Symantec™ Data Loss Prevention System Maintenance Guide

Version 11.0

Symantec

Symantec™ Data Loss Prevention System Maintenance Guide

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: 11.0

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

Performing system maintenance

This chapter includes the following topics:

About the system maintenance schedule

You should perform system maintenance regularly to keep the Symantec Data Loss Prevention system working properly. You should set up a regular schedule for the maintenance that operates after key events in the system such as installation or upgrades. You can also set up regular backup times to create restore points of your system. System maintenance also includes the diagnostic tools that let you troubleshoot issues as they arise.

Develop a schedule for the following system maintenance tasks:

- Respond to system events as they occur.
  See "About system events" on page 27.
- Back up your system
- Use diagnostic tools

Back up your system at the following time:

- After installation
- Before upgrades
- After custom configuration changes
- After the encrypted key is generated
- Before you change network topology or system configuration by adding new detection servers

- On a regular basis, such as weekly or bi-weekly; or, if your company already has internal backup policies, follow them as a general proactive maintenance procedure

See "About backup and recovery on Windows" on page 47.

See "About backup and recovery on Linux" on page 71.

Use Diagnostic Tools at the following times:

- After installation but before initial setup and configuration changes
- After new detection servers are added
- Before calling Symantec Support to help troubleshoot issues
- Periodically to monitor system health

See "About diagnostic tools" on page 43.

Chapter 2

Understanding underlying system resources

This chapter includes the following topics:

About the Enforce Server directory structure

The Symantec Data Loss Prevention installer creates these directories on the Enforce Server during the installation process. Never modify the directory structure.

See "About the detection server directory structure" on page 15.

Table 2-1 Enforce Server directory structures

Linux directory structure	Windows directory structure	Description
`/opt/Vontu/Protect`	`\Vontu\Protect`	Core product (includes manager.ver).
`/opt/Vontu/Protect/agentupdates`	`\Vontu\Protect\agentupdates`	Files that are used to update Endpoint Agents.
`/opt/Vontu/Protect/ant`	`\Vontu\Protect\ant`	Files that the Apache Ant software uses.

Table 2-1 Enforce Server directory structures *(continued)*

Linux directory structure	Windows directory structure	Description
/opt/Vontu/Protect/bin	\Vontu\Protect\bin	Executable files that reside in this directory are described in the *Symantec Data Loss Prevention Administration Guide.*
/opt/Vontu/Protect/config	\Vontu\Protect\config	The files with extensions of .properties and .conf store server configurations.
/var/Vontu/datafiles	\Vontu\Protect\datafiles	Exact Data: database profiles to be indexed.
/var/Vontu/documentprofiles	\Vontu\Protect\documentprofiles	Index Document: document archives uploaded for indexes and whitelists.
/opt/Vontu/Protect/ECU	\Vontu\Protect\ECU	Environment Check Utility.
/opt/Vontu/Protect/EULA	\Vontu\Protect\EULA	End User License Agreement.
/var/Vontu/incidents	\Vontu\Protect\incidents	Incidents that are stored on the Enforce Server before they are written to the database.
/var/Vontu/index	\Vontu\Protect\index	Profile indices for protected content (EDM, IDM, DGM); .rdx file extension.
/opt/Vontu/Protect/install	\Vontu\Protect\install	SQL used in table creation.
/opt/Vontu/Protect/keystore	\Vontu\Protect\keystore	Keystore files for TLS (Transport Layer Security) encryption of communication between Symantec Data Loss Prevention servers.
/opt/Vontu/Protect/languages	\Vontu\Protect\languages	Language pack files.
/opt/Vontu/Protect/lib	\Vontu\Protect\lib	.jar files with libraries used by Enforce processes. Used by Notifier and Persist Data, and so forth.
/opt/Vontu/Protect/license	\Vontu\Protect\license	Symantec Data Loss Prevention license files.
/var/log/Vontu	\Vontu\Protect\logs	Enforce Server log files.

Table 2-1 Enforce Server directory structures *(continued)*

Linux directory structure	Windows directory structure	Description
/opt/Vontu/Protect/plugins	\Vontu\Protect\plugins	Custom code, data, and configuration changes, usually added with the help of Symantec Support or Professional Services.
/opt/Vontu/Protect/Pstdepositfolder	\Vontu\Protect\Pstdepositfolder	A temporary directory used when the application processes the Personal Storage Table (.pst) files.
/opt/Vontu/Protect/Pstlocalcopy	\Vontu\Protect\Pstlocalcopy	A temporary directory used when the application processes Personal Storage Table (.pst) files.
/var/Vontu/sharelists	\Vontu\Protect\sharelists	Discover target share lists.
/opt/Vontu/Protect/temp	\Vontu\Protect\temp	Temporary, Enforce-generated files are stored here. Duration of files depends on the type of file.
/opt/Vontu/Protect/tomcat	\Vontu\Protect\tomcat	Contains the code that runs the Enforce Web server. You must have the assistance of Symantec Support if you want to make changes.
/opt/Vontu/Protect/tools	\Vontu\Protect\tools	Additional SQL to clear events: ClearSystemEvents.sql.
/opt/Vontu/Protect/updates	\Vontu\Protect\updates	Directory for product upgrades.

About the detection server directory structure

The following table describes the detection server directory structure.

See "About Enforce Server services" on page 17.

Table 2-2 Detection server directory structures

Linux directory structure	Windows directory structure	Description
/var/Vontu/drop	\drop	Used to induct email traffic with SMTP copy rule and test with MIME email files (.eml).

Table 2-2 Detection server directory structures *(continued)*

Linux directory structure	Windows directory structure	Description
/var/Vontu/drop_discover	\drop_discover	Used with Discover Universal Data Store API.
/var/Vontu/drop_ep	\drop_ep	Temporary storage directory for data from the endpoint agents.
/var/Vontu/drop_pcap	\drop_pcap	Temporary storage for reassembled network streams.
/var/Vontu/packet_spool, icap_spool	\packet_spool, icap_spool	Spool location for traffic capture.
/opt/Vontu/Protect	\Vontu\Protect	Core product (includes monitor.ver).
/opt/Vontu/Protect/agentupdates	\Vontu\Protect\agentupdates	Directory for product upgrades.
/opt/Vontu/Protect/ant	\Vontu\Protect\ant	Files that Apache Ant software uses.
/opt/Vontu/Protect/bin	\Vontu\Protect\bin	.exe files, including Endace drivers (dag) for the Network Monitor Server. These files are described in the *Symantec Data Loss Prevention Administration Guide*.
/opt/Vontu/Protect/config	\Vontu\Protect\config	The files with extensions of .properties and .conf store configurations for the detection server.
/opt/Vontu/Protect/ECU	\Vontu\Protect\ECU	Environment Check Utility.
/var/Vontu/incidents	\Vontu\Protect\incidents	Incidents that are stored on the detection server (monitors) before they are sent to the Enforce Server.
/var/Vontu/index	\Vontu\Protect\index	Profile indices for protected content (EDM, IDM, DGM); .rdx file extension.
/opt/Vontu/Protect/install	\Vontu\Protect\install	

Table 2-2 Detection server directory structures *(continued)*

Linux directory structure	Windows directory structure	Description
/opt/Vontu/Protect/keystore	\Vontu\Protect\keystore	Keystore files for TLS (Transport Layer Security) encryption of communication between Symantec Data Loss Prevention servers.
/opt/Vontu/Protect/lib	\Vontu\Protect\lib	
/var/log/Vontu	\Vontu\Protect\logs	Detection server log files.
/opt/Vontu/Protect/plugins	\Vontu\Protect\plugins	Custom code, data, or configuration changes, usually added with the help of Symantec Support or Professional Services.
/opt/Vontu/Protect/Pstdepositfolder	\Vontu\Protect\Pstdepositfolder	A temporary folder that the application uses when it processes the Personal Storage Table (.pst) files.
/opt/Vontu/Protect/Pstlocalcopy	\Vontu\Protect\Pstlocalcopy	A temporary folder that the application uses when it processes the Personal Storage Table (.pst) files.
/opt/Vontu/Protect/temp	\Vontu\Protect\temp	
/opt/Vontu/Protect/updates	\Vontu\Protect\updates	Directory for product upgrades.

About Enforce Server services

The Symantec Data Loss Prevention services may need to be stopped and started periodically. This section provides a brief description of each service and how to start and stop the services on supported platforms.

The Symantec Data Loss Prevention services for the Enforce Server are described in the following table:

Table 2-3 Services on the Enforce Server

Service Name	Description
Vontu Manager	Provides the centralized reporting and management services for Symantec Data Loss Prevention.
Vontu Monitor Controller	Controls the detection servers (monitors).

Table 2-3 Services on the Enforce Server *(continued)*

Service Name	Description
Vontu Notifier	Provides the database notifications.
Vontu Incident Persister	Writes the incidents to the database.
Vontu Update	Installs the Symantec Data Loss Prevention system updates. This service only runs during system updates and upgrades.

See "About starting and stopping services on Windows" on page 18.

About starting and stopping services on Windows

The procedures for starting and stopping services vary according to installation configurations and between Enforce and detection servers.

- See "Starting an Enforce Server on Windows" on page 18.
- See "Stopping an Enforce Server on Windows" on page 19.
- See "Starting a Detection Server on Windows" on page 19.
- See "Stopping a Detection Server on Windows" on page 19.
- See "Starting services on single-tier Windows installations" on page 20.
- See "Stopping services on single-tier Windows installations" on page 20.

Starting an Enforce Server on Windows

Use the following procedure to start the Symantec Data Loss Prevention services on a Windows Enforce Server.

To start the Symantec Data Loss Prevention services on a Windows Enforce Server

1. On the computer that hosts the Enforce Server, navigate to **Start > All Programs > Administrative Tools > Services** to open the Windows Services menu.
2. Before starting other Symantec Data Loss Prevention services, start the Vontu Notifier service.
3. Start the remaining Symantec Data Loss Prevention services, including the following services:
   - Vontu Manager
   - Vontu Incident Persister
   - Vontu Update

- Vontu Monitor Controller

See "Stopping an Enforce Server on Windows" on page 19.

Stopping an Enforce Server on Windows

Use the following procedure to stop the Symantec Data Loss Prevention services on a Windows Enforce Server.

To stop the Symantec Data Loss Prevention Services on a Windows Enforce Server

1. On the computer that hosts the Enforce Server, navigate to **Start > All Programs > Administrative Tools > Services** to open the Windows Services menu.
2. From the Services menu, stop all running Symantec Data Loss Prevention services, which might include the following services:
   - Vontu Update
   - Vontu Incident Persister
   - Vontu Manager
   - Vontu Monitor Controller
   - Vontu Notifier

See "Starting an Enforce Server on Windows" on page 18.

Starting a Detection Server on Windows

To start the Symantec Data Loss Prevention services on a Windows detection server

1. On the computer that hosts the detection server, navigate to **Start > All Programs > Administrative Tools > Services** to open the Windows Services menu.
2. Start the Symantec Data Loss Prevention services, which might include the following services:
   - Vontu Monitor
   - Vontu Update

See "Stopping a Detection Server on Windows" on page 19.

Stopping a Detection Server on Windows

Use the following procedure to stop the Symantec Data Loss Prevention services on a Windows detection server.

To stop the Symantec Data Loss Prevention Services on a Windows detection server

1. On the computer that hosts the detection server, navigate to **Start > All Programs > Administrative Tools > Services** to open the Windows Services menu.
2. From the **Services** menu, stop all running Symantec Data Loss Prevention services, which might include the following services:
   - Vontu Update
   - Vontu Monitor

See "Starting a Detection Server on Windows" on page 19.

Starting services on single-tier Windows installations

Use the following procedure to start the Symantec Data Loss Prevention services on a single-tier installation on Windows.

To start the Symantec Data Loss Prevention services on a single-tier Windows installation

1. On the computer that hosts the Symantec Data Loss Prevention server applications, navigate to **Start > All Programs > Administrative Tools > Services** to open the Windows Services menu.
2. Before starting other Symantec Data Loss Prevention services, start the Vontu Notifier service.
3. Start the remaining Symantec Data Loss Prevention services, which might include the following services:
   - Vontu Manager
   - Vontu Monitor
   - Vontu Incident Persister
   - Vontu Update
   - Vontu Monitor Controller

See "Stopping services on single-tier Windows installations" on page 20.

Stopping services on single-tier Windows installations

Use the following procedure to stop the Symantec Data Loss Prevention services on a single-tier installation on Windows.

To stop the Symantec Data Loss Prevention services on a single-tier Windows installation

1. On the computer that hosts the Symantec Data Loss Prevention server applications, navigate to **Start > All Programs > Administrative Tools > Services** to open the Windows Services menu.
2. From the Services menu, stop all running Symantec Data Loss Prevention services, which might include the following services:
   - Vontu Update
   - Vontu Incident Persister
   - Vontu Manager
   - Vontu Monitor Controller
   - Vontu Notifier
   - Vontu Monitor

See "Starting services on single-tier Windows installations" on page 20.

Starting and stopping services on Linux

The procedures for starting and stopping services vary according to installation configurations and between Enforce and detection servers.

- See "Starting an Enforce Server on Linux" on page 21.
- See "Stopping an Enforce Server on Linux" on page 22.
- See "Starting a detection server on Linux" on page 22.
- See "Stopping a detection server on Linux" on page 23.
- See "Starting services on single-tier Linux installations" on page 23.
- See "Stopping services on single-tier Linux installations" on page 24.

Starting an Enforce Server on Linux

Use the following procedure to start the Symantec Data Loss Prevention services on a Linux Enforce Server.

To start the Symantec Data Loss Prevention services on a Linux Enforce Server

1. On the computer that hosts the Enforce Server, log on as root.
2. Change directory to `/opt/Vontu/Protect/bin`.

3 Before starting other Symantec Data Loss Prevention services, to start the Vontu Notifier service, enter:

```
./VontuNotifier.sh start
```

4 To start the remaining Symantec Data Loss Prevention services, enter:

```
./VontuManager.sh start
./VontuIncidentPersister.sh start
./VontuUpdate.sh start
./VontuMonitorController.sh start
```

See "Stopping an Enforce Server on Linux" on page 22.

Stopping an Enforce Server on Linux

Use the following procedure to stop the Symantec Data Loss Prevention services on a Linux Enforce Server.

To stop the Symantec Data Loss Prevention services on a Linux Enforce Server

1 On the computer that hosts the database, log on as root.

2 Change directory to `/opt/Vontu/Protect/bin`.

3 To stop all running Symantec Data Loss Prevention services, enter:

```
./VontuUpdate.sh stop
./VontuIncidentPersister.sh stop
./VontuManager.sh stop
./VontuMonitorController.sh stop
./VontuNotifier.sh stop
```

See "Starting an Enforce Server on Linux" on page 21.

Starting a detection server on Linux

Use the following procedure to start the Symantec Data Loss Prevention services on a Linux detection server.

To start the Symantec Data Loss Prevention services on a Linux detection server

1. On the computer that hosts the Enforce Server, log on as root.
2. Change directory to `/opt/Vontu/Protect/bin`.
3. To start the Symantec Data Loss Prevention services, enter:

```
./VontuMonitor.sh start
./VontuUpdate.sh start
```

See "Stopping a detection server on Linux" on page 23.

Stopping a detection server on Linux

Use the following procedure to stop the Symantec Data Loss Prevention services on a Linux detection server.

To stop the Symantec Data Loss Prevention services on a Linux detection server

1. On the computer that hosts the database, log on as root.
2. Change directory to `/opt/Vontu/Protect/bin`.
3. To stop all running Symantec Data Loss Prevention services, enter:

```
./VontuUpdate.sh stop
./VontuMonitor.sh stop
```

See "Starting a detection server on Linux" on page 22.

Starting services on single-tier Linux installations

Use the following procedure to start the Symantec Data Loss Prevention services on a single-tier installation on Linux.

To start the Symantec Data Loss Prevention services on a single-tier Linux installation

1. On the computer that hosts the Symantec Data Loss Prevention server applications, log on as root.
2. Change directory to `/opt/Vontu/Protect/bin`.

3 Before starting other Symantec Data Loss Prevention services, to start the Vontu Notifier service, enter:

```
./VontuNotifier.sh start
```

4 To start the remaining Symantec Data Loss Prevention services, enter:

```
./VontuManager.sh start
./VontuMonitor.sh start
./VontuIncidentPersister.sh start
./VontuUpdate.sh start
./VontuMonitorController.sh start
```

See "Stopping services on single-tier Linux installations" on page 24.

Stopping services on single-tier Linux installations

Use the following procedure to stop the Symantec Data Loss Prevention services on a single-tier installation on Linux.

To stop the Symantec Data Loss Prevention services on a single-tier Linux installation

1 On the computer that hosts the Symantec Data Loss Prevention servers, log on as root.

2 Change directory to `/opt/Vontu/Protect/bin`.

3 To stop all running Symantec Data Loss Prevention services, enter:

```
./VontuUpdate.sh stop
./VontuIncidentPersister.sh stop
./VontuManager.sh stop
./VontuMonitor.sh stop
./VontuMonitorController.sh stop
./VontuNotifier.sh stop
```

See "Starting services on single-tier Linux installations" on page 23.

About using log files

Symantec Data Loss Prevention provides many log files that can be used to interpret how the system is running.

See "About log files" on page 95.

About Symantec Data Loss Prevention system statistics

Symantec Data Loss Prevention provides summary statistics for the Enforce Server and each detection server. To view the general system statistics, go to the **System > Servers > Overview** screen.

To view statistics for an individual server, click on the server's name. For individual servers, the following statistics are displayed:

- The **Avg. CPU** item is a snapshot of the CPU utilization at the time it was measured. CPU utilization is measured periodically.
- The **Physical Memory** item is the amount of physical memory available to the CPU at a given time. The physical memory usage for the Enforce Server is fairly constant.
- The **Disk Usage** item is defined as follows:

Windows	Total number of free bytes/total number of available bytes
Linux	Disk usage of the root partition

Symantec recommends using standard system tools to determine the system state. Do not rely solely on the system statistics that are provided on the **Server Detail** page.

See "About diagnostic tools" on page 43.

Chapter 3

Using system event reports and alerts

This chapter includes the following topics:

About system events

System events related to your Symantec Data Loss Prevention installation are monitored, reported, and logged.

System event reports are viewed from the Enforce Server administration console:

- The five most recent system events of severity Warning or Severe are listed on the **Servers Overview** screen (**System > Servers > Overview**).
  See the *Symantec Data Loss Prevention Administration Guide* for information on the **Servers Overview** screen.
- Reports on all system events of any severity can be viewed by going to **System > Servers > Events**.
  See "System events reports" on page 28.
- Recent system events for a particular detection server are listed on the **Server Detail** screen for that server.
  See the *Symantec Data Loss Prevention Administration Guide* for information on the **Server Detail** screen.
- Click on any event in an event list to go to the **Event Details** screen for that event. The **Event Details** screen provides additional information about the event.
  See "Server event detail" on page 31.

There are three ways that system events can be brought to your attention:

- System event reports displayed on the administration console
- System alert email messages
  See "About system alerts" on page 38.
- Syslog functionality
  See "Enabling a syslog server" on page 36.

Some system events require a response.

See "About system event responses" on page 34.

To narrow the focus of system event management you can:

- Use the filters in the various system event notification methods.
  See "System events reports" on page 28.
- Configure the system event thresholds for individual servers.
  See "Configuring event thresholds and triggers" on page 32.

System events reports

To view all system events, go to the system events report screen (**System > Servers > Events**). This screen lists events, one event per line. The list contains those events that match the selected data range, and any other filter options that are listed in the **Applied Filters** bar. For each event, the following information is displayed:

Table 3-1 System events list

Type	The type (severity) of the event. Type may be any one of those listed in Table 3-2.
Time	The date and time of the event.
Server	The name of the server on which the event occurred.
Host	The IP address or host name of the server on which the event occurred.
Code	A number that identifies the kind of event. See the *Symantec Data Loss Prevention Administration Guide* for information on event code numbers.
Summary	A brief description of the event. Click on the summary for more detail about the event.

Table 3-2 System event types

	System information
	Warning
	Severe

You can select from several report handling options.

Click any event in the list to go to the **Event Details** screen for that event. The **Event Details** screen provides additional information about the event.

See "Server event detail" on page 31.

Since the list of events can be long, filters are available to help you select only the events that you are interested in. By default, only the Date filter is enabled and it is initially set to All Dates. The Date filter selects events by the dates the events occurred.

To filter the list of system events by date of occurrence

1. Go to the Filter section of the events report screen and select one of the date range options.
2. Click **Apply**.
3. Select **Custom** from the date list to specify beginning and end dates.

In addition to filtering by date range, you can also apply advanced filters. Advanced filters are cumulative with the current date filter. This means that events are only listed if they match the advanced filter and also fall within the current date range. Multiple advanced filters can be applied. If multiple filters are applied, events are only listed if they match all the filters and the date range.

To apply additional advanced filters

1. Click on **Advanced Filters and Summarization**.
2. Click on **Add Filter**.
3. Choose the filter you want to use from the left-most drop-down list. Available filters are listed in Table 3-3.
4. Choose the filter-operator from the middle drop-down list.

   For each advanced filter you can specify a filter-operator **Is Any Of** or **Is None Of**.
5. Enter the filter value, or values, in the right-hand text box, or click a value in the list to select it.

- To select multiple values from a list, hold down the Control key and click each one.
- To select a range of values from a list, click the first one, then hold down the Shift key and click the last value in the range you want.

6 (Optional) Specify additional advanced filters if needed.

7 When you have finished specifying a filter or set of filters, click **Apply**.

Click the red X to delete an advanced filter.

The **Applied Filters** bar lists the filters that are used to produce the list of events that is displayed. Note that multiple filters are cumulative. For an event to appear on the list it must pass all the applied filters.

The following advanced filters are available:

Table 3-3 System events advanced filter options

Event Code	Filter events by the code numbers that identify each kind of event. You can filter by a single code number or multiple code numbers separated by commas (2121, 1202, 1204). Filtering by code number ranges, or greater than, or less than operators is not supported.
Event type	Filter events by event severity type (Info, Warning, or Severe).
Server	Filter events by the server on which the event occurred.

Note: A small subset of the parameters that trigger system events have thresholds that can be configured. These parameters should only be adjusted with advice from Symantec Support or Professional Services. Before changing these settings, you should have a thorough understanding of the implications that are involved. The default values are appropriate for most installations.

See "Configuring event thresholds and triggers" on page 32.

See "About system events" on page 27.

See "Server event detail" on page 31.

See " Working with saved system reports" on page 31.

See "Configuring event thresholds and triggers" on page 32.

See "About system alerts" on page 38.

Server event detail

The **Server Event Detail** screen is reached by **System > Servers > Events** and then clicking on one of the listed events.

See "System events reports" on page 28.

The **Server Event Detail** screen displays all of the information available for the selected event. None of the information on this screen is editable.

The **Server Event Detail** screen is divided into two sections—**General** and **Message**.

Table 3-4 Event detail — General

Type	The event is one of the following types: ■ Info: Information about the system. ■ Warning: A problem that is not severe enough to generate an error. ■ Severe: An error that requires immediate attention.
Time	The date and time of the event.
Server	The name of the server.
Host	The host name or IP address of the server.

Table 3-5 Event detail — Message

Code	A number that identifies the kind of event. See the *Symantec Data Loss Prevention Administration Guide* for information on event code numbers.
Summary	A brief description of the event.
Detail	Detailed information about the event.

See "About system events" on page 27.

See "Server event detail" on page 31.

See "System events reports" on page 28.

See "About system alerts" on page 38.

Working with saved system reports

The **System Reports** screen lists system and agent-related reports that have previously been saved. To display the **System Reports** screen, click **System > System Reports**. Use this screen to work with saved system reports.

To create a saved system report

1. Go to one of the following screens:
   - System Events (**System > Events**)
   - Agents Overview (**System > Agents > Overview**)
   - Agents Events (**System > Agents > Events**)
2. Select the filters and summaries for your custom report.
3. Select **Report > Save As**.
4. Enter the saved report information.
5. Click **Save**.

The **System Reports** screen is divided into two sections:

- **System Event - Saved Reports** lists saved system reports.
- **Agent Management - Saved Reports lists saved agent reports.**

For each saved report you can perform the following operations:

- Share the report. Click **share** to allow other Symantec Data Loss Prevention uses who have the same role as you to share the report. Sharing a report cannot be undone; after a report is shared it cannot be made private. After a report is shared, all users with whom it is shared can view, edit, or delete the report.
- Change the report name or description. Click the pencil icon to the right of the report name to edit it.
- Change the report scheduling. Click the calendar icon to the right of the report name to edit the delivery schedule of the report and to whom it is sent.
- Delete the report. Click the red X to the right of the report name to delete the report.

See the *Symantec Data Loss Prevention Administration Guide* for information on creating and using reports.

Configuring event thresholds and triggers

A small subset of the parameters that trigger system events have thresholds that can be configured. These parameters are configured for each detection server separately. These parameters should only be adjusted with advice from Symantec Support or Professional Services. Before changing these settings, you should have a thorough understanding of the implications. The default values are appropriate for most installations.

See "About system events" on page 27.

To view and change the configurable parameters that trigger system events

1. Go to the **Server Overview** screen (**System > Servers > Overview**).
2. Click on the name of a detection server to display that server's **Server Detail** screen.
3. Click the **Server Settings** tab.

   The **Advanced Server Settings** screen for that server is displayed.
4. Change the configurable parameters, as needed.

Table 3-6 Configurable parameters that trigger events

Parameter	Description	Event
BoxMonitor.DiskUsageError	Indicates the amount of filled disk space (as a percentage) that triggers a severe system event. For example, a Severe event occurs if a detection server is installed on the C drive and the disk space error value is 90. The detection server creates a Severe system event when the C drive usage is 90% or greater. The default is 90.	Low disk space
BoxMonitor.DiskUsageWarning	Indicates the amount of filled disk space (as a percentage) that triggers a Warning system event. For example, a Warning event occurs if the detection server is installed on the C drive and the disk space warning value is 80. Then the detection server generates a Warning system event when the C drive usage is 80% or greater. The default is 80.	Low disk space
BoxMonitor.MaxRestartCount	Indicates the number of times that a system process can be restarted in one hour before a Severe system event is generated. The default is 3.	*process name* restarts excessively
IncidentDetection.MessageWaitSevere	Indicates the number of minutes messages need to wait to be processed before a Severe system event is sent about message wait times. The default is 240.	Long message wait time

Table 3-6 Configurable parameters that trigger events *(continued)*

Parameter	Description	Event
IncidentDetection.MessageWaitWarning	Indicates the number of minutes messages need to wait to be processed before sending a Severe system event about message wait times. The default is 60.	Long message wait time
IncidentWriter.BacklogInfo	Indicates the number of incidents that can be queued before an Info system event is generated. This type of backlog usually indicates that incidents are not processed or are not processed correctly because the system may have slowed down or stopped. The default is 1000.	*N* incidents in queue
IncidentWriter.BacklogWarning	Indicates the number of incidents that can be queued before generating a Warning system event. This type of backlog usually indicates that incidents are not processed or are not processed correctly because the system may have slowed down or stopped. The default is 3000.	*N* incidents in queue
IncidentWriter.BacklogSevere	Indicates the number of incidents that can be queued before a Severe system event is generated. This type of backlog usually indicates that incidents are not processed or are not processed correctly because the system may have slowed down or stopped. The default is 10000.	*N* incidents in queue

About system event responses

There are three ways that system events can be brought to your attention:

- System event reports displayed on the administration console
- System alert email messages
  See "About system alerts" on page 38.
- Syslog functionality
  See "Enabling a syslog server" on page 36.

In most cases, the system event summary and detail information should provide enough information to direct investigation and remediation steps. The following table provides some general guidelines for responding to system events.

Table 3-7 System event responses

System Event or Category	Appropriate Response
Low disk space	If this event is reported on a detection server, recycle the Symantec Data Loss Prevention services on the detection server. The detection server may have lost its connection to the Enforce Server. The detection server then queues its incidents locally, and fills up the disk. If this event is reported on an Enforce Server, check the status of the Oracle and the Vontu Incident Persister services. Low disk space may result if incidents do not transfer properly from the file system to the database. This event may also indicate a need to add additional disk space.
Tablespace is almost full	Add additional data files to the database. When the hard disk is at 80% of capacity, obtain a bigger disk instead of adding additional data files. Refer to the *Symantec Data Loss Prevention Installation Guide*.
Licensing and versioning	Contact Symantec Support.
Monitor not responding	Restart the Symantec Monitor service. If the event persists, check the network connections. Make sure the computer that hosts the detections server is turned on by connecting to it. You can connect with terminal services or another remote desktop connection method. If necessary, contact Symantec Support. See "About Enforce Server services" on page 17.
Alert or scheduled report sending failed	Go to **System > Settings > General** and ensure that the settings in the Reports and Alerts and SMTP sections are configured correctly. Check network connectivity between the Enforce Server and the SMTP server. Contact Symantec Support.
Auto key ignition failed	Contact Symantec Support.
Cryptographic keys are inconsistent	Contact Symantec Support.

Table 3-7 System event responses *(continued)*

System Event or Category	Appropriate Response
Long message wait time	Increase detection server capacity by adding more CPUs or replacing the computer with a more powerful one. Decrease the load on the detection server. You can decrease the load by applying the traffic filters that have been configured to detect fewer incidents. You can also re-route portions of the traffic to other detection servers. Increase the threshold wait times if all of the following items are true: ■ This message is issued during peak hours. ■ The message wait time drops down to zero before the next peak. ■ The business is willing to have such delays in message processing.
process_name restarts excessively	Check the process by going to **System > Servers > Overview**. To see individual processes on this screen, Process Control must be enabled by going to **System > Settings > General > Configure**.
N incidents in queue	Investigate the reason for the incidents filling up the queue. The most likely reasons are as follows: ■ Connection problems. Response: Make sure the communication link between the Endpoint Server and the detection server is stable. ■ Insufficient connection bandwidth for the number of generated incidents (typical for WAN connections). Response: Consider changing policies (by configuring the filters) so that they generate fewer incidents.

Enabling a syslog server

Syslog functionality sends Severe system events to a syslog server. Syslog servers allow system administrators to filter and route the system event notifications on a more granular level. System administrators who use syslog regularly for monitoring their systems may prefer to use syslog instead of alerts. Syslog may be preferred if the volume of alerts seems unwieldy for email.

Syslog functionality is an on or off option. If syslog is turned on, all Severe events are sent to the syslog server.

To enable syslog functionality

1. Go to the `\Vontu\Protect\config` directory on Windows or the `/opt/Vontu/Protect/config` directory on Linux.
2. Open the `Manager.properties` file.
3. Uncomment the `#systemevent.syslog.host=` line by removing the # symbol from the beginning of the line, and enter the hostname or IP address of the syslog server.
4. Uncomment the `#systemevent.syslog.port=` line by removing the # symbol from the beginning of the line. Enter the port number that should accept connections from the Enforce Server server. The default is 514.
5. Uncomment the `#systemevent.syslog.format= [{0}] {1} - {2}` line by removing the # symbol from the beginning of the line. Then define the system event message format to be sent to the syslog server:

   If the line is uncommented without any changes, the notification messages are sent in the format: [server name] summary - details. The format variables are:

   - {0} - the name of the server on which the event occurred
   - {1} - the event summary
   - {2} - the event detail

   For example, the following configuration specifies that Severe system event notifications are sent to a syslog host named server1 which uses port 600.

   ```
   systemevent.syslog.host=server1
   systemevent.syslog.port=600
   systemevent.syslog.format= [{0}] {1} - {2}
   ```

Using this example, a low disk space event notification from an Enforce Server on a host named dlp-1 would look like:

```
dlp-1 Low disk space - Hard disk space for
incident data storage server is low. Disk usage is over 82%.
```

Note: Be sure to comment out the `#systemevent.syslog.format= [{0}] {1} - {2}` line. Do not comment out the `#systemevent.jmx.format= [{0}] {1} - {2}` line. The `jmx` option is not compatible with syslog servers.

See "About system events" on page 27.

About system alerts

System alerts are email messages that are sent to designated addresses when a particular system event occurs. You define what alerts (if any) that you want to use for your installation. Alerts are specified and edited on the **Configure Alert** screen, which is reached by **System > Servers > Alerts > Add Alert**.

Alerts can be specified based on event severity, server name, or event code, or a combination of those factors. Alerts can be sent for any system event.

The email that is generated by the alert has a subject line that begins with `Symantec Data Loss Prevention System Alert` followed by a short event summary. The body of the email contains the same information that is displayed by the **Event Detail** screen to provide complete information about the event.

See "Configuring the Enforce Server to send email alerts" on page 38.

See "Configuring system alerts" on page 39.

See "Server event detail" on page 31.

Configuring the Enforce Server to send email alerts

To send out email alerts regarding specified system events, the Enforce Server has to be configured to support sending of alerts and reports. This section describes how to specify the report format and how to configure Symantec Data Loss Prevention to communicate with an SMTP server.

After completing the configuration described here, you can schedule the sending of specific reports and create specific system alerts.

To configure Symantec Data Loss Prevention to send alerts and reports

1. Go to **System > Settings > General** and click **Configure**.

   The **Edit General Settings** screen is displayed.

2. In the **Reports and Alerts** section, select one of the following distribution methods:

   - **Send reports as links, logon is required to view**. Symantec Data Loss Prevention sends email messages with links to reports. You must log on to the Enforce Server to view the reports.

     Note: Reports with incident data cannot be distributed if this option is set.

- **Send report data with emails**. Symantec Data Loss Prevention sends email messages and attaches the report data.

3 Enter the Enforce Server domain name or IP address in the **Fully Qualified Manager Name** field.

If you send reports as links, Symantec Data Loss Prevention uses the domain name as the basis of the URL in the report email.

Do not specify a port number unless you have modified the Enforce Server to run on a port other than the default of 443.

4 If you want alert recipients to see any correlated incidents, check the **Correlations Enabled** box.

When correlations are enabled, users see them on the **Incident Snapshot** screen.

5 In the **SMTP** section, identify the SMTP server to use for sending out alerts and reports.

Enter the relevant information in the following fields:

- Server: The fully qualified hostname or IP address of the SMTP server that Symantec Data Loss Prevention uses to deliver system events and scheduled reports.
- System email: The email address for the alert sender. Symantec Data Loss Prevention specifies this email address as the sender of all outgoing email messages. Your IT department may require the system email to be a valid email address on your SMTP server.
- User ID: If your SMTP server requires it, type a valid user name for accessing the server. For example, enter *DOMAIN*\bsmith.
- Password: If your SMTP server requires it, enter the password for the User ID.

6 Click **Save**.

See "About system alerts" on page 38.

See "Configuring system alerts" on page 39.

See "About system events" on page 27.

Configuring system alerts

You can configure Symantec Data Loss Prevention to send an email alert whenever it detects a specified system event. Alerts can be specified based on event severity, server name, or event code, or a combination of those factors. Alerts can be sent for any system event.

See "About system alerts" on page 38.

Note that the Enforce Server must first be configured to send alerts and reports.

See "Configuring the Enforce Server to send email alerts" on page 38.

Alerts are specified and edited on the **Configure Alert** screen, which is reached by **System > Servers > Alerts** and then choosing **Add Alert** to create a new alert, or clicking on the name of an existing alert to modify it.

To create or modify an alert

1. Go the **Alerts** screen (**System > Servers > Alerts**).
2. Click the **Add Alert** tab to create a new alert, or click on the name of an alert to modify it.

   The Configure Alert screen is displayed.
3. Fill in (or modify) the name of the alert. The alert name is displayed in the subject line of the email alert message.
4. Fill in (or modify) a description of the alert.
5. Click **Add Condition** to specify a condition that will trigger the alert.

   Each time you click **Add Condition** you can add another condition. If you specify multiple conditions, every one of the conditions must be met to trigger the alert.

   Click on the red X next to a condition to remove it from an existing alert.
6. Enter the email address that the alert is to be sent to. Separate multiple addresses by commas.
7. Limit the maximum number of times this alert can be sent in one hour by entering a number in the **Max Per Hour** box.

   If no number is entered in this box, there is no limit on the number of times this alert can be sent out. The recommended practice is to limit alerts to one or two per hour, and to substitute a larger number later if necessary. If you specify a large number, or no number at all, recipient mailboxes may be overloaded with continual alerts.
8. Click **Save** to finish.

   The Alerts list is displayed.

There are three kinds of conditions that you can specify to trigger an alert:

- Event type - the severity of the event.
- Server - the server associated with the event.
- Event code - a code number that identifies a particular kind of event.

For each kind of condition, you can choose one of two operators:

- Is any of.
- Is none of.

For each kind of condition, you can specify appropriate parameters:

- Event type. You can select one, or a combination of, **Information**, **Warning**, **Severe**. Click on an event type to specify it. To specify multiple types, hold down the Control key while clicking on event types. You can specify one, two, or all three types.
- Server. You can select one or more servers from the list of available servers. Click on the name of server to specify it. To specify multiple servers, hold down the Control key while clicking on server names. You can specify as many different servers as necessary.
- Event code. Enter the code number. To enter multiple code numbers, separate them with commas or use the Return key to enter each code on a separate line. See the *Symantec Data Loss Prevention Administration Guide* for information on event codes.

By combining multiple conditions, you can define alerts that cover a wide variety of system conditions.

Note: If you define more than one condition, the conditions are treated as if they were connected by the Boolean "AND" operator. This means that the Enforce Server only sends the alert if all conditions are met. For example, if you define an event type condition and a server condition, the Enforce Server only sends the alert if the specified event occurs on the designated server.

See "About system alerts" on page 38.

See "Configuring the Enforce Server to send email alerts" on page 38.

See "System events reports" on page 28.

Chapter 4

Using diagnostic tools

This chapter includes the following topics:

About diagnostic tools

Symantec Data Loss Prevention provides diagnostic tools that can be used to monitor system health and troubleshoot problems with the underlying system.

The following tools are included:

- Diagnostic system information is displayed on-screen in the dashboard pages of the Enforce Server administration console.
  See "About system information review" on page 43.
- A utility for checking the system environment is installed with Symantec Data Loss Prevention.
  See "About the Environment Check Utility" on page 44.

About system information review

Various on-screen pages of the Symantec Data Loss Prevention software provide sources of information relevant to system maintenance.

The *Symantec Data Loss Prevention Administration Guide* and the online Help provide instructions for using most of the system administration tools.

The on-screen system administration pages provide access to features that are helpful in performing system maintenance.

These pages are referenced in many other sections of this guide in specific system maintenance tasks. Become familiar with their general contents for ease of use when you perform system maintenance.

See "About diagnostic tools" on page 43.

Table 4-1 System Administration pages

System Administration Page	Description
System > Servers > Overview	Displays a list of the system servers as well as recent error-level and warning-level system events. The overview provides functionality for adding servers, upgrading, and accessing the **Server Detail** pages.
System > Servers > Overview > Server Detail	Displays the detailed information about the server, provides functionality to stop, start, and recycle services, configure the server, and access the **Server Settings** page.
System > Servers > Overview > Server Detail > Server Settings	Enables the system administrators to modify Advanced Server settings.
System > Servers > Events	Provides a system events report.
System > Servers > Events > Sever Event Detail	Provides the additional details for the individual events that are listed in the system events report.
System > Servers > Alerts	Enables the system administrators to enable alerts for system events.

About the Environment Check Utility

The Environment Check Utility (ECU) performs a set of standard checks. These checks validate that the system environment is stable and that the system is likely to run efficiently.

The ECU checks the following items:

- The OS version of the servers
- The status of the Symantec Data Loss Prevention services
- The Symantec Data Loss Prevention version and build numbers
- Database parameters that are required for Symantec Data Loss Prevention
- Installation configuration settings

- The Enforce Server–to–detection server connections

See the *Symantec Data Loss Prevention System Administration Guide* for more information about the Environment Check Utility.

Chapter 5

Backing up and recovering on Windows

This chapter includes the following topics:

About backup and recovery on Windows

Perform system backups in case the Symantec Data Loss Prevention system crashes and needs to be restored. The system that should be backed up includes the Enforce Server, the detection servers, and the database. These backup procedures can be used for single-tier, two-tier, and three-tier installations.

The cold backup procedures for the Oracle 10g database are for non-database administrators who have no standard backup methods for databases.

Symantec recommends that administrators perform backups of their entire system. Administrators should follow all of the backup instructions that are in this section in the order in which they are presented.

Administrators who would prefer to back up only part of their system must determine which subsets of the system backup instructions to follow.

See "About periodic system backups on Windows" on page 48.

See "About partial backups on Windows" on page 49.

About periodic system backups on Windows

Perform system backups regularly. The frequency of system backups should be determined based on the size of the system and the internal company policies.

Large databases may take longer to back up. Database backups should be performed at least weekly.

Server configuration and file system backups should be performed after configuration changes are made on the Enforce Server or detection servers. Backups should also be made when you generate encrypted keys.

Symantec recommends that administrators perform backups of their entire system. Administrators should follow all of the backup instructions that are in this section in the order in which they are presented.

Complete system backups should be performed at the following times:

- After installation
- Before any system upgrades
- Any time the system changes, such as when a Symantec Data Loss Prevention server is added to or removed from the system configuration

See "About scheduling a system backup on Windows" on page 48.

About scheduling a system backup on Windows

When scheduling system backups, keep in mind the following concepts:

- Administrators of single-tier installations should note that the system is offline during backups while the files are copied.
  During backups, Symantec Data Loss Prevention does not scan or find incidents. Reports are inaccessible during backups. For these reasons, backups should be scheduled during times when the system is typically not very active. Such times may be on weekends when users are unlikely to use the system and when incidents are less likely to be generated.

For a description of single-tier installations, refer to the *Symantec Data Loss Prevention Installation Guide*.

- The backup methods that are described in this section do not accommodate point-in-time recovery. If the last system backup was two days ago and the system crashes, the information from those two days is lost. The system cannot be restored to times other than the time of the last backup.
- Before performing a backup, use regular company or system notifications to let users know that the system is offline and unavailable during the system backup.

See "About periodic system backups on Windows" on page 48.

About partial backups on Windows

Administrators who want to perform partial system backups can use either of the following subsets of the instructions.

Table 5-1 Performing partial backups

To back up a database only:	See "Preparing the backup location on Windows" on page 49. See "Performing a cold backup of the Oracle 10g database on Windows" on page 54.
To back up an Enforce Server or detection server only:	See "Preparing the backup location on Windows" on page 49. See "Backing up the server configuration files on Windows" on page 58. See "Backing up files stored on the file system on Windows" on page 59.

Preparing the backup location on Windows

Preparing the backup location involves determining the size of the backup and identifying a suitable backup location. Symantec Data Loss Prevention provides a Recovery Information Worksheet to help record the locations of the backup directories. The procedures in this section include instructions for when to record information in the worksheet. These instructions are for performing backups on hard drives. After you perform the backup on a hard drive, the data should be archived to tape.

See "About the Windows recovery information worksheet" on page 62.

Preparing the backup location consists of the following steps:

Table 5-2 Preparation of the backup location

Step	Action	Description
Step 1	Determine the size of the backup sections.	See "Determining the size of the backup on Windows" on page 50.
Step 2	Calculate the total size of the backup.	See "Calculating the total size of the backup on Windows" on page 52.
Step 3	Identify a backup location.	See "Identifying a backup location on Windows" on page 52.
Step 4	Create the backup directories.	See "Creating backup directories on Windows " on page 53.

See "About the Windows recovery information worksheet" on page 62.

See "About partial backups on Windows" on page 49.

Determining the size of the backup on Windows

The size of a full backup is the sum of the following items:

- The size of the database
- The size of the file system files to be backed up
- The size of the server configuration files to be backed up

However, file system and server configuration files do not need to be backed up as often as the database. The size of the backup varies depending on what is backed up. Only follow the sizing procedures in this section that are relevant to the backup being performed.

See "Preparing the backup location on Windows" on page 49.

To determine the size of the database

1. Log on to the computer that hosts the database as a user with administrative privileges.
2. Navigate to **Windows > Start > All Programs > Oracle - OraDb10g_home1 > Application Development > SQL Plus** to open Oracle SQL*Plus.

   See the *Symantec Data Loss Prevention Installation Guide*.
3. In the logon dialog box, in the **User Name** field, enter:

   ```
   /nolog
   ```

4 Click **OK**.

5 At the SQL> command prompt, to connect as the sysdba user, enter:

```
connect sys/password@protect as sysdba
```

where *password* is the password created for single-tier and two-tier installations.

See the *Symantec Data Loss Prevention Installation Guide*.

6 After receiving the *Connected* message, run the following SQL query by copying or entering it at the command prompt:

```
SELECT ROUND(SUM(bytes)/1024/1024/1024, 4) GB
FROM (
  SELECT SUM(bytes) bytes
  FROM   dba_data_files
  UNION ALL
  SELECT SUM(bytes) bytes
  FROM   dba_temp_files
  UNION ALL
  SELECT SUM(bytes) bytes
  FROM   v$log
);
```

7 Note the size of the database.

See "Calculating the total size of the backup on Windows" on page 52.

8 To exit Oracle SQL*Plus, enter:

```
exit
```

To determine the size of the file system files

1 On the computer that hosts the server on which customizations were added or changes were made, select the `\Vontu\Protect\plugins` directory.

2 Right-click the directory. Select **Properties**.

3 On the **General** tab, note the Size.

4 Repeat steps 1–3 for the `\Vontu\Protect\logs` directory.

5 Repeat steps 1–4 for any other computers that host Symantec Data Loss Prevention server applications.

6 Calculate the total size of the directories and record this number.

See "Calculating the total size of the backup on Windows" on page 52.

To determine the size of the server configuration files

1. On the computer that hosts the server on which configuration changes were made, select the `\Vontu\Protect\config` directory.
2. Right-click the directory and select **Properties**.
3. On the **General** tab, note the **Size**.
4. Repeat steps 1–3 for any other computers that host Symantec Data Loss Prevention server applications.
5. Calculate the total size of the configuration directories on all servers and record this number.

   See "Calculating the total size of the backup on Windows" on page 52.

Calculating the total size of the backup on Windows

Use the sizes from the individual procedures to sum the total size of the backup.

To calculate the total size of the backup

1. Enter the size of the database here: _____
2. Enter the size of the file system files here: _____
3. Enter the size of the server configuration files here: _____
4. Add the size of the database to the size of the configuration files and file system files for a total size here: _____

See "Preparing the backup location on Windows" on page 49.

Identifying a backup location on Windows

The backup location should be on a computer other than the ones that host the database, the Enforce Server, or the detection servers. The backup location must have enough available space for the backup files.

To identify a backup location

1. Make sure that the backup location is accessible from the computers that host the servers and databases that need to be backed up.
2. Verify that the amount of available disk space in a potential backup location is greater than the size of the backup.

   To determine the amount of space available on the hard disk, on the **General** tab, check the capacity.

   Make sure that this number is greater than the size of the database.

   See "Determining the size of the backup on Windows" on page 50.
3. After you identify a computer with enough disk space, note down its fully qualified domain name. Enter this information on the Recovery Information Worksheet.

   To determine the name of a computer, navigate to **My Computer > Properties > Computer Name**.

   See Table 5-5 on page 62.

   See "Preparing the backup location on Windows" on page 49.

Creating backup directories on Windows

To create the backup directory structure

1. Create a directory in which to store the backup files:

   ```
   \Vontu_Backup_Files
   ```

   Remember that this directory should be created on a computer other than the one that hosts the database, the Enforce Server, or the detection servers.
2. Create the following subdirectories in which to store the backup files:

   ```
   \Vontu_Backup_Files\File_System
   \Vontu_Backup_Files\Server_Configuration_Files
   \Vontu_Backup_Files\Database
   \Vontu_Backup_Files\Recovery_Aid
   ```
3. Complete the Recovery Information Worksheet with the Drive used in step 2.

   See Table 5-5 on page 62.

   See "Preparing the backup location on Windows" on page 49.

Performing a cold backup of the Oracle 10g database on Windows

Cold backups are recommended primarily for non-database administrator users.

A cold backup is performed by

- Shutting down the Oracle database
- Stopping the Symantec Data Loss Prevention system
- Copying important files to a safe backup location

For more information, see the *Symantec Data Loss Prevention Installation Guide*.

If your company has a three-tier installation and its own database administration team and backup policies, you may not need to perform cold backups.

Be aware that Symantec only provides support for the cold backup procedures that are described here.

See "Oracle hot backups on Windows platforms" on page 61.

Table 5-3 Steps to perform a cold backup of the Oracle 10g database

Step	Action	Description
Step 1	Create recovery aid files.	See "Creating recovery aid files on Windows" on page 54.
Step 2	Shut down all of the Symantec Data Loss Prevention and Oracle services.	See "Shutting down the Symantec Data Loss Prevention system on Windows" on page 56.
Step 3	Copy the database files to the backup location.	See "Copying the database files to the backup location on Windows" on page 57.
Step 4	Restart the Oracle and Symantec Data Loss Prevention services.	See "Restarting the system on Windows" on page 58.

Creating recovery aid files on Windows

You should create recovery aid files for use in recovery procedures. A trace file of the control file and a copy of the init.ora file are very helpful for database recoveries.

The trace file of the control file contains the names and locations of all of the data files. This trace includes any additional data files that have been added to the

database. It also contains the redo logs and the commands that can be used to recreate the database structure.

The init.ora file contains the initialization parameters for Oracle, including the names and locations of the database control files.

To generate a trace file of the control file

1. To open Oracle SQL*Plus, navigate to **Windows > Start > All Programs > Oracle - OraDb10g_home1 > Application Development > SQL Plus**.

   Refer to the *Symantec Data Loss Prevention Installation Guide* and the *Symantec Data Loss Prevention Oracle Installation and Upgrade Guide*.

2. At the SQL> command prompt, to connect as the sysdba user, enter

   ```
   connect sys/password@protect as sysdba
   ```

   where *password* is the password created for single-tier and two-tier installations.

   See the *Symantec Data Loss Prevention Installation Guide*.

3. After receiving the *Connected* message, at the SQL> command prompt, enter:

   ```
   alter database backup controlfile to trace;
   ```

4. Click **Enter**.

5. To find the directory in which the trace file was created, in the next line, enter:

   ```
   show parameter user_dump;
   ```

6. Navigate to the directory from step 5.

7. In Windows, copy the trace file from the directory in step 5 to the `\Recovery_Aid` subdirectory that you created earlier on the backup computer.

   Other trace files are located in the `\user_dump` directory. Be sure to copy the file with the most recent date and timestamp.

   See "Creating backup directories on Windows " on page 53.

8. Rename the file so that it can be easily identified, for example:

   ```
   controlfilebackupMMDDYY.trc.
   ```

After you generate a trace file of the control file, you must create a copy of the spfile.

See "Creating a copy of the spfile on Windows" on page 56.

See "Performing a cold backup of the Oracle 10g database on Windows" on page 54.

Creating a copy of the spfile on Windows

After you generate a trace file of the control file, you must create a copy of the spfile.

See "Creating recovery aid files on Windows" on page 54.

To create a copy of the spfile

1. In Oracle SQL*Plus, at the SQL> command prompt, enter:

   ```
   create pfile='/Temp/inittemp.ora' from spfile;
   ```

2. To exit Oracle SQL*Plus, enter:

   ```
   exit
   ```

3. Navigate to the `\Temp` directory and verify that the inittemp.ora file was created.
4. In Windows, copy the inittemp.ora file from the `\Temp` directory to the `\Recovery_Aid` subdirectory that you created earlier on the backup computer.

   See "Creating backup directories on Windows " on page 53.

See "Performing a cold backup of the Oracle 10g database on Windows" on page 54.

Shutting down the Symantec Data Loss Prevention system on Windows

To shut down the system

1. On the computer that hosts the database, navigate to **Start > All Programs > Administrative Tools > Services** to open the Windows Services menu.
2. Open the Services menu and stop all running Symantec Data Loss Prevention services, which might include the following:
   - Vontu Update
   - Vontu Incident Persister (on the computers that also host the Enforce Server)
   - Vontu Manager (on the computers that also host the Enforce Server)
   - Vontu Monitor (on the computers that also host a detection server)
   - Vontu Monitor Controller (on the computers that also host the Enforce Server)

- Vontu Notifier (on the computers that also host the Enforce Server)

3 Stop the OracleService*databasename*, where *databasename* is the Global Database Name and SID selected during installation.

The database must be named *protect* for Symantec Data Loss Prevention to work correctly.

Refer to the *Symantec Data Loss Prevention Installation Guide*.

See "Performing a cold backup of the Oracle 10g database on Windows" on page 54.

Copying the database files to the backup location on Windows

The database files that should be backed up include the files in the `\protect` directory and the database password file.

To copy the database files to the backup location

1 Make sure that the Oracle services are stopped.

If the Oracle services are not stopped, the backup files may be corrupt and unusable.

See "Shutting down the Symantec Data Loss Prevention system on Windows" on page 56.

2 On the computer that hosts the database, select the `\oracle\product\10.2.0\oradata\protect` directory (if default locations were accepted during installation). Copy the protect directory into the `\Backup_Files\Database` directory of the computer that hosts the backup files.

The drive and the name of the computer that hosts the backup files should have been recorded in the Recovery Information Worksheet for reference.

See Table 5-5 on page 62.

3 On the computer that hosts the database, select the `\oracle\product\10.2.0\db_1\database\PWDprotect.ora` file and copy it into the `/Backup_Files\Database` directory of the computer that hosts the backup files.

See "Performing a cold backup of the Oracle 10g database on Windows" on page 54.

Restarting the system on Windows

To restart the system

1. On the computer that hosts the database, navigate to **Start > All Programs > Administrative Tools > Services** to open the Windows Services menu.
2. From the Services menu, start all of the Oracle services:
   - OracleServiceDATABASENAME
   - OracleDBConsoledatabasename

   where *databasename* is the Global Database Name and SID selected during installation. For single- and two-tier installations, the database must be named *protect* for Symantec Data Loss Prevention to work correctly.

   Refer to the *Symantec Data Loss Prevention Installation Guide*.
3. In single-tier and two-tier installations, before starting other Symantec Data Loss Prevention services, start the Vontu Notifier service.
4. In single-tier and two-tier installations, start the remaining Symantec Data Loss Prevention services, which might include the following:
   - Vontu Manager (on the computers that also host the Enforce Server)
   - Vontu Monitor (on the computers that also host a detection server)
   - Vontu Incident Persister (on the computers that also host the Enforce Server)
   - Vontu Update
   - Vontu Monitor Controller (on the computers that also host the Enforce Server)

See "Performing a cold backup of the Oracle 10g database on Windows" on page 54.

Backing up the server configuration files on Windows

Server configuration files should be backed up any time configuration changes are made on the Enforce Server or detection servers. These changes can be made on the **System > Overview > *server_name* > Server Details** page. To make these changes, you can also edit any of the .properties files that reside in the `\Vontu\Protect\config` directory.

To back up the server configuration files

1. On the computer that hosts the Enforce Server or detection server on which configuration changes were made, select the `\Vontu\Protect\config` directory. Copy it to the `\Backup_Files\Server_Configuration_Files` directory on the computer that hosts the backup files. The drive and the name of the computer that hosts the backup files was recorded in the Recovery Information Worksheet for reference.

   See Table 5-5 on page 62.

2. Rename the directory that was copied in the previous step to indicate which server it came from, such as `config_ServerName`.

   This renamed directory is especially important for multi-tier installations, where configuration directories reside on multiple servers.

See "Performing a cold backup of the Oracle 10g database on Windows" on page 54.

Backing up files stored on the file system on Windows

Some files that are stored on the file system for the Enforce Server and detection servers should be backed up whenever they are changed. These files include:

- Custom configuration changes
  See "Backing up custom configuration changes on Windows" on page 59.
- System logs
  See "Backing up system logs on Windows" on page 60.
- Keystore file
  See "Backing up a keystore file on Windows" on page 60.

Backing up custom configuration changes on Windows

The `\plugins` directory may contain custom code, data, or configuration changes. This directory should be backed up any time you make changes to its default settings. It should also be backed up when custom code is added.

Custom code is usually added with the help of Symantec Support or Professional Services.

To back up customized changes stored in the \plugins directory

1. On the computer that hosts the Enforce Server, select the `\Vontu\Protect\plugins` directory. Copy it into the `\Backup_Files\File_System` directory on the computer that hosts the backup files. The drive and the name of the computer that hosts the backup files was recorded in the Recovery Information Worksheet for reference.

   See Table 5-5 on page 62.

2. Rename the directory that was copied in the previous step to indicate which server it came from, such as `plugins_ServerName`.

See "Backing up files stored on the file system on Windows" on page 59.

Backing up system logs on Windows

You should back up server log files any time configuration changes are made on the Enforce Server or detection servers.

To back up the system log files

1. On the computer that hosts the server on which configuration changes were made, select the `\Vontu\Protect\logs` directory. Copy it into the `\Backup_Files\File_System` directory of the computer that hosts the backup files.

   The drive and the name of the computer that hosts the backup files was recorded in the Recovery Information Worksheet for reference.

   See Table 5-5 on page 62.

2. Rename the directory that was copied in the previous step to indicate which server it came from, such as `logs_ServerName`.

   This renamed directory is especially important for multi-tier installations, where configuration directories reside on multiple servers.

See "Backing up files stored on the file system on Windows" on page 59.

Backing up a keystore file on Windows

If the administrators in your organization generate their own Tomcat server certificate, back up the keystore file containing the certificate.

To back up the keystore file

- Copy the `\Vontu\Protect\tomcat\conf\.keystore` file from the computer that hosts the Enforce Server or detection servers for which the certificate was generated. Copy this file to the `\Backup_Files\File_System` directory on the computer that hosts the backup files.

  The file path and the name of the computer that hosts the backup files was recorded in the Recovery Information Worksheet for reference.

  See Table 5-5 on page 62.

See "Backing up files stored on the file system on Windows" on page 59.

Backing up the Network Discover incremental scan index on Windows

Incremental scanning is a way to let you resume a scan from where you left off. Some Network Discover targets have an option for incremental scanning.

The incremental scan index keeps track of which items have already been scanned. This index is automatically created and updated during incremental scans.

The incremental scan index is in the directory `C:\Vontu\Protect\scan\incremental_index`.

To back up the incremental scan index

1. Pause or stop any incremental scans that are in progress or scheduled to run.
2. Stop the `VontuMonitorController` service.
3. Copy the incremental scan index directory to a backup location.
4. If you need to restore the incremental scan index, copy the files back into this directory.

   Make sure all the Network Discover targets have the same target identifiers as when the incremental scan index was backed up.

Oracle hot backups on Windows platforms

If you are an experienced Oracle database administrator accustomed to managing enterprise-level Oracle installation, you may choose to perform hot backups. If you do, you should also perform archive logging. However, keep in mind that Symantec Data Loss Prevention does not support hot backup procedures and Symantec Support may not be able to provide assistance.

See "Performing a cold backup of the Oracle 10g database on Windows" on page 54.

About Windows system recovery

Symantec Data Loss Prevention contains recovery options should your database or system ever experience a failure. The process for Windows system recovery is described in the following table. For additional guidance, contact Symantec Support for help with recovery. If installation and system maintenance recommendations were not followed before the system failure, contact Symantec Support. Before contacting Symantec Support, make sure that the backup files are available for use in a recovery installation.

Table 5-4 Windows system recovery components

Component	Description
Windows recovery information worksheet	See "About the Windows recovery information worksheet" on page 62.
Windows recovery process	See "About recovering your system on Windows platforms" on page 63.

About the Windows recovery information worksheet

If you followed the recommended backup instructions, the backup files are located on an alternate computer in the directories in the Recovery Information Worksheet. Store this worksheet in a secure location because it contains sensitive data.

See "Performing a cold backup of the Oracle 10g database on Windows" on page 54.

See "About Windows system recovery" on page 62.

Table 5-5 Recovery Information Worksheet

Backup file information	Example names and locations	Customer names and locations
Name of the computer that hosts backup files	machine_name	
Directory containing backup files	`\Vontu_Backup_Files`	___:\Vontu_Backup_Files
Subdirectory containing file system backup files	`\Vontu_Backup_Files\File_System`	___:\Vontu_Backup_Files\File_System
Subdirectory containing Enforce and detection server configuration backup files	`\Vontu_Backup_Files\Server_Configuration_Files`	___:\Vontu_Backup_Files\Server_Configuration_Files

Table 5-5 Recovery Information Worksheet *(continued)*

Backup file information	Example names and locations	Customer names and locations
Subdirectory containing database backup files	`\Vontu_Backup_Files\Database`	___:\Vontu_Backup_Files\Database
Subdirectory containing Database Recovery Aid files	`\Vontu_Backup_Files\Recovery_Aid`	___:\Vontu_Backup_Files\Recovery_Aid

About recovering your system on Windows platforms

The recovery process recreates the part of the system that failed.

After a successful recovery, you should copy the backup files to their previous location in the system.

Note: System recovery procedures do not vary according to installation tier. These instructions are appropriate for single-tier, two-tier, and three-tier installations.

If you did not follow the backup procedures as documented in this guide, these recovery steps would not be appropriate.

See "About Windows system recovery" on page 62.

The following table describes the steps necessary to recover Windows.

Table 5-6 Windows recovery

Step	Action	Description
Step 1	Recover the database.	See "About recovering the database on Windows" on page 63.
Step 2	Recover the Enforce Server.	See "Recovering the Enforce Server on Windows" on page 67.
Step 3	Recover the detection server.	See "Recovering a detection server on Windows" on page 68.

About recovering the database on Windows

Based on the type of database failure you experienced, choose the appropriate database recovery procedure:

- If the previous database can no longer be used, create a new database.

- If the database malfunctioned due to a system failure or user error, restore the previously existing database. For example, if an important file was accidentally deleted, you can restore the database to a point in time when the important file still existed.

See "Restoring an existing database on Windows" on page 64.

See "Creating a new database on Windows" on page 65.

See "About recovering your system on Windows platforms" on page 63.

Restoring an existing database on Windows

See "About recovering the database on Windows" on page 63.

To recover the database by restoring the existing database

1. Make sure that the database environment is healthy. Check the existing database, the database server that hosts the existing database, and the computer that hosts the database server.
2. On the computer that hosts the database, navigate to **Start > All Programs > Administrative Tools > Services**. This navigation opens the Windows Services menu.
3. From the Windows Services menu, if you have a single-tier or a two-tier installation, stop all Symantec Data Loss Prevention services, which might include the following:
   - Vontu Update
   - Vontu Incident Persister (on the computer hosting the Enforce Server)
   - Vontu Manager (on the computer hosting the Enforce Server)
   - Vontu Monitor (on the computer or computers hosting a detection server)
   - Vontu Monitor Controller (on the computer hosting the Enforce Server)
   - Vontu Notifier (on the computer hosting the Enforce Server)
4. Stop all of the Oracle services.

   Refer to the *Symantec Data Loss Prevention Installation Guide*.
5. Copy the contents of the `\Backup_Files\Database` directory to the `\oracle\product\10.2.0\oradata\protect` directory on the computer that hosts the new database. The information about the computers and directories is located on the Recovery Information Worksheet.

   See "About the Windows recovery information worksheet" on page 62.

6 To open Oracle SQL*Plus, navigate to **Windows > Start > All Programs > Oracle - OraDb10g_home1 > Application Development > SQL Plus**. This navigation assumes the default locations from the Oracle installation process.

This process is described in the *Symantec Data Loss Prevention Installation Guide*.

7 At the SQL> command prompt, to connect as the sysdba user, enter:

```
connect sys\password@protect as sysdba
```

where *password* is the password created for single- and two-tier installations.

See the *Symantec Data Loss Prevention Installation Guide*.

8 At the SQL> prompt, enter:

```
startup
```

See "About recovering your system on Windows platforms" on page 63.

Creating a new database on Windows

See "About recovering the database on Windows" on page 63.

To recover the database by creating a new database

1 If you have not co-located the database and the database server, make sure that each is in a healthy state.

2 Follow the instructions in the *Symantec Data Loss Prevention Installation Guide* to install an Oracle database.

This step assumes that the drive structure of the new database is the same as the drive structure of the old database. Perform the following tasks in the order presented:

- Copy the contents of the `\Backup_Files\Database` directory to the `\oracle\product\10.2.0\oradata\protect` directory on the computer that hosts the new database. The information about the computers and directories is located on the Recovery Information Worksheet.
  See "About the Windows recovery information worksheet" on page 62.
- To open Oracle SQL*Plus, navigate to **Windows > Start > All Programs > Oracle - OraDb10g_home1 > Application Development > SQL Plus**. This navigation assumes the default locations from the Oracle installation process.
  This process is described in the *Symantec Data Loss Prevention Installation Guide*.

- At the SQL> command prompt, to connect as the sysdba user, enter

  ```
  connect sys/password@protect as sysdba
  ```

  where *password* is the password created for single- and two-tier installations.
  See the *Symantec Data Loss Prevention Installation Guide*.

- At the SQL> prompt, enter

  ```
  startup
  ```

3 If the drive structure of the new database is different from the drive of the old database, perform the following tasks in the order presented:

- Edit the inittemp.ora file in the `\Backup_Files\Recovery_Aid` directory to reflect the drive structure of the new database. The information about this computer is in the Recovery Information Worksheet.
  See "About the Windows recovery information worksheet" on page 62.
  The following parameters might need to be modified to accommodate differences in directory structure:

  ```
  *.background_dump_dest
    *.control_files
    *.core_dump_dest
    *.user_dump_dest
  ```

- Rename the edited inittemp.ora file to initprotect.ora.
- Copy the initprotect.ora file to the `$ORACLE_HOME\database` directory on the computer that hosts the new database.
- Copy the contents of the `\Backup_Files\Database` directory to the `\oracle\product\10.2.0\oradata\protect` directory on the computer that hosts the new database. The information about this computer is in the Recovery Information Worksheet.
  See "About the Windows recovery information worksheet" on page 62.
- On the computer that hosts the new database, open Oracle SQL*Plus. Navigate to **Windows > Start > All Programs > Oracle - OraDb10g_home1 > Application Development > SQL Plus**.
  This navigation assumes that the default locations were accepted during the Oracle installation process that is described in the *Symantec Data Loss Prevention Installation Guide*.
- At the SQL> command prompt, to connect as the sysdba user, enter:

```
connect sys/password@protect as sysdba
```

Where *password* is the password created for single- and two-tier installations.
See the *Symantec Data Loss Prevention Installation Guide*.

- At the SQL> prompt, enter:

```
create spfile from pfile='%ORACLE_HOME%\database\
  initprotect.ora';
```

- To shut down, enter:

```
shutdown
```

- To start up, enter:

```
startup
```

See "About recovering your system on Windows platforms" on page 63.

Recovering the Enforce Server on Windows

To recover the Enforce Server

1. Make sure that the Enforce Server application and the computer hosting it are in a healthy state.
2. Make sure that the Oracle database is intact and running correctly.

   See "About recovering the database on Windows" on page 63.
3. Reinstall the Enforce Server.

   See the *Symantec Data Loss Prevention Installation Guide*.
4. When you get to the **Final Confirmation** window in the installation procedure, make sure that the **Initialize Enforce Data** box is not checked.
5. Continue with the installation procedure as described in the *Symantec Data Loss Prevention Installation Guide*.

6 After reinstalling the Enforce Server, restore the server configuration files.

Copy the contents of the `Backup_Files\Server_Configuration_Files\config` directory to the `\Vontu\Protect\config` directory on the computer that hosts the new Enforce Server. The information about the computers and directories is located on the Recovery Information Worksheet.

See "About the Windows recovery information worksheet" on page 62.

7 To restore customized changes, copy the contents of the `\Backup_Files\File_System\plugins` directory to the `\Vontu\Protect\plugins` directory on the computer that hosts the new Enforce Server. The information about the computers and directories is located on the Recovery Information Worksheet.

See "About the Windows recovery information worksheet" on page 62.

8 To restore the keystore file, copy the contents of the `\Backup_Files\File_System\.keystore` directory to the `\Vontu\Protect\tomcat\conf` directory on the computer that hosts the new Enforce Server. The information about the computers and directories is located on the Recovery Information Worksheet.

See "About the Windows recovery information worksheet" on page 62.

See "About recovering your system on Windows platforms" on page 63.

Recovering a detection server on Windows

To recover a detection server

1 Make sure the server to host the recovered detection server application and the computer that hosts the server are in a healthy state.

2 Follow the instructions in the *Symantec Data Loss Prevention Installation Guide* to create a detection server.

3 After creating the detection server, restore the server configuration files. Copy the contents of the `\Backup_Files\Server_Configuration_Files\config` directory to the `\Vontu\Protect\config` directory on the computer that hosts the new detection server. The information about the computers and directories is located on the Recovery Information Worksheet.

See "About the Windows recovery information worksheet" on page 62.

4 To restore customized changes, copy the contents of the `\Backup_Files\File_System\plugins` directory to the `\Vontu\Protect\plugins` directory on the computer that hosts the new detection server. The information about the computers and directories is located on the Recovery Information Worksheet.

See "About the Windows recovery information worksheet" on page 62.

5 To restore the keystore file, copy the contents of the `\Backup_Files\File_System\.keystore` directory to the `\Vontu\Protect\tomcat\conf` directory on the computer that hosts the new detection server. The information about the computers and directories is located on the Recovery Information Worksheet.

See "About the Windows recovery information worksheet" on page 62.

See "About recovering your system on Windows platforms" on page 63.

Chapter 6

Backing up and recovering on Linux

This chapter includes the following topics:

About backup and recovery on Linux

Perform system backups in case the Symantec Data Loss Prevention system crashes and needs to be restored. The system that should be backed up includes the Enforce Server, the detection servers, and the database. These backup procedures can be used for single-tier, two-tier, and three-tier installations.

The cold backup procedures for the Oracle 10g database are for non-database administrators who have no standard backup methods for databases.

Symantec recommends that administrators perform backups of their entire system. Administrators should follow all of the backup instructions that are in this section in the order in which they are presented.

Administrators who would prefer to back up only part of their system must determine which subsets of the system backup instructions to follow.

See "About periodic system backups on Linux" on page 72.

See "About partial backups on Linux" on page 73.

About periodic system backups on Linux

Perform system backups regularly. The frequency of system backups should be determined based on the size of the system and the internal company policies.

Large databases may take longer to back up. Database backups should be performed at least weekly.

Server configuration and file system backups should be performed after configuration changes are made on the Enforce Server or detection server. You should also perform backups when you generate encrypted keys.

Symantec recommends that administrators perform backups of their entire system. Administrators should follow all of the backup instructions that are in this section in the order in which they are presented.

Complete system backups should be performed at the following times:

- After installation
- Before any system upgrades
- Any time the system changes, such as when a Symantec Data Loss Prevention server is added to or removed from the system configuration

Keep in mind schedule considerations when performing your backups.

See "About scheduling a system backup on Linux" on page 72.

See "About partial backups on Linux" on page 73.

See "About backup and recovery on Linux" on page 71.

About scheduling a system backup on Linux

When scheduling system backups, keep in mind the following concepts:

- For single-tier installations, the system is offline during backups while the files are copied.

During backups, Symantec Data Loss Prevention does not scan or find incidents. Reports are also inaccessible during backups. For these reasons, backups should be scheduled during times when the system is typically not very active. Such times may be on weekends when users are unlikely to use the system and when incidents are less likely to be generated.
Refer to the *Symantec Data Loss Prevention Installation Guide*.

- The backup methods that are described in this section do not accommodate point-in-time recovery. If the last system backup was two days ago and the system crashes, the information from those two days is lost. The system cannot be restored to times other than the time of the last backup.
- Before performing a backup, use regular company or system notifications to let users know that the system is offline and unavailable during the system backup.

See "About periodic system backups on Linux" on page 72.

About partial backups on Linux

Administrators who want to perform partial system backups can use either of the following subsets of the instructions.

Table 6-1 Types of partial backups

To back up a database only:	See "Preparing the backup location on Linux" on page 73. See "Performing a cold backup of the Oracle 10g database on Linux" on page 78.
To back up an Enforce Server or detection server only:	See "Preparing the backup location on Linux" on page 73. See "Backing up the server configuration files on Linux" on page 85. See "About backed up files stored on the file system on Linux" on page 85.

Preparing the backup location on Linux

Preparing the backup location involves determining the size of the backup and identifying a suitable backup location. Symantec Data Loss Prevention provides a convenient Recovery Information Worksheet to help record the locations of the

backup directories. The procedures in this section include instructions for when to record information in the worksheet. These instructions are for performing backups on hard drives. After you perform the backup on a hard drive, the data should be archived to tape.

See "About the Linux recovery information worksheet" on page 88.

Preparing the backup location consists of the following steps:

Table 6-2 Preparing the backup location

Step	Action	Description
Step 1	Determine the size of the backup sections.	See "Determining the size of the backup on Linux" on page 74.
Step 2	Calculate the total size of the backup.	See "Calculating the total size of the backup on Linux" on page 76.
Step 3	Identify the backup location.	See "Identifying a backup location on Linux" on page 76.
Step 4	Create the backup directories.	See "Creating backup directories on Linux" on page 77.

Determining the size of the backup on Linux

The size of a full backup is the sum of the following items:

- The size of the database
- The size of the file system files to be backed up
- The size of the server configuration files to be backed up

However, file system and server configuration files do not need to be backed up as often as the database. The size of the backup varies depending on what is backed up. Only follow the sizing procedures in this section that are relevant to the backup being performed.

See "Preparing the backup location on Linux" on page 73.

To determine the size of the database

1. Log on to the computer that hosts the Oracle database as the `oracle` user.
2. To open Oracle SQL*Plus, enter:

```
sqlplus /nolog
```

3 At the SQL> command prompt, to connect as the sysdba user, enter:

```
connect sys/password@protect as sysdba
```

where *password* is the password created for single-tier and two-tier installations.

See the *Symantec Data Loss Prevention Installation Guide*.

4 After receiving the *Connected* message, run the following SQL query by copying or entering it into the command prompt:

```
SELECT ROUND(SUM(bytes)/1024/1024/1024, 4) GB
FROM (
   SELECT SUM(bytes) bytes
   FROM   dba_data_files
   UNION ALL
   SELECT SUM(bytes) bytes
   FROM   dba_temp_files
   UNION ALL
   SELECT SUM(bytes) bytes
   FROM   v$log
);
```

5 Note the size of the database.

See "Calculating the total size of the backup on Linux" on page 76.

6 To exit Oracle SQL*Plus, enter:

```
exit
```

To determine the size of the file system files

1 On the computer that hosts the server on which customizations were added or changes were made, logon as `root`.

2 Change to the `/opt/Vontu/Protect/plugins` directory.

3 Use the disk usage command to determine the sizes of the directory trees and their contents. The output is displayed in kilobytes, megabytes, and gigabytes.

```
du -h
```

4 Note the Size.

5 Repeat steps 2 through 4 for the `/var/log/Vontu` directory.

6 Repeat steps 1 through 5 for any other computers that host Symantec Data Loss Prevention servers.

7 Calculate the total size of the directories and record this number.

See "Calculating the total size of the backup on Linux" on page 76.

To determine the size of the server configuration files

1 On the computer that hosts the server on which configuration changes were made, logon as root.

2 Change to the `/opt/Vontu/Protect/config` directory.

3 Use the disk usage command to determine the sizes of the directory trees and their contents:

```
du -h
```

The output is displayed in kilobytes, megabytes, and gigabytes.

4 Note the total size of the directory.

5 Repeat steps 1 through 4 for any other computers that host Symantec Data Loss Prevention servers.

6 Calculate the total size of the configuration directories on all servers and record this number.

See "Calculating the total size of the backup on Linux" on page 76.

Calculating the total size of the backup on Linux

Use the sizes from the individual procedures to sum the total size of the backup

To calculate the total size of the backup

1 Enter the size of the database here: _____

2 Enter the size of the file system files, here: _____

3 Enter the size of the server configuration files here: _____

4 Add the size of the database to the size of the configuration files and file system files for a total size here: _____

See "Preparing the backup location on Linux" on page 73.

Identifying a backup location on Linux

The backup location should be on a computer other than the ones that host the database, the Enforce Server, or the detection servers. The backup location must have enough available space for the backup files.

To identify a backup location

1. Make sure that the backup location is accessible from the computers that host the servers and databases that need to be backed up.
2. Verify that the amount of available disk space in a potential backup location is greater than the size of the backup:

   To determine the amount of space available on the hard disk, while logged on as root, enter:

   ```
   df
   ```

   Make sure that this number is greater than the size of the database.

   See "Determining the size of the backup on Linux" on page 74.
3. After you identify a computer that has enough disk space, note down its fully qualified domain name. Enter this information on the Recovery Information Worksheet.

   See "About the Linux recovery information worksheet" on page 88.
4. To determine the name of a computer, enter:

   ```
   hostname -f
   ```

See "Preparing the backup location on Linux" on page 73.

Creating backup directories on Linux

To create the backup directory structure

1. Create a directory in which to store the backup files:

   ```
   mkdir /opt/Vontu_Backup_Files
   ```

   This directory is usually under `/opt` if the backup computer has a Linux operating system. It can be created in any directory.

   Remember that this directory should be created on a computer other than the one that hosts the database, the Enforce Server, or the detection servers.
2. Create the following subdirectories in which to store the backup files:

   ```
   mkdir /opt/Vontu_Backup_Files/File_System
   mkdir /opt/Vontu_Backup_Files/Server_Configuration_Files
   mkdir /opt/Vontu_Backup_Files/Database
   mkdir /opt/Vontu_Backup_Files/Recovery_Aid
   ```

3 Complete the Recovery Information Worksheet, making use of the `/opt/Vontu` directory that was described in the previous two steps.

See "About the Linux recovery information worksheet" on page 88.

4 To grant permissions to these directories to the Oracle user, enter:

```
chmod 777 /opt/Vontu/ -R
```

See "Preparing the backup location on Linux" on page 73.

Performing a cold backup of the Oracle 10g database on Linux

Cold backups are recommended primarily for non-database administrator users, and they are appropriate for single- and two-tier installations. A cold backup is performed by

- Shutting down the Oracle database
- Stopping the Symantec Data Loss Prevention system
- Copying important files to a safe backup location

Refer to the *Symantec Data Loss Prevention Installation Guide*.

If your company has a three-tier installation and its own database administration team, you may not need to perform cold backups. Also, you may not need to perform a cold backup if your company already has its own database backup policies and procedures.

The cold backup procedures that are included in this guide are the only backup procedures that Symantec supports.

See "Oracle hot backups on Linux platforms" on page 87.

Table 6-3 Steps to perform a cold backup of the Oracle 10g database

Step	Action	Description
Step 1	Create recovery aid files.	See "Creating recovery aid files on Linux" on page 79.
Step 2	Shut down all of the Symantec Data Loss Prevention and Oracle Services.	See "Shutting down the Symantec Data Loss Prevention system on Linux" on page 81.

Table 6-3 Steps to perform a cold backup of the Oracle 10g database *(continued)*

Step	Action	Description
Step 3	Copy the database files to the backup location.	See "Copying the database files to the backup location on Linux" on page 83.
Step 4	Restart the Oracle and Symantec Data Loss Prevention services.	See "Copying the database files to the backup location on Windows" on page 57.

Creating recovery aid files on Linux

You should create recovery aid files for use in recovery procedures. A trace file of the control file and a copy of the init.ora file are very helpful for database recovery.

The trace file of the control file contains the names and locations of all of the data files. This trace includes any additional data files that have been added to the database. It also contains the redo logs and the commands that can be used to recreate the database structure.

The init.ora file contains the initialization parameters for Oracle, including the names and locations of the database control files.

To create a trace file of the control file

1. Log on to the computer that hosts the Oracle database as the `oracle` user.
2. To open Oracle SQL*Plus, enter:

   ```
   sqlplus /nolog
   ```

3. At the SQL> command prompt, to connect as the sysdba user, enter

   ```
   connect sys/password@protect as sysdba
   ```

   where *password* is the password created for single-tier and two-tier installations.

   See the *Symantec Data Loss Prevention Installation Guide*.
4. After receiving the *Connected* message, at the SQL> command prompt, enter:

   ```
   alter database backup controlfile to trace;
   ```

5 To find the directory in which the trace file was created, in the next line, enter:

```
show parameter user_dump;
```

6 To exit Oracle SQL*Plus, enter:

```
exit
```

7 Change to the directory from step 5. Copy the trace file to the `/Recovery_Aid` subdirectory on the backup computer that you created earlier.

See "Creating backup directories on Linux" on page 77.

Other trace files are located in the `/user_dump` directory. Be sure to copy the file with the most recent date and timestamp.

To check the date and the timestamps of the files in the directory, enter:

```
ls -l
```

8 Rename the file so that it can be easily identified, for example:

```
controlfilebackupMMDDYY.trc.
```

After you create the trace file, you must create a copy of the spfile.

See "Creating a copy of the spfile on Linux" on page 80.

See "Performing a cold backup of the Oracle 10g database on Linux" on page 78.

Creating a copy of the spfile on Linux

After you create a trace file of the control file, you must create a copy of the spfile.

See "Creating recovery aid files on Linux" on page 79.

To create a copy of the spfile

1 Log on to the computer that hosts the Oracle database as the `oracle` user.

2 To open Oracle SQL*Plus, enter:

```
sqlplus /nolog
```

3 At the SQL> command prompt, to connect as the sysdba user, enter:

```
connect sys/password@protect as sysdba
```

where *password* is the password created for single- and two-tier installations in the *Symantec Data Loss Prevention Installation Guide*.

4 After receiving the *Connected* message, at the SQL> command prompt, enter:

```
create pfile='/tmp/inittemp.ora' from spfile;
```

5 To exit Oracle SQL*Plus, enter:

```
exit
```

6 Change to the `/tmp` directory and verify that the inittemp.ora file was created.

7 Copy the inittemp.ora file to the `/Recovery_Aid` subdirectory on the backup computer that you created earlier.

See "Creating backup directories on Linux" on page 77.

See "Performing a cold backup of the Oracle 10g database on Linux" on page 78.

Shutting down the Symantec Data Loss Prevention system on Linux

To shut down the system

1 On the computer that hosts the database, log on as root.

2 Go to the `/opt/Vontu/Protect/bin` directory.

3 Stop all running Symantec Data Loss Prevention services:

`./VontuUpdate.sh stop`

`./VontuIncidentPersister.sh stop` (on the computers that also host the Enforce Server)

`./VontuManager.sh stop` (on the computers that also host the Enforce Server)

`./VontuMonitor.sh stop` (on the computers that also host a detection server)

`./VontuMonitorController.sh stop` (on the computers that also host the Enforce Server)

`./VontuNotifier.sh stop` (on the computers that also host the Enforce Server)

Services can be started by going to the `/etc` directory and running the following command:

`.init.d/`*`VontuServiceName`* `start`

Services can be stopped by changing to the `/etc` directory and running the following command:

`.init.d/`*`VontuServiceName`* `stop`

4 On the computer that hosts the database, log on as the oracle user.

5 To open Oracle SQL*Plus, enter:

```
sqlplus /nolog
```

6 At the SQL> command prompt, to connect as the sysdba user, enter:

`connect sys/`*`password`*`@protect as sysdba`

where *password* is the password created for single-tier and two-tier installations.

See the *Symantec Data Loss Prevention Installation Guide*.

7 After receiving the *Connected* message, at the SQL> command prompt, to stop all of the Oracle services, enter:

```
shutdown immediate
```

See "Performing a cold backup of the Oracle 10g database on Linux" on page 78.

Copying the database files to the backup location on Linux

The database files that should be backed up include the files in the `/protect` directory and the database password file.

To copy the database files to the backup location

1. Make sure that the Oracle services are stopped.

   If the Oracle services are not stopped, the backup files may be corrupt and unusable.

   See "Shutting down the Symantec Data Loss Prevention system on Linux" on page 81.

2. On the computer that hosts the database, copy the `/opt/oracle/oradata/protect` directory into the `/opt/Backup_Files/Database` directory of the computer that hosts the backup files.

   The file path and the name of the computer that hosts the backup files should have been recorded in the Recovery Information Worksheet for reference.

   See "About the Linux recovery information worksheet" on page 88.

3. On the computer that hosts the database, copy the `/opt/oracle/product/10.2.0/db_1/dbs/orapwdprotect` file into the `/opt/Backup_Files/Database` directory of the computer that hosts the backup files.

   The file path and the name of the computer that hosts the backup files should have been recorded in the Recovery Information Worksheet for reference.

See "Performing a cold backup of the Oracle 10g database on Linux" on page 78.

Restarting the system on Linux

To restart the system

1. On the computer that hosts the database, log on as the oracle user.
2. To open Oracle SQL*Plus, enter:

   ```
   sqlplus /nolog
   ```

3 At the SQL> command prompt, to connect as the sysdba user, enter:

```
connect sys/password@protect as sysdba
```

where *password* is the password created for single-tier and two-tier installations.

Refer to the *Symantec Data Loss Prevention Installation Guide*.

4 After you receive the *Connected* message, at the SQL> command prompt, start all of the Oracle services. To start all of the Oracle services, enter the following command:

```
startup
```

5 On the computer that hosts the database, log on as root.

6 In single-tier and two-tier installations, change directory to `/opt/Vontu/Protect/bin`.

7 In single-tier and two-tier installations, before starting other Symantec Data Loss Prevention services, start the Vontu Notifier service.

```
./VontuNotifier.sh start
```

8 In single-tier and two-tier installations, start the remaining Symantec Data Loss Prevention services.

`./VontuManager.sh start` (on the computers that also host the Enforce Server)

`./VontuMonitor.sh start` (on the computers that also host a detection server)

`./VontuIncidentPersister.sh start` (on the computers that also host the Enforce Server)

```
./VontuUpdate.sh start
```

`./VontuMonitorController.sh start` (on the computers that also host the Enforce Server)

Services can be started by changing to the `etc` directory and running the following command:

`.init.d/`*`VontuServiceName`* `start`

Services can be stopped by changing to the `etc` directory and running the following command:

`.init.d/`*`VontuServiceName`* `stop`.

See "Performing a cold backup of the Oracle 10g database on Linux" on page 78.

Backing up the server configuration files on Linux

Server configuration files should be backed up any time configuration changes are made on the Enforce Server or detection servers. These changes can be made on the **System > Overview > *server_name* > Server Details** page. To make these changes, you can also edit any of the files with a .properties extension that reside in the `/opt/Vontu/Protect/config` directory.

To back up the server configuration files

1. On the computer that hosts the Enforce Server or detection server on which configuration changes were made, copy the `/opt/Vontu/Protect/config` directory. Copy it to the `/opt/Vontu_Backup_Files/Server_Configuration_Files` directory on the computer that hosts the backup files. The file path and the name of the computer that hosts the backup files was recorded in the Recovery Information Worksheet for reference.

   See "About the Linux recovery information worksheet" on page 88.

2. Rename the directory that was copied in the previous step to indicate which server it came from, such as `config_ServerName`.

   This renamed directory is especially important for multi-tier installations, where configuration directories reside on multiple servers.

See "Performing a cold backup of the Oracle 10g database on Linux" on page 78.

About backed up files stored on the file system on Linux

Some files that are stored on the file system for the Enforce Server and detection servers should be backed up whenever they are changed. These files include:

- Custom configuration changes
  See "Backing up custom configuration changes on Linux" on page 86.
- System logs
  See "Backing up system logs on Linux" on page 86.
- Keystore files
  See "Backing up a keystore file on Linux" on page 87.

Backing up custom configuration changes on Linux

The `plugins` directory may contain custom code, data, or configuration changes. This directory should be backed up any time you make changes to the default settings in this directory. It should also be backed up when custom code is added.

Custom code is usually added with the help of Symantec Support or Professional Services.

To back up customized changes stored in the /plugins directory

1. On the computer that hosts the Enforce Server, copy the `/opt/Vontu/Protect/plugins` directory. Copy it into the `/opt/Backup_Files/File_System` directory on the computer that hosts the backup files. The file path and the name of the computer that hosts the backup files was recorded in the Recovery Information Worksheet for reference.

   See "About the Linux recovery information worksheet" on page 88.

2. Rename the directory that was copied in the previous step to indicate which server it came from, such as `plugins_ServerName`.

See "About backed up files stored on the file system on Linux" on page 85.

Backing up system logs on Linux

You should back up server log files any time configuration changes are made on the Enforce Server or detection servers.

To back up the system log files

1. On the computer that hosts the server on which configuration changes were made, copy the `/opt/Vontu/Protect/logs` directory. Copy it into the `/opt/Backup_Files/File_System` directory of the computer that hosts the backup files.

   The file path and the name of the computer that hosts the backup files was recorded in the Recovery Information Worksheet for reference.

   See "About the Linux recovery information worksheet" on page 88.

2. Rename the directory that was copied in the previous step to indicate which server it came from, such as `logs_ServerName`.

   This renamed directory is especially important for multi-tier installations with log directories on multiple servers.

See "About backed up files stored on the file system on Linux" on page 85.

Backing up a keystore file on Linux

If the administrators in your organization generate their own Tomcat server certificate, back up the keystore file containing the certificate.

To back up the keystore file

- Copy the `/opt/Vontu/Protect/tomcat/conf/.keystore` file from the computer that hosts the Enforce Server or detection servers for which the certificate was generated. Copy this file to the `/opt/Backup_Files/File_System` directory on the computer that hosts the backup files.

  The file path and the name of the computer that hosts the backup files was recorded in the Recovery Information Worksheet for reference.

  See "About the Linux recovery information worksheet" on page 88.

See "About backed up files stored on the file system on Linux" on page 85.

Backing up the Network Discover incremental scan index on Linux

Incremental scanning is a way to let you resume a scan from where you left off. Some Network Discover targets have an option for incremental scanning.

The incremental scan index keeps track of which items have already been scanned. This index is automatically created and updated during incremental scans.

The incremental scan index is in the directory `/opt/Vontu/Protect/scan/incremental_index`.

To back up the incremental scan index

1. Pause or stop any incremental scans that are in progress or scheduled to run.
2. Stop the `VontuMonitorController` service.
3. Copy the incremental scan index directory to a backup location.
4. If you need to restore the incremental scan index, copy the files back into this directory.

   Make sure all the Network Discover targets have the same target identifiers as when the incremental scan index was backed up.

Oracle hot backups on Linux platforms

If you are an experienced Oracle database administrator accustomed to managing enterprise-level Oracle installation, you may choose to perform hot backups. If you perform a hot backup, you should run the Oracle database in archive log mode.

However, keep in mind that Symantec does not support hot backup procedures and may not be able to provide assistance.

See "Performing a cold backup of the Oracle 10g database on Linux" on page 78.

About the Linux recovery information worksheet

If you followed the recommended backup instructions, the backup files are on another computer in the directories you noted in the Recovery Information Worksheet. Most users choose to create these files under `/opt`, but the person who created the recovery files may use another directory. Store this worksheet in a secure location because it contains sensitive data.

See "Performing a cold backup of the Oracle 10g database on Linux" on page 78.

Table 6-4 Recovery Information Worksheet

Backup file Information	Example Names and Locations	Customer Names and Locations
Name of Computer that Hosts backup files	machine_name	
Directory Containing backup files	opt/Vontu_Backup_Files	_____/Vontu_Backup_Files
Subdirectory Containing File System backup files	opt/Vontu_Backup_Files/File_System	_____/Vontu_Backup_Files/ File_System
Subdirectory Containing Enforce and Detection Server Configuration backup files	opt/Vontu_Backup_Files/ Server_Configuration_Files	_____/Vontu_Backup_Files/ Server_Configuration_Files
Subdirectory Containing Database backup files	opt/Vontu_Backup_Files/Database	_____/Vontu_Backup_Files/ Database
Subdirectory Containing Database Recovery Aid Files	opt/Vontu_Backup_Files/ Recovery_Aid	_____/Vontu_Backup_Files/ Recovery_Aid

About recovering your system on Linux

The recovery process re-creates the part of the system that failed.

After a successful recovery, you should copy the backup files to their previous location in the system.

Note: System recovery procedures do not vary according to installation tier. These instructions are appropriate for single-tier, two-tier, and three-tier installations.

If you did not follow the backup procedures as documented in this guide, these recovery steps are not appropriate.

The following table describes the steps necessary to perform a Linux system recovery:

Table 6-5 Performing a Linux system recovery

Step	Action	Description
Step 1	Recover the database.	See "About recovering the database on Linux" on page 89.
Step 2	Recover the Enforce Server.	See "Creating a new database on Linux" on page 89.
Step 3	Recover the detection server.	See "Recovering a detection server on Linux" on page 92.

About recovering the database on Linux

Based on the type of database failure you experienced, choose the appropriate database recovery procedure:

- If the previous database can no longer be used, create a new database.
- If the database malfunctioned due to a system failure or user error, restore the previously existing database. For example, if an important file was accidentally deleted, you can restore the database to a point in time when the important file still existed.

See "Creating a new database on Linux" on page 89.

See "About recovering your system on Linux" on page 88.

Creating a new database on Linux

To recover the database by creating a new database

1. Make sure that the database environment is healthy. Check the existing database, the database server that hosts the existing database, and the computer that hosts the database server.
2. Follow the instructions in the *Symantec Data Loss Prevention Installation Guide* to install an Oracle database.
3. This step assumes that the drive structure of the new database is the same as the drive structure of the old database. Perform the following tasks in the order that is presented:

- Copy the contents of the `Backup_Files/Database` directory to the `opt/oracle/oradata/protect` directory on the computer that hosts the new database. The information about the computers and directories is located on the Recovery Information Worksheet
  See "About the Linux recovery information worksheet" on page 88.
- To open Oracle SQL*Plus, enter:

  ```
  sqlplus /nolog
  ```

- At the SQL> command prompt, to connect as the sysdba user, enter:

  ```
  connect sys/password@protect as sysdba
  ```

  where *password* is the password created for single- and two-tier installations.
  See the *Symantec Data Loss Prevention Installation Guide*.
- At the SQL> prompt, enter:

  ```
  startup
  ```

The following step assumes that the drive structure of the new database is different from the drive structure of the old database.

4 Perform the following tasks in the order presented:

- Edit the inittemp.ora file in the `\Backup_Files\Recovery_Aid` directory to reflect the drive structure of the new database. The information about this computer is in the Recovery Information Worksheet.
  See "About the Linux recovery information worksheet" on page 88.
  The following parameters might need to be modified to accommodate differences in directory structure:

  ```
  *.background_dump_dest
  *.control_files
  *.core_dump_dest
  *.user_dump_dest
  ```

- Rename the edited inittemp.ora file to initprotect.ora.
- Copy the edited initprotect.ora file to the `$ORACLE_HOME/dbs` directory on the computer that hosts the new database.
- Copy the contents of the `/Backup_Files/Database` directory to the `opt/oracle/oradata/protect` directory on the computer that hosts the

new database. The information about this computer is in the Recovery Information Worksheet.
See "About the Linux recovery information worksheet" on page 88.

- To open Oracle SQL*Plus, enter:

```
sqlplus /nolog
```

- At the SQL> command prompt, to connect as the sysdba user, enter:

```
connect sys/password@protect as sysdba
```

where *password* is the password created for single- and two-tier installations.
See the *Symantec Data Loss Prevention Installation Guide*.

- At the SQL> prompt, enter:

```
create spfile from pfile='$ORACLE_HOME/dbs/initprotect.ora';
```

- To shut down, enter:

```
shutdown
```

- To start up, enter:

```
startup
```

See "About recovering your system on Linux" on page 88.

Recovering the Enforce Server on Linux

To recover the Enforce Server

1. Make sure that the Enforce Server application and the computer hosting it are in a healthy state.
2. Make sure that the Oracle database is intact and running correctly.

   See "About recovering the database on Linux" on page 89.
3. Reinstall the Enforce Server from scratch as described in the *Symantec Data Loss Prevention Installation Guide*.
4. When you get to the **Final Confirmation** window in the installation procedure, make sure that the **Initialize Enforce Data** box is not checked.
5. Continue with the installation procedure as described in the *Symantec Data Loss Prevention Installation Guide*.

6 After reinstalling the Enforce Server, restore the server configuration files. Copy the contents of the `/Backup_Files/Server_Configuration_Files/config` directory to the `/opt/Vontu/Protect/config` directory on the computer that hosts the new Enforce Server. The information about the computers and directories is located on the Recovery Information Worksheet.

See "About the Linux recovery information worksheet" on page 88.

7 To restore customized changes, copy the contents of the `/Backup_Files/File_System/plugins` directory to the `/opt/Vontu/Protect/plugins` directory on the computer that hosts the new Enforce Server. The information about the computers and directories is located on the Recovery Information Worksheet.

See "About the Linux recovery information worksheet" on page 88.

8 To restore the keystore file, copy the contents of the `/Backup_Files/File_System/.keystore` directory to the `/opt/Vontu/Protect/tomcat/conf` directory on the computer that hosts the new Enforce Server. The information about the computers and directories is located on the Recovery Information Worksheet.

See "About the Linux recovery information worksheet" on page 88.

See "About recovering your system on Linux" on page 88.

Recovering a detection server on Linux

To recover a detection server

1 Make sure the server to host the recovered detection server application and the computer that hosts the server are in a healthy state.

2 Follow the instructions in the *Symantec Data Loss Prevention Installation Guide* to create a detection server.

3 After creating the detection server, restore the server configuration files. Copy the contents of the `/Backup_Files/Server_Configuration_Files/config` directory to the `/opt/Vontu/Protect/config` directory on the computer that hosts the new detection server. The information about the computers and directories is located on the Recovery Information Worksheet.

See "About the Linux recovery information worksheet" on page 88.

4 To restore customized changes, copy the contents of the `/Backup_Files/File_System/plugins` directory to the `/opt/Vontu/Protect/plugins` directory on the computer that hosts the new detection server. The information about the computers and directories is located on the Recovery Information Worksheet.

See "About the Linux recovery information worksheet" on page 88.

5 To restore the keystore file, copy the contents of the `/Backup_Files/File_System/.keystore` directory to the `/opt/Vontu/Protect/tomcat/conf` directory on the computer that hosts the new detection server. The information about the computers and directories is located on the Recovery Information Worksheet.

See "About the Linux recovery information worksheet" on page 88.

See "About recovering your system on Linux" on page 88.

Appendix A

Log files and codes

This appendix includes the following topics:

About log files

Symantec Data Loss Prevention provides a number of different log files that record information about the behavior of the software. Log files fall into these categories:

- Operational log files record detailed information about the tasks the software performs and any errors that occur while the software performs those tasks. You can use the contents of operational log files to verify that the software functions as you expect it to. You can also use these files troubleshoot any problems in the way the software integrates with other components of your system.
  For example, you can use operational log files to verify that a Network Prevent (Email) Server communicates with a specific MTA on your network.
  See "Operational log files" on page 96.

- Debug log files record fine-grained technical details about the individual processes or software components that comprise Symantec Data Loss Prevention. The contents of debug log files are not intended for use in diagnosing system configuration errors or in verifying expected software functionality. You do not need to examine debug log files to administer or maintain an Symantec Data Loss Prevention installation. However, Symantec Support may ask you to provide debug log files for further analysis when you report a problem. Some debug log files are not created by default. Symantec Support can explain how to configure the software to create the file if necessary.
  See "Debug log files" on page 99.
- Installation log files record information about the Symantec Data Loss Prevention installation tasks that are performed on a particular computer. You can use these log files to verify an installation or troubleshoot installation errors. Installation log files reside in the following locations:
  - *installdir*\Vontu\.install4j\installation.log stores the installation log for Symantec Data Loss Prevention.
  - *installdir**oracle_home*\admin\protect\ stores the installation log for Oracle 10g.

  See the *Symantec Data Loss Prevention Installation Guide* for more information.

Operational log files

The Enforce Server and the detection servers store operational log files in the \Vontu\Protect\logs\ directory on Windows installations and in the /var/log/Vontu/ directory on Linux installations. A number at the end of the log file name indicates the count (shown as 0 in Table A-1).

Table A-1 lists and describes the Symantec Data Loss Prevention operational log files.

Table A-1 Operational log files

Log file name	Description	Server
boxmonitor_operational_0.log	The BoxMonitor process oversees the detection server processes that pertain to that particular server type. For example, the processes that run on Network Monitor are file reader and packet capture. The BoxMonitor log file is typically very small, and it shows how the application processes are running.	All detection servers
detection_operational_0.log	The detection operation log file provides details about how the detection server configuration and whether it is operating correctly.	All detection servers
detection_operational_trace_0.log	The detection trace log file provides details about each message that the detection server processes. The log file includes information such as: ■ The policies that were applied to the message ■ The policy rules that were matched in the message ■ The number of incidents the message generated.	All detection servers
manager_operational.log.0	Logs information about the Symantec Data Loss Prevention manager process, which implements the Enforce Server administration console user interface.	Enforce Server

Table A-1 Operational log files *(continued)*

Log file name	Description	Server
monitorcontroller_operational_0.log	Records a detailed log of the connections between the Enforce Server and all detection servers. It provides details about the information that is exchanged between these servers including whether policies have been pushed to the detection servers or not.	Enforce Server
SmtpPrevent0.log	This operational log file pertains to SMTP Prevent only. It is the primary log for tracking the health and activity of a Network Prevent (Email) system. Examine this file for information about the communication between the MTAs and the detection server.	SMTP Prevent detection servers
WebPrevent_Access0.log	This access log file pertains to Web Prevent only. It records all the requests that Web Prevent processes. It is similar to Web access logs for a proxy server.	Web Prevent detection servers
WebPrevent_Operational0.log	This operational log file pertains to Web Prevent only. It reports the operating condition of Web Prevent such as whether the system is up or down, connection management, and so on. This log is the primary log file for tracking Web Prevent operations.	Web Prevent detection servers
webservices_access0.log	This log file records successful and failed attempts to access the reporting Web Service.	Enforce Server

Table A-1 Operational log files *(continued)*

Log file name	Description	Server
`webservices_soap0.log`	Contains the entire SOAP request and response for most requests to the Reporting API Web Service. This log records all requests and responses except responses to incident binary requests. This log file is not created by default. See the *Symantec Data Loss Prevention Reporting API Developers Guide* for more information.	Enforce server

See "Network Prevent (Web) operational log files and event codes" on page 102.

See "Network Prevent (Web) access log files and fields" on page 104.

See "Network Prevent (Email) log levels" on page 106.

See "Network Prevent (Email) operational log codes" on page 107.

See "Network Prevent (Email) originated responses and codes" on page 111.

Debug log files

The Enforce Server and the detection servers store debug log files in the `\Vontu\Protect\logs\` directory on Windows installations and in the `/var/log/Vontu/` directory on Linux installations. A number at the end of the log file name indicates the count (shown as 0 in Table A-2).

Table A-2 lists and describes the Symantec Data Loss Prevention debug log files.

Table A-2 Debug log files

Log file name	Description	Server
`Aggregator0.log`	This file describes communications between the detection server and the agents. Look at this log to troubleshoot the following problems: ■ Connection to the agents ■ To find out why incidents do not appear when they should ■ If unexpected agent events occur	Endpoint detection servers

Table A-2 Debug log files *(continued)*

Log file name	Description	Server
`BoxMonitor0.log`	This file is typically very small, and it shows how the application processes are running. The `BoxMonitor` process oversees the detection server processes that pertain to that particular server type. For example, the processes that run on Network Monitor are file reader and packet capture.	All detection servers
`ContentExtractor0.log`	This log file may be helpful for troubleshooting `ContextExtractor` issues.	All detection servers, Enforce Server
`DiscoverNative.log.0`	Contains the log statements that the Network Discover native code emits. Currently contains the information that is related to `.pst` scanning. This log file applies only to the Network Discover Servers that run on Windows platforms.	Discover detection servers
`FileReader0.log`	This log file pertains to the file reader process and contains application-specific logging, which may be helpful in resolving issues in detection and incident creation. Look at this log file to find out why an incident was not detected. One symptom that shows up is content extractor timeouts.	All detection servers
`IncidentPersister0.log`	This log file pertains to the Incident Persister process. This process reads incidents from the incidents folder on the Enforce Server, and writes them to the database. Look at this log if the incident queue on the Enforce Server (manager) grows too large. This situation can be observed also by checking the incidents folder on the Enforce Server to see if incidents have backed up.	Enforce Server
`Indexer0.log`	This log file contains information when an EDM profile or IDM profile is indexed. It also includes the information that is collected when the external indexer is used. If indexing fails then this log should be consulted.	Enforce Server (or computer where the external indexer is running)
`jdbc.log`	This log file is a trace of JDBC calls to the database. By default, writing to this log is turned off.	Enforce Server
`MonitorController0.log`	This log file is a detailed log of the connections between the Enforce Server and the detection servers. It gives details around the information that is exchanged between these servers including whether policies have been pushed to the detection servers or not.	Enforce Server

Table A-2 Debug log files *(continued)*

Log file name	Description	Server
`PacketCapture.log`	This log file pertains to the packet capture process that reassembles packets into messages and writes to the `drop_pcap` directory. Look at this log if there is a problem with dropped packets or traffic is lower than expected. `PacketCapture` is not a Java process, so it does not follow the same logging rules as the other Symantec Data Loss Prevention system processes.	Network Monitor
`PacketCapture0.log`	This log file describes issues with `PacketCapture` communications.	Network Monitor
`RequestProcessor0.log`	This log file pertains to SMTP Prevent only. The log file is primarily for use in cases where `SmtpPrevent0.log` is not sufficient.	SMTP Prevent detection servers
`ScanDetail-`*`target`*`-0.log`	Where *target* is the name of the scan target. All white spaces in the target's name are replaced with hyphens. This log file pertains to Discover server scanning. It is a file by file record of what happened in the scan. If the scan of the file is successful, it reads success, and then the path, size, time, owner, and ACL information of the file scanned. If it failed, a warning appears followed by the file name.	Discover detection servers
`tomcat\localhost.`*`date`*`.log`	These Tomcat log files contain information for any action that involves the user interface. The logs include the user interface errors from red error message box, password failures when logging on, and Oracle errors (ORA –#).	Enforce Server
`VontuIncidentPersister.log`	This log file contains minimal information: `stdout` and `stderr` only (fatal events).	Enforce Server
`VontuManager.log`	This log file contains minimal information: `stdout` and `stderr` only (fatal events).	Enforce Server
`VontuMonitor.log`	This log file contains minimal information: `stdout` and `stderr` only (fatal events).	All detection servers
`VontuMonitorController.log`	This log file contains minimal information: `stdout` and `stderr` only (fatal events).	Enforce Server
`VontuNotifier.log`	This log file pertains to the Notifier service and its communications with the Enforce Server and the `MonitorController` service. Look at this file to see if the `MonitorController` service registered a policy change.	Enforce Server

Table A-2 Debug log files *(continued)*

Log file name	Description	Server
`VontuUpdate.log`	This log file is populated when you update Symantec Data Loss Prevention.	Enforce Server

See "Network Prevent (Web) protocol debug log files" on page 106.

See "Network Prevent (Email) log levels" on page 106.

About log event codes

Operational log file messages are formatted to closely match industry standards for the various protocols involved. These log messages contain event codes that describe the specific task that the software was trying to perform when the message was recorded. Log messages are generally formatted as:

```
Timestamp [Log Level] (Event Code) Event description [event parameters]
```

- See "Network Prevent (Web) operational log files and event codes" on page 102.
- See "Network Prevent (Email) operational log codes" on page 107.
- See "Network Prevent (Email) originated responses and codes" on page 111.

Network Prevent (Web) operational log files and event codes

Network Prevent (Web) log file names use the format of `WebPrevent_OperationalX.log` (where *X* is a number). The number of files that are stored and their sizes can be specified by changing the values in the `FileReaderLogging.properties` file. This file is in the `Vontu\Protect\config` directory. By default, the values are:

- com.vontu.icap.log.IcapOperationalLogHandler.limit = 5000000
- com.vontu.icap.log.IcapOperationalLogHandler.count = 5

Table A-3 lists the Network Prevent (Web) defined operational logging codes by category. The italicized part of the text contains event parameters.

Table A-3 Status codes for Network Prevent (Web) operational logs

Code	Text and Description
Operational Events	
1100	`Starting Network Prevent (Web)`
1101	`Shutting down Network Prevent (Web)`
Connectivity Events	
1200	`Listening for incoming connections at` *`icap_bind_address`*`:`*`icap_bind_port`* Where: ■ *icap_bind_address* is the Network Prevent (Web) bind address to which the server listens. This address is specified with the Icap.BindAddress Advanced Setting. ■ *icap_bind_port* is the port at which the server listens. This port is set in the **Server > Configure** page.
1201 .	`Connection (`*`id=conn_id`*`) opened from` *`host(icap_client_ip:icap_client_port)`* Where: ■ *conn_id* is the connection ID that is allocated to this connection. This ID can be helpful in doing correlations between multiple logs. ■ *icap_client_ip* and *icap_client_port* are the proxy's IP address and port from which the connect operation to Network Prevent (Web) was performed.
1202	`Connection (`*`id=conn_id`*`) closed (`*`close_reason`*`)` Where: ■ *conn_id* is the connection ID that is allocated to the connect operation. ■ *close_reason* provides the reason for closing the connection.
1203	`Connection states: REQMOD=`*`N`*`, RESPMOD=`*`N`*`,` `OPTIONS=`*`N`*`, OTHERS=`*`N`* Where *N* indicates the number of connections in each state, when the message was logged. This message provides the system state in terms of connection management. It is logged whenever a connection is opened or closed.
Connectivity Errors	

Table A-3 Status codes for Network Prevent (Web) operational logs *(continued)*

Code	Text and Description
5200	`Failed to create listener at icap_bind_address:icap_bind_port` Where: ■ *icap_bind_address* is the Network Prevent (Web) bind address to which the server listens. This address can be specified with the Icap.BindAddress Advanced Setting. ■ *icap_bind_port* is the port at which the server listens. This port is set on the **Server > Configure** page.
5201	`Connection was rejected from unauthorized host (host_ip:port)` Where *host_ip* and *port* are the proxy system IP and port address from which a connect attempt to Network Prevent (Web) was performed. If the host is not listed in the Icap.AllowHosts Advanced setting, it is unable to form a connection.

See "About log files" on page 95.

Network Prevent (Web) access log files and fields

Network Prevent (Web) log file names use the format of `WebPrevent_OperationalX.log` (where *X* is a number). The number of files that are stored and their sizes can be specified by changing the values in the FileReaderLogging.properties file. By default, the values are:

- com.vontu.icap.log.IcapAccessLogHandler.limit = 5000000
- com.vontu.icap.log.IcapAccessLogHandler.count = 5

A Network Prevent (Web) access log is similar to a proxy server's Web access log. The "start" log message format is:

```
# Web Prevent starting: start_time
```

Where start_time format is `date:time`, for example: `13/Aug/2008:03:11:22:015-0700`.

The description message format is:

```
# host_ip "auth_user" time_stamp "request_line" icap_status_code
request_size "referer" "user_agent" processing_time(ms) conn_id client_ip
client_port action_code icap_method_code
```

Table A-4 lists the fields. The values of fields that are enclosed in quotes in this example are quoted in an actual message. If field values cannot be determined, the message displays - or "" as a default value.

Table A-4 Network Prevent (Web) access log fields

Fields	Explanation
host_ip	IP address of the host that made the request.
auth_user	Authorized user for this request.
time_stamp	Time that Network Prevent (Web) receives the request.
request_line	Line that represents the request.
icap_status_code	ICAP response code that Network Prevent (Web) sends by for this request.
request_size	Request size in bytes.
referer	Header value from the request that contains the URI from which this request came.
user_agent	User agent that is associated with the request.
processing_time (microsecond)	Request processing time in milliseconds. This value is the total of the receiving, content inspection, and sending times.
conn_id	Connection ID associated with the request.
client_ip	IP of the ICAP client (proxy).
client_port	Port of the ICAP client (proxy).
action_code	An integer representing the action that Network Prevent (Web) takes. Where the action code is one of the following: 0 = UNKNOWN 1 = ALLOW 2 = BLOCK 3 = REDACT 4 = ERROR 5 = ALLOW_WITHOUT_INSPECTION 6 = OPTIONS_RESPONSE 7 = REDIRECT.
icap_method_code	An integer representing the ICAP method that is associated with this request. Where the ICAP method code is one of the following: -1 = ILLEGAL 0 = OPTIONS 1 = REQMOD 2 = RESPMOD 3 = LOG.

See "About log files" on page 95.

Network Prevent (Web) protocol debug log files

To enable ICAP trace logging, set the Icap.EnableTrace Advanced setting to `true` and use the Icap.TraceFolder Advanced setting to specify a directory to receive the traces. The Network Prevent (Web) service must be restarted for this change to take effect.

Trace files that are placed in the specified directory have file names in the format: *timestamp-conn_id*. The first line of a trace file provides information about the connecting host IP and port along with a timestamp. File data that is read from the socket is displayed in the format `<<timestamp number_of_bytes_read`. Data that is written to the socket is displayed in the format `>>timestamp number_of_bytes_written`. The last line should note that the connection has been closed.

Note: Trace logging produces a large amount of data and therefore requires a large amount of free disk storage space. Trace logging should be used only for debugging an issue because the data that is written in the file is in clear text.

See "About log files" on page 95.

Network Prevent (Email) log levels

Network Prevent (Email) log file names use the format of `EmailPrevent_OperationalX.log` (where *X* is a number). The number of files that are stored and their sizes can be specified by changing the values in the FileReaderLogging.properties file. By default, the values are:

- com.vontu.mta.log.SmtpOperationalLogHandler.limit = 5000000
- com.vontu.mta.log.SmtpOperationalLogHandler.count = 5

At various log levels, components in the com.vontu.mta.rp package output varying levels of detail. The com.vontu.mta.rp.level setting specifies log levels in the `RequestProcessorLogging.properties` file which is stored in the `Vontu\Protect\config` directory. For example, com.vontu.mta.rp.level = FINE specifies the FINE level of detail.

Table A-5 describes the Network Prevent (Email) log levels.

Table A-5 Network Prevent (Email) log levels

Level	Guidelines
INFO	General events: connect and disconnect notices, information on the messages that are processed per connection.
FINE	Some additional execution tracing information.
FINER	Envelope command streams, message headers, detection results.
FINEST	Complete message content, deepest execution tracing, and error tracing.

See "About log files" on page 95.

Network Prevent (Email) operational log codes

Table A-6 lists the defined Network Prevent (Email) operational logging codes by category.

Table A-6 Status codes for Network Prevent (Email) operational log

Code	Description
Core Events	
1100	`Starting Network Prevent (Email)`
1101	`Shutting down Network Prevent (Email)`
1102	`Reconnecting to FileReader (tid=`*`id`*`)` Where *id* is the thread identifier. The RequestProcessor attempts to re-establish its connection with the FileReader for detection.
1103	`Reconnected to the FileReader successfully (tid=`*`id`*`)` The RequestProcessor was able to re-establish its connection to the FileReader.
Core Errors	
5100	`Could not connect to the FileReader (tid=`*`id`*` timeout=.3s)` An attempt to re-connect to the FileReader failed.

Table A-6 Status codes for Network Prevent (Email) operational log *(continued)*

Code	Description
5101	`FileReader connection lost (tid=id)` The RequestProcessor connection to the FileReader was lost.
Connectivity Events	
1200	`Listening for incoming connections (local=hostname)` *Hostnames* is an IP address or fully-qualified domain name.

1201	`Connection accepted (tid=id cid=N`
	`local=hostname:port`
	`remote=hostname:port)`
	
	Where *N* is the connection identifier.

1202	`Peer disconnected (tid=id cid=N`
	`local=hostname:port`
	`remote=hostname:port)`

1203	`Forward connection established (tid=id cid=N`
	`local=hostname:port`
	`remote=hostname:port)`

1204	`Forward connection closed (tid=id cid=N`
	`local=hostname:port`
	`remote=hostname:port)`

1205	`Service connection closed (tid=id cid=N`
	`local=hostname:port`
	`remote=hostname:port messages=1 time=0.14s)`

Connectivity Errors	

5200	`Connection is rejected from the unauthorized host (tid=id`
	`local=hostname:port`
	`remote=hostname:port)`

5201	`Local connection error (tid=id cid=N`
	`local=hostname:port`
	`remote=hostname:port reason=Explanation)`

Table A-6 Status codes for Network Prevent (Email) operational log *(continued)*

Code	Description
5202	Sender connection error (tid=*id* cid=*N* local=*hostname*:*port* remote=*hostname*:*port* reason=*Explanation*)
5203	Forwarding connection error (tid=*id* cid=*N* local=*hostname*:*port* remote=*hostname*:*port* reason=*Explanation*)
5204	Peer disconnected unexpectedly (tid=*id* cid=*N* local=*hostname*:*port* remote=*hostname*:*port* reason=*Explanation*)
5205	Could not create listener (address=local=*hostname*:*port* reason=*Explanation*)
5206	Authorized MTAs contains invalid hosts: *hostname*, *hostname*, ...
5207	MTA restrictions are active, but no MTAs are authorized to communicate with this host
5208	TLS handshake failed (reason=*Explanation* tid=*id* cid=*N* local=*hostname* remote=*hostname*)
5209	TLS handshake completed (tid=*id* cid=*N* local=*hostname* remote=*hostname*)
5210	All forward hosts unavailable (tid=*id* cid=*N* reason=*Explanation*)
5211	DNS lookup failure (tid=*id* cid=*N* NextHop=*hostname* reason=*Explanation*)
5303	Failed to encrypt incoming message (tid=*id* cid=*N* local=*hostname* remote=*hostname*)
5304	Failed to decrypt outgoing message (tid=*id* cid=*N* local=*hostname* remote=*hostname*)

Table A-6 Status codes for Network Prevent (Email) operational log *(continued)*

Code	Description
Message Events	
1300	`Message complete (cid=N message_id=3 dlp_id=message_identifier size=number sender=email_address recipient_count=N disposition=response estatus=statuscode rtime=N dtime=N mtime=N` Where: ■ Recipient_count is the total number of addressees in the To, CC, and BCC fields. ■ Response is the Network Prevent (Email) response which can be one of: PASS, BLOCK, BLOCK_AND_REDIRECT, REDIRECT, MODIFY, or ERROR. ■ Thee status is an Enhanced Status code. See "Network Prevent (Email) originated responses and codes" on page 111. ■ The rtime is the time in seconds for Network Prevent (Email) to fully receive the message from the sending MTA. ■ The dtime is the time in seconds for Network Prevent (Email) to perform detection on the message. ■ The mtime is the total time in seconds for Network Prevent (Email) to process the message Message Errors.
Message Errors	
5300	`Error while processing message (cid=N message_id=header_ID dlp_id=message_identifier size=0 sender=email_address recipient_count=N disposition=response estatus=statuscode rtime=N dtime=N mtime=N reason=Explanation` Where *header_ID* is an RFC 822 Message-Id header if one exists.
5301	`Sender rejected during re-submit`
5302	`Recipient rejected during re-submit`

See "About log files" on page 95.

Network Prevent (Email) originated responses and codes

Network Prevent (Email) originates the following responses. Other protocol responses are expected as Network Prevent (Email) relays command stream responses from the forwarding MTA to the sending MTA. Table A-7 shows the responses that occur in situations where Network Prevent must override the receiving MTA. It also shows the situations where Network Prevent generates a specific response to an event that is not relayed from downstream.

“Enhanced Status” is the RFC1893 Enhanced Status Code associated with the response.

Table A-7 Network Prevent (Email) originated responses

Code	Enhanced Status	Text	Description
250	2.0.0	`Ok: Carry on.`	Success code that Network Prevent (Email) uses.
221	2.0.0	`Service closing.`	The normal connection termination code that Network Prevent (Email) generates if a QUIT request is received when no forward MTA connection is active.
451	4.3.0	`Error: Processing error.`	This “general, transient” error response is issued when a (potentially) recoverable error condition arises. This error response is issued when a more specific error response is not available. Forward connections are sometimes closed, and their unexpected termination is occasionally a cause of a code 451, status 4.3.0. However sending connections should remain open when such a condition arises unless the sending MTA chooses to terminate.
421	4.3.0	`Fatal: Processing error. Closing connection.`	This “general, terminal” error response is issued when a fatal, unrecoverable error condition arises. This error results in the immediate termination of any sender or receiver connections.
421	4.4.1	`Fatal: Forwarding agent unavailable.`	That an attempt to connect the forward MTA was refused or otherwise failed to establish properly.

Table A-7 Network Prevent (Email) originated responses *(continued)*

Code	Enhanced Status	Text	Description
421	4.4.2	`Fatal: Connection lost to forwarding agent.`	Closing connection. The forwarded MTA connection is lost in a state where further conversation with the sending MTA is not possible. The loss usually occurs in the middle of message header or body buffering. The connection is terminated immediately.
451	4.4.2	`Error: Connection lost to forwarding agent.`	The forward MTA connection was lost in a state that may be recoverable if the connection can be re-established. The sending MTA connection is maintained unless it chooses to terminate.
421	4.4.7	`Error: Request timeout exceeded.`	The last command issued did not receive a response within the time window that is defined in the RequestProcessor.DefaultCommandTimeout. (The time window may be from RequestProcessor.DotCommandTimeout if the command issued was the “.”). The connection is closed immediately.
421	4.4.7	`Error: Connection timeout exceeded.`	The connection was idle (no commands actively awaiting response) in excess of the time window that is defined in RequestProcessor.DefaultCommandTimeout.
501	5.5.2	`Fatal: Invalid transmission request.`	A fatal violation of the SMTP protocol (or the constraints that are placed on it) occurred. The violation is not expected to change on a resubmitted message attempt. This message is only issued in response to a single command or data line that exceeds the boundaries that are defined in RequestProcessor.MaxLineLength.
502	5.5.1	`Error: Unrecognized command.`	Defined but not currently used.
550	5.7.1	`User Supplied.`	This combination of code and status indicates that a Blocking response rule has been engaged. The text that is returned is supplied as part of the response rule definition.

Note that a 4xx code and a 4.x.x enhanced status indicate a temporary error. In such cases the MTA can resubmit the message to the Network Prevent (Email) Server. A 5xx code and a 5.x.x enhanced status indicate a permanent error. In such cases the MTA should treat the message as undeliverable.

See "About log files" on page 95.