during testing	The simulated Agents sent only connection and disconnection events as those activities occurred. No other types of events were sent.

Figure 2-1 shows the architecture that was used for testing.

Figure 2-1 Endpoint Server scalability test architecture



Test scenarios and execution

The tests were designed to simulate load on a newly installed Endpoint Server. The tests used simulated Agents that connect to the Endpoint Server. The number of simulated Agents was gradually increased until the system stopped performing at the expected level.

The tests begin with a newly installed Endpoint Server, and then the following steps were performed to increase the Agent load:

1. Add 1,000 Agents to the Endpoint Server.
2. Wait for all Agents connect.
3. Update and push a policy to all Agents.
4. Wait for the policy to deploy to all Agents.
5. The connected Agents continuously send incidents to the Endpoint Server.
6. Restart the Endpoint Server.
7. Repeat these steps and record the performance data.

These steps exercised the following functionality of the Endpoint Server:

- Policy management—receiving, storing, and pushing policies to connected Agents

- Incident management—receiving, processing, and sending incidents to the Enforce Server
- Agent connections—process incoming connections from new Agents
- Agent re-connections—process reconnections from all Agents when the Endpoint Server restarts

The following functions were not tested:

- Two-tier detection
- Sending events from the Agent to the Enforce Server
- Endpoint Discover scans

Note: The tests were performed a minimum of three times and performance measurements were averaged among the test results.

Performance measurements

The following aspects of Endpoint Server performance were measured:

- Overall CPU usage
- CPU usage of Endpoint Server processes
- Overall system memory usage
- Memory usage for all Endpoint Server processes
- Process crashes and restarts
- Disconnection of Agents (if any)
- Number of disconnected Agents
- Time that is required for all Agents to reconnect
- Time that is required for a new policy to reach all Agents

Break point conditions

The testing attempted to find the maximum load for an Endpoint Server. When the server reaches its maximum load, one of the following conditions occurs:

- The Endpoint Server does not respond to new connections.
- Connected Agents disconnect and are not able to reconnect within the expected amount of time.

- A new policy or updated policy that is sent to the Agents does not reach the Agents.
- A new policy or updated policy that is sent to the Agents takes longer than expected to reach the Agent.
- Endpoint Server or system CPU usage remains consistently high (greater than 80%).
- The Endpoint Server consumes all available memory, resulting in overall performance degradation.
- Incidents are lost, or it takes an abnormally long period of time for incidents to reach the Enforce Server.

Chapter 3

Test results and recommendations

This chapter includes the following topics:

About the test results

This chapter presents the observations, test results, and recommendations for scalability of Endpoint Servers running in a VMware ESX container. The performance of a Symantec Data Loss Prevention deployment varies depending on the infrastructure, Enforce Server configuration, and the overall workload of the deployment. The test results, observations, and recommendations provide a point of reference based on the configurations and the hardware that were specified for the testing. Limitations in scalability cannot be attributed to any one variable in these tests.

Test results

Table 3-1 displays the test results for the two tested configurations. (See "Product setup and configuration" on page 11.)

Table 3-1 Test results

Observation	Results: Configuration 1 (2 CPU / 8 GB RAM)	Results: Configuration 2 (4 CPU / 16GB RAM)
Number of Agents supported	5,000 With 5,000 Agents connected, a restart of the Endpoint Server did not have negative effect on the ability of the Agents to reconnect. All Agents reconnected successfully.	7,000 With 7,000 Agents connected, a restart of the Endpoint Server did not have negative effect on the ability of the Agents to reconnect. All Agents reconnected successfully.
Limitations on the number of Agents supported	When more than 5,000 Agents connected to an Endpoint Server: ■ CPU usage exceeded 80%. ■ Sending policies caused spikes of CPU usage up to 100%. ■ The time that is required to send a policy to the Agents increased. ■ No Agents disconnected. Agents started to disconnect during policy updates when the number of Agents increased to 6,000. ■ When the Endpoint Server was restarted, all Agents reconnected successfully.	When more than 7,000 Agents connected to an Endpoint Server: ■ CPU usage exceeded 80%. ■ Sending policies caused spikes of CPU usage up to 100%. ■ The time that is required to send a policy to the Agents increased. ■ No Agents disconnected. Agents started to disconnect during policy updates when the number of Agents increased to 9,000. ■ When the Endpoint Server was restarted, all Agents reconnected successfully.
Memory consumption	Memory consumption was not a limiting factor. Average memory consumption was around 300 MB.	Memory consumption was not a limiting factor. Average memory consumption was around 500 MB.

Deployment recommendations

Symantec recommends the following based on the test results:

- Configure the VMware container for the Endpoint Server to use static allocation of resources. Static resources are resources from the host operating system that are always available to the guest operating system that hosts the Endpoint Server. Using static resources prevents contention for resources and provides for consistent throughput.

- Configure your Endpoint Servers on multiple, smaller virtual machines, as tested in Configuration 1.

In addition to these scalability recommendations, the following general recommendations can also improve scalability and performance:

- Changes in policy size affect overall performance of the Endpoint Server. Policies that are larger or more complex require more processing power and memory usage by the Endpoint Server.
- Two-tier detection activities greatly increase the load on the Endpoint Server and are also network-intensive. Two-tier detection reduces the overall performance and scalability of the Endpoint Server. (Two-tier detection occurs when the Agent sends data to the Endpoint Server for analysis.)
- Networking speed, latency, and the use of load balancers in the network can affect the overall performance of the Endpoint Server.

Test limitations compared to actual deployments

The testing that is described in this document attempted to simulate actual Symantec Data Loss Prevention deployments. When using these results to plan your deployment, note the following regarding the tests:

- The tests used simulated DLP Agents to simulate connection and disconnection events .
- The simulated Agents only sent one incident per hour.
- The simulated Agents were deployed on a small number of endpoint computers where each computer hosted approximately 700 simulated endpoint Agents. This design caused contention for resources and contributed some additional performance delay to the test results.
- Due to the design of these tests, the following features were not exercised: Endpoint Server failover, Endpoint Discover scans, and two-tier detection using Exact Data Matching (EDM) or Indexed Document Matching (IDM).
- When disconnected Agents reconnect to their associated Endpoint Server they send any accumulated incidents that were stored in the Agent's incident database. Because the simulated Agents did not persist incidents in an incident database, the performance effect of Agents reconnecting was not measured.