Symantec™ Event Collector 4.4 for Symantec DLP Quick Reference

Symantec™ Event Collector 4.4 for Symantec DLP Quick Reference

Documentation version: 1.0

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Additional enterprise services

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

Enterprise services that are available include the following:

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

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

www.symantec.com/business/services/

Select your country or language from the site index.

Contents

Chapter 1

Introducing Symantec Event Collector for Symantec DLP

This chapter includes the following topics:

About this quick reference

This quick reference includes information that is specific to Symantec™ Event Collector for Symantec DLP. General knowledge about installing and configuring collectors is assumed, as well as basic knowledge of Symantec DLP.

For detailed information on how to install and configure event collectors, please see the *Symantec Event Collectors Integration Guide*.

For information on Symantec DLP, see your product documentation.

Compatibility requirements for the Symantec DLP Event Collector

The collector is compatible with Symantec Data Loss Prevention 9.0.

The collector runs on the following operating systems:

- Microsoft Windows 2000 (all editions) with Service Pack 4 or later
- Microsoft Windows Server 2003 (all editions) with Service Pack 2 or later
- Microsoft Windows Server 2008 with Service Pack 1 or later
- Microsoft Windows XP with Service Pack 2 or later
- Microsoft Windows Vista with Service Pack 1 or later
- Microsoft Windows 7

Note: Home Editions of Microsoft client operating systems are not supported.

- Red Hat Enterprise Linux AS 3.0
- Red Hat Enterprise Linux AS 4.0
- Red Hat Enterprise Linux 5.0 (32-bit x86 only)
- Sun Solaris (SPARC) 8, 9, and 10

Note: The 4.4 collectors can be installed on both 32-bit and 64-bit versions of Windows Server 2000/2003/2008/Vista/Windows 7.

If you install the collector on a computer that runs Windows 7, Windows Vista, or Windows Server 2008, you must adhere to the following conditions: You must use Symantec Event Agent 4.7, and you must run the collector installer from an Administrator command prompt.

System requirements for the Symantec DLP Event Collector computer

Minimum system requirements for a remote collector installation are as follows:

- Intel Pentium-compatible 133-MHz processor (up to and including Xeon-class)
- 512 MB minimum, 1 GB of memory recommended for the Symantec Event Agent
- 35 MB of hard disk space for collector program files
- 95 MB of hard disk space to accommodate the Symantec Event Agent, the JRE, and the collector
- TCP/IP connection to a network from a static IP address

About the installation sequence for the Symantec DLP Event Collector

For all procedures that are not covered in the quick reference, see the *Symantec Event Collectors Integration Guide*.

Configuring Symantec DLP to send syslog events to the collector

In order for the collector to receive events, you must complete the following tasks in the order shown:

- Create a response rule to send syslog events to the collector computer.
  See "To create a response rule to send syslog events to the collector computer" on page 11.
- Configure policies to use the response rule that sends syslog events to the collector computer.
  See "To configure policies to use the response rule that sends syslog events to the collector computer" on page 12.

To create a response rule to send syslog events to the collector computer

1. Launch the **Vontu Data Loss Prevention from Symantec** console and log on with an administrator account.
2. In the left pane, under **Policy**, click **Response Rules**.

3 In the **Response Rules** pane, click **Add Response Rule**.

In the **New Response Rule** pane, then click **Automated Reponse**, and then click **Next**.

4 In the **Add Response Rule** pane, do the following tasks:

- Enter a rule name and description.
- Under **Actions**, from the list, select **All: Log to a Syslog Server**, and then click **Add Action**.

5 Under **Actions > All: Log to a Syslog Server**, enter the following information:

Host	Type the host name or the IP address of the collector computer.
Port	Type the port number of the collector computer.
Message	Navigate to the utils directory of the collector installation, and then copy and paste the contents of the `SyslogFormat.txt` file into the **message** field. Do not add any spaces or carriage returns. The contents of the SyslogFormat.txt file is as follows: `BLOCKED|$BLOCKED$|INCIDENT_ID|$INCIDENT_ID$| RECIPIENTS|$RECIPIENTS$|SENDER|$SENDER$|RULES| $RULES$|SEVERITY|$SEVERITY$|INCIDENT_SNAPSHOT| $INCIDENT_SNAPSHOT$|MATCH_COUNT|$MATCH_COUNT$| POLICY|$POLICY$|SUBJECT|$SUBJECT$|FILE_NAME| $FILE_NAME$|PARENT_PATH|$PARENT_PATH$|PATH| $PATH$|QUARANTINE_PARENT_PATH| $QUARANTINE_PARENT_PATH$|SCAN|$SCAN $\|TARGET\|$TARGET$`
Level	From the list, select the appropriate alert level. This value is used to populate the collector's vendor signature field.

6 To save the new rule, click **Save**.

To configure policies to use the response rule that sends syslog events to the collector computer

1 Launch the **Vontu Data Loss Prevention from Symantec** console and log on with an administrator account.

2 In the left pane, under **Policy**, click **Policies**.

3 In the **Policies** pane, select a policy for which you want to send syslog events.

4 In the **Edit Policy** pane, click the **Response** tab.

5 In the **Response Rule** list, select the response rule that you created in To create a response rule to send syslog events to the collector computer, and then click **Add Response Rule**.

6 Click **Save**.

Sensor properties for the Symantec DLP Event Collector

You must create a new sensor configuration and a new sensor for all collectors.

For detailed procedures, see the *Symantec Event Collectors Integration Guide*.

Table 1-1 Syslog sensor properties

Sensor property	Description
Protocol	Specify UDP as the syslog protocol that Symantec DLP uses to send events. TCP is not supported.
Host Names	Specify the IP addresses or names of the host computers that the collector monitors. Specify * (or any) to allow any host to send events to the collector, or specify multiple host names. Separate multiple host names with commas or semicolons.
Port Number	The default port number is 10559.

About syslog event forwarding

If you forward events to a standard syslog server, you can use a syslog forwarder on that server rather than change the settings on your security device. A syslog forwarder can receive and forward events to both Information Manager and your existing syslog server.

About renaming policy names

In order for DeepSight to correctly map EMR values, you must rename all standard policies that are included with Symantec DLP. You must rename these policies so that DeepSight does recognize these policies as custom rules.

You must rename all policy names before you export the policies and groups from Symantec DLP.

See “Exporting policies and groups from Symantec DLP” on page 14.

All Symantec DLP Event Collector policy names must adhere to the following format:

Standard_Policy_Name: *Your_Policy_Name*

You must follow this convention for all policies that are created. This includes policies that are created from scratch, as well as policies that are created based on a standard policy that is included with Symantec DLP.

Exporting policies and groups from Symantec DLP

Information Manager uses rules to filter known false positives and declare security incidents. Symantec DLP Event Collector includes a set of rules that collect Symantec DLP incidents and correlates them against CIA values and vulnerability data. The incidents are then prioritized. These sample rules also allow incident declaration by policy violation type, as well as incident assignments for various groups and teams.

The Symantec DLP Event Collector includes an SQL script that allows customers to export their policies and corresponding groups. This information is required to trigger rules. These rules are also included in the collector installation package.

The script exports and copies the following files to a specified directory:

- Vontu.tab
- Vontu.cfg

Once the export of the Symantec DLP policies and groups is complete, you use the Vontu.tab and Vontu.cfg files to import data into Information Manager Lookup Tables.

See "Importing Symantec DLP policies and groups into Information Manager" on page 15.

Note: You must have sufficient privileges to copy a file from the collector computer to the computer that hosts the Oracle database for Symantec DLP. You must also have sysdba privileges to be able to export the policies and groups from the Symantec DLP database.

To export policies and groups from Symantec DLP

1. On the collector computer, navigate to the utils directory of collector installation directory.
2. Copy the following files to the computer that hosts the Oracle database for Symantec DLP:

   `export.sql`

   `export.bat`
3. On the Oracle computer, create a directory to which to save the Symantec DLP policies and groups.
4. Do one of the following steps:
   - For UNIX, at command prompt, type the following commands:

     `chmod +x export.sql`

     `export.sql`
   - For Windows prompt, double-click **export.bat**.

   The scripts prompt you to enter the following information:
   - sysdba password
   - Security identifier (SID) of the Vontu database. The default SID for the Symantec DLP database is PROTECT.
   - Export path that you created in step 3

   The following files are copied: `Vontu.tab` and `Vontu.cfg`.

Importing Symantec DLP policies and groups into Information Manager

The Symantec DLP Event Collector includes an SQL script that allows customers to export their policies and corresponding groups.

See "Exporting policies and groups from Symantec DLP" on page 14.

After you complete the export of the Symantec DLP policies and groups, you import them into Information Manager Lookup Tables.

Note: You must have sysdba privileges to copy a file from the computer that hosts the Oracle database for Symantec DLP to the collector computer. You must also have sysdba privileges to import the policies and groups into Information Manager.

To import Symantec DLP policies and groups into Information Manager

1. Copy the `Vontu.tab` and Vontu.cfg files that you created when you exported policies and groups from the Vontu database to a computer that has the SSIM Client installed.

   See "Exporting policies and groups from Symantec DLP" on page 14.

2. Launch the SSIM Client.
3. In the left pane, click **Rules**.
4. In the right pane, expand **Lookup Tables**, and then click **User Lookup Tables**.
5. In the console toolbar, click **Import from disk** and navigate to the Vontu.tab file that you copied in step 1.
6. Click **Import**.

   A lookup table that is named **Vontu** appears under **User Lookup Tables**.

Installing Symantec DLP rules on Information Manager

Information that is available in policies and their corresponding groups is required to trigger rules.

In order to import Symantec DLP rules into Information Manager, you must complete the following tasks:

- Export policies and groups from Symantec DLP.
  See "Exporting policies and groups from Symantec DLP" on page 14.
- Import policies and groups into Information Manager.
  See "Importing Symantec DLP policies and groups into Information Manager" on page 15.
- Import custom rules into Information Manager
  See "To install Symantec DLP rules on Information Manager" on page 17.

You can launch the SSIM Client to view the new rules. The rules are listed under Rules > Correlation Rules > System Rules.

Note: If you have multiple Information Manager servers, you must install the collector rules package on the primary directory server for Information Manager. You must then replicate the rules from the primary directory server to all of the secondary Information Manager servers.

See "To replicate the rules to other servers" on page 17.

Table 1-2 Custom rules for Symantec DLP Event Collector

Rule name	Description
Confidential Data Policy Violation	Monitors DLP Incidents for confidential policy violations.
Customer Data Leakage Detected	Monitors DLP Incidents for customer data leaks.
Employee Data Leakage Detected	Monitors DLP Incidents for employee data leaks.
Privacy Policy Violation Detected	Monitors DLP Incidents for privacy policy violations.
Regulatory Policy Violations	Monitors DLP Incidents for regulatory policy violations.

To install Symantec DLP rules on Information Manager

1. On the collector computer, launch the Information Manager Configuration Web site at the following URL:

   `https://` ***`Information_Manager_IP_address`***

2. From the toolbar, click **Maintenance > System Updates**.
3. In the left pane, click **Install**.
4. In the right pane, click **Browse** to navigate to the .jar file that is located in the utils subdirectory of the collector installation directory:
5. `..\utils\rulespackage\symcdlprules.jar`
6. Click **Upload and Install**.
7. To verify that you have installed the rules package, click **Status**.

To replicate the rules to other servers

1. Launch the Information Manager Configuration Web site at the following URL:

   `https://` ***`Information_Manager_IP_address`***

2. In the toolbar, click **Settings > Collector Registration**.
3. In the left pane, click **Synchronize**.

4 Complete the following fields:

Source Database	Specify the primary directory server for Information Manager.
Target Database	Specify all secondary Information Manager servers.

5 Click **Start**.

Creating a user action to drill-down to incidents in the Symantec DLP Web console

To provide you with detailed information about an incident, you can create a custom user action that launches Symantec DLP reports.

Note: You must launch the Symantec DLP user action from the Option 8 field that is viewable in Event Details. The value of the Event Details field includes a URL that launches a DLP report.

To create a user action to open Symantec DLP reports

1 Launch the **SSIM Client**.

2 Click **Tools > Preferences**.

3 To add a new user action, in the **Preferences** dialog, on the **User Actions** tab, click **+** (the plus button.)

4 In the **Modify Custom Action** dialog, specify field values as follows:

Name	Specify a name for the **Action**. The name appears when you right-click on a field in an Information Manager event. For example, Open DLP Report.
Command	Specify the parameters that are required to open a Web browser of your choice. ***Web_Browser*** **{0}** An example for Internet Explorer is as follows: `iexplore {0}` An example for Mozilla Firefox is as follows: `firefox {0}` The examples assume that iexplore and firefox are in the PATH of the system.
Public	To share the action with other SSIM Client users, check this box.
Use Output Viewer	To display a window that displays output that is generated when the command is run, check this box. This field is useful for text-based commands but is not useful in this context; leave this box unchecked.

Installing queries on Information Manager

The collector package includes several queries. You can import these queries into the Information Manager appliance to provide detailed reporting on Symantec DLP events. You can use queries as a template from which to create new queries.

You can launch the SSIM Client to view the new queries. The queries are listed in Events > System Queries > Product Queries > *Collector_Name*.

The collector includes the following predefined queries:

- Top 10 Action Taken within 48 hours
- Top 15 Events by IP Destination Address within 48 hours
- Top 15 Events by IP Source Address within 48 hours

- Top 15 Policies Triggered within 48 hours
- Top 15 Rules Triggered within 48 hours

Note: If you have multiple Information Manager servers, you must install the collector query package on the primary directory server for Information Manager. You must then replicate the queries from the primary directory server to all of the secondary Information Manager servers.

See "To replicate the queries to other servers" on page 20.

To install queries on an Information Manager appliance

1. On the collector computer, launch the Information Manager Configuration Web site at the following URL:

   https:// *Information_Manager_IP_address*

2. In the toolbar, click **Maintenance > System Updates**.
3. In the left pane, click **Install**.
4. In the right pane, click **Browse** to navigate to the .tar file that is located in the utils subdirectory of the collector installation directory:

   `..\utils\queriespackage\symcdlpqueries.tar`

5. Click **Upload and Install**.
6. To verify that you have installed the queries package, click **Status**.

To replicate the queries to other servers

1. Launch the Information Manager Configuration Web site at the following URL:

   https:// *Information_Manager_IP_address*

2. In the toolbar, click **Settings > Collector Registration**.
3. In the left pane, click **Synchronize**.
4. Complete the following fields:

Source Database	Specify the primary directory server for Information Manager.
Target Database	Specify all secondary Information Manager servers.

5. Click **Start**.

About Syslog Director

If you use the collector on the Information Manager appliance, you can use this collector with Syslog Director. Syslog Director accepts syslog events from any device or application that sends events to the standard port for syslog messages, UDP port 514. (You can also configure Syslog Director to listen on other UDP or TCP ports.) Syslog Director identifies the incoming events by their signatures (specific patterns that identify each collector) and redirects the events that are received to the appropriate collector. All events that are not identified by a signature are sent to the Generic Syslog Collector.

Syslog Director can only receive events from UDP only, or TCP only. Syslog Director cannot receive events simultaneously from two different protocols.

Note: In all deployments, you must list the Generic Syslog Collector last, and you must leave its Collector Signature empty.

The default Syslog Director settings for this collector are as follows:

Collector name	Symantec DLP Event Collector
Collector signature	Vontu Incident:
Default port	10559

For detailed procedures about Syslog Director, see the *Symantec Event Collectors Integration Guide*.

Configuring Syslog Director with syslog collectors

You can configure Syslog Director to receive and redirect syslog messages to a collector. When the Syslog Director sensor is configured, or when a change is made to a sensor setting, you must distribute the settings to the collectors.

Additional syslog collectors automatically appear in Syslog Director.

See "About Syslog Director" on page 21.

A collector signature is a specific pattern that identifies a collector.

You complete the following procedures to enable and define signatures for each collector that you want to redirect:

- Create a Syslog Director sensor configuration.
  See "To create a Syslog Director sensor configuration" on page 22.

- Enable syslog collectors to receive syslog events from Syslog Director.
  See "To enable syslog collectors to receive syslog events from Syslog Director" on page 23.
- Add collector signatures to Syslog Director, optional.
  See "To add collector signatures to Syslog Director" on page 23.
- Import collector signatures to Syslog Director, optional.
  The collector includes an xml file that you can use to update collector signatures. The xml file is located in the utils subdirectory of the collector installation directory.
  See "To import collector signatures to Syslog Director" on page 24.

To create a Syslog Director sensor configuration

1. In the Information Manager console, in the left pane, click **System**.
2. On the **Product Configurations** tab, expand **Syslog Director** until you see the Default configuration.

   You cannot use the Default configuration.
3. To create a configuration, right-click **Syslog Director**, and then click **New**.
4. Follow the prompts in the **Create a New Configuration Wizard**.

   This new configuration should only be applied to a Symantec Event Agent running on an Information Manager appliance.
5. Select the new configuration.
6. On the **Director Settings** tab, on the **Syslog Sensor** tab, do the following steps in the order presented:
   - Click **Sensor 0**.
   - In the sensor property table under the Value column, change any of the following fields.

Protocol	UDP or TCP
Host Names	Specify * or any to allow any host to send events to the Syslog Director. If you want to restrict the hosts from which Syslog Director receives events, you can specify multiple host names or IP addresses. Separate multiple host names or IP address by a comma or semicolon.

   - In the **Port Number** field, leave 10514.
     514 is the standard port for syslog messages. Symantec Security Information Manager is configured to forward all messages that are

received on port 514 to port 10514, where Syslog Director can handle them.

- Click **Save**.

To enable syslog collectors to receive syslog events from Syslog Director

1. On the **Director Settings** tab, on the Director Settings sub-tab, click **Refresh**.

   The Refresh list automatically displays all of the syslog collectors that are installed on the appliance.

2. Check the corresponding Redirect check box for each collector that you want to set up to receive syslog events from Syslog Director.

3. In the left pane, right-click the appropriate configuration, and then click **Distribute**.

4. At the prompt to distribute the configuration, click **Yes**.

5. In the **Configuration Viewer** window, click **Close**.

To add collector signatures to Syslog Director

1. To add collector signatures, click **Add**.

   You should only change collector signatures if directed by Symantec.

   A collector signature is a specific pattern that identifies a collector. In individual collectors using the syslog sensor, the documentation has a section on the Syslog Director. The collector signature that is specified in this section is the match signature used. To add collector signatures, click **Add**. Collectors with syslog sensors are displayed in a drop-down box. Select the collector and add the collector match signature that is specified in the documentation.

2. To reorder the collector signatures, click **Move Up** or **Move Down**.

   Collector signatures are handled in order, top to bottom.

   When an event has matched a signature, Syslog Director redirects it to the appropriate collector and does not try to match any other signatures.

   You should place the unique signatures at the top of the list for performance reasons and to eliminate possible false matches with more general signatures.

   You must leave the Generic Syslog Event Collector as the last collector with its collector signature empty.

3. In the left pane, right-click the appropriate configuration, and then click **Distribute**.

4. At the prompt to distribute the configuration, click **Yes**.

5. In the **Configuration Viewer** window, click **Close**.

To import collector signatures to Syslog Director

1. Launch the SSIM Client.
2. In the left pane, click **System**.
3. On the **Product Configurations** tab, click **Syslog Director 4.3 > Syslog Director**.
4. Double-click an existing configuration (not Default.)
5. On the **Director Settings** tab, on the Director Settings sub-tab, click **Advanced Options**.
6. Click **Import**.
7. In the **Select Import Type** dialog box, click **Import Only New Signatures**.
8. Browse to the **utils** directory of the collector installation package, select `symcdlp_match.xml`, click **Open**, and then click **OK**.
9. Use **Move Up** or **Move Down** to position the new signature.

   Make sure that the Generic Syslog Collector is the last collector in the list.
10. Click **Save**.
11. In the middle pane, right-click the configuration, and then click **Distribute**.
12. At the prompt to distribute the configuration, click **Yes**.
13. In the **Configuration Viewer** window, click **Close**.

Running LiveUpdate for collectors

You can run LiveUpdate to receive collector updates such as support for new events and query updates.

If you install a collector on Information Manager, or if you use a collector that is preinstalled on Information Manager, you use the Administrator Web page to run LiveUpdate. You also use the Administrator Web page to verify that LiveUpdate ran successfully.

See "To run LiveUpdate from the Administrator Web page" on page 25.

If you installed the collector on a separate computer, you must complete the following tasks in the order presented:

- Run LiveUpdate for a collector installed on a separate computer.
  See "To run LiveUpdate for a collector installed on a separate computer" on page 25.

- Verify that LiveUpdate ran successfully for a collector installed on a separate computer.
  See "To verify that LiveUpdate ran successfully for a collector installed on a separate computer" on page 25.

For information about running LiveUpdate on internal LiveUpdate servers, see the *Symantec LiveUpdate Administrator User's Guide*.

To run LiveUpdate from the Administrator Web page

1. From a Web browser, navigate to the Information Manager Administrator Web page, and then log in with administrator credentials.
2. From the list on the left, click **LiveUpdate**.
3. In the list of products, to select the items to update, in the corresponding check box, check **Update**.

   At the bottom of the page, you can also click **Check All**.
4. At the bottom of the page, click **Update**.

   If LiveUpdate runs successfully, the status column in the Summary page displays Success.
5. To troubleshoot a problem with LiveUpdate, under Session Log, click **View Log File**.

To run LiveUpdate for a collector installed on a separate computer

1. On the collector computer, navigate to the collector directory as follows:
   - On Windows, the default directory is as follows:
     C:\Program Files\Symantec\Event Agent\collectors\symcdlp
   - On UNIX, the default directory is as follows:
     /opt/Symantec/sesa/Agent/collectors/symcdlp
2. At a command prompt, do one of following tasks:
   - On Windows, type the following command:
     `runliveupdate.bat`
   - On UNIX, as the root user, type the following command:
     `runliveupdate.sh`

To verify that LiveUpdate ran successfully for a collector installed on a separate computer

1. On the collector computer, navigate to the collector directory as follows:
   - On Windows, the default directory is as follows:
     C:\Program Files\Symantec\Event Agent\collectors\symcdlp

- On UNIX, the default directory is as follows:
  /opt/Symantec/sesa/Agent/collectors/symcdlp

2. Verify that a file named LiveUpdate-Collector.txt exists.

   This text file shows the date of the last LiveUpdate and contains information about any defects that were addressed and any enhancements that were added.

3. Navigate to the LiveUpdate directory as follows:

   - On Windows, the default LiveUpdate directory is as follows:
     C:\Documents and Settings\All Users\Application Data\Symantec\Java LiveUpdate
   - On UNIX, the default LiveUpdate directory is as follows:
     /opt/Symantec/LiveUpdate

4. To view the liveupdt.log file, do one of the following tasks:

   - On Windows, use a text editor such as Notepad to view the liveupdt.log file.
   - On UNIX, to view the last 100 lines of the liveupdt.log file, type the following command:

     ```
     tail -100 liveupdt.log | more
     ```

   The first part of the log is in text format; the second part of the log repeats the information in XML format.

   If LiveUpdate was unsuccessful, a status message that notes the failure appears at the end of the log file.

   For example, Status = Failed (return code - 2001).

Chapter 2

Implementation notes

This chapter includes the following topics:

Product ID for Symantec DLP Event Collector

The product ID of the collector is 3423.

Event example

The structure of the event is as follows:

```
BLOCKED|$BLOCKED$|INCIDENT_ID|$INCIDENT_ID$|
RECIPIENTS|$RECIPIENTS$|SENDER|$SENDER$|RULES|$RULES$|
SEVERITY|$SEVERITY$|INCIDENT_SNAPSHOT|$INCIDENT_SNAPSHOT$|
MATCH_COUNT|$MATCH_COUNT$|POLICY|$POLICY$|SUBJECT|$SUBJECT$|
FILE_NAME|$FILE_NAME$|PARENT_PATH|$PARENT_PATH$|PATH|$PATH$|
QUARANTINE_PARENT_PATH|$QUARANTINE_PARENT_PATH$|SCAN|$SCAN$|
TARGET|$TARGET$
```

where:

BLOCKED	Status of the attempt (is it blocked or not).
INCIDENT_ID	The ID of the incident.

INCIDENT_SNAPSHOT	The fully qualified URL of the incident snapshot page for the incident.
MATCH_COUNT	
POLICY	The name of the policy that was violated.
RECIPIENTS	A comma-separated list of one or more message recipients.
RULES	A comma-separated list of one or more policy rules that were violated.
SENDER	The message sender.
SEVERITY	The severity that is assigned to the incident.
SUBJECT	The subject of the message.
FILE_NAME	The name of the file in which the incident was found.
PARENT_PATH	The path to the parent directory of the file in which the incident was found.
PATH	The full path to the file in which the incident was found.
QUARANTINE_PARENT_PATH	The path to the parent directory in which the file was quarantined.
SCAN	The date of the scan that found the incident.
TARGET	The name of the target in which the incident was found.

An example event is as follows:

```
Aug 18 12:33:26 XX.XXX.XX.XX Vontu Incident:
BLOCKED|Action Blocked|INCIDENT_ID|2410|RECIPIENTS|N/A|
SENDER|N/A|RULES|Keyword|SEVERITY|1: High|INCIDENT_SNAPSHOT
|a href="https://xxxxxxxxxx/ProtectManager/EndpointIncidentDetail.do?
value(variable_1)=incident.id(operator_1)=in(operand_1)=2410
"Incident Snapshot|MATCH_COUNT|3|POLICY|Keyword|SUBJECT
|N/A|FILE_NAME|av.txt|PARENT_PATH|G:|PATH|G:\av.txt|QUARANTINE_PARENT_PATH
|N/A|SCAN|N/A|TARGET|N/A
```

Schema packages

The collector uses the following schema packages:

- symc_base
- symc_data_incident
- symc_data_scan
- symc_firewall_network
- symc_host_intrusion
- symc_network
- symc_intrusion
- symc_vpn_net

Event mapping for Information Manager

Table 2-1 Event mapping

Information Manager field name	Symantec DLP field name	Comment
Category ID		30007606 - Security
Data Status ID	BLOCKED	Status of attempt Possible values are as follows: ■ 117232 - Uncorrected ■ 117234 - Blocked ■ 117238 - Quarantined
Data Type ID		117207 - SMTP mail
data_scan_name	TARGET	Scan name
Destination Host Name	RECIPIENTS	Host name of the destination machine
Event Date		Date of the event

Table 2-1 Event mapping *(continued)*

Information Manager field name	Symantec DLP field name	Comment
Event Type ID		Event type Possible values are as follows: ■ 111001 - "Scan Events" ■ 111002 - "Data Incident" ■ 112056 - "Unscannable Violation" ■ 132000 - "Generic Content" ■ 1732000 - "Generic Firewall" ■ 512000 - "Connection Accepted" ■ 512001 - "Connection Rejected"
EventClassName		Possible values are as follows: ■ symc_data_incident ■ symc_data_scan ■ symc_firewall_network
IP Destination Address	RECIPIENTS	IP address of the destination machine
IP Source Address	SENDER	IP address of the source machine
Logging Device IP		IP address of the logging device
Logging Device Name		Host name of the logging device
Option 1	FILE_NAME	Contains the file name, if accessible
Option 2	INCIDENT_ID	Contains the incident ID
Option 3	POLICY	Contains the policy name
Option 4	RULES	Contains the rule name
Option 5	BLOCKED	Contains the outcome of the action
Option 6	SCAN	Contains the start date of scan if event contains this.
Option 7	QUARANTINE_PARENT_PATH	Contains the path where the item is quarantined

Table 2-1 Event mapping *(continued)*

Information Manager field name	Symantec DLP field name	Comment
Option 8	INCIDENT_SNAPSHOT	Contains the incident snapshot. You can use the contents of this field with a User Action. The User Action can launch Symantec DLP reports that are specific to the incident. See "Creating a user action to drill-down to incidents in the Symantec DLP Web console" on page 18.
Recipients	RECIPIENTS	The list of recipients from the letter that is scanned
Rule	RULES	Rule names
Scan GUID	SCAN	Scan identificator
Sender	SENDER	Sender from the letter that is scanned
Severity ID	SEVERITY	This field is populated based on the SEVERITY field. See Table 2-2 on page 31.
Source Host Name	SENDER	Host name of the source machine
Subject	SUBJECT	Letter subject
Target Resource		Target of the operation
User Name		User name
Vendor Severity	SEVERITY	Vendor severity
Vendor Signature		Event signature as it represented in Symantec DLP

Table 2-2 SEVERITY mapping

TEXT in SEVERITY field	Severity in Information Manager
4:	1
3:	2
2:	3

Table 2-2 SEVERITY mapping *(continued)*

TEXT in SEVERITY field	Severity in Information Manager
1:	4

Chapter 3

Event filtering and aggregation

This chapter includes the following topics:

Event filtering and aggregation for Symantec DLP Event Collector

Because of the role that intrusion-detection point products such as Symantec DLP play in defense-in-depth scenarios, filtering or aggregating these events is not recommended. However, it is possible that systems on a network play a specific role to ensure the security of an organization. This type of role may result in false positives from the device. For example, computers within the network that assess vulnerability risks may use techniques that cause intrusion-detection point products to report that the network is under attack. If you have this type of scenario, you can aggregate the events from that computer.

The collector includes the following default filter that is enabled by default:

Catch All events filtering out	Removes events where "not_translated is equal to true.

Table 3-1 Possible filters and aggregators

Filter criteria: ■ Event Type ID = 512001	Connection rejected events indicate that the firewall is operating as it is configured. These events do not ordinarily pose security threats and you can filter them at the collector.

Table 3-1 Possible filters and aggregators *(continued)*

Aggregation criteria: ■ Event Type ID = 912001 ■ IP Source Address as the similar property	Connection accepted events are generated by legitimate network traffic. You can filter or aggregate these events by IP address. This aggregation consolidates successful ICMP connections from a single source.
Aggregation criteria: ■ Data Status ID = 117238	Consolidates all quarantined events.