

Symantec™ Data Loss Prevention System Maintenance Guide

Version 15.0



Symantec Data Loss Prevention System Maintenance Guide

Documentation version: 15.0a

Legal Notice

Copyright © 2017 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo and the Checkmark 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 Legal Notice Appendix to this Documentation or TPIP ReadMe File 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, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Symantec as on premises or hosted services. 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>

Contents

| | | |
|-----------|--|----|
| Chapter 1 | Performing system maintenance | 8 |
| | About the system maintenance schedule | 8 |
| Chapter 2 | Understanding underlying system resources | 10 |
| | About the Enforce Server directory structure | 10 |
| | About the detection server directory structure | 13 |
| | About the incident attachment external storage directory | 15 |
| | About Symantec Data Loss Prevention services | 18 |
| | About starting and stopping services on Windows | 18 |
| | Starting and stopping services on Linux | 21 |
| | About using log files | 25 |
| | About DLP Agent logs | 25 |
| | About Symantec Data Loss Prevention system statistics | 25 |
| | Monitoring the incident count | 26 |
| | About incident hiding | 28 |
| Chapter 3 | Using system event reports and alerts | 30 |
| | About system events | 30 |
| | System events reports | 31 |
| | Server and Detectors event detail | 34 |
| | Working with saved system reports | 35 |
| | Configuring event thresholds and triggers | 36 |
| | About system event responses | 38 |
| | Enabling a syslog server | 40 |
| | About system alerts | 42 |
| | Configuring the Enforce Server to send email alerts | 42 |
| | Configuring system alerts | 43 |
| Chapter 4 | Using diagnostic tools | 46 |
| | About diagnostic tools | 46 |
| | About system information review | 46 |

| | | |
|-----------|--|----|
| Chapter 5 | Working with the Symantec Data Loss Prevention database | 48 |
| | Working with Symantec Data Loss Prevention database diagnostic tools | 48 |
| | Viewing tablespaces and data file allocations | 49 |
| | Adjusting warning thresholds for tablespace usage in large databases | 50 |
| | Generating a database report | 50 |
| | Viewing table details | 51 |
| | Recovering from Symantec Data Loss Prevention database connectivity issues | 52 |
| | Reclaiming space in the Symantec Data Loss Prevention database | 53 |
| Chapter 6 | Backing up and recovering on Windows | 55 |
| | About backup and recovery on Windows | 55 |
| | About periodic system backups on Windows | 56 |
| | About scheduling a system backup on Windows | 56 |
| | About partial backups on Windows | 57 |
| | Preparing the backup location on Windows | 57 |
| | Determining the size of the backup on Windows | 58 |
| | Identifying a backup location on Windows | 60 |
| | Creating backup directories on Windows | 61 |
| | Performing a cold backup of the Oracle database on Windows | 62 |
| | Creating recovery aid files on Windows | 63 |
| | Collecting a list of files to be backed up | 65 |
| | Creating a copy of the <code>spfile</code> on Windows | 65 |
| | Shutting down the Symantec Data Loss Prevention system on Windows | 66 |
| | Copying the database files to the backup location on Windows | 67 |
| | Restarting the system on Windows | 67 |
| | Backing up the server configuration files on Windows | 68 |
| | Backing up files stored on the file system on Windows | 69 |
| | Backing up custom configuration changes on Windows | 69 |
| | Backing up system logs on Windows | 69 |
| | Backing up a keystore file on Windows | 70 |
| | Backing up the Network Discover incremental scan index on Windows | 70 |
| | Oracle hot backups on Windows platforms | 71 |
| | About Windows system recovery | 71 |
| | About the Windows recovery information worksheet | 72 |

| | | |
|------------|--|-----|
| | About recovering your system on Windows platforms | 73 |
| Chapter 7 | Backing up and recovering on Linux | 80 |
| | About backup and recovery on Linux | 80 |
| | About periodic system backups on Linux | 81 |
| | About scheduling a system backup on Linux | 81 |
| | About partial backups on Linux | 82 |
| | Preparing the backup location on Linux | 82 |
| | Determining the size of the backup on Linux | 83 |
| | Identifying a backup location on Linux | 85 |
| | Creating backup directories on Linux | 86 |
| | Performing a cold backup of the Oracle database on Linux | 87 |
| | Creating recovery aid files on Linux | 88 |
| | Collecting a list of files to be backed up | 89 |
| | Creating a copy of the <code>spfile</code> on Linux | 90 |
| | Shutting down the Symantec Data Loss Prevention system on Linux | 91 |
| | Copying the database files to the backup location on Linux | 92 |
| | Restarting the system on Linux | 93 |
| | Backing up the server configuration files on Linux | 94 |
| | About backed up files stored on the file system on Linux | 95 |
| | Backing up custom configuration changes on Linux | 95 |
| | Backing up system logs on Linux | 96 |
| | Backing up a keystore file on Linux | 96 |
| | Backing up the Network Discover incremental scan index on Linux | 97 |
| | Oracle hot backups on Linux platforms | 97 |
| | About the Linux recovery information worksheet | 98 |
| | About recovering your system on Linux | 98 |
| | About recovering the database on Linux | 99 |
| | Restoring an existing database on Linux | 99 |
| | Creating a new database on Linux | 101 |
| | Recovering the Enforce Server on Linux | 103 |
| | Recovering a detection server on Linux | 104 |
| Appendix A | Log files and codes | 106 |
| | About log files | 106 |
| | About log event codes | 107 |
| | Network Prevent for Web operational log files and event codes | 107 |
| | Network Prevent for Web access log files and fields | 109 |
| | Network Prevent for Web protocol debug log files | 111 |
| | Network Prevent for Email log levels | 112 |

Network Prevent for Email operational log codes 113

Network Prevent for Email originated responses and codes 116

Performing system maintenance

This chapter includes the following topics:

- [About the system maintenance schedule](#)

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 30.
- 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 55.

See [“About backup and recovery on Linux”](#) on page 80.

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 46.

Understanding underlying system resources

This chapter includes the following topics:

- [About the Enforce Server directory structure](#)
- [About the detection server directory structure](#)
- [About the incident attachment external storage directory](#)
- [About Symantec Data Loss Prevention services](#)
- [About using log files](#)
- [About DLP Agent logs](#)
- [About Symantec Data Loss Prevention system statistics](#)
- [Monitoring the incident count](#)
- [About incident hiding](#)

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 13.

Table 2-1 Enforce Server directory structures

| Linux directory structure | Windows directory structure | Description |
|---------------------------------------|---------------------------------------|---|
| /opt/SymantecDLP/Protect | \SymantecDLP\Protect | Core product (includes manager.ver). |
| /opt/SymantecDLP/Protect/agentupdates | \SymantecDLP\Protect\agentupdates | Files that are used to update Endpoint Agents. |
| /opt/SymantecDLP/Protect/bin | \SymantecDLP\Protect\bin | The executable files that reside in this directory are described in the <i>Symantec Data Loss Prevention Administration Guide</i> . |
| /opt/SymantecDLP/Protect/config | \SymantecDLP\Protect\config | The files with extensions of .properties and .conf store server configurations. |
| /var/SymantecDLP/datafiles | \SymantecDLP\Protect\datafiles | Exact Data: database profiles to be indexed. |
| /var/SymantecDLP/documentprofiles | \SymantecDLP\Protect\documentprofiles | Index Document: document archives uploaded for indexes and whitelists. |
| /opt/SymantecDLP/Protect/EULA | \SymantecDLP\Protect\EULA | End User License Agreement. |
| /var/SymantecDLP/incidents | \SymantecDLP\Protect\incidents | Incidents that are stored on the Enforce Server before they are written to the database. |
| /var/SymantecDLP/index | \SymantecDLP\Protect\index | Profile indices for protected content (EDM, IDM, DGM, Form Recognition); .rdx file extension. |
| /opt/SymantecDLP/Protect/install | \SymantecDLP\Protect\install | SQL used in table creation. |

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

| Linux directory structure | Windows directory structure | Description |
|---|---------------------------------------|--|
| /opt/SymantecDLP/Protect/keystore | \SymantecDLP\Protect\keystore | Keystore files for TLS (Transport Layer Security) encryption of communication between Symantec Data Loss Prevention servers. |
| /opt/SymantecDLP/Protect/languages | \SymantecDLP\Protect\languages | Language pack files. |
| /opt/SymantecDLP/Protect/lib | \SymantecDLP\Protect\lib | .jar files with libraries used by Enforce processes. Used by Notifier and Persist Data, for example. |
| /opt/SymantecDLP/Protect/license | \SymantecDLP\Protect\license | Symantec Data Loss Prevention license files. |
| /var/log/SymantecDLP | \SymantecDLP\Protect\logs | Enforce Server log files. |
| /opt/SymantecDLP/Protect/plugins | \SymantecDLP\Protect\plugins | Custom code, data, and configuration changes, usually added with the help of Symantec Support. |
| /opt/SymantecDLP/Protect/Pstdepositfolder | \SymantecDLP\Protect\Pstdepositfolder | A temporary directory that is used when the application processes the Personal Storage Table (.pst) files. |
| /opt/SymantecDLP/Protect/Pstlocalcopy | \SymantecDLP\Protect\Pstlocalcopy | A temporary directory that is used when the application processes Personal Storage Table (.pst) files. |
| /opt/SymantecDLP/Protect/scan | \SymantecDLP\Protect\scan | Catalog and incremental index files for Discover. |
| /var/SymantecDLP/sharelists | \SymantecDLP\Protect\sharelists | Discover target share lists. |

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

| Linux directory structure | Windows directory structure | Description |
|----------------------------------|------------------------------|---|
| /opt/SymantecDLP/Protect/temp | \SymantecDLP\Protect\temp | Temporary, Enforce-generated files are stored here. Duration of files depends on the type of file. |
| /opt/SymantecDLP/Protect/tomcat | \SymantecDLP\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/SymantecDLP/Protect/tools | \SymantecDLP\Protect\tools | Contains various SQL scripts and Server FlexResponse examples. |
| /opt/SymantecDLP/Protect/updates | \SymantecDLP\Protect\updates | Directory for product upgrades. |

About the detection server directory structure

The following table describes the detection server directory structure.

See [“About Symantec Data Loss Prevention services”](#) on page 18.

Table 2-2 Detection server directory structures

| Linux directory structure | Windows directory structure | Description |
|--------------------------------|-----------------------------|---|
| /var/SymantecDLP/drop | \drop | Used to induct email traffic with SMTP copy rule and test with MIME email files (.eml). |
| /var/SymantecDLP/drop_discover | \drop_discover | Used with Discover Universal Data Store API. |
| /var/SymantecDLP/drop_ep | \drop_ep | Temporary storage directory for data from the endpoint agents. |

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

| Linux directory structure | Windows directory structure | Description |
|---|-----------------------------------|--|
| /var/SymantecDLP/drop_pcap | \drop_pcap | Temporary storage for reassembled network streams. |
| /var/SymantecDLP/packet_spool, icap_spool | \packet_spool, icap_spool | Spool location for traffic capture. |
| /opt/SymantecDLP/Protect | \SymantecDLP\Protect | Core product (includes monitor.ver). |
| /opt/SymantecDLP/Protect/agentupdates | \SymantecDLP\Protect\agentupdates | Directory for product upgrades. |
| /opt/SymantecDLP/Protect/ant | \SymantecDLP\Protect\ant | Files that Apache Ant software uses. |
| /opt/SymantecDLP/Protect/bin | \SymantecDLP\Protect\bin | .exe files, including Endace drivers (dag) for the Network Monitor Server. These files are described in the <i>Symantec Data Loss Prevention Administration Guide</i> . |
| /opt/SymantecDLP/Protect/config | \SymantecDLP\Protect\config | The files with extensions of .properties and .conf store configurations for the detection server. |
| /var/SymantecDLP/incidents | \SymantecDLP\Protect\incidents | Incidents that are stored on the detection server (monitors) before they are sent to the Enforce Server. |
| /var/SymantecDLP/index | \SymantecDLP\Protect\index | Profile indices for protected content (EDM, IDM, DGM, Form Recognition); .rdx file extension. |
| /opt/SymantecDLP/Protect/install | \SymantecDLP\Protect\install | |

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

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

About the incident attachment external storage directory

You can store incident attachments such as email messages or documents on a file system rather than in the Symantec Data Loss Prevention database. Storing incident attachments externally saves a great deal of space in your database, providing you with a more cost-effective storage solution.

You can store incident attachments either in a directory on the Enforce Server host computer, or on an stand-alone computer. You can use any file system you choose. Symantec recommends that you work with your data storage administrator to set up an appropriate directory for incident attachment storage.

To set up an external storage directory, Symantec recommend these best practices:

- If you choose to store your incident attachments on the Enforce Server host computer, do not place your storage directory under the `/SymantecDLP` folder.
- If you choose to store incident attachments on a computer other than your Enforce Server host computer, take the following steps:
 - Ensure that both the external storage server and the Enforce Server are in the same domain.
 - Create a "protect" user with the same password as your Enforce Server "protect" user to use with your external storage directory.
 - If you are using a Linux system for external storage, change the owner of the external storage directory to the external storage "protect" user.
 - If you are using a Microsoft Windows system for external storage, share the directory with Read/Writer permissions with the external storage "protect" user.

After you have set up your storage location you can enable external storage for incident attachments in the Installation Wizard. All incident attachments will be stored in the external storage directory. Incident attachments in the external storage directory cannot be migrated back to the database. All incidents attachments stored in the external storage directory are encrypted and can only be accessed from the Enforce Server administration console.

The incident deletion process deletes incident attachments in your external storage directory after it deletes the associated incident data from your database. You do not need to take any special action to delete incidents from the external storage directory.

Configuring the incident attachment external storage directory after installation or upgrade

If you did not configure the incident attachment external storage directory during the installation or upgrade process, you can enable or update external storage settings in the `Protect.properties` configuration file. You can also disable external storage of incident attachments in this file.

To configure external storage for incident attachments

- 1 On the Enforce Server host, open the following file in a text editor:

Microsoft Windows: `\SymantecDLP\Protect\config\Protect.properties`

Linux: `/opt/SymantecDLP/Protect/config/Protect.properties`

(Where *SymantecDLP* is the name of the directory where Symantec Data Loss Prevention was installed.)

- 2 Enable incident attachment external storage:

```
com.symantec.dlp.incident.blob.externalize=true
```

- 3 Specify the path to the external storage directory:

```
com.symantec.dlp.incident.blob.externalization.dir=<PATH TO DIRECTORY>
```

- 4 Save the file.

- 5 Restart the `VontuManager` service. See [“About Symantec Data Loss Prevention services”](#) on page 18.

To disable external storage for incident attachments

If you choose to disable incident attachment external storage, be sure to preserve the setting that specifies the path to the external storage directory to ensure that the Enforce Server retains access to the incident attachments.

- 1 On the Enforce Server host, open the following file in a text editor:

Microsoft Windows: `\SymantecDLP\Protect\config\Protect.properties`

Linux: `/opt/SymantecDLP/Protect/config/Protect.properties`

(Where *SymantecDLP* is the name of the directory where Symantec Data Loss Prevention was installed.)

- 2 Disable incident attachment external storage:

```
com.symantec.dlp.incident.blob.externalize=false
```

Do not change or delete the parameter specifying the path to the external storage directory.

- 3 Save the file.

- 4 Restart the `VontuManager` service. See [“About Symantec Data Loss Prevention services”](#) on page 18.

About Symantec Data Loss Prevention 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 Symantec Data Loss Prevention services

| Service Name | Description |
|-----------------------------------|---|
| Vontu Manager | Provides the centralized reporting and management services for Symantec Data Loss Prevention. |
| Vontu Detection Server Controller | Controls the detection servers. |
| 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. |

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 20.
- See [“Stopping a Detection Server on Windows”](#) on page 20.
- See [“Starting services on single-tier Windows installations”](#) on page 20.
- See [“Stopping services on single-tier Windows installations”](#) on page 21.

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 Start the Symantec Data Loss Prevention services in the following order:
 - VontuNotifier
 - VontuManager
 - VontuIncidentPersister
 - VontuMonitorController (if applicable)
 - VontuUpdate (if necessary)

Note: Start the VontuNotifier service first before starting other services.

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 in the following order:
 - VontuMonitorController (if applicable)
 - VontuIncidentPersister
 - VontuManager
 - VontuNotifier
 - VontuUpdate (if necessary)

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:
 - VontuMonitor
 - VontuUpdate

See [“Stopping a Detection Server on Windows”](#) on page 20.

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:
 - VontuUpdate
 - VontuMonitor

See [“Starting a Detection Server on Windows”](#) on page 20.

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 Start the Symantec Data Loss Prevention in the following order:
 - VontuNotifier

- VontuManager
- VontuIncidentPersister
- VontuMonitorController (if applicable)
- VontuMonitor
- VontuUpdate (if necessary)

Note: Start the `VontuNotifier` service before starting other services.

See [“Stopping services on single-tier Windows installations”](#) on page 21.

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 in the following order:
 - VontuMonitor
 - VontuMonitorController (if applicable)
 - VontuIncidentPersister
 - VontuManager
 - VontuNotifier
 - VontuUpdate (if necessary)

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 22.
- See [“Stopping an Enforce Server on Linux”](#) on page 22.

- See [“Starting a detection server on Linux”](#) on page 23.
- See [“Stopping a detection server on Linux”](#) on page 23.
- See [“Starting services on single-tier Linux installations”](#) on page 24.
- 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/SymantecDLP/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 Enforce Server, log on as root.
- 2 Change directory to `/opt/SymantecDLP/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 22.

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 detection server, log on as root.
- 2 Change directory to `/opt/SymantecDLP/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 detection server, log on as root.
- 2 Change directory to `/opt/SymantecDLP/Protect/bin`.
- 3 To stop all running Symantec Data Loss Prevention services, enter:

```
./SymantecDLPUUpdate.sh stop
./VontuMonitor.sh stop
```

See [“Starting a detection server on Linux”](#) on page 23.

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/SymantecDLP/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/SymantecDLP/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 24.

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 106.

About DLP Agent logs

DLP Agent logs contain service and operational data for every DLP Agent. Each DLP Agent has multiple components that are logged. The amount of information that is logged can be configured by setting the log level for each DLP Agent component. After the log level for an DLP Agent component has been configured, the log can be collected and sent to Symantec Support. Symantec Support can use the log to troubleshoot a problem or to improve performance for a Symantec Data Loss Prevention Endpoint installation.

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 and Detectors > 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 divided by the 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/Detector Detail** page.

See [“About diagnostic tools”](#) on page 46.

Monitoring the incident count

When Symantec Data Loss Prevention identifies new policy violations, it creates and stores incidents in the Oracle database that is used by the Enforce Server. Over time, the number of incidents that are stored in the database grows and can affect the performance of incident reports. To alert administrators when the number of incidents has grown too large, Symantec Data Loss Prevention runs the Incident Counter process daily and generates a system event when the number of incidents exceeds a configurable threshold. The number of incidents does not include archived incidents.

The Incident Counter generates system event code **2316** when the number of incidents exceeds the threshold. You can see this event in the Enforce Server administration console, on the **Servers > Events** page. The summary text for this event is:

Over *<num>* incidents currently contained in the database.

You can also define a system alert that sends an email when the event occurs.

See [“About system alerts”](#) on page 42.

By default, the Incident Counter is enabled and the threshold is set to 1,000,000 incidents. The Incident Counter runs daily at 2:05 A.M. Using the configuration parameters described in [Table 2-4](#), you can configure the threshold, specify when the Incident Counter runs, and you can enable or disable the Incident Counter.

To configure the Incident Counter

- 1 On the Enforce Server host, open the following file in a text editor:

Microsoft Windows: `\SymantecDLP\Protect\config\Manager.properties`

Linux: `/opt/SymantecDLP/Protect/config/Manager.properties`

(Where *SymantecDLP* is the name of the directory where Symantec Data Loss Prevention was installed.)

- 2 Set the parameters that are described in [Table 2-4](#) to configure the Incident Counter.

If you need to use either of the two optional parameters, you must add them.

- 3 Save the file.
- 4 Restart the `VontuManager` service. See [“About Symantec Data Loss Prevention services”](#) on page 18.

Table 2-4 Incident counter parameters

| Property | Description |
|--|--|
| <code>com.vontu.manager.system.IncidentCounter.enabled</code> | Set to True to enable the Incident Counter task. Default value: True . |
| <code>com.vontu.manager.system.IncidentCounter.max_incident_count</code> | The number of incidents that trigger the system event. Default value: 1000000 . Note: Reporting performance often deteriorates when the number of incidents exceeds 1,000,000. However, reporting performance also depends on a variety of other factors. If performance has already deteriorated before the number of incidents exceeds the threshold, lower the threshold. |
| (Optional) <code>com.vontu.manager.system.statistics.IncidentCounter.delay</code> | The number of milliseconds after the <code>VontuManager</code> service starts before the Incident Counter task runs. By default, this parameter is omitted. This parameter is intended for testing purposes only unless you have other reasons to change when the Incident Counter task runs. If this parameter is omitted, the Incident Counter runs daily at 2:05 A.M. |

Table 2-4 Incident counter parameters (*continued*)

| Property | Description |
|---|---|
| (Optional) <code>com.vontu.manager.system.statistics.IncidentCounter.period</code> | <p>The number of milliseconds the Incident Counter waits between each invocation of the task.</p> <p>By default, this parameter is omitted. This parameter is intended for testing purposes only unless you have other reasons to change when the Incident Counter task runs.</p> |

See [“About system events”](#) on page 30.

See [“About system alerts”](#) on page 42.

About incident hiding

Incident hiding lets you flag specified incidents as "hidden." Because these hidden incidents are excluded from normal incident reporting, you can improve the reporting performance of your Symantec Data Loss Prevention deployment by hiding any incidents that are no longer relevant. The hidden incidents remain in the database; they are not moved to another table, database, or other type of offline storage.

You can set filters on incident reports in the Enforce Server administration console to display only hidden incidents or to display both hidden and non-hidden incidents. Using these reports, you can flag one or more incidents as hidden by using the **Hide/Unhide** options that are available when you select one or more incidents and click the **Incident Actions** button. The **Hide/Unhide** options are:

- **Hide Incidents**—Flags the selected incidents as hidden.
- **Unhide Incidents**—Restores the selected incidents to the unhidden state.
- **Do Not Hide**—Prevents the selected incidents from being hidden.
- **Allow Hiding**—Allows the selected incidents to be hidden.

The hidden state of an incident displays in the incident snapshot screen in the Enforce Server administration console. The **History** tab of the incident snapshot includes an entry for each time the **Do Not Hide** or **Allow Hiding** flags are set for the incident.

Access to hiding functionality is controlled by roles. You can set the following user privileges on a role to control access:

- **Hide Incidents**—Grants permission for a user to hide incidents.
- **Unhide Incidents**—Grants permission for a user to show hidden incidents.
- **Remediate Incidents**—Grants permission for a user to set the **Do Not Hide** or **Allow Hiding** flags.

Using system event reports and alerts

This chapter includes the following topics:

- [About system events](#)
- [About system alerts](#)

About system events

System events related to your Symantec Data Loss Prevention installation are monitored, reported, and logged. System events include notifications from Cloud Operations for cloud services.

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 **Overview** screen (**System > Servers and Detectors > 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 and Detectors > Events**.
See [“System events reports”](#) on page 31.
- Recent system events for a particular detection server or cloud service are listed on the **Server/Detector Detail** screen for that server or detector.
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 and Detectors event detail”](#) on page 34.

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 42.
- Syslog functionality
See [“Enabling a syslog server”](#) on page 40.

Some system events require a response.

See [“About system event responses”](#) on page 38.

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 31.
- Configure the system event thresholds for individual servers.
See [“Configuring event thresholds and triggers”](#) on page 36.




System events reports

To view all system events, go to the system events report screen (**System > Servers and Detectors > 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

| Events | Description |
|---------|---|
| 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 <i>Symantec Data Loss Prevention Administration Guide</i> 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

| Event | Description |
|---|--------------------|
|  | 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 and Detectors event detail”](#) on page 34.

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.

Note: You can use the **Cloud Operations** filter value to view events from Cloud Operations for your detectors.

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

| Filter | Description |
|------------|--|
| 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. 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 36.

See [“About system events”](#) on page 30.

See [“Server and Detectors event detail”](#) on page 34.

See [“Working with saved system reports”](#) on page 35.

See [“Configuring event thresholds and triggers”](#) on page 36.

See [“About system alerts”](#) on page 42.

Server and Detectors event detail

To view the **Server and Detectors Event Detail** screen, go to **System > Servers and Detectors > Events** and click one of the listed events.

See [“System events reports”](#) on page 31.

The **Server and Detectors Event Detail** screen displays all of the information available for the selected event. The information on this screen is not editable.

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

Table 3-4 Event detail — General

| Item | Description |
|--------------------|---|
| Type | The event is one of the following types: <ul style="list-style-type: none">■ 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 or Detector | The name of the server or detector. |
| Host | The host name or IP address of the server. |

Table 3-5 Event detail — Message

| Item | Description |
|---------|---|
| Code | A number that identifies the kind of event. See the <i>Symantec Data Loss Prevention Administration Guide</i> 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 30.

See [“System events reports”](#) on page 31.

See [“About system alerts”](#) on page 42.

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 users 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 or detector separately. These parameters should only be adjusted with advice from Symantec Support. 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 30.

To view and change the configurable parameters that trigger system events

- 1 Go to the **Overview** screen (**System > Servers and Detectors > Overview**).
- 2 Click on the name of a detection server or detector to display that server's **Server/Detector Detail** screen.
- 3 Click **Server/Detector Settings**.

The **Advanced Server/Detector 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. | <i>process name</i> 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 |
| 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 |

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

| Parameter | Description | Event |
|-------------------------------|--|-----------------------------|
| 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. | <i>N</i> 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. | <i>N</i> 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. | <i>N</i> 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 42.
- Syslog functionality
See [“Enabling a syslog server”](#) on page 40.

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 | <p>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.</p> <p>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.</p> |
| Tablespace is almost full | <p>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.</p> <p>Refer to the <i>Symantec Data Loss Prevention Installation Guide</i>.</p> |
| Licensing and versioning | Contact Symantec Support. |
| Monitor not responding | <p>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.</p> <p>See "About Symantec Data Loss Prevention services" on page 18.</p> |
| 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 | <p>Increase detection server capacity by adding more CPUs or replacing the computer with a more powerful one.</p> <p>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.</p> <p>Increase the threshold wait times if all of the following items are true:</p> <ul style="list-style-type: none">■ 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 | <p>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.</p> |
| N incidents in queue | <p>Investigate the reason for the incidents filling up the queue.</p> <p>The most likely reasons are as follows:</p> <ul style="list-style-type: none">■ 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 `\SymantecDLP\Protect\config` directory on Windows or the `/opt/SymantecDLP/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%.
```

See [“About system events”](#) on page 30.

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 and Detectors > 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 42.

See [“Configuring system alerts”](#) on page 43.

See [“Server and Detectors event detail”](#) on page 34.

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 42.

See [“Configuring system alerts”](#) on page 43.

See [“About system events”](#) on page 30.

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 42.

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 42.

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 and Detectors > 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 42.

See [“Configuring the Enforce Server to send email alerts”](#) on page 42.

See [“System events reports”](#) on page 31.

Using diagnostic tools

This chapter includes the following topics:

- [About diagnostic tools](#)
- [About system information review](#)

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 46.
- Diagnostic information about the Symantec Data Loss Prevention is displayed on-screen in the dashboard pages of the Enforce Server administration console.
See [“Working with Symantec Data Loss Prevention database diagnostic tools”](#) on page 48.
- A utility for bundling system log files is installed with Symantec Data Loss Prevention.

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 46.

Table 4-1 System Administration pages

| System Administration Page | Description |
|---|--|
| System > Servers and Detectors > 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/Detector Detail pages. |
| System > Servers and Detectors > Overview > Server/Detector Detail | Displays the detailed information about the server, provides functionality to stop, start, and recycle services, configure the server, and access the Server/Detector Settings page. |
| System > Servers and Detectors > Overview > Server/Detector Detail > Server Settings | Enables the system administrators to modify Advanced Server settings. |
| System > Servers and Detectors > Events | Provides a system events report. |
| System > Servers and Detectors > Events > Server/Detector Event Detail | Provides the additional details for the individual events that are listed in the system events report. |
| System > Servers and Detectors > Alerts | Enables the system administrators to enable alerts for system events. |

Working with the Symantec Data Loss Prevention database

This chapter includes the following topics:

- [Working with Symantec Data Loss Prevention database diagnostic tools](#)
- [Viewing tablespaces and data file allocations](#)
- [Adjusting warning thresholds for tablespace usage in large databases](#)
- [Generating a database report](#)
- [Viewing table details](#)
- [Recovering from Symantec Data Loss Prevention database connectivity issues](#)
- [Reclaiming space in the Symantec Data Loss Prevention database](#)

Working with Symantec Data Loss Prevention database diagnostic tools

The Enforce Server administration console lets you view diagnostic information about the tablespaces and tables in your database to help you better manage your database resources. You can see how full your tablespaces and tables are, and whether or not the files in the tables are automatically extensible to accommodate more data. This information can help you manage your database by understanding where you may want to enable the Oracle Autoextend feature on data files, or otherwise manage your database resources. You can also generate a detailed

database report to share with Symantec Technical Support for help with troubleshooting database issues.

You can view the allocation of tablespaces, including the size, memory usage, extensibility, status, and number of files in each tablespace. You can also view the name, size, and Autoextend setting for each file in a tablespace. In addition, you can view table-level allocations for incident data tables, other tables, indexes, and locator object (LOB) tables.

You can generate a full database report in HTML format to share with Symantec Technical Support at any time by clicking **Get full report**. The data in the report can help Symantec Technical Support troubleshoot issues in your database.

See [“Generating a database report”](#) on page 50.

Viewing tablespaces and data file allocations

You can view tablespaces and data file allocations on the **Database Tablespaces Summary** page (**System > Database > Tablespaces Summary**).

The **Database Tablespaces Summary** page displays the following information:

- **Name:** The name of the tablespace.
- **Size:** The size of the tablespace in megabytes.
- **Used (%):** The percentage of the tablespace currently in use.
- **Used (MB):** The amount of the tablespace currently in use, in megabytes.
- **Extendable To (MB):** The size to which the tablespace can be extended. This value is based on the Autoextend settings of the files within the tablespace.
- **Status:** The current status of the tablespace according to the percentage of the tablespace currently in use, depending on the warning thresholds. If you are using the default warning threshold settings, the status is:
 - **OK:** The tablespace is under 80% full, or the tablespace can be automatically extended.
 - **Warning:** The tablespace is between 80% and 90% full. If you see a warning on a tablespace, you may consider enabling Autoextend on the data files in the tablespace or extending the maximum value for data file auto-extensibility.
 - **Severe:** The tablespace is more than 90% full. If you see a severe warning on a tablespace, you should enable Autoextend on the data files in the tablespace, extend the maximum value for data file auto-extensibility, or determine whether you can purge some of the data in the tablespace.
- **Number of Files:** The number of data files in the tablespace.

Select a tablespace from the list to view details about the files it contains. The tablespace file view displays the following information:

- **Name:** The name of the file.
- **Size:** The size of the file, in megabytes.
- **Auto Extendable:** Specifies if the file is automatically extensible based on the Autoextend setting of the file in the Oracle database.
- **Extendable To (MB):** The maximum size to which the file can be automatically extended, in megabytes.
- **Path:** The path to the file.

Adjusting warning thresholds for tablespace usage in large databases

If your database contains a very large amount of data (1 terabyte or more), you may want to adjust the warning thresholds for tablespace usage. For such large databases, Symantec recommends adjusting the **Warning** threshold to 85% full, and the **Severe** threshold to 95% full. You may want to set these thresholds even higher for larger databases. You can specify these values in the */SymantecDLP/protect/config/Manager.properties* file.

To adjust the tablespace usage warning thresholds

- 1 Open the **Manager.properties** file in a text editor.
- 2 Set the **Warning** and **Severe** thresholds to the following values:

```
com.vontu.manager.tablespaceThreshold.warning=85  
com.vontu.manager.tablespaceThreshold.severe=95
```

- 3 Save the changes to the **Manager.properties** file and close it.
- 4 Restart the Vontu Manager service to apply your changes.

Generating a database report

You can generate a full database report in HTML format at any time by clicking **Get full report** on the **Database Tablespaces Summary** page. The database report includes the following information:

- Detailed database information
- Incident data distribution

- Message data distribution
- Policy group information
- Policy information
- Endpoint agent information
- Detection server (monitor) information

Symantec Technical Support may request this report to help troubleshoot database issues.

To generate a database report

- 1 Navigate to **System > Database > Tablespaces Summary**.
- 2 Click **Get full report**.
- 3 The report takes several minutes to generate. Refresh your screen after several minutes to view the link to the report.
- 4 To open or save the report, click the link above the **Tablespaces Allocation** table. The link includes the timestamp of the report for your convenience.
- 5 In the **Open File** dialog box, chose whether to open the file or save it.
- 6 To view the report, open it in a web browser or text editor.
- 7 To update the report, click **Update full report**.

Viewing table details

You can view table-level allocations on the **Database Table Details** page (**System > Database > Table Details**). Viewing table-level allocations can be useful after a large data purge to see the de-allocation of space within your database segments. You can refresh the information displayed on this page by clicking **Update table data** at any time.

The **Database Table Details** page displays your table-level allocations on one of four tabs:

- **Incident Tables:** This tab lists all the incident data tables in the Symantec Data Loss Prevention database schema. The tab displays the following information:
 - **Table Name:** The name of the table.
 - **In Tablespace:** The name of the tablespace that contains the table.
 - **Size (MB):** The size of the table, in megabytes.
 - **% Full:** The percentage of the table currently in use.

- **Other Tables:** This tab lists all other tables in the schema. The tab displays the following information:
 - **Table Name:** The name of the table.
 - **In Tablespace:** The name of the tablespace that contains the table.
 - **Size (MB):** The size of the table, in megabytes.
 - **% Full:** The percentage of the table currently in use.
- **Indices:** This table lists all of the indexes in the schema. The tab displays the following information:
 - **Index Name:** The name of the index.
 - **Table Name:** The name of the table that contains the index.
 - **In Tablespace:** The name of the tablespace that contains the table.
 - **Size (MB):** The size of the table, in megabytes.
 - **% Full:** The percentage of the table currently in use.
- **LOB Segments:** This table lists all of the locator object (LOB) tables in the schema. The tab displays the following information:
 - **Table Name:** The name of the table.
 - **Column Name:** The name of the table column containing the LOB data.
 - **In Tablespace:** The name of the tablespace that contains the table.
 - **LOB Segment Size (MB):** The size of the LOB segment, in megabytes.
 - **LOB Index Size:** The size of the LOB index, in megabytes.
 - **% Full:** The percentage of the table currently in use.

Note: The percentage used value for each table displays the percentage of the table currently in use as reported by the Oracle database in dark blue. It also includes an additional estimated percentage used range in light blue. Symantec Data Loss Prevention calculates this range based on tablespace utilization.

Recovering from Symantec Data Loss Prevention database connectivity issues

If the connection between Symantec Data Loss Prevention and the database is lost for any reason, you must restart all Vontu Services on the Enforce Server after the connection is restored.

See [“About Symantec Data Loss Prevention services”](#) on page 18.

Reclaiming space in the Symantec Data Loss Prevention database

The database space reclamation utility lets you reclaim unused incident LOB space in your Symantec Data Loss Prevention Oracle 11g Standard database. For example, you can use the database space reclamation utility after migrating incident attachments to external storage, or after deleting a large number of incidents.

The utility is a SQL script named `DLP_Lobspace_reclaim.sql`. You can find the utility in the `opt/SymantecDLP/Protect/install/sql` directory on Linux systems, or in the `c:\SymantecDLP\Protect\install\sql` folder on Windows systems.

Your Oracle database must be in `NOARCHIVE` mode to run this utility.

Note: If you are using Oracle 12c Enterprise, you can reclaim space using the Oracle Manager/Segment Advisor tool.

To use the database space reclamation utility

- 1 Optional: if you are using a three-tier deployment of Symantec Data Loss Prevention, copy the `DLP_Lobspace_reclaim.sql` file to the computer that hosts your Oracle database.

You can find the utility in `opt/SymantecDLP/Protect/install/sql/` on Linux systems, or `c:\SymantecDLP\Protect\install\sql` folder on Windows systems.
- 2 On the computer that hosts your Oracle 11g Standard database, open a command shell and navigate to the location of the `DLP_Lobspace_reclaim.sql` file.
- 3 Log in to SQL*Plus as the Oracle `sysdba`:


```
sqlplus sys/<password> as sysdba
```
- 4 At the SQL*Plus prompt, run the utility:


```
@@DLP_lobspace_reclaim.sql
```
- 5 The database space reclamation utility may take some time to complete its process. While it is running, the utility logs its progress to the `lobspace_reclamation.log` file.

Note: If the database space reclamation utility returns any invalid objects, you must recompile your database using the `utlirp` and package provided by Oracle. You can find the `utlirp` package in `ORACLE_HOME/RDBMS/ADMIN`. If you see any other errors in the logs, contact Symantec Support and provide them a copy of the `lobspace_reclamation.log` file.

Backing up and recovering on Windows

This chapter includes the following topics:

- [About backup and recovery on Windows](#)
- [About periodic system backups on Windows](#)
- [About partial backups on Windows](#)
- [Preparing the backup location on Windows](#)
- [Performing a cold backup of the Oracle database on Windows](#)
- [Backing up the server configuration files on Windows](#)
- [Backing up files stored on the file system on Windows](#)
- [Oracle hot backups on Windows platforms](#)
- [About Windows system recovery](#)

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, the database, and the incident attachment external storage directory, if present. These backup procedures can be used for single-tier, two-tier, and three-tier installations.

The cold backup procedures for the Oracle 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.

Symantec recommends that your data storage administrator perform all backups of your incident attachment external storage directories.

See [“About periodic system backups on Windows”](#) on page 56.

See [“About partial backups on Windows”](#) on page 57.

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 56.

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 56.

About partial backups on Windows

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

Table 6-1 Performing partial backups

| | |
|--|--|
| To back up a database only: | <p>See “Preparing the backup location on Windows” on page 57.</p> <p>See “Performing a cold backup of the Oracle database on Windows” on page 62.</p> |
| To back up an Enforce Server or detection server only: | <p>See “Preparing the backup location on Windows” on page 57.</p> <p>See “Backing up the server configuration files on Windows” on page 68.</p> <p>See “Backing up files stored on the file system on Windows” on page 69.</p> |

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 72.

Preparing the backup location consists of the following steps:

Table 6-2 Preparation of the backup location

| Step | Action | Description |
|------|--|---|
| 1 | Determine the size of the backup sections. | See “Determining the size of the backup on Windows” on page 58. |
| 2 | Calculate the total size of the backup. | See “Calculating the total size of the backup on Windows” on page 60. |
| 3 | Identify a backup location. | See “Identifying a backup location on Windows” on page 60. |
| 4 | Create the backup directories. | See “Creating backup directories on Windows” on page 61. |

See [“About the Windows recovery information worksheet”](#) on page 72.

See [“About partial backups on Windows”](#) on page 57.

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 57.

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 - OraDb11g_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 as sysdba
```

where *password* is the `sys` password.

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 60.

- 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 `\SymantecDLP\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 `\SymantecDLP\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 60.

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 `\SymantecDLP\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 60.

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 57.

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 58.

- 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 6-5](#) on page 72.

See [“Preparing the backup location on Windows”](#) on page 57.

Creating backup directories on Windows

Create the following directories, preferably on a external storage device or on a system separate from the computer that hosts the Oracle database.

To create the backup directory structure

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

```
\SymantecDLP_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:

```
\SymantecDLP_Backup_Files\File_System
\SymantecDLP_Backup_Files\Server_Configuration_Files
\SymantecDLP_Backup_Files\Database
\SymantecDLP_Backup_Files\Recovery_Aid
```

- 3 Complete the Recovery Information Worksheet with the Drive you used in the previous step.

See [Table 6-5](#) on page 72.

See [“Preparing the backup location on Windows”](#) on page 57.

Performing a cold backup of the Oracle database on Windows

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

You perform a cold backup by

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

If your company has 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 71.

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

| Step | Action | Description |
|------|----------------------------|--|
| 1 | Create recovery aid files. | See “Creating recovery aid files on Windows” on page 63. |

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

| Step | Action | Description |
|------|---|---|
| 2 | Collect a list of directories that should be backed up. | See “Collecting a list of files to be backed up” on page 65. |
| 3 | 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 66. |
| 4 | Copy the database files to the backup location. | See “Copying the database files to the backup location on Windows” on page 67. |
| 5 | Optional: back up the incident attachment external storage directory | If you are using an external storage directory for incident attachments, work with your storage system administrator to back up that directory. |
| 6 | Restart the Oracle and Symantec Data Loss Prevention services. | See “Restarting the system on Windows” on page 67. |

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 re-create the database structure.

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

Note: The following steps assume you created the backup directory

`c:\SymantecDLP_Backup_Files\Recovery_Aid`. If you did not, do so now. See [“Creating backup directories on Windows”](#) on page 61.

To generate a trace file of the control file

- 1 At the command prompt, enter `sqlplus /nolog`.

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

Note: The Oracle SQL*Plus application is case sensitive.

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

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

where *password* is the `sys` password.

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

```
alter database backup controlfile to trace as  
'C:\SymantecDLP_Backup_Files\Recovery_Aid\controlfile.trc';
```

Success is indicated by the message "Database altered."

With this command you are generating a copy of the backup control file and outputting this file to the `\SymantecDLP_Backup_Files\Recovery_Aid` directory that you created previously. See [“Creating backup directories on Windows”](#) on page 61.

Note: The normal destination of a trace file is the `user_dump` directory. Assuming you followed the installation steps in the *Symantec Data Loss Prevention Oracle Installation and Upgrade Guide*, this directory is `\oracle\diag\rdbms\protect\trace`. If you installed Oracle differently, issue SQL*Plus command `show parameter user_dump_dest;` to display the `user_dump` directory.

- 4 Issue the following command to backup the `init.ora` file.

```
create pfile='C:\SymantecDLP_Backup_Files\Recovery_Aid\init.ora' from spfile;
```

Exit Sql*Plus:

```
exit;
```


- 5 Navigate to the `C:\SymantecDLP_Backup_Files\Recovery_Aid` directory. You should see the `controlfile.trc` and `init.ora` files in this directory.
- 6 Rename the file `controlfile.trc` so that it can be easily identified, for example:

```
controlfilebackupMMDDYY.trc
```

See [“Collecting a list of files to be backed up”](#) on page 65.

See [“Performing a cold backup of the Oracle database on Windows”](#) on page 62.

Collecting a list of files to be backed up

You can create a list of files that need to be backed up. These lists are used in a later step.

To create a list of files for back up

- 1 Open SQL*Plus using the following command:

```
sqlplus sys/<password> as sysdba
```

- 2 Enter the following SQL commands to create lists of files that must be backed up:

```
SELECT file_name FROM dba_data_files
UNION
SELECT file_name FROM dba_temp_files
UNION
SELECT name FROM v$controlfile
UNION
SELECT member FROM v$logfile;
```

- 3 Save the list of files returned by the query to use in the following procedures:
`C:\SymantecDLP_Backup_Files\Recovery_Aid\oracle_datafile_directories.txt`.
- 4 Exit SQL*Plus:

```
exit;
```

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 63.

To create a copy of the `spfile`

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

```
create pfile='c:\Temp\inittemp.ora' from spfile;
```

- 2 To exit Oracle SQL*Plus, enter:

```
exit
```

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

See [“Creating backup directories on Windows”](#) on page 61.

See [“Performing a cold backup of the Oracle database on Windows”](#) on page 62.

Shutting down the Symantec Data Loss Prevention system on Windows

To shut down the system

- 1 On the computer that hosts the Enforce Server, 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:
 - `VontuUpdate`
 - `VontuIncidentPersister` (on the computers that also host the Enforce Server)
 - `VontuManager` (on the computers that also host the Enforce Server)
 - `VontuMonitor` (on the computers that also host a detection server)
 - `VontuMonitorController` (on the computers that also host the Enforce Server)
 - `VontuNotifier` (on the computers that also host the Enforce Server)
- 3 On the computer that hosts the database, stop the `OracleServicedatabasename`, where `databasename` is the Global Database Name and SID selected during installation.

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

See [“Performing a cold backup of the Oracle database on Windows”](#) on page 62.

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 66.
- 2 On the computer that hosts the database, copy the files from the list that you collected in the procedure [Collecting a list of files to be backed up](#) to the computer that hosts the backup files. Copy the protect directory into the `c:\Symantec_DLP_Backup_Files\Database` directory of the computer that hosts the backup files.

Note: If you are performing this backup as part of a complete backup of a Symantec Data Loss Prevention deployment, 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. Otherwise, create a backup location on a computer that is accessible from the Oracle host.

See [Table 6-5](#) on page 72.

- 3 On the computer that hosts the database, select the `%ORACLE_HOME%\database\PWDprotect.ora` file and copy it into the `c:\Backup_Files\Database` directory of the computer that hosts the backup files.

See [“Performing a cold backup of the Oracle database on Windows”](#) on page 62.

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`

where *DATABASENAME* is the Global Database Name and SID selected during installation.

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

- 3 On the computer that hosts the Enforce Server, start the `VontuNotifier` service before starting other Symantec Data Loss Prevention services.
- 4 Start the remaining Symantec Data Loss Prevention services, which might include the following:
 - `VontuManager` (on the computer that also host the Enforce Server)
 - `VontuMonitor` (on the computers that also host a detection server)
 - `VontuIncidentPersister` (on the computer that also host the Enforce Server)
 - `VontuUpdate`
 - `VontuMonitorController` (on the computers that also hosts the Enforce Server)

See [“Performing a cold backup of the Oracle database on Windows”](#) on page 62.

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 > Servers and Detectors > Overview > *server_name* > Server/Detector Details** page. To make these changes, you can also edit any of the `.properties` files that reside in the `\SymantecDLP\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 `\SymantecDLP\Protect\config` directory. Copy it to the `\SymantecDLP_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 6-5](#) on page 72.

- 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 database on Windows”](#) on page 62.

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 69.
- System logs
See [“Backing up system logs on Windows”](#) on page 69.
- Keystore file
See [“Backing up a keystore file on Windows”](#) on page 70.

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.

To back up customized changes stored in the `\plugins` directory

- 1 On the computer that hosts the Enforce Server, select the `\SymantecDLP\Protect\plugins` directory. Copy it into the `\SymantecDLP_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 6-5](#) on page 72.
- 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 69.

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 `\SymantecDLP\Protect\logs` directory. Copy it into the `\SymantecDLP_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 6-5](#) on page 72.

- 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 69.

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 `\SymantecDLP\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 `\SymantecDLP_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 6-5](#) on page 72.

See [“Backing up files stored on the file system on Windows”](#) on page 69.

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:\SymantecDLP\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 database on Windows”](#) on page 62.

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 6-4 Windows system recovery components

| Component | Description |
|--|---|
| Windows recovery information worksheet | See “About the Windows recovery information worksheet” on page 72. |
| Windows recovery process | See “About recovering your system on Windows platforms” on page 73. |

About the Windows recovery information worksheet

Assuming you followed the recommended backup instructions, the backup files are located on an alternate computer in directory \SymantecDLP_Backup_Files and its subdirectories, each of which is listed in [Table 6-5](#).

See [“Performing a cold backup of the Oracle database on Windows”](#) on page 62.

See [“About Windows system recovery”](#) on page 71.

To use the Recovery Information Worksheet

- 1 Print this page containing the Recovery Information Worksheet.
- 2 In the first row of the "Customer names and locations" column, write in the computer name of the host where you have setup the backup directory.
- 3 In the subsequent rows in the "Customer names and locations" column, in the space provided preceding the backup directory, write in the volume drive letter where the backup directory is located.

For example, if the drive is "D" you would enter:

D:\SymantecDLP_Backup_Files

- 4 Store this worksheet in a secure location because it contains sensitive data.

Table 6-5 Recovery Information Worksheet

| Backup file information | Example names and locations | Customer names and locations |
|---|--|--|
| Name of the computer that hosts backup files | <i>machine_name</i> | |
| Directory containing backup files | \SymantecDLP_Backup_Files | ___:\SymantecDLP_Backup_Files |
| Subdirectory containing file system backup files | \SymantecDLP_Backup_Files\ File_System | ___:\SymantecDLP_Backup_Files\ File_System |
| Subdirectory containing Enforce and detection server configuration backup files | \SymantecDLP_Backup_Files\ Server_Configuration_Files | ___:\SymantecDLP_Backup_Files\ Server_Configuration_Files |
| Subdirectory containing database backup files | \SymantecDLP_Backup_Files\ Database | ___:\SymantecDLP_Backup_Files\ Database |
| Subdirectory containing Database Recovery Aid files | \SymantecDLP_Backup_Files\ Recovery_Aid | ___:\SymantecDLP_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 71.

The following table describes the steps necessary to recover Windows.

Table 6-6 Windows recovery

| Step | Action | Description |
|--------|-------------------------------|--|
| Step 1 | Recover the database. | See “About recovering the database on Windows” on page 73. |
| Step 2 | Recover the Enforce Server. | See “Recovering the Enforce Server on Windows” on page 77. |
| Step 3 | Recover the detection server. | See “Recovering a detection server on Windows” on page 78. |

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 74.

See [“Creating a new database on Windows”](#) on page 75.

See [“About recovering your system on Windows platforms”](#) on page 73.

Restoring an existing database on Windows

See [“About recovering the database on Windows”](#) on page 73.

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 Enforce Server, navigate to **Start > All Programs > Administrative Tools > Services**. This navigation opens the Windows Services menu.
- 3 From the Windows Services menu, stop all Symantec Data Loss Prevention services, which might include the following:
 - `VontuUpdate`
 - `VontuIncidentPersister` (on the computer hosting the Enforce Server)
 - `VontuManager` (on the computer hosting the Enforce Server)
 - `VontuMonitor` (on the computer or computers hosting a detection server)
 - `VontuMonitorController` (on the computer hosting the Enforce Server)
 - `VontuNotifier` (on the computer hosting the Enforce Server)
- 4 On the computer that hosts the database, stop all of the Oracle services.
- 5 Copy the contents of the `\SymantecDLP_Backup_Files\Database` directory to the `%ORACLE_BASE%\oradata\protect` directory (for example, `c:\oracle\oradata\protect`) 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 72.
- 6 To open Oracle SQL*Plus, navigate to **Windows > Start > All Programs > Oracle - OraDb11g_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 as sysdba
```

where *password* is the `sys` password.

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 73.

Creating a new database on Windows

See [“About recovering the database on Windows”](#) on page 73.

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\11.2.0.4\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 72.
- To open Oracle SQL*Plus, navigate to **Windows > Start > All Programs > Oracle - OraDb11g_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 `inittmp.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 72.

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 `inittmp.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\11.2.0.4\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 72.
- On the computer that hosts the new database, open Oracle SQL*Plus. Navigate to **Windows > Start > All Programs > Oracle - OraDb11g_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, enter:

```
startup
```

See [“About recovering your system on Windows platforms”](#) on page 73.

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 73.

- 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 \SymantecDLP\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 72.

- 7 To restore customized changes, copy the contents of the
`\Backup_Files\File_System\plugins` directory to the
`\SymantecDLP\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 72.
 - 8 To restore the keystore file, copy the contents of the
`\Backup_Files\File_System\.keystore` directory to the
`\SymantecDLP\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 72.
- See [“About recovering your system on Windows platforms”](#) on page 73.

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 `\SymantecDLP\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 72.

- 4 To restore customized changes, copy the contents of the
 \Backup_Files\File_System\plugins directory to the
 \SymantecDLP\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 72.

- 5 To restore the keystore file, copy the contents of the
 \Backup_Files\File_System\.keystore directory to the
 \SymantecDLP\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 72.

See [“About recovering your system on Windows platforms”](#) on page 73.

Backing up and recovering on Linux

This chapter includes the following topics:

- [About backup and recovery on Linux](#)
- [About periodic system backups on Linux](#)
- [About partial backups on Linux](#)
- [Preparing the backup location on Linux](#)
- [Performing a cold backup of the Oracle database on Linux](#)
- [Backing up the server configuration files on Linux](#)
- [About backed up files stored on the file system on Linux](#)
- [Oracle hot backups on Linux platforms](#)
- [About the Linux recovery information worksheet](#)
- [About recovering your system on Linux](#)

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, the database, and the incident attachment external storage directory, if present. These backup procedures can be used for single-tier, two-tier, and three-tier installations.

The cold backup procedures for the Oracle 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.

Symantec recommends that your storage system administrator perform all backups of your incident attachment external storage directories.

See [“About periodic system backups on Linux”](#) on page 81.

See [“About partial backups on Linux”](#) on page 82.

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 81.

See [“About partial backups on Linux”](#) on page 82.

See [“About backup and recovery on Linux”](#) on page 80.

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 81.

About partial backups on Linux

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

Table 7-1 Types of partial backups

| | |
|--|--|
| To back up a database only: | See “ Preparing the backup location on Linux ” on page 82. |
| | See “ Performing a cold backup of the Oracle database on Linux ” on page 87. |
| To back up an Enforce Server or detection server only: | See “ Preparing the backup location on Linux ” on page 82. |
| | See “ Backing up the server configuration files on Linux ” on page 94. |
| | See “ About backed up files stored on the file system on Linux ” on page 95. |

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 98.

Preparing the backup location consists of the following steps:

Table 7-2 Preparing the backup location

| Step | Action | Description |
|------|--|---|
| 1 | Determine the size of the backup sections. | See “Determining the size of the backup on Linux” on page 83. |
| 2 | Calculate the total size of the backup. | See “Calculating the total size of the backup on Linux” on page 85. |
| 3 | Identify the backup location. | See “Identifying a backup location on Linux” on page 85. |
| 4 | Create the backup directories. | See “Creating backup directories on Linux” on page 86. |

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 82.

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 as sysdba
```

where *password* is the `sys` password.

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 85.

- 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/SymantecDLP/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/SymantecDLP` 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 85.

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/SymantecDLP/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 85.

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 82.

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 83.

- 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 98.

- 4 To determine the name of a computer, enter:

```
hostname -f
```

See [“Preparing the backup location on Linux”](#) on page 82.

Creating backup directories on Linux

To create the backup directory structure

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

```
mkdir /opt/SymantecDLP_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/SymantecDLP_Backup_Files/File_System
mkdir /opt/SymantecDLP_Backup_Files/Server_Configuration_Files
mkdir /opt/SymantecDLP_Backup_Files/Database
mkdir /opt/SymantecDLP_Backup_Files/Recovery_Aid
```

- 3 Complete the Recovery Information Worksheet, making use of the `/opt/SymantecDLP` directory as described in the previous two steps.

See [“About the Linux recovery information worksheet”](#) on page 98.

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

```
chmod 777 /opt/SymantecDLP/ -R
```

See [“Preparing the backup location on Linux”](#) on page 82.

Performing a cold backup of the Oracle database on Linux

Cold backups are recommended primarily for non-database administrator users. You perform a cold backup by

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

If your company has 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 97.

Table 7-3 Steps to perform a cold backup of the Oracle database

| Step | Action | Description |
|------|---|---|
| 1 | Create recovery aid files. | See “Creating recovery aid files on Linux” on page 88. |
| 2 | Collect a list of directories that should be backed up. | See “Collecting a list of files to be backed up” on page 89. |
| 3 | 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 91. |
| 4 | Copy the database files to the backup location. | See “Copying the database files to the backup location on Linux” on page 92. |

Table 7-3 Steps to perform a cold backup of the Oracle database (*continued*)

| Step | Action | Description |
|------|--|---|
| 5 | Optional: back up the incident attachment external storage directory | If you are using an external storage directory for incident attachments, work with your storage system administrator to back up that directory. |
| 6 | Restart the Oracle and Symantec Data Loss Prevention services. | See “Restarting the system on Linux” on page 93. |

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 re-create 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 as sysdba
```

where *password* is the `sys` password.

See the *Symantec Data Loss Prevention Installation Guide*.

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

```
alter session set tracefile_identifier = 'controlfile';
```

- 5 Run the following command:

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


- 6 If you have not already done so, create the recovery aid directory on the computer that hosts the Oracle database:

```
/opt/oracle/Recovery_Aid
```

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

```
show parameter user_dump;
```

- 8 Enter the following command:

```
create pfile='/opt/oracle/Recovery_Aid/init.ora' from spfile;
```

- 9 To exit Oracle SQL*Plus, enter:

```
exit
```

- 10 Change to the directory from step 7. Copy the trace file from the `Recovery_Aid` subdirectory on the computer that hosts the Oracle database to the `/Recovery_Aid` subdirectory on the backup computer that you created earlier.

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 *controlfile.trc
```

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

```
controlfilebackupMMDDYY.trc.
```

See [“Collecting a list of files to be backed up”](#) on page 89.

See [“Performing a cold backup of the Oracle database on Linux”](#) on page 87.

Collecting a list of files to be backed up

You can create a list of files that need to be backed up. These lists are used in a later step.

To create a list of files for back up

- 1 Open SQL*Plus using the following command:

```
sqlplus sys/<password> as sysdba
```

- 2 Enter following SQL commands to create lists of files that must be backed up:

```
SELECT file_name FROM dba_data_files
UNION
SELECT file_name FROM dba_temp_files
UNION
SELECT name FROM v$controlfile
UNION
SELECT member FROM v$logfile;
```

- 3 Save the list of files returned by the query:

```
/opt/SymantecDLP_Backup_Files/Recovery_Aid/oracle_datafile_directories.txt.
```

- 4 Exit SQL*Plus:

```
exit;
```

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 88.

To create a copy of the `spfile`

- 1 Log on to the computer that hosts the Enforce Server 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 as sysdba
```

where *password* is the `sys` password.

- 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 86.

See [“Performing a cold backup of the Oracle database on Linux”](#) on page 87.

Shutting down the Symantec Data Loss Prevention system on Linux

To shut down the system

- 1 On the computer that hosts the Enforce Server, log on as root.
- 2 Go to the `/opt/SymantecDLP/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)
```

```
./VontuDetectServerController.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 as sysdba
```

where *password* is the `sys` password.

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 database on Linux”](#) on page 87.

Copying the database files to the backup location on Linux

The database files that should be backed up include the files in the `/Recovery_Aid` 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 will be corrupt and unusable.

See [“Shutting down the Symantec Data Loss Prevention system on Linux”](#) on page 91.

- 2 On the computer that hosts the database, copy the directories (and their contents) using the list of directories that you collected previously (see [Collecting a list of files to be backed up](#)) to the `/opt/Backup_Files/Database` directory of the computer or storage device that hosts the backup files.

Note: If you are performing this backup as part of a complete backup of a Symantec Data Loss Prevention deployment, 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. Otherwise, create a backup location on a computer that is accessible from the Oracle host.

See [“About the Linux recovery information worksheet”](#) on page 98.

- 3 Copy the `/Recovery_Aid/` subdirectory from the computer that hosts the database to the backup computer.

If you have not yet created this directory, create the following directory on a computer or storage device other than the computer that hosts the Oracle database:

```
/opt/SymantecDLP_Backup_Files/Recovery_Aid
```

Set permissions for this directory for the Oracle user by running the following command:

```
chmod 777 /opt/SymantecDLP_Backup_Files/ -R
```

- 4 On the computer that hosts the database, copy the `$ORACLE_HOME/dbs/orapwprotect` file into the `/opt/Backup_Files/Database` directory of the computer or storage device that hosts the backup files.

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

See [“Performing a cold backup of the Oracle database on Linux”](#) on page 87.

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 as sysdba
```

where *password* is the `sys` password.

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 Enforce Server, log on as root.
- 6 Change directory to `/opt/SymantecDLP/Protect/bin`.

- 7 Before starting other Symantec Data Loss Prevention services, start the VontuNotifier service.

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

- 8 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)
```

```
./SymantedDLPUUpdate.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 database on Linux”](#) on page 87.

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 > Servers and Detectors > Overview > *server_name* > Server/Detector Details** page. To make these changes, you can also edit any of the files with a `.properties` extension that reside in the `/opt/SymantecDLP/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/SymantecDLP/Protect/config` directory. Copy it to the `/opt/SymantecDLP_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 98.

- 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 database on Linux”](#) on page 87.

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 95.
- System logs
 See [“Backing up system logs on Linux”](#) on page 96.
- Keystore files
 See [“Backing up a keystore file on Linux”](#) on page 96.

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.

To back up customized changes stored in the /plugins directory

- 1 On the computer that hosts the Enforce Server, copy the `/opt/SymantecDLP/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 98.
- 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 95.

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/SymantecDLP/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 98.
- 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 95.

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/SymantecDLP/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 98.

See [“About backed up files stored on the file system on Linux”](#) on page 95.

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/SymantecDLP/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 database on Linux”](#) on page 87.

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 database on Linux”](#) on page 87.

Table 7-4 Recovery Information Worksheet

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

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 7-5 Performing a Linux system recovery

| Step | Action | Description |
|------|-------------------------------|---|
| 1 | Recover the database. | See “About recovering the database on Linux” on page 99. |
| 2 | Recover the Enforce Server. | See “Recovering the Enforce Server on Linux” on page 103. |
| 3 | Recover the detection server. | See “Recovering a detection server on Linux” on page 104. |

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 [“Restoring an existing database on Linux”](#) on page 99.

See [“Creating a new database on Linux”](#) on page 101.

See [“About recovering your system on Linux”](#) on page 98.

Restoring an existing database on Linux

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 Enforce Server, log on as root.
- 3 Change directory to `/opt/SymantecDLP/Protect/bin`.

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

```
./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 stopped by changing to the `etc` directory and running the following command:

```
./init.d/SymantedDLPSERVICEName stop
```

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

```
./init.d/VontuSERVICEName start
```

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

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-tier and two-tier installations.

See the *Symantec Data Loss Prevention Installation Guide*.

- 6 After receiving the "Connected" message, at the `SQL>` command prompt, stop all of the Oracle services by entering:

```
shutdown immediate
```

- 7 To exit Oracle SQL*Plus, enter:

```
exit
```

- 8 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 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 98.

- 9 To open Oracle SQL*Plus, enter:

```
sqlplus /nolog
```

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

```
connect sys/password as sysdba
```

where *password* is the `sys` password.

See the *Symantec Data Loss Prevention Installation Guide*.

- 11 At the `SQL>` prompt, enter:

```
startup
```

See [“About recovering your system on Linux”](#) on page 98.

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 98.
 - To open Oracle SQL*Plus, enter:

```
sqlplus /nolog
```

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

```
connect sys/password as sysdba
```

Where *password* is the `sys` password.

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 98.

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 98.
- 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, enter:

```
startup
```

See [“About recovering your system on Linux”](#) on page 98.

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 99.
- 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/SymantecDLP/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 98.

- 7 To restore customized changes, copy the contents of the `/Backup_Files/File_System/plugins` directory to the `/opt/SymantecDLP/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 98.
 - 8 To restore the keystore file, copy the contents of the `/Backup_Files/File_System/.keystore` directory to the `/opt/SymantecDLP/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 98.
- See [“About recovering your system on Linux”](#) on page 98.

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/SymantecDLP/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 98.

- 4 To restore customized changes, copy the contents of the `/Backup_Files/File_System/plugins` directory to the `/opt/SymantecDLP/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 98.

- 5 To restore the keystore file, copy the contents of the `/Backup_Files/File_System/.keystore` directory to the `/opt/SymantecDLP/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 98.

See [“About recovering your system on Linux”](#) on page 98.

Log files and codes

This appendix includes the following topics:

- [About log files](#)
- [About log event codes](#)
- [Network Prevent for Web operational log files and event codes](#)
- [Network Prevent for Web access log files and fields](#)
- [Network Prevent for Web protocol debug log files](#)
- [Network Prevent for Email log levels](#)
- [Network Prevent for Email operational log codes](#)
- [Network Prevent for Email originated responses and codes](#)

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 to 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 for Email Server communicates with a specific MTA on your network.
- 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.

- 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:
 - `installldir\SymantecDLP\.install14j\installation.log` stores the installation log for Symantec Data Loss Prevention.
 - `installldir\oracle_home\admin\protect\` stores the installation log for Oracle.

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

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 for Web operational log files and event codes”](#) on page 107.
- See [“Network Prevent for Email operational log codes”](#) on page 113.
- See [“Network Prevent for Email originated responses and codes”](#) on page 116.

Network Prevent for Web operational log files and event codes

Network Prevent for 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 `SymantecDLP\Protect\config` directory. By default, the values are:

- `com.vontu.icap.log.IcapOperationalLogHandler.limit = 5000000`

- `com.vontu.icap.log.IcapOperationalLogHandler.count = 5`

Table A-1 lists the Network Prevent for Web-defined operational logging codes by category. The italicized part of the text contains event parameters.

Table A-1 Status codes for Network Prevent for Web operational logs

| Code | Text and Description |
|---------------------|---|
| Operational Events | |
| 1100 | Starting Network Prevent for Web |
| 1101 | Shutting down Network Prevent for Web |
| Connectivity Events | |
| 1200 | <p>Listening for incoming connections at <i>icap_bind_address:icap_bind_port</i></p> <p>Where:</p> <ul style="list-style-type: none"> ■ <i>icap_bind_address</i> is the Network Prevent for Web bind address to which the server listens. This address is specified with the Icap.BindAddress Advanced Setting. ■ <i>icap_bind_port</i> is the port at which the server listens. This port is set in the Server > Configure page. |
| 1201 | <p>Connection (<i>id=conn_id</i>) opened from <i>host(icap_client_ip:icap_client_port)</i></p> <p>Where:</p> <ul style="list-style-type: none"> ■ <i>conn_id</i> is the connection ID that is allocated to this connection. This ID can be helpful in doing correlations between multiple logs. ■ <i>icap_client_ip</i> and <i>icap_client_port</i> are the proxy's IP address and port from which the connect operation to Network Prevent for Web was performed. |
| 1202 | <p>Connection (<i>id=conn_id</i>) closed (<i>close_reason</i>)</p> <p>Where:</p> <ul style="list-style-type: none"> ■ <i>conn_id</i> is the connection ID that is allocated to the connect operation. ■ <i>close_reason</i> provides the reason for closing the connection. |

Table A-1 Status codes for Network Prevent for Web operational logs
(continued)

| Code | Text and Description |
|---------------------|--|
| 1203 | <p>Connection states: REQMOD=<i>N</i>, RESPMOD=<i>N</i>, OPTIONS=<i>N</i>, OTHERS=<i>N</i></p> <p>Where <i>N</i> indicates the number of connections in each state, when the message was logged.</p> <p>This message provides the system state in terms of connection management. It is logged whenever a connection is opened or closed.</p> |
| Connectivity Errors | |
| 5200 | <p>Failed to create listener at <i>icap_bind_address:icap_bind_port</i></p> <p>Where:</p> <ul style="list-style-type: none"> ■ <i>icap_bind_address</i> is the Network Prevent for Web bind address to which the server listens. This address can be specified with the Icap.BindAddress Advanced Setting. ■ <i>icap_bind_port</i> is the port at which the server listens. This port is set on the Server > Configure page. |
| 5201 | <p>Connection was rejected from unauthorized host (<i>host_ip:port</i>)</p> <p>Where <i>host_ip</i> and <i>port</i> are the proxy system IP and port address from which a connect attempt to Network Prevent for Web was performed. If the host is not listed in the Icap.AllowHosts Advanced setting, it is unable to form a connection.</p> |

See “[About log files](#)” on page 106.

Network Prevent for Web access log files and fields

Network Prevent for Web log file names use the format of `WebPrevent_AccessX.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 for 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 "referrer" "user_agent" processing_time(ms) conn_id client_ip
client_port action_code icap_method_code traffic_source_code
```

[Table A-2](#) 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-2 Network Prevent for 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 for Web receives the request. |
| request_line | Line that represents the request. |
| icap_status_code | ICAP response code that Network Prevent for Web sends by for this request. |
| request_size | Request size in bytes. |
| referrer | 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 (milliseconds) | 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). |

Table A-2 Network Prevent for Web access log fields (*continued*)

| Fields | Explanation |
|---------------------|---|
| action_code | <p>An integer representing the action that Network Prevent for Web takes. Where the action code is one of the following:</p> <ul style="list-style-type: none"> ■ 0 = UNKNOWN ■ 1 = ALLOW ■ 2 = BLOCK ■ 3 = REDACT ■ 4 = ERROR ■ 5 = ALLOW_WITHOUT_INSPECTION ■ 6 = OPTIONS_RESPONSE ■ 7 = REDIRECT |
| icap_method_code | <p>An integer representing the ICAP method that is associated with this request. Where the ICAP method code is one of the following:</p> <ul style="list-style-type: none"> ■ -1 = ILLEGAL ■ 0 = OPTIONS ■ 1 = REQMOD ■ 2 = RESPMOD ■ 3 = LOG |
| traffic_source_code | <p>An integer that represents the source of the network traffic. Where the traffic source code is one of the following:</p> <ul style="list-style-type: none"> ■ 1 = WEB ■ 2 = UNKNOWN |

See [“About log files”](#) on page 106.

Network Prevent for 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. Symantec Data Loss Prevention 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 106.

Network Prevent for Email log levels

Network Prevent for 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.SmtopOperationalLogHandler.limit = 5000000`
- `com.vontu.mta.log.SmtopOperationalLogHandler.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 `SymantecDLP\Protect\config` directory. For example, `com.vontu.mta.rp.level = FINE` specifies the FINE level of detail.

[Table A-3](#) describes the Network Prevent for Email log levels.

Table A-3 Network Prevent for 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 106.

Network Prevent for Email operational log codes

Table A-4 lists the defined Network Prevent for Email operational logging codes by category.

Table A-4 Status codes for Network Prevent for Email operational log

| Code | Description |
|---------------------|--|
| Core Events | |
| 1100 | Starting Network Prevent for Email |
| 1101 | Shutting down Network Prevent for Email |
| 1102 | Reconnecting to FileReader (tid= <i>id</i>) Where <i>id</i> is the thread identifier. The RequestProcessor attempts to re-establish its connection with the FileReader for detection. |
| 1103 | Reconnected to the FileReader successfully (tid= <i>id</i>) The RequestProcessor was able to re-establish its connection to the FileReader. |
| Core Errors | |
| 5100 | Could not connect to the FileReader (tid= <i>id</i> timeout=.3s) An attempt to re-connect to the FileReader failed. |
| 5101 | FileReader connection lost (tid= <i>id</i>) The RequestProcessor connection to the FileReader was lost. |
| Connectivity Events | |
| 1200 | Listening for incoming connections (local= <i>hostname</i>) <i>Hostnames</i> is an IP address or fully-qualified domain name. |
| 1201 | Connection accepted (tid= <i>id</i> cid= <i>N</i> local= <i>hostname:port</i> remote= <i>hostname:port</i>) Where <i>N</i> is the connection identifier. |

Table A-4 Status codes for Network Prevent for Email operational log
(continued)

| Code | Description |
|----------------------------|---|
| 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) |
| 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) |

Table A-4 Status codes for Network Prevent for Email operational log
(continued)

| Code | Description |
|----------------|---|
| 5205 | Could not create listener (address=local=hostname:port reason= <i>Explanation</i>) |
| 5206 | Authorized MTAs contains invalid hosts: <i>hostname</i> , <i>hostname</i> , ... |
| 5207 | MTA restrictions are active, but no MTAs are authorized to communicate with this host |
| 5208 | TLS handshake failed (reason= <i>Explanation</i> tid= <i>id</i> cid= <i>N</i> local= <i>hostname</i> remote= <i>hostname</i>) |
| 5209 | TLS handshake completed (tid= <i>id</i> cid= <i>N</i> local= <i>hostname</i> remote= <i>hostname</i>) |
| 5210 | All forward hosts unavailable (tid= <i>id</i> cid= <i>N</i> reason= <i>Explanation</i>) |
| 5211 | DNS lookup failure (tid= <i>id</i> cid= <i>N</i> NextHop= <i>hostname</i> reason= <i>Explanation</i>) |
| 5303 | Failed to encrypt incoming message (tid= <i>id</i> cid= <i>N</i> local= <i>hostname</i> remote= <i>hostname</i>) |
| 5304 | Failed to decrypt outgoing message (tid= <i>id</i> cid= <i>N</i> local= <i>hostname</i> remote= <i>hostname</i>) |
| Message Events | |

Table A-4 Status codes for Network Prevent for Email operational log
(continued)

| Code | Description |
|----------------|--|
| 1300 | <p>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)</p> <p>Where:</p> <ul style="list-style-type: none"> ■ Recipient_count is the total number of addressees in the To, CC, and BCC fields. ■ Response is the Network Prevent for 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 for Email originated responses and codes” on page 116. ■ The rtime is the time in seconds for Network Prevent for Email to fully receive the message from the sending MTA. ■ The dtime is the time in seconds for Network Prevent for Email to perform detection on the message. ■ The mtime is the total time in seconds for Network Prevent for Email to process the message Message Errors. |
| Message Errors | |
| 5300 | <p>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)</p> <p>Where header_ID is an RFC 822 Message-Id header if one exists.</p> |
| 5301 | Sender rejected during re-submit |
| 5302 | Recipient rejected during re-submit |

See [“About log files”](#) on page 106.

Network Prevent for Email originated responses and codes

Network Prevent for Email originates the following responses. Other protocol responses are expected as Network Prevent for Email relays command stream

responses from the forwarding MTA to the sending MTA. [Table A-5](#) 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-5 Network Prevent for Email originated responses

| Code | Enhanced Status | Text | Description |
|------|-----------------|--|--|
| 250 | 2.0.0 | Ok: Carry on. | Success code that Network Prevent for Email uses. |
| 221 | 2.0.0 | Service closing. | The normal connection termination code that Network Prevent for 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. |
| 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. |

Table A-5 Network Prevent for Email originated responses (*continued*)

| Code | Enhanced Status | Text | Description |
|------|-----------------|---|--|
| 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 for 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 106.