Cluster Server Agent for Symantec Data Loss Prevention Installation and Configuration Guide

Linux

7.0

VERITAS™

Veritas InfoScale™ Availability Agents

Last updated: 2019-07-05

Legal Notice

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

http://www.veritas.com

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

https://sort.veritas.com/documents

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

xyz@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Chapter 1

Introducing the agent for Symantec Data Loss Prevention

This chapter includes the following topics:

About the Cluster Server agent for Symantec Data Loss Prevention

Cluster Server (VCS) agents monitor specific resources within an enterprise application. They determine the status of resources and start or stop them according to external events.

The Cluster Server agent for Data Loss Prevention (DLP) provides high availability to the DLP Enforce Server component in a cluster. The agent brings Symantec Data Loss Prevention services online, monitors the services, and takes them offline.

About Symantec Data Loss Prevention

Symantec Data Loss Prevention enables you to:

- Discover and locate confidential information on file and Web servers, in databases, and on endpoints (desk and laptop systems).
- Protect confidential information through quarantine.
- Monitor network traffic for transmission of confidential data.
- Monitor the use of sensitive data on endpoint computers.
- Prevent transmission of confidential data to outside locations.
- Automatically enforce data security and encryption policies.

Typical Symantec Data Loss Prevention configuration in a VCS cluster

A typical Symantec Data Loss Prevention configuration in a VCS cluster has the following characteristics:

- VCS is installed and configured in a two-node cluster.
  For more information on installing and configuring Cluster Server, refer to the Cluster Server installation and configuration guides.
- The Symantec DLP Enforce Server is installed. For more information, see the *Symantec Data Loss Prevention Installation Guide* and the *Symantec Data Loss Prevention Administration Guide*.
- Veritas recommends making the following directories available on the shared storage:

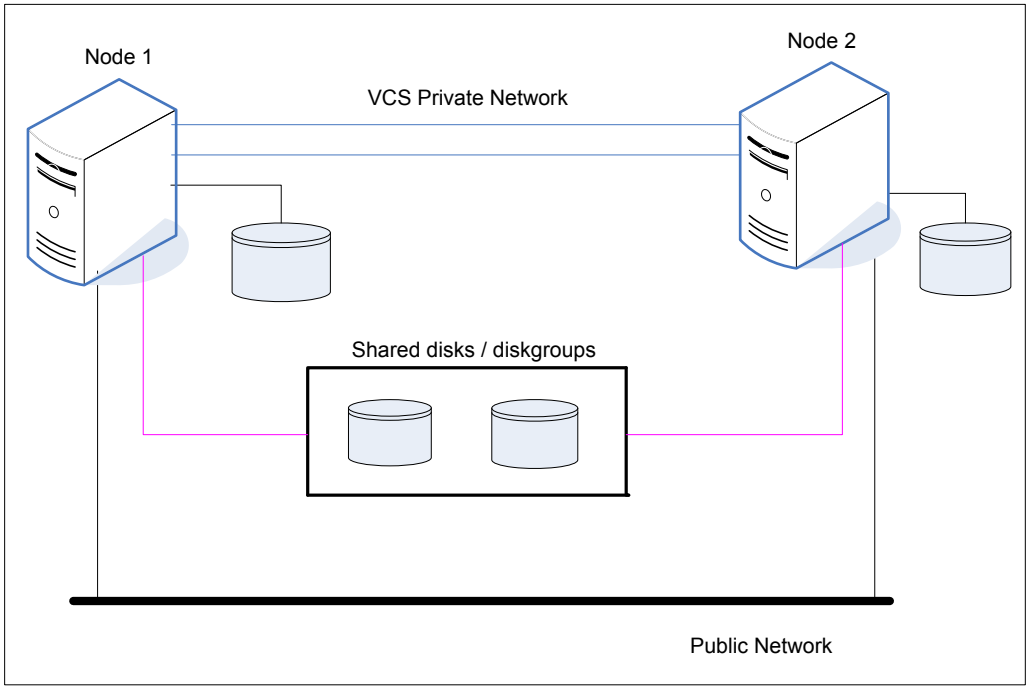
  For Symantec Data Loss Prevention 11.6 or later:

  - `/opt/SymantecDLP`
  - `/var/SymantecDLP`
  - `/var/log/SymantecDLP`

  For Symantec Data Loss Prevention 11.5 or earlier:

  - `/opt/Vontu`
  - `/var/Vontu`
  - `/var/log/Vontu`
- The Cluster Server agent for Symantec Data Loss Prevention is installed on the both nodes.

Figure 1-1 A typical Symantec Data Loss Prevention configuration in a VCS cluster



Supported software

For information on the software versions that the Cluster Server agent for Symantec Data Loss Prevention supports, see the Veritas Services and Operations Readiness Tools (SORT) site: https://sort.veritas.com/agents.

Features of the agent

The following are the features of the Cluster Server agent for Symantec Data Loss Prevention:

- Support for validation of attributes that are based on the agent functions
  The agent can validate attributes in each agent function before the actual data processing starts.
- Support for First Failure Data Capture (FFDC)
  In case of a fault, the agent generates a huge volume of the debug logs that enable troubleshooting of the fault.

- Support for Fast First Level Monitor (FFLM)
  The agent maintains PID files based on search patterns to expedite the monitoring process.
- Support for external user-supplied monitor utilities
  The agent enables user-specified monitor utilities to be plugged in, in addition to the built-in monitoring logic. This enables administrators to completely customize the monitoring of the application.
- Support for intelligent resource monitoring and poll-based monitoring
  The agent supports the Cluster Server Intelligent Monitoring Framework (IMF) feature. IMF allows the agent to register the resources to be monitored with the IMF notification module so as to receive immediate notification of resource state changes without having to periodically poll the resources. See "About Intelligent Monitoring Framework" on page 23.
- Delayed agent function
  The agent manages the first monitor after online for slow initializing applications.

How the agent supports intelligent resource monitoring

With Intelligent Monitoring Framework (IMF), VCS supports intelligent resource monitoring in addition to the poll-based monitoring. Poll-based monitoring polls the resources periodically whereas intelligent monitoring performs asynchronous monitoring.

When an IMF-enabled agent starts up, the agent initializes the Asynchronous Monitoring Framework (AMF) kernel driver. After the resource is in a steady state, the agent registers with the AMF kernel driver, the details of the resource that are required to monitor the resource. For example, the agent for Symantec Data Loss Prevention registers the PIDs of the Symantec Data Loss Prevention processes with the AMF kernel driver. The agent's imf_getnotification function waits for any resource state changes. When the AMF kernel driver module notifies the imf_getnotification function about a resource state change, the agent framework runs the monitor agent function to ascertain the state of that resource. The agent notifies the state change to VCS, which then takes appropriate action.

For more information, see the *Cluster Server Administrator's Guide*.

Symantec Data Loss Prevention agent functions

The operations or functions that the Cluster Server agent for Symantec Data Loss Prevention can perform are described as follows:

Online

The online function performs the following tasks:

- Verifies that the required attributes are set correctly.
- Changes the directory to DLPInstallDir.
- Attempts to start the Symantec DLP service with the command:

  DLPInstallDir/*DLPServiceName*.sh start

  The command always gets executed in the context of a root user.

  Note: For DLP 15.5 and later, the script name does not include the string "Service". For example, the script name for SymantecDLPManagerService is SymantecDLPManager.sh.

- Checks if the service has started.
- Gives the control back to HAD.

Offline

The offline function performs the following tasks:

- Verifies that the required attributes are set correctly.
- Verifies that the Symantec DLP service is not offline. If the Symantec DLP service is already offline, the operation exits.
- Attempts to stop the Symantec DLP service with the command:

  DLPInstallDir/*DLPServiceName*.sh stop

  The command always gets executed in the context of a root user.

  Note: For DLP 15.5 and later, the script name does not include the string "Service". For example, the script name for SymantecDLPManagerService is SymantecDLPManager.sh.

- Checks if the service has stopped.
- Gives the control back to HAD.

Monitor

The monitor function monitors the states of the Symantec DLP service on all nodes within the cluster. The operation performs the following tasks:

- The monitor function conducts a check to determine that the Symantec DLP service process is running on the system in the cluster. If this check does not find this process running on the node, the check exits and reports the instance as OFFLINE.
- The agent verifies that the process for Symantec DLP service is run in the context of the user that is specified as part of the User attribute. The default user name is 'protect'.
- The agent for Symantec Data Loss Prevention also supports Intelligent Monitoring Framework (IMF) in the first-level check. IMF enables intelligent resource monitoring. The agent for Symantec Data Loss Prevention is IMF-aware and uses the asynchronous monitoring framework (AMF) kernel driver for resource state change notifications. See "How the agent supports intelligent resource monitoring" on page 9.
  You can use the MonitorFreq key of the IMF attribute to specify the frequency at which the agent invokes the monitor function. See "MonitorFreq" on page 25.
- Depending upon the value of the MonitorProgram attribute, the monitor operation can perform a customized check using a user-supplied monitoring utility. Refer to the agent attributes for more details regarding this attribute: See "Symantec Data Loss Prevention agent attributes" on page 19.

Clean

In case of a failure or after an unsuccessful attempt to bring the DLP service online or take the DLP service offline , the clean operation performs the following tasks:

- Attempts to gracefully stop the DLP service with the command:

  DLPInstallDir`/`*DLPServiceName*`.sh stop`

  The command always gets executed in the context of a root user.

  Note: For DLP 15.5 and later, the script name does not include the string "Service". For example, the script name for `SymantecDLPManagerService` is `SymantecDLPManager.sh`.

- The clean operation kills the DLP service process if the DLP service process does not stop after a graceful shutdown attempt

- Gives the control back to HAD.

Note: For information about the additional functions of the agent for Symantec Data Loss Prevention when IMF is enabled:

See "Agent functions for the IMF functionality" on page 24.

Chapter 2

Installing, upgrading, and removing the agent for Symantec Data Loss Prevention

This chapter includes the following topics:

Before you install the Cluster Server agent for Symantec Data Loss Prevention

You must install the Cluster Server agent for Symantec Data Loss Prevention on all the systems that will host Symantec Data Loss Prevention service groups.

Before you install the agent for Symantec Data Loss Prevention, ensure that the following prerequisites are met.

- Install and configure Cluster Server.

For more information on installing and configuring Cluster Server, refer to the Cluster Server installation and configuration guides.

- Install the latest version of ACC Library.
  To install or update the ACC Library package, locate the library and related documentation in the Agent Pack tarball.
  See "About the ACC library" on page 14.

About the ACC library

The operations of a Cluster Server agent depend on a set of Perl modules known as the ACC library. The library must be installed on each system in the cluster that runs the agent. The ACC library contains common, reusable functions that perform tasks, such as process identification, logging, and system calls.

Instructions to install or remove the ACC library on a single system in the cluster are given in the following sections. The instructions assume that the ACCLib tar file has already been extracted.

Note: The LogDbg attribute should be used to enable debug logs for the ACCLib-based agents when the ACCLib version is 6.2.0.0 or later and VCS version is 6.2 or later.

Installing the ACC library

Install the ACC library on each system in the cluster that runs an agent that depends on the ACC library.

To install the ACC library

1. Log in as a superuser.
2. Download ACC Library.

   You can download either the complete Agent Pack tar file or the individual ACCLib tar file from the Veritas Services and Operations Readiness Tools (SORT) site (https://sort.veritas.com/agents).
3. If you downloaded the complete Agent Pack tar file, navigate to the directory containing the package for the platform running in your environment.

Linux	*cd1*/linux/generic/vcs/application/acc_library/*version*_library/rpms

4 If you downloaded the individual ACCLib tar file, navigate to the pkgs directory (for AIX and Solaris), or rpms directory (for Linux).

5 Install the package. Enter **Yes**, if asked to confirm overwriting of files in the existing package.

Linux
```
# rpm -i \
VRTSacclib-VersionNumber-GA_GENERIC.noarch.rpm
```

Note: The LogDbg attribute should be used to enable debug logs for the ACCLib-based agents when the ACCLib version is 6.2.0.0 or later and VCS version is 6.2 or later.

Installing the agent in a VCS environment

Install the agent for Symantec Data Loss Prevention on each node in the cluster.

To install the agent in a VCS environment

1 Download the agent from the Veritas Services and Operations Readiness Tools (SORT) site: https://sort.veritas.com/agents.

You can download either the complete Agent Pack tar file or an individual agent tar file.

2 Uncompress the file to a temporary location, say /tmp.

3 If you downloaded the complete Agent Pack tar file, navigate to the directory containing the package for the platform running in your environment.

Linux
```
cd1/linux/generic/vcs/application/dlp_agent/
vcs_version/version_agent/rpms
```

If you downloaded the individual agent tar file, navigate to the pkgs directory (for AIX and Solaris), or rpms directory (for Linux).

4 Log in as a superuser.

5 Install the package.

Linux
```
# rpm -ihv \
VRTSvcsdlp-AgentVersion-GA_GENERIC.noarch.rpm
```

After installing the agent package, you must import the agent type configuration file.

See “Importing the agent types files in a VCS environment” on page 19.

Uninstalling the agent in a VCS environment

You must uninstall the agent for Symantec Data Loss Prevention from a cluster while the cluster is active.

To uninstall the agent in a VCS environment

1. Log in as a superuser.
2. Set the cluster configuration mode to read/write by running the following command from any node in the cluster:

   ```
   # haconf -makerw
   ```

3. Remove all Symantec Data Loss Prevention resources from the cluster. Run the following command to verify that all resources have been removed:

   ```
   # hares -list Type=DLP
   ```

4. Remove the agent type from the cluster configuration by running the following command from any node in the cluster:

   ```
   # hatype -delete DLP
   ```

   Removing the agent’s type file from the cluster removes the include statement for the agent from the `main.cf` file, but the agent's type file is not removed from the cluster configuration directory. You can remove the agent’s type file later from the cluster configuration directory.
5. Save these changes. Then set the cluster configuration mode to read-only by running the following command from any node in the cluster:

   ```
   # haconf -dump -makero
   ```

6. Use the platform's native software management program to remove the agent for Symantec Data Loss Prevention from each node in the cluster.

   Run the following command to uninstall the agent:

   Linux `# rpm -e VRTSvcsdlp`

Removing the ACC library

Perform the following steps to remove the ACC library.

To remove the ACC library

1. Ensure that all agents that use ACC library are removed.
2. Run the following command to remove the ACC library package:

   Linux `# rpm -e VRTSacclib`

Chapter 3

Configuring the agent for Symantec Data Loss Prevention

This chapter includes the following topics:

About configuring the Cluster Server agent for Symantec Data Loss Prevention

After installing the Cluster Server agent for Symantec Data Loss Prevention, you must import the agent type configuration file. After importing this file, review the attributes table that describes the resource type and its attributes, and then create and configure Symantec Data Loss Prevention resources.

To view the sample agent type definition and service groups configuration:

See "About sample configurations for the agents for Symantec Data Loss Prevention" on page 37.

Importing the agent types files in a VCS environment

To use the agent for Symantec Data Loss Prevention, you must import the agent types file into the cluster. You can import the agent types file using the VCS graphical user interface or using the command line interface.

To import the agent types file using the VCS Java GUI

1. Start the Cluster Manager (Java Console) and connect to the cluster on which the agent is installed.
2. Click **File > Import Types**.
3. In the **Import Types** dialog box, select the following file:

VCS 5.1 or later	Linux	`/etc/VRTSagents/ha/conf/DLP/DLPTypes.cf`

4. Click **Import**.
5. Save the VCS configuration.

You can now create Symantec Data Loss Prevention resources. For additional information about using the VCS GUI, refer to the *Cluster Server Administrator's Guide*.

To import the agent types file using the CLI

1. If VCS is running, run the `/etc/VRTSagents/ha/conf/DLP/DLPTypes.cmd` file from the command line.
2. If VCS is not running, perform the following steps sequentially:
   - Copy the agent types file from `/etc/VRTSagents/ha/conf/DLP/DLPTypes.cf` to the `/etc/VRTSvcs/conf/config` directory.
   - Include the agent types file in the `main.cf` file.
   - Start HAD.

Symantec Data Loss Prevention agent attributes

Refer to the required and optional attributes while configuring the agent for Symantec Data Loss Prevention.

Table 3-1 lists the required attributes for the Symantec Data Loss Prevention agent.

Table 3-1 Required attributes

Attribute	Description
ResLogLevel	Specifies the logging detail that the agent performs for the resource. The valid values are as follows: ■ ERROR: Only logs error messages. ■ WARN: Logs error messages and warning messages. ■ INFO: Logs error messages, warning messages, and informational messages ■ TRACE: Logs error messages, warning messages, informational messages, and trace messages. TRACE is very verbose and should be used only during initial configuration or for troubleshooting and diagnostic operations. Default Value: INFO Example: INFO
User	The UNIX user name that the agent uses for identifying the DLP services. The user name must be synchronized across the systems in the cluster. In other words, the user name must resolve to the same UID and have the same default shell on each system in the cluster. The agent functions use the getpwnam (3c) function call to obtain the UNIX user attributes. As a result, the user can be defined locally or can be defined in a common repository (that is, NIS, NIS+, or LDAP). In the latter case, the agent fails if the access to this repository fails. The supported shell environments are: ksh, sh, and csh. Default Value: protect Example: protect
DLPInstallDir	Full path of directory in which the DLP wrapper script and binary files are located. Default Value: /opt/Vontu/Protect/bin Example 1: /opt/app/Vontu/Protect/bin Example 2: /opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/services

Table 3-1 Required attributes *(continued)*

Attribute	Description
DLPServiceName	Name of the DLP service to be made highly available. Default Value: No default value The valid service name values for DLP versions older than 15.1 are: `VontuIncidentPersister`, `VontuManager`, `VontuMonitor`, `VontuMonitorController`, `VontuNotifier`, and `VontuUpdate`. The valid service name values for DLP 15.1 and later are: `SymantecDLPDetectionServerController`, `SymantecDLPIncidentPersister`, `SymantecDLPManager`, `SymantecDLPNotifier`, and `SymantecDLPUpdate`. The valid service name values for DLP 15.5 and later are: `SymantecDLPDetectionServerControllerService`, `SymantecDLPDetectionServerService`, `SymantecDLPIncidentPersisterService`, `SymantecDLPManagerService`, and `SymantecDLPNotifierService`. **Note:** In case of DLP 15.5, if the string "Service" is present at the end of the service name, confirm that the DLP process pattern has the service name included.
DelayAfterOnline	Number of seconds after the Online function, and before the next monitor cycle is invoked. Default Value: 0 Example: 5

Table 3-2 lists the optional attributes for the Symantec Data Loss Prevention agent.

Table 3-2 Optional attributes

Attribute	Description
EnvFile	Full path to the env file that the agent sources to set the environment before executing any DLP server commands. Veritas recommends storing the file on shared disk. The following shell environments are supported: ksh, sh, and csh. Default Value: No default value Example: /opt/Vontu/Protect/envfile

Table 3-2 Optional attributes *(continued)*

Attribute	Description
MonitorProgram	Full path and file name of an external, user-supplied monitor executable. If specified, the monitor function executes this file to perform an additional server state check. There are no restrictions for what actions the external monitor program performs to determine the state of a DLP service. The only constraint is that the external monitor program must return one of the following integer values: ■ 0 or 110: The server is online ■ 1 or 100: The server is offline ■ All other values: The server state is unknown. The utility is executed in the context of the UNIX user that is defined in the User attribute. Veritas recommends storing the external monitor utility on the shared disk directory to ensure the file is always available on the online system. Arguments are supported. For information about setting this attribute: Default Value: No default value Example 1.: ServerRoot/bin/myMonitor.pl Example 2: ServerRoot/bin/myMonitor.sh arg1 arg2

Note: For information about the additional attributes of the agent for Symantec Data Loss Prevention when IMF is enabled: See "Attributes that enable IMF" on page 25.

Chapter 4

Enabling the agent for Symantec Data Loss Prevention to support IMF

This chapter includes the following topics:

About Intelligent Monitoring Framework

With the IMF feature, VCS supports intelligent resource monitoring in addition to the poll-based monitoring. Poll-based monitoring polls the resources periodically whereas intelligent monitoring performs asynchronous monitoring. You can enable or disable the intelligent resource monitoring functionality of the Symantec Data Loss Prevention agent.

VCS process and mount-based agents use the AMF kernel driver that provides asynchronous event notifications to the agents that are enabled for IMF.

You can enable the Symantec Data Loss Prevention agent for IMF, provided the following software versions are installed:

- Cluster Server (VCS) 5.1 SP1 or later
- Cluster Server agent for Symantec Data Loss Prevention version 5.1.0.0 or later

Refer to the *Cluster Server Administrator's Guide* for more information about IMF notification module functions and administering the AMF kernel driver.

Benefits of IMF

IMF offers the following benefits:

- Performance
  Enhances performance by reducing the monitoring of each resource at a default of 60 seconds for online resources, and 300 seconds for offline resources. IMF enables the agent to monitor a large number of resources with a minimal effect on performance.
- Faster detection
  Asynchronous notifications would detect a change in the resource state as soon as it happens. Immediate notification enables the agent to take action at the time of the event.

Agent functions for the IMF functionality

If the Symantec Data Loss Prevention agent is enabled for IMF support, the agent supports the following functions, in addition to the functions mentioned in the Symantec Data Loss Prevention agent functions topic.

imf_init

This function initializes the Symantec Data Loss Prevention agent to interface with the AMF kernel driver, which is the IMF notification module for the agent for Symantec Data Loss Prevention. This function runs when the agent starts up.

imf_getnotification

This function gets notifications about resource state changes. This function runs after the agent initializes with the AMF kernel module. This function continuously waits for notification and takes action on the resource upon notification.

imf_register

This function registers or unregisters resource entities with the AMF kernel module. This function runs for each resource after the resource goes into a steady state—online or offline.

Attributes that enable IMF

If the agent for Symantec Data Loss Prevention is enabled for IMF support, the agent uses type-level attributes in addition to the agent-specific attributes.

IMF

This resource type-level attribute determines whether the Symantec Data Loss Prevention agent must perform intelligent resource monitoring. You can also override the value of this attribute at the resource level.

This attribute includes the following keys:

Mode

Define this attribute to enable or disable intelligent resource monitoring. Valid values are as follows:

- 0—Does not perform intelligent resource monitoring
- 1—Performs intelligent resource monitoring for offline resources and performs poll-based monitoring for online resources
- 2—Performs intelligent resource monitoring for online resources and performs poll-based monitoring for offline resources
- 3—Performs intelligent resource monitoring for both online and for offline resources.

Note: The agent for Symantec Data Loss Prevention supports intelligent resource monitoring for online resources only. Hence, Mode should be set to either 0 or 2.

Type and dimension: integer-association

Default: 0 for VCS 5.1 SP1, 3 for VCS 6.0 and later.

MonitorFreq

This key value specifies the frequency at which the agent invokes the monitor agent function. The value of this key is an integer.

Default: 1

You can set this key to a non-zero value for cases where the agent requires to perform both poll-based and intelligent resource monitoring.

If the value is 0, the agent does not perform poll-based process check monitoring.

After the resource registers with the AMF kernel driver, the agent calls the monitor agent function as follows:

- After every (MonitorFreq x MonitorInterval) number of seconds for online resources
- After every (MonitorFreq x OfflineMonitorInterval) number of seconds for offline resources

RegisterRetryLimit

If you enable intelligent resource monitoring, the agent invokes the imf_register agent function to register the resource with the AMF kernel driver.

The value of the RegisterRetryLimit key determines the number of times the agent must retry registration for a resource. If the agent cannot register the resource within the limit that is specified, then intelligent monitoring is disabled until the resource state changes or the value of the Mode key changes.

Default: 3.

IMFRegList

An ordered list of attributes whose values are registered with the IMF notification module.

Type and dimension: string-vector

Default: No default value

Note: The attribute values can be overriden at the resource level.

Before you enable the agent to support IMF

Before you enable the Symantec Data Loss Prevention agent to support IMF, ensure that the AMF kernel module is loaded and AMF is configured. For details, refer to the ‘Administering the AMF kernel driver' section of the *Cluster Server Administrator's Guide*. For details about the commands you can configure AMF using the `amfconfig -h` command.

Enabling the agent to support IMF

In order to enable the Symantec Data Loss Prevention agent to support IMF, you must make the following configuration changes to the attributes of the agent:

- AgentFile: Set the AgentFile attribute to **Script51Agent**
- IMF Mode: Set the IMF Mode attribute to **2**
- IMFRegList: Update the IMFRegList attribute

The following sections provide more information about the commands you can use to make these configuration changes, depending on whether VCS is in a running state or not.

Note: If you have upgraded VCS from an earlier version to version 5.1 SP1 or later, and you already have Symantec Data Loss Prevention agent 5.1.00 or later installed, ensure that you run the following commands to create appropriate symbolic links:

```
# cd /opt/VRTSagents/ha/bin/DLP

# ln -s /opt/VRTSamf/imf/imf_getnotification imf_getnotification

# ln -s /opt/VRTSagents/ha/bin/DLP/monitor imf_register
```

If VCS is in a running state

To enable the Symantec Data Loss Prevention resource for IMF when VCS is in a running state:

1. Make the VCS configuration writable.

   ```
   # haconf -makerw
   ```

2. Run the following command to update the AgentFile attribute.

   ```
   # hatype -modify DLP AgentFile\
   /opt/VRTSvcs/bin/Script51Agent
   ```

3 For VCS version 6.0 or later, run the following commands to add the IMF attributes:

```
# haattr -add -static  DLP IMF -integer -assoc Mode 0 \
MonitorFreq 1 RegisterRetryLimit 3

# haattr -add -static DLP IMFRegList -string -vector
```

Note: Run these commands only once after you first enable IMF support for the agent.

4 Run the following command to update the IMF attribute.

```
# hatype -modify DLP IMF Mode num MonitorFreq num
RegisterRetryLimit num
```

For example, to enable intelligent monitoring of online resources, with the MonitorFreq key set to 5, and the RegisterRetryLimit key is set to 3, run the following command:

```
# hatype -modify DLP IMF Mode 2 MonitorFreq 5 \
RegisterRetryLimit 3
```

Note: The valid values for the Mode key of the IMF attribute are 0 (disabled) and 2 (online monitoring).

5 Run the following command to update the IMFRegList attribute:

```
# hatype -modify DLP IMFRegList User DLPServiceName
```

6 Save the VCS configuration.

```
# haconf -dump -makero
```

7 If the Symantec Data Loss Prevention agent is running, restart the agent.

For information on the commands you can use to restart the agent, see Restarting the agent.

Restarting the agent

To restart the agent:

1. Run the following command to stop the agent forcefully:

   ```
   # haagent -stop DLP -force -sys <system>
   ```

   Note: Stopping the agent forcefully eliminates the need to take the resource offline.

2. Run the following command to start the agent:

   ```
   # haagent -start DLP -sys <system>.
   ```

If VCS is not in a running state

To change the DLP type definition file when VCS is not in a running state:

1. Update the AgentFile attribute.

   ```
   static str AgentFile = "/opt/VRTSvcs/bin/Script51Agent"
   ```

2. Update the IMF attribute.

   The valid values for the Mode key of the IMF attribute are 0 (disabled) and 2 (online monitoring).

   ```
   static int IMF{} = { Mode=num, MonitorFreq=num,
   RegisterRetryLimit=num }
   ```

   For example, to update the IMF attribute such that the Mode key is set to 2, the MonitorFreq key is set to 5, and the RegisterRetryLimit key is set to 3:

   ```
   static int IMF{} = { Mode=2, MonitorFreq=5, RegisterRetryLimit=3
   }
   ```

3. Update the IMFRegList attribute.

   ```
   static str IMFRegList[] = { User, DLPServiceName }
   ```

Disabling intelligent resource monitoring

To disable intelligent resource monitoring

1. Make the VCS configuration writable.

   ```
   # haconf -makerw
   ```

2. To disable intelligent resource monitoring for all the resources of a certain type, run the following command:

   ```
   # hatype -modify DLP IMF -update Mode 0
   ```

3. To disable intelligent resource monitoring for a specific resource, run the following command:

   ```
   # hares -override resource_name IMF
   ```

   ```
   # hares -modify resource_name IMF -update Mode 0
   ```

4. Save the VCS configuration.

   ```
   # haconf -dump -makero
   ```

Sample IMF configurations

An example of a type definition file for a Symantec Data Loss Prevention agent that is IMF-enabled is as follows.

```
type DLP (
     static str AgentDirectory = "/opt/VRTSagents/ha/bin/DLP"
     static str AgentFile = "/opt/VRTSvcs/bin/Script51Agent"
     static str ArgList[] = { ResLogLevel, State, IState, User,
     EnvFile, DLPInstallDir, DLPServiceName, DelayAfterOnline,
     MonitorProgram }
     static boolean AEPTimeout = 1
     static int IMF{} = { Mode=2, MonitorFreq=5, RegisterRetryLimit=3 }
     static str IMFRegList[] = { User, DLPServiceName }
     str ResLogLevel = INFO
     str User = protect
     str EnvFile
     str DLPInstallDir = "/opt/Vontu/Protect/bin"
     str DLPServiceName
     int DelayAfterOnline
     str MonitorProgram
)
```

A sample resource configuration from the /etc/VRTSvcs/conf/config/main.cf file is as follows:

```
DLP VontuNotifier_res (
                User = protect
                DLPInstallDir = "/opt/Vontu/Protect/bin"
                DLPServiceName = VontuNotifier
                DelayAfterOnline = 2
                IMF = { Mode = 2, MonitorFreq = 10,
                         RegisterRetryLimit = 3 }
                )
```

Chapter 5

Troubleshooting the agent for Symantec Data Loss Prevention

This chapter includes the following topics:

Using the correct software and operating system versions

Ensure that you use correct software and operating system versions.

For information on the software versions that the agent for Symantec Data Loss Prevention supports, see the Veritas Services and Operations Readiness Tools (SORT) site: https://sort.veritas.com/agents.

Meeting prerequisites

Before installing the agent for Symantec Data Loss Prevention, ensure that the following prerequisites are met.

For example, you must install the ACC library on VCS before installing the agent for Symantec Data Loss Prevention.

See "Before you install the Cluster Server agent for Symantec Data Loss Prevention" on page 13.

Reviewing error log files

If you face problems while using Symantec Data Loss Prevention or the agent for Symantec Data Loss Prevention, use the log files described in this section to investigate the problems.

Reviewing Symantec Data Loss Prevention log files

By default, operational logs for the Enforce Server are stored in the `/var/log/Vontu` directory.

Refer to the *Symantec Data Loss Prevention Administration Guide* and the *Symantec Data Loss Prevention System Maintenance Guide* for additional information about Symantec Data Loss Prevention logs.

Using trace level logging

The ResLogLevel attribute controls the level of logging that is written in a cluster log file for each Symantec Data Loss Prevention resource. You can set this attribute to TRACE, which enables very detailed and verbose logging.

If you set ResLogLevel to TRACE, a very high volume of messages are produced. Veritas recommends that you localize the ResLogLevel attribute for a particular resource.

The LogDbg attribute should be used to enable the debug logs for the ACCLib-based agents when the ACCLIB version is 6.2.0.0 or later and the VCS version is 6.2 or later.

To localize ResLogLevel attribute for a resource

1. Identify the resource for which you want to enable detailed logging.
2. Localize the ResLogLevel attribute for the identified resource:

   ```
   # hares -local Resource_Name ResLogLevel
   ```

3. Set the ResLogLevel attribute to TRACE for the identified resource:

   ```
   # hares -modify Resource_Name ResLogLevel TRACE -sys SysA
   ```

4. Note the time before you begin to operate the identified resource.

5. Test the identified resource. The function reproduces the problem that you are attempting to diagnose.
6. Note the time when the problem is reproduced.
7. Set the ResLogLevel attribute back to INFO for the identified resource:

```
# hares -modify Resource_Name ResLogLevel INFO -sys SysA
```

8. Save the configuration changes.

```
# haconf -dump
```

9. Review the contents of the log file.

   Use the time noted in the previous steps to diagnose the problem.

   You can also contact Veritas support for more help.

To enable debug logs for all resources of type DLP

- Enable the debug log.

```
# hatype -modify DLP LogDbg DBG_5
```

To override the LogDbg attribute at resource level

- Override the LogDbg attribute at the resource level and enable the debug logs for the specific resource.

```
# hares -override DLP LogDbg
# hares -modify DLP LogDbg DBG_5
```

Troubleshooting the configuration for IMF

If you face problems with the IMF configuration or functionality, consider the following:

- Ensure that the following attributes are configured with appropriate values.
  - AgentFile
  - IMF
  - IMFRegList
    If IMFRegList is not configured correctly, the Symantec Data Loss Prevention resources that have been registered for IMF get unregistered every time the monitor function is run.

- If you have configured the required attributes to enable the Symantec Data Loss Prevention agent for IMF, but the agent is still not IMF-enabled, restart the agent. The imf_init function runs only when the agent starts up, so when you restart the agent, imf_init runs and initializes the Symantec Data Loss Prevention agent to interface with the AMF kernel driver.
- You can run the following command to check the value of the MonitorMethod attribute and to verify that a resource is registered for IMF.

  ```
  # hares -value resource MonitorMethod system
  ```

  The MonitorMethod attribute specifies the monitoring method that the agent uses to monitor the resource:
  - Traditional—Poll-based resource monitoring
  - IMF—Intelligent resource monitoring
- You can use the `amfstat` command to see a list of registered PIDs for a DLP service.

  Following is a sample output of the `ps -ef` command for the DLP VontuNotifier process. This same PID - PID 31186 - is registered with the AMF kernel driver.

  ```
  # ps -ef|grep VontuNotifier
  protect  31186    1  0 19:52 ?     00:00:00 ./VontuNotifier
  ../config/VontuNotifier.conf wrapper.pidfile=./VontuNotifier.pid
  wrapper.daemonize=TRUE
  ```

  The output of the `amfstat` command is as follows:

  ```
  [root@vcslx202 ~]# amfstat
  AMF Status Report

  Registered Reapers (1):
  =======================
  RID    PID     EVENT   REAPER
  116    1774    5       0       DLP

  Process ONLINE Monitors (5):
  ============================
  RID    R_RID   PID     GROUP
  134    116     31186   VontuNotifier_res
  135    116     31193   VontuUpdate_res
  136    116     31404   VontuManager_res
  137    116     31322   VontuMonitorController_res
  138    116     31386   VontuIncidentPersister_res
  ```

- Run the following command to set the ResLogLevel attribute to TRACE. When you set ResLogLevel to TRACE, the agent logs messages in the DLP_A.log file.

  ```
  # hares -modify ResourceName ResLogLevel TRACE
  ```

- Run the following command to view the content of the AMF in-memory trace buffer.

  ```
  # amfconfig -p dbglog
  ```

Known issues

This release of the agent for Symantec Data Loss Prevention has the following known issues:

Problem

An error message might appear when you run the `hares -offline` command to take a resource offline.

Description

When a resource is taken offline, it is unregistered from the AMF module. However, the imf_register function attempts to unregister the resource again.

Workaround

It is safe to ignore this error message.

Appendix A

Sample Configurations

This appendix includes the following topics:

About sample configurations for the agents for Symantec Data Loss Prevention

The sample configuration graphically depicts the resource types, resources, and resource dependencies within the service group. Review these dependencies carefully before configuring the agents for Symantec Data Loss Prevention. For more information about these resource types, refer to the *Cluster Server Bundled Agents Reference Guide*.

Sample agent type definition for Symantec Data Loss Prevention

```
type DLP (
        static boolean AEPTimeout = 1
        static str AgentFile = "/opt/VRTSvcs/bin/Script50Agent"
        static str AgentDirectory = "/opt/VRTSagents/ha/bin/DLP"
        static str ArgList[] = { ResLogLevel, State, IState,
        User, EnvFile, DLPInstallDir, DLPServiceName,
        DelayAfterOnline, MonitorProgram }
        str ResLogLevel = INFO
```

```
        str User = "protect"
        str EnvFile
        str DLPInstallDir = "/opt/Vontu/Protect/bin"
        str DLPServiceName
        int DelayAfterOnline = 0
        str MonitorProgram
)
```

Sample configuration files

A sample main.cf file is as follows:

```
include "OracleASMTypes.cf"
include "types.cf"
include "DLPTypes.cf"
include "Db2udbTypes.cf"
include "OracleTypes.cf"
include "SybaseTypes.cf"

cluster dlpclus (
 UserNames = { admin = IpqIpkPmqLqqOyqKpn }
 Administrators = { admin }
 )

system DLPVM1 (
 )

system DLPVM2 (
 )

group DLP_DB_SG (
 SystemList = { DLPVM1 = 0, DLPVM2 = 1 }
 )

 DiskGroup DLP_DB_DG (
  DiskGroup = DLPDG
  )

 IP SAP_DB_VIP (
  Device = eth0
  Address = "10.209.79.127"
  NetMask = "255.255.252.0"
  )
```

```
Mount DLP_DB_mnt (
 MountPoint = "/home/oracle/app"
 BlockDevice = "/dev/vx/dsk/DLPDG/DLPDG_VOL"
 FSType = vxfs
 MountOpt = rw
 FsckOpt = "-y"
 )

NIC DLP_DB_NIC (
 Device = eth0
 NetworkHosts = { "10.209.76.1" }
 )

Netlsnr DLP_ORA_LISTNER (
 Owner = oracle
 Home = "/home/oracle/app/oracle/product/11.2.0/dbhome_1"
 )

Oracle DLP_ORA_Res (
 Sid = protect
 Owner = oracle
 Home = "/home/oracle/app/oracle/product/11.2.0/dbhome_1"
 DBAUser = oracle
 DBAPword = Vcs12345
 User = SYS
 Pword = gqmSjuJmhMimJmkMl
 )

Volume DLP_DB_Vol (
 DiskGroup = DLPDG
 Volume = DLPDG_VOL
 )

DLP_DB_Vol requires DLP_DB_DG
DLP_DB_mnt requires DLP_DB_Vol
DLP_ORA_LISTNER requires DLP_ORA_Res
DLP_ORA_Res requires DLP_DB_mnt
DLP_ORA_Res requires SAP_DB_VIP
SAP_DB_VIP requires DLP_DB_NIC


// resource dependency tree
```

```
//
// group DLP_DB_SG
// {
// Netlsnr DLP_ORA_LISTNER
//     {
//     Oracle DLP_ORA_Res
//         {
//         Mount DLP_DB_mnt
//             {
//             Volume DLP_DB_Vol
//                 {
//                 DiskGroup DLP_DB_DG
//                 }
//             }
//         IP SAP_DB_VIP
//             {
//             NIC DLP_DB_NIC
//             }
//         }
//     }
// }


group DLP_ENF_SG (
 SystemList = { DLPVM1 = 0, DLPVM2 = 1 }
 )

 DLP VontuIncidentPersister_res (
  ResLogLevel = TRACE
  DLPServiceName = VontuIncidentPersister
  )

 DLP VontuManager_res (
  ResLogLevel = TRACE
  DLPServiceName = VontuManager
  )

 DLP VontuMonitorController_res (
  ResLogLevel = TRACE
  DLPServiceName = VontuMonitorController
  )

 DLP VontuNotifier_res (
```

```
 ResLogLevel = TRACE
 DLPServiceName = VontuNotifier
 DelayAfterOnline = 2
 IMF = { Mode = 2, MonitorFreq = 5,
   RegisterRetryLimit = 300 }
 )

DLP VontuUpdate_res (
 ResLogLevel = TRACE
 DLPServiceName = VontuUpdate
 )

DiskGroup DLP_Vontu_conf (
 DiskGroup = sbl81sfs_dg
 )

DiskGroup DLP_Vontu_dg (
 DiskGroup = sbl81db_dg
 )

DiskGroup DLP_Vontu_log_dg (
 DiskGroup = sbl81gtw_dg
 )

IP DLP_ENF_VIP (
 Device = eth0
 Address = "10.209.79.128"
 NetMask = "255.255.252.0"
 )

Mount DLP_Vontu_conf_mnt (
 MountPoint = "/opt/Vontu"
 BlockDevice = "/dev/vx/dsk/sbl81db_dg/sbl81db_vol"
 FSType = vxfs
 MountOpt = rw
 FsckOpt = "-y"
 )

Mount DLP_Vontu_log_mnt (
 MountPoint = "/var/log/Vontu/"
 BlockDevice = "/dev/vx/dsk/sbl81gtw_dg/sbl81gtw_vol"
 FSType = vxfs
 MountOpt = rw
```

```
 FsckOpt = "-y"
 )

Mount DLP_Vontu_mnt (
 MountPoint = "/var/Vontu"
 BlockDevice = "/dev/vx/dsk/sbl81sfs_dg/sbl81sfs_vol"
 FSType = vxfs
 MountOpt = rw
 FsckOpt = "-y"
 )

NIC DLP_ENF_NIC (
 Device = eth0
 NetworkHosts = { "10.209.76.1" }
 )

Volume DLP_Vontu_conf_vol (
 DiskGroup = sbl81db_dg
 Volume = sbl81db_vol
 )

Volume DLP_Vontu_log_vol (
 DiskGroup = sbl81gtw_dg
 Volume = sbl81gtw_vol
 )

Volume DLP_Vontu_vol (
 DiskGroup = sbl81sfs_dg
 Volume = sbl81sfs_vol
 )

requires group DLP_DB_SG online global firm
DLP_ENF_VIP requires DLP_ENF_NIC
DLP_Vontu_conf_mnt requires DLP_Vontu_conf_vol
DLP_Vontu_conf_vol requires DLP_Vontu_conf
DLP_Vontu_log_mnt requires DLP_Vontu_log_vol
DLP_Vontu_log_vol requires DLP_Vontu_log_dg
DLP_Vontu_mnt requires DLP_Vontu_vol
DLP_Vontu_vol requires DLP_Vontu_dg
VontuIncidentPersister_res requires VontuNotifier_res
VontuManager_res requires VontuNotifier_res
VontuMonitorController_res requires VontuNotifier_res
VontuNotifier_res requires DLP_ENF_VIP
```

```
VontuNotifier_res requires DLP_Vontu_conf_mnt
VontuNotifier_res requires DLP_Vontu_log_mnt
VontuNotifier_res requires DLP_Vontu_mnt
VontuUpdate_res requires DLP_Vontu_conf_mnt
VontuUpdate_res requires DLP_Vontu_log_mnt
VontuUpdate_res requires DLP_Vontu_mnt


// resource dependency tree
//
// group DLP_ENF_SG
// {
// DLP VontuIncidentPersister_res
//     {
//     DLP VontuNotifier_res
//         {
//         IP DLP_ENF_VIP
//             {
//             NIC DLP_ENF_NIC
//             }
//         Mount DLP_Vontu_conf_mnt
//             {
//             Volume DLP_Vontu_conf_vol
//                 {
//                 DiskGroup DLP_Vontu_conf
//                 }
//             }
//         Mount DLP_Vontu_log_mnt
//             {
//             Volume DLP_Vontu_log_vol
//                 {
//                 DiskGroup DLP_Vontu_log_dg
//                 }
//             }
//         Mount DLP_Vontu_mnt
//             {
//             Volume DLP_Vontu_vol
//                 {
//                 DiskGroup DLP_Vontu_dg
//                 }
//             }
//         }
//     }
```

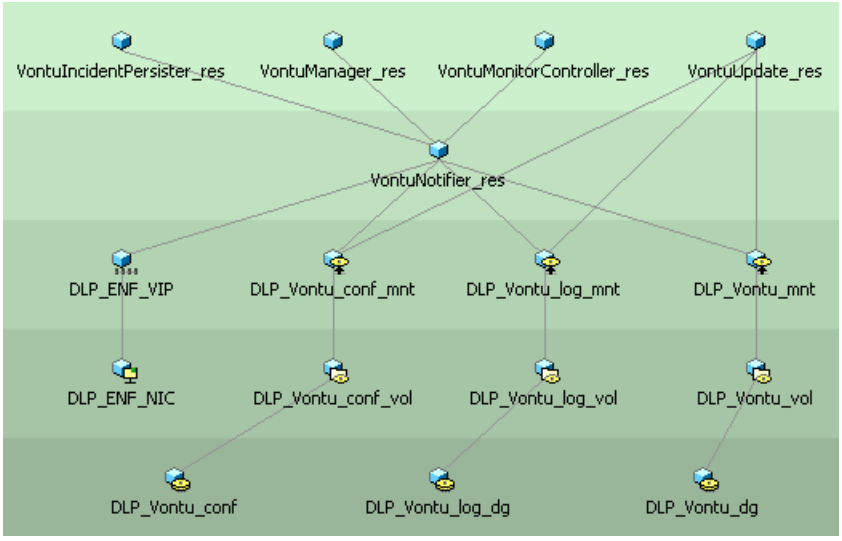
```
// DLP VontuManager_res
//     {
//     DLP VontuNotifier_res
//         {
//         IP DLP_ENF_VIP
//             {
//             NIC DLP_ENF_NIC
//             }
//         Mount DLP_Vontu_conf_mnt
//             {
//             Volume DLP_Vontu_conf_vol
//                 {
//                 DiskGroup DLP_Vontu_conf
//                 }
//             }
//         Mount DLP_Vontu_log_mnt
//             {
//             Volume DLP_Vontu_log_vol
//                 {
//                 DiskGroup DLP_Vontu_log_dg
//                 }
//             }
//         Mount DLP_Vontu_mnt
//             {
//             Volume DLP_Vontu_vol
//                 {
//                 DiskGroup DLP_Vontu_dg
//                 }
//             }
//         }
//     }
// DLP VontuMonitorController_res
//     {
//     DLP VontuNotifier_res
//         {
//         IP DLP_ENF_VIP
//             {
//             NIC DLP_ENF_NIC
//             }
//         Mount DLP_Vontu_conf_mnt
//             {
//             Volume DLP_Vontu_conf_vol
//                 {
```

```
//                  DiskGroup DLP_Vontu_conf
//                  }
//              }
//          Mount DLP_Vontu_log_mnt
//              {
//              Volume DLP_Vontu_log_vol
//                  {
//                  DiskGroup DLP_Vontu_log_dg
//                  }
//              }
//          Mount DLP_Vontu_mnt
//              {
//              Volume DLP_Vontu_vol
//                  {
//                  DiskGroup DLP_Vontu_dg
//                  }
//              }
//          }
//      }
// DLP VontuUpdate_res
//      {
//      Mount DLP_Vontu_conf_mnt
//          {
//          Volume DLP_Vontu_conf_vol
//              {
//              DiskGroup DLP_Vontu_conf
//              }
//          }
//      Mount DLP_Vontu_log_mnt
//          {
//          Volume DLP_Vontu_log_vol
//              {
//              DiskGroup DLP_Vontu_log_dg
//              }
//          }
//      Mount DLP_Vontu_mnt
//          {
//          Volume DLP_Vontu_vol
//              {
//              DiskGroup DLP_Vontu_dg
//              }
//          }
//      }
```

```
// }
```

Sample service group configurations for DLP

The following figure represents a sample service group that shows the dependencies between the resources of the Cluster Server agent for Symantec Data Loss Prevention.



The following figure represents the dependency between two sample service groups.

The service group containing the resource for Symantec DPL Enforce Server has an online global (firm) dependency on the service group containing the resource for the Oracle database.

In this configuration, the Symantec Data Loss Prevention components are deployed with the three-tier type of installation. The Enforce Server and Oracle database are installed on different machines, and hence, the online global (firm) dependency is set.

When the Symantec Data Loss Prevention components are installed with the two-tier type of installation, the service group containing the resource for the DLP Enforce Server has an online local (firm) dependency on the service group containing the resource for the Oracle database.

In the two-tier type of installation, the Enforce Server and Oracle database are installed on the same machine, and hence, online local (firm) dependency is recommended.

Refer to the *Symantec Data Loss Prevention Installation Guide for Linux* for information about the Symantec Data Loss Prevention installation tiers.