

Symantec Endpoint Protection 11.0

Architecture, Sizing, and Performance Recommendations

Introduction

This guide will outline Symantec recommended architectures and review sizing considerations for Symantec Endpoint Protection 11.0. The Symantec Endpoint Protection Manager (SEPM) can be configured and deployed in several different configurations. This guide will detail the recommendations for single and multiple site environments. A site is defined as a physical location that contains a database.

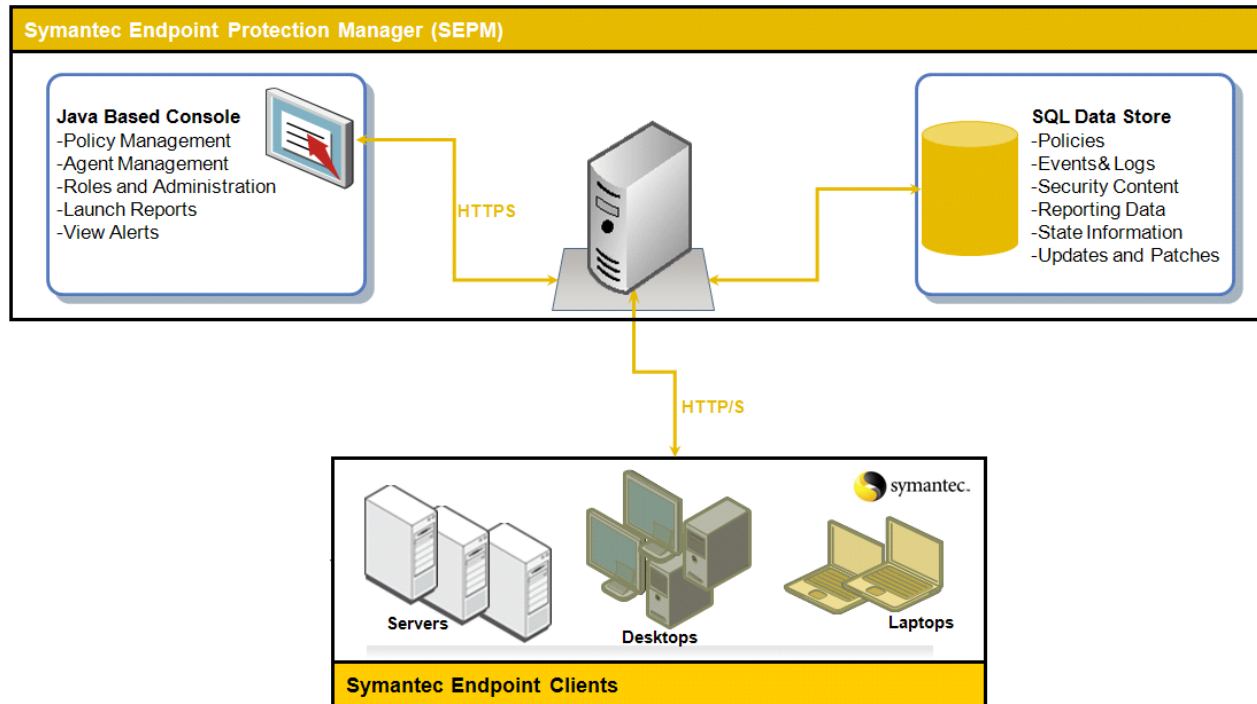
The guide will also provide recommendations for client/server ratio, as well as database sizing recommendations.

The following architectures and designs are based on metrics from internal testing of the product done in a closed environment. Implementations in production environments may encounter different metrics which would affect the recommended sizing and architecture. Any changes or planned modifications to product capability, functionalities, metrics, and/or features discussed are subject to ongoing evaluation by Symantec, and should not be considered as firm commitments by Symantec.

When designing a SEP environment, several design decisions must be considered such as:

- Which Technologies will be deployed?
- Is there a need for different security policies when users are in different locations?
- Will desktops/servers/laptops/users/departments have different policies?
- How many geographic locations are there within the company?
- How often does the customer want to provide content updates?
- Ability to automatically deploy SEP patches?
- Which method of content distribution does the customer want to use?
- Is a High Available Management Infrastructure desired?
- How long does the customer need to retain logs?
- What is the frequency of requests for log or reporting data older than one week, one month, and one year?
- Which metrics need to be gathered frequently?
- Who needs access to the Data and where are they located?
- Are there multiple administrative groups in the organization (i.e., IT, Sec, Desktop, Server)?
- Is there need to tie in to an existing 3rd party tool or authentication scheme?

Architecture



Symantec Endpoint Protection contains four main architectural components that work together to protect your company from security threats.

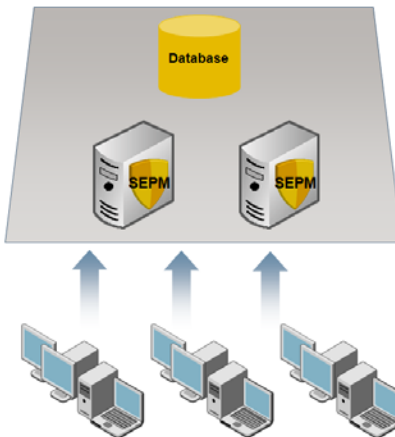
- **Symantec Endpoint Protection Manager** – The management server that facilitates configuring clients, reporting, and alerting
- **Symantec Endpoint Protection SQL Datastore** – Location where all configuration, updates, and reporting information resides
- **Symantec Endpoint Protection Client** – Software that you deploy to company computers to monitor policies and automate restoration of compliance to policies
- **Symantec Endpoint Protection Console** – A lightweight console that provides the ability manage the deployment, configuration, updating, and reporting of SEP Clients.

Site Design

When designing the environment, there are several architectural design options. Symantec recommends that customers adhere to one of three basic architectures:

- Single Site
- Multiple Site Distributed
- Multiple Site with Centralized Logging

Single Site Design

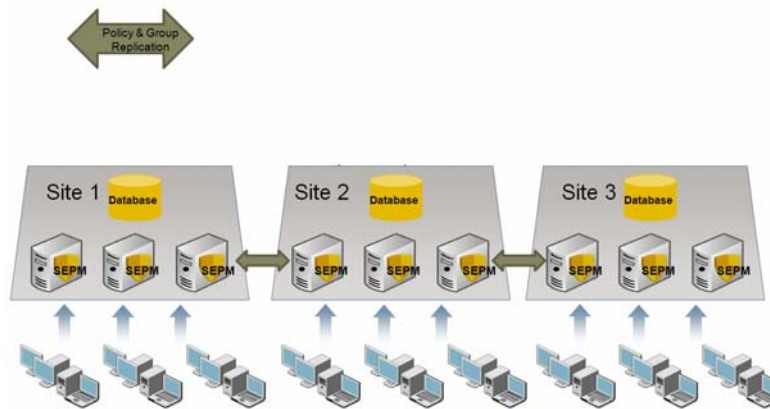


In an organization that has only one datacenter, Symantec recommends the single site design. In this single site scenario, it is recommended that two Symantec Endpoint Protection Managers be used for redundancy. Customers with high availability needs should consider clustering the DB to ensure high availability of the database. The use of multiple Symantec Endpoint Protection Managers within the same site will also provide automatic load balancing as well.

Multiple Site Designs

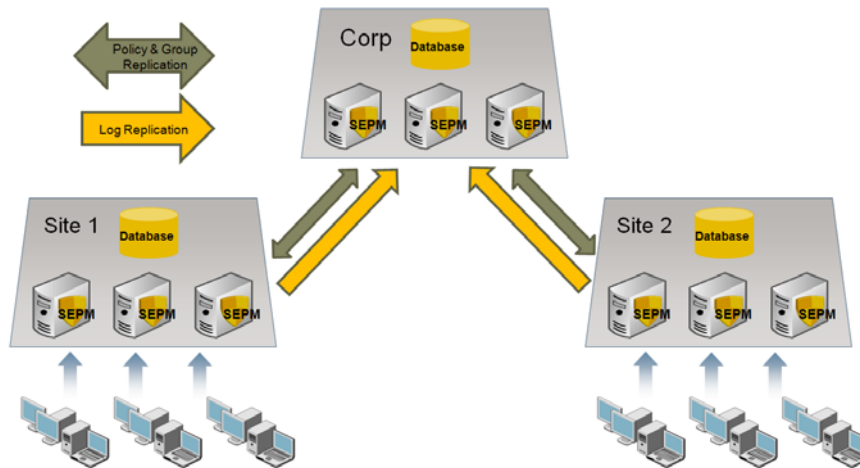
In an organization that has more than one datacenter or multiple large physical locations, Symantec recommends a multiple site design. There are two preferred options in a multiple site environment.

Distributed



In this scenario, each site is performing bi-directional replication of Groups and Policies, but logs and content are not replicated by default. In this model, administrators would have to use the console to connect to each manager in the remote sites to see the reporting information for that site. This option is preferred when access to remote site data is not critical.

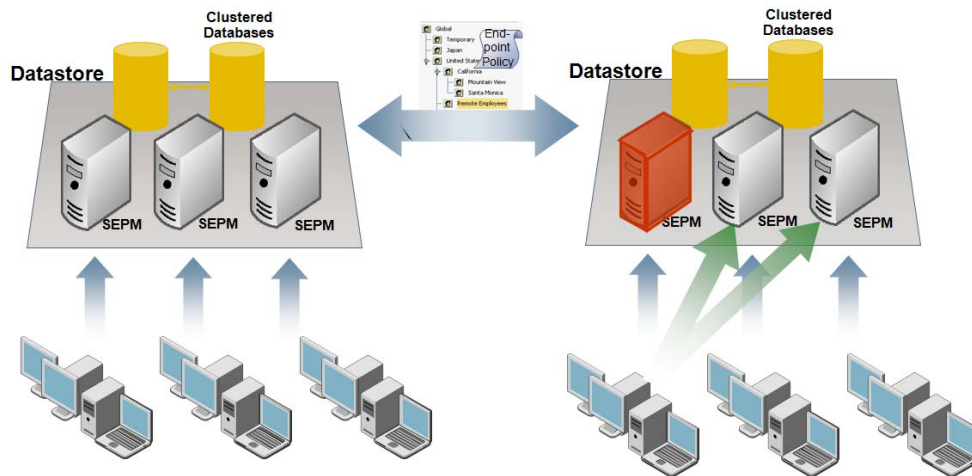
Central Logging



The centralized logging site design is similar to the distributed design. The distinction between these two designs is that in the centralized logging design, all logs are forwarded to a centralized site. In the above example, the Corp Headquarters site is acting as a central repository for the logs between Corp Sites 1 and 2. This design is recommended when centralized reporting is required.

High Availability option

Failover between Management Servers & Data Stores



In the event that a SEPM server goes down, client machines will fail over to another SEPM server. In order to achieve true high availability the use of database clustering and the use of multiple SEPM servers is required.

Determining Client/Server Ratios

Communication Sizing & Performance

Clients initiate communication with the SEPM from an ephemeral port to the SEPM server on TCP port 80 (or 443). The frequency of this communication depends on the *heartbeat* and communication configuration. The heartbeat size is between 2-3 KB when there are no new policies or updates to download. Symantec Endpoint Protection clients can be configured to communicate with the Symantec Endpoint Manager using Push Mode or Pull Mode. For best performance, it is recommended to keep the SEP database close to the SEPM server and use Pull Mode.

Below are general communication considerations for each mode.

Communications Settings for Global

Management Server List
Specify the management servers this group will communicate with:
Default Management Server List for SEPM

Download

Download policies and content from the management server

Push mode
Keep the connection between clients and the management server open so that clients can download policies as soon as they are available.

Pull mode
Clients will connect to the management server at a regular interval to check if new policies are available.

Upload

Upload a list of applications that the clients have run
Clients will keep track of every application that is executed and send the results to the management server.

Heartbeat Interval
Frequency in which clients will upload data and if using the pull mode mentioned above, also download policies.
Heartbeat interval: 5 minutes

OK Cancel Help

Pull mode

In pull mode, the client connects to the manager periodically, depending on the frequency of the heartbeat setting. This procedure repeats indefinitely. In pull mode, the number of agents that can be supported on a single server is dependent on the server performance, network bandwidth used for agents, server communication, and heartbeat frequency. In general, the less frequent the heartbeat, the more agents the server can support.

- There is no maximum to the number of clients that can connect to a given Management Server in Pull Mode
- It is recommend that setting for the heartbeat be set to no lower than the number of clients connecting to the management server divided by 1,000.
(# clients /1000 per minute)
Ex. 10,000 Clients on the Management Sever. Polling should not be set lower the 10 Minutes.

Push mode

In push mode, the agent establishes a persistent TCP connection to the server. If the client cannot connect to the management server it retries periodically, depending on the frequency of the heartbeat setting. When there is a change in the server status, the server notifies the agent. Logs are sent from the client to the SEPM server based upon the heartbeat interval set. Due to the persistent TCP connection, push mode is more intensive than pull mode.

- Client to Server Ratio Maximum: 50,000 clients to Management server in Push Mode
- It is recommend setting the heartbeat to no lower than the number of clients connecting to the management server divided by 1,000.
(# clients /1000 per minute)

Example of Heartbeat Interval

Number of Clients	Minimum Polling Interval
5,000	5 minutes
15,000	15 minutes
25,000	25 minutes

Calculating Content Distribution Time

The SEPM server can accommodate a larger number of clients, therefore sizing is typically done by determining the amount of time it takes for content updates to occur across the organization. Content updates can consist of the following types: Antivirus definitions, Intrusion Prevention signatures, and engines updates. These content updates with vary in size and frequency.

To determine the length of time needed to perform a content distribution update in a best case scenario, please follow the formula of:

$$\text{Concurrent Connections} \times \text{Content Size} \div \text{Available Bandwidth} = \text{Content Distribution Time}$$

*Average Content Size = 70-100kB

Example Content Distribution Time using 70kB update. The example assumes the use of the entire bandwidth

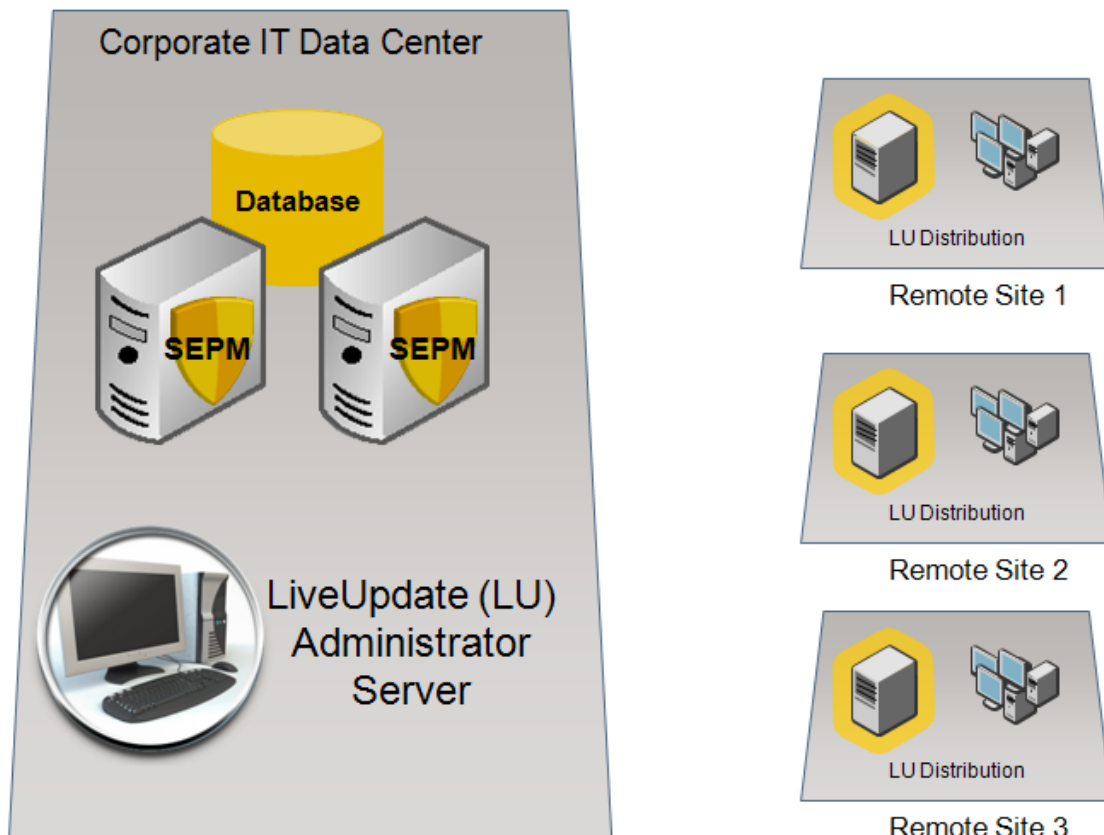
Bandwidth	# Clients	Time
T1 (1.54Mbps)	5,000	30 Minutes
	15,000	2 Hours
10 Mbps	5,000	4 Minutes
	15,000	14 Minutes
100 Mbps	5,000	30 Seconds
	15,000	2 Minutes
1 Gbps	5,000	3 Seconds
	15,000	9 Seconds

**Note that latency can also be affected by network utilization and protocol overhead.*

To decrease the amount of time it takes to perform content distribution updates, consider distributing the load of clients across multiple managers, deploy Group Update Providers, or use alternative methods for deploying content updates, ie. LiveUpdate Servers, 3rd party distribution tools.

The Group Update Provider (GUP) provides updates to clients in the group, and any subgroups that inherit policies as set on the Clients tab. If there is a concern of multiple updates occurring across a given link, then Administrators should consider deploying a GUP. It is recommended to consider an alternative update method if supplying updates to more than 50-100 nodes. On average, a client configured as a GUP will require an additional 50MB of disk space to store content updates. This number can vary depending upon the age of the clients connecting for updates and the size of the delta created to update them.

For customer environments where there is a need to provide content updates to more than 100 nodes, and adding a separate Symantec Endpoint Protection Manager (SEPM) is not a viable solution, consider the use of a Symantec LiveUpdate Server. Below is an example architecture of using the LiveUpdate Server in an environment.

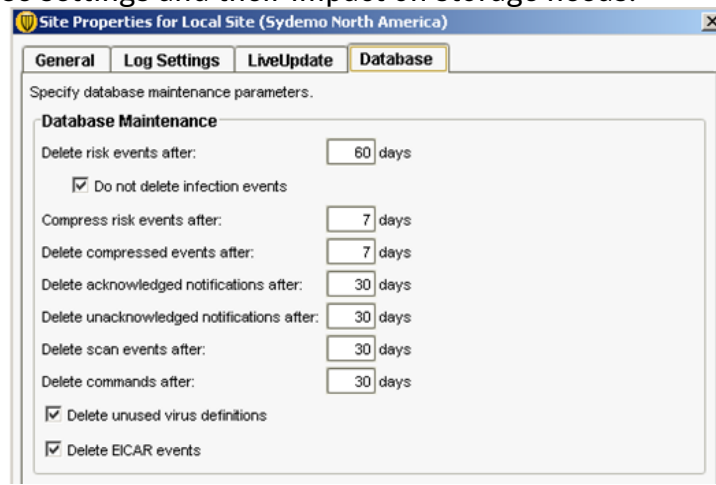


In the above scenario, the Corporate Site (HQ) has a central LiveUpdate Server that redistributes content to each remote sites' LiveUpdate Server. LiveUpdate Distribution servers are simply acting as a distribution point using HTTP, FTP, or Network Shares. LiveUpdate Distribution Servers add very little overhead to an existing server.

For a complete list of hardware and software requirements for the SEP client, please refer to the "Installation Guide for Symantec Endpoint Protection and Network Access Control" document.

SEPM Server and Database Sizing

Several factors can influence the size of the SEP database, as well as the storage space required on the SEPM server itself. These factors include settings such as database maintenance and log sizing/expiration, content updates, client installation packages, and backup information. Detailed below are some examples of these settings and their impact on storage needs.



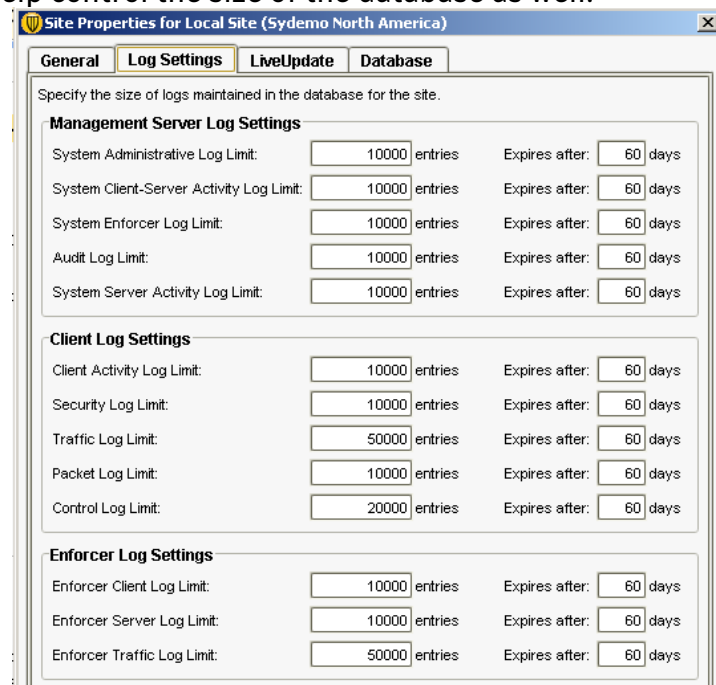
The screenshot shows the 'Database' tab of the 'Site Properties for Local Site (Sydemo North America)' window. The 'Database Maintenance' section includes the following settings:

Setting	Value
Delete risk events after:	60 days
Compress risk events after:	7 days
Delete compressed events after:	7 days
Delete acknowledged notifications after:	30 days
Delete unacknowledged notifications after:	30 days
Delete scan events after:	30 days
Delete commands after:	30 days

Additional options checked:

- Do not delete infection events
- Delete unused virus definitions
- Delete EICAR events

Administrators can configure maintenance options for the data stored in the database. Database maintenance options such as deleting risk events, event compression, and deleting events after a certain amount of time help you to manage the size of your database by specifying how long to keep data. These options will help control the size of the database as well.



The screenshot shows the 'Log Settings' tab of the 'Site Properties for Local Site (Sydemo North America)' window. It is divided into three sections:

Management Server Log Settings

Log Type	Limit (entries)	Expires after (days)
System Administrative Log Limit:	10000	60
System Client-Server Activity Log Limit:	10000	60
System Enforcer Log Limit:	10000	60
Audit Log Limit:	10000	60
System Server Activity Log Limit:	10000	60

Client Log Settings

Log Type	Limit (entries)	Expires after (days)
Client Activity Log Limit:	10000	60
Security Log Limit:	10000	60
Traffic Log Limit:	50000	60
Packet Log Limit:	10000	60
Control Log Limit:	20000	60

Enforcer Log Settings

Log Type	Limit (entries)	Expires after (days)
Enforcer Client Log Limit:	10000	60
Enforcer Server Log Limit:	10000	60
Enforcer Traffic Log Limit:	50000	60

Logging options can be configured by the Administrator for the maximum number of entries stored in the logs and the length of time (days) to store those entries. Maintenance options help the Administrator to manage the size of the database by specifying which logs they may want to retain longer, as well as maximum log count.

Log Size Examples

Example of Log Event Storage Costs

Log	Size per 10,000 Log Entries
System Admin	10 MB
System Client Server Activity	9 MB
System Enforcer	6 MB
Audit Log	6 MB
System Server Activity	66 MB
Client Activity	45 MB
Security Log	45 MB
Traffic Log	45 MB
Packet	45 MB
Control	45 MB
Enforcer Client	16 MB
Enforcer Server	14 MB
Enforcer Traffic	9 MB

The above chart example shows the size of the various log data per 10,000 entries in MB.

Example of Detected/Quarantined Virus Event Storage Costs

Number of Viruses in DB	Approximate Space
1,000	0.8 MB
5,000	4.3 MB
15,000	12.9 MB
25,000	21.6 MB
50,000	43.2 MB

The above chart shows the approximate size required to store information on detected/quarantined virus' ranging from 1,000 to 50,000 viruses in the database. The average, for an implementation of 17,000 nodes is roughly 15,000 detected and quarantined every 60 days.

Example of Log Data Statistics for a 17,000 Node Environment*

Log	Average Events per Log
System Admin	10 Events per Day per Admin
System Client Server Activity	5 Events per Day per Machine
Audit Log	Usually Very Small
System Server Activity	650 Events per Server Per Day
Client Activity	120 Events per machine per Day
Security Log	1 Event per Day per Machine
Traffic Log	2400 Events per Machine per Day
Packet	Could be Extremely Large Depending on Policies
Control	Could be Extremely Large Depending on Policies
Viruses	Average is 250 Viruses per Month per 1000 Clients

**Log Metric Data will vary from customer to customer*

Symantec Endpoint Protection Manager Hardware Recommendations

For Servers with less than 10,000 clients

- 2GB RAM Minimum Requirement
- Single Processor

For Servers with more than 10,000 clients

- 4GB RAM Minimum Requirement
- Dual Processor recommended

For installations with a client/server ratio of 5,000 clients or less using the default log settings, Symantec recommends the use of the embedded Sybase database. For installations with a client/server ratio greater than 5,000 clients or using a higher level of log settings, Symantec recommends the use of an off-box Microsoft SQL database.

For SQL Database Sizing, Symantec recommends using the Database Vendors recommended sizing tools/guides.

For added performance, Symantec recommends using Microsoft Windows Server 2003 64-bit, Microsoft SQL Server 2005 64-bit, and hard drives with 10,000 RPM capability or higher (SCSI).

Additional optimization can be obtained for disk I/O performance on the Symantec Endpoint Protection Manager (SEPM). It is recommended to install the different components (manager software, IIS server, data) on different disk drives if possible, or use a SAN environment with a product such as Symantec Storage Foundation.

Backups

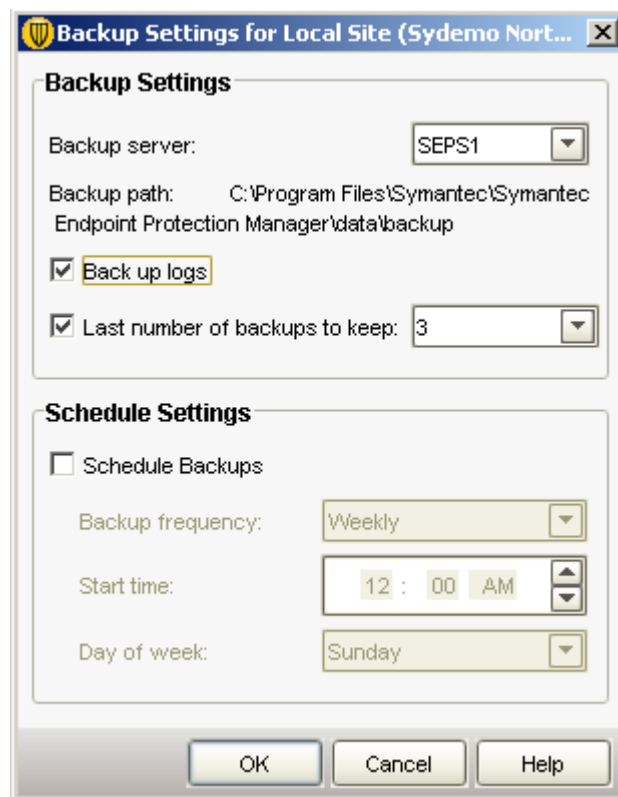
When backing up a database, a separate copy of the database is created. In the event that data corruption or hardware failure occur, the Administrator can revert to a previous copy of a backup to restore lost data. A back up the database can be created using the Symantec Endpoint Protection Manager console or by using the Symantec Database Backup and Restore utility. The Symantec Database Backup and Restore utility is automatically installed during the installation of the SEPM server.

Back up options:

- Microsoft SQL database only—by using the Microsoft SQL Server Enterprise Manager to set up a maintenance plan that includes automatic backups.
- Embedded or an MS SQL database—from the Symantec Endpoint Protection Manager console. Perform an on-demand backup and also schedule automatic backups to occur.

Backups should preferably be stored on a separate disk drive. Symantec recommends backing up the disk drive regularly.

Backup Sizing Example



The size and number of backups retained will impact the total disk space required on the SEPM server. The backup size is approximately 75% of database size multiplied by the number of copies being retained.

eg. 1GB db * 0.75 * 3 Copies = 2.3 GB of Disk Space needed on SEPS1

Content Updates and Installation packages

Client update packages, patches, and content updates are also stored in the SEP database and will affect storage requirements. Product updates and patches contain information for client packages as well as information for each language or locale. Please note that patches also create new full client builds as well. Each full client package requires approximately 64MB space in the database.

Content updates require approximately 300MB worth of space in the database. These updates contain information for the following technologies:

- Definitions and Eraser
- Intrusion Prevention Signatures
- Proactive Threat Scan Engine
- Proactive Threat Scan White Lists
- Decomposer

Calculating Total Disk Space Requirements: Example

The scenario gives an example of the space required for a customer Symantec Endpoint Protection implementation with 17,000 nodes. This example assumes the following metrics:

- An average 15,000 viruses over 60 days
- Keeping 20,000 Events of each Log
- Keeping 5 Versions of each SEP client (32/64 Bit, English and French language)
- 7 Backups are being retained

Item	Space Required
15,000 Viruses Detected/Quarantined	12.9 MB
20,000 Events per Log	722 MB
20 Client versions in DB	1280 MB
Content Updates	300 MB

TOTAL Database Size = 3.2GB*

*The database size of 2.3GB must be multiplied by 1.4 to account for the overhead of indexes and other tables in the database.

The space required on the SEPM server to store 7 backups is approximately 14.5GB. A key component of the SEPM server is Internet Information Server (IIS) content which equals approximately 4GB.

Symantec Network Access Control Enforcer Appliance Throughput

- Gateway Enforcer: 25,000 concurrent sessions (1 Gbps throughput)
- DHCP Enforcer: 50,000 concurrent sessions
- LAN Enforcer: 10,000 concurrent sessions

Copyright © 2007 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, Symantec Network Access Control, Symantec Sygate Enterprise Protection 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.

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.

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
<http://www.symantec.com>