



Configuring Brightmail with Sun Java System Messaging Server

Sun Java™ Enterprise System Technical Note



Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 819-5195-10
August 2006

Copyright 2006 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more U.S. patents or pending patent applications in the U.S. and in other countries.

U.S. Government Rights – Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

This distribution may include materials developed by third parties.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, the Solaris logo, the Java Coffee Cup logo, docs.sun.com, Java, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

Products covered by and information contained in this publication are controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical or biological weapons or nuclear maritime end uses or end users, whether direct or indirect, are strictly prohibited. Export or reexport to countries subject to U.S. embargo or to entities identified on U.S. export exclusion lists, including, but not limited to, the denied persons and specially designated nationals lists is strictly prohibited.

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.

Copyright 2006 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. Tous droits réservés.

Sun Microsystems, Inc. détient les droits de propriété intellectuelle relatifs à la technologie incorporée dans le produit qui est décrit dans ce document. En particulier, et ce sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plusieurs brevets américains ou des applications de brevet en attente aux Etats-Unis et dans d'autres pays.

Cette distribution peut comprendre des composants développés par des tierces personnes.

Certains composants de ce produit peuvent être dérivées du logiciel Berkeley BSD, licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays; elle est licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, le logo Solaris, le logo Java Coffee Cup, docs.sun.com, Java et Solaris sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui, en outre, se conforment aux licences écrites de Sun.

Les produits qui font l'objet de cette publication et les informations qu'il contient sont régis par la législation américaine en matière de contrôle des exportations et peuvent être soumis au droit d'autres pays dans le domaine des exportations et importations. Les utilisations finales, ou utilisateurs finaux, pour des armes nucléaires, des missiles, des armes chimiques ou biologiques ou pour le nucléaire maritime, directement ou indirectement, sont strictement interdites. Les exportations ou réexportations vers des pays sous embargo des Etats-Unis, ou vers des entités figurant sur les listes d'exclusion d'exportation américaines, y compris, mais de manière non exclusive, la liste de personnes qui font objet d'un ordre de ne pas participer, d'une façon directe ou indirecte, aux exportations des produits ou des services qui sont régis par la législation américaine en matière de contrôle des exportations et la liste de ressortissants spécifiquement désignés, sont rigoureusement interdites.

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFACON.

Configuring Brightmail with Sun Java System Messaging Server

This technical note describes how to install, configure, and verify Symantec Brightmail AntiSpam with Sun Java™ System Messaging Server.

The component products affected by this technical note are:

- Sun Java System Messaging Server 6 2005Q4 (These instructions should also work with these previous releases: Sun Java System Messaging Server 6 2005Q1, Sun Java System Messaging Server 6 2004Q2, and Sun™ ONE Messaging Server 6.0.)
- Symantec Brightmail AntiSpam 6 and subsequent releases

This technical note contain the following sections:

- [“Technical Note Revision History”](#) on page 3
- [“Overview of Symantec Brightmail AntiSpam”](#) on page 4
- [“Installing and Configuring Symantec Brightmail”](#) on page 6
- [“Troubleshooting the Configuration”](#) on page 14
- [“Documentation, Support, and Training”](#) on page 15
- [“Third-Party Web Site References”](#) on page 15
- [“Sun Welcomes Your Comments”](#) on page 15

Technical Note Revision History

TABLE 1 Revision History

Date	Description of Changes
August 15, 2006	Re-issue of this technical note for Sun Java Enterprise System 2005Q4.

Overview of Symantec Brightmail AntiSpam

The Symantec Brightmail solution consists of the Brightmail AntiSpam software along with realtime anti-spam and anti-virus rule updates downloaded to email servers.

How Symantec Brightmail Works

An organization deploys the Symantec Brightmail software at its site. Symantec has email probes set around the Internet for detection of new spam. Symantec technicians create custom rules to block this spam in realtime. These rules are downloaded to Symantec Brightmail servers, also in realtime. The Symantec Brightmail database is updated and the Symantec Brightmail server runs this database filter against the email for the specified users or domains.

Brightmail Architecture

Figure 1 depicts the Symantec Brightmail architecture.

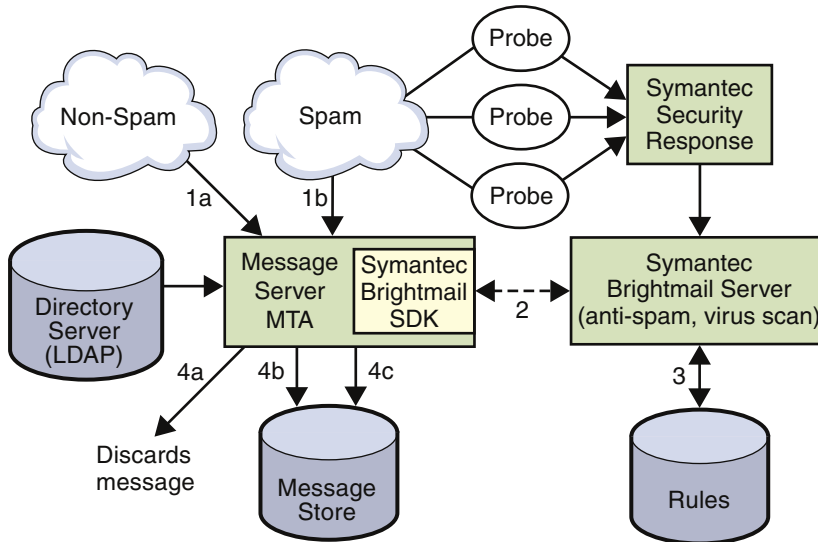


FIGURE 1 Brightmail and Messaging Server Architecture

Symantec Brightmail and Messaging Server Architecture

When Symantec Security Response receives spam from email probes, operators immediately create appropriate spam filtering rules, which are downloaded to Symantec Brightmail customer machines. Similarly, Symantec Security Response sends realtime virus rules. These rules are used by customer's Symantec Brightmail servers to catch spam and viruses.

The Sun Java System Messaging Server MTA uses the Symantec Brightmail SDK to communicate with the Symantec Brightmail server. The MTA dispatches messages based on the response from Brightmail. After the mail (1a) or (1b) is received by the MTA, the MTA sends a copy of the message contents to the Symantec Brightmail server (2). The Symantec Brightmail server uses its rules and data to determine if the message is a spam or virus (3), and returns a verdict to the MTA. Based on the verdict, the MTA either (4a) discards the message, or (4b) delivers it to a particular folder in the Message Store, or (4c) delivers it to the default INBOX folder.

Because the Symantec Brightmail SDK is third-party software, it is not included in the Messaging Server installation kit. You must obtain the Symantec Brightmail SDK and server software from Symantec. The MTA has configuration settings to tell it whether and where to load the Symantec Brightmail SDK to enable Symantec Brightmail integration.

Once the SDK is loaded, Symantec Brightmail message processing is determined by several factors and levels of granularity. Symantec Brightmail scanning can be selected in the MTA in a variety of ways, including via use of a per-user LDAP attribute, or via use of a per-domain LDAP attribute, or according to source or destination channel.

The Messaging Server MTA passes an `optin` variable to the Symantec Brightmail server. If a `destinationspamfilternoptin` *optin-value* or `sourcespamfilternoptin` *optin-value* marking is placed on a relevant channel in the `imta.cnf` file, or if a domain or user has the appropriate LDAP attribute set to some string (*optin-value*), then that *optin-value* is passed as the value of the `optin` variable to Brightmail. If you enable the Brightmail client-side `optin`, and the `optin` value is not set, the Brightmail default is `NULL`, which means that emails are not going to be filtered with any Symantec Brightmail services (spam or virus).

Symantec Brightmail offers only two distinguishable services, spam and virus. However, Symantec Brightmail supports the concept of "group policies," enabling different actions for different users based on the same verdict. See the Symantec Brightmail AntiSpam documentation for more information. Symantec Brightmail also provides "content-filtering" service, but this functionality is provided using Sieve, so there is no added value to have Symantec Brightmail do the Sieve filtering.

When a message is determined to contain a virus, the Symantec Brightmail software can be configured to clean the virus and resubmit the cleaned message back to the MTA. (Due to some undesirable side effects caused by loss of information about the original message in a resubmitted cleaned message, do not configure Symantec Brightmail to resubmit the cleaned message back to the MTA.) When the message is spam, the verdict back from Symantec Brightmail along with the MTA configuration for how to interpret that verdict determine what happens to the message. The message can be discarded, filed into a folder, tagged as spam or virus on the subject line, passed to a Sieve rule, delivered normally in the INBOX, and so on.

The Symantec Brightmail software can be located on the same system as the MTA, or it can be on a separate host. In fact, you can have a farm of Symantec Brightmail servers serving one or more MTAs. The Symantec Brightmail SDK uses the `bmi config_client.xml` file to determine which Symantec Brightmail servers to use.

Symantec Brightmail Requirements and Performance Considerations

- Symantec Brightmail servers must run the Solaris™ Operating System.
- Because spam and virus filtering involve significant work, adding Symantec Brightmail server (configured to perform both spam and virus filtering) to an existing Messaging Server host serving as an MTA can, due to the additional work performed, reduce overall message throughput on that host by as much as 50 percent. To allow Symantec Brightmail to perform its valuable work without reducing overall message throughput, a rule of thumb might be to add two dedicated Symantec Brightmail servers for each MTA, so that the Symantec Brightmail servers can “keep up” with the usual MTA message throughput.

Installing and Configuring Symantec Brightmail

Use the steps in this section to install the Symantec Brightmail server then configure Messaging Server to use Symantec Brightmail. These steps assume that you are installing Symantec Brightmail server and Messaging Server on the same host. For a multi-node installation, see [“Configuring a Multi-node Symantec Brightmail and Messaging Server Deployment”](#) on page 13 for more information.

Installing Symantec Brightmail

▼ To Install Symantec Brightmail on a Solaris 10 System

There is a problem with the Symantec Brightmail install script on Solaris 10. The problem prevents the script from continuing beyond the OS level check, and warns that the `/tmp` directory does not have enough space, even though there is enough space. To fix this problem, perform the following before running the Symantec Brightmail install script.

- ▶ **Change the `DF_CMD` variable from `df` to `df -k` in the `.bin` file(s).**

▼ To Prepare the System

- ▶ **Add a `mailwall` user to the `bmi` group.**

```
groupadd bmi
useradd -d /export/mailwall -s /bin/sh -g bmi mailwall
```

▼ To Install Symantec Brightmail

- 1 **Download the latest Symantec Brightmail AntiSpam release from the following location:**

<http://ses.symantec.com/trybrightmail>

Note – The version for download at the time of this publication was BAS 6.0.1.

You will also receive a Symantec license file through email. Be sure to register the Symantec Brightmail software later.

- 2 **Obtain the Symantec Brightmail AntiSpam.**

You need the Symantec Brightmail SDK for a Messaging Server host that has Symantec Brightmail filtering enabled. You copy and untar the Symantec Brightmail SDK on the Messaging Server host. Deployments with Symantec Brightmail server-only hosts (that is, a multi-node deployment where the Symantec Brightmail server is running on a separate host from the Messaging Server host) don't need the Symantec Brightmail SDK on such Brightmail server-only hosts. Contact your Symantec sales representative to access the Symantec Brightmail SDK.

- 3 **Copy the Symantec Brightmail SDK tar file to a new directory on the Messaging Server host where the SDK should initially be unpacked.**

- 4 **Untar the Symantec Brightmail SDK into its own directory.**

For example:

```
tar -xvf tar -xvf BSDK_6*_*.tar
```

This creates a BSDK subdirectory with the following directories files, as shown in the following example (the installation directory is SYMSDK):

```
/SYMSDK/BSDK/
/SYMSDK/BSDK/docs/
/SYMSDK/BSDK/docs/LEGAL.NOTICES.txt
/SYMSDK/BSDK/docs/bas_sdk_60.pdf
/SYMSDK/BSDK/etc/
/SYMSDK/BSDK/etc/bmiconfig_client.xml
/SYMSDK/BSDK/etc/bmiconfig.xsd
/SYMSDK/BSDK/include/
/SYMSDK/BSDK/include/bmi_api.h
/SYMSDK/BSDK/lib/
/SYMSDK/BSDK/lib/libbmiclient_loader.a
/SYMSDK/BSDK/lib/libbmishareddata.so
/SYMSDK/BSDK/lib/libxml2.so.2
/SYMSDK/BSDK/lib/libxml2_single.so.2
/SYMSDK/BSDK/lib/libbmiclient.so.1
/SYMSDK/BSDK/lib/libbmiclient_single.so.1
/SYMSDK/BSDK/lib/libbmiclient.so
/SYMSDK/BSDK/lib/libbmiclient_single.so
```

```
/SYMSDK/BSDK/lib/libxml2.so
/SYMSDK/BSDK/lib/libxml2_single.so
```

5 Change the permissions on the preceding directories and files so that Message Server can read the `bmiconfig_client.xml` file.

For example, if Messaging Server is running as `mailsrv:mail`, then the `mailsrv` user should have permissions to read and write to the `bmiconfig_client.xml` file. That is, perform a `chmod -R 755 base_dir/BSDK`, or at least make sure that the permissions are `ReadWriteExecute` by any group, as shown below.

```
# pwd
/SYMSDK/BSDK

# ls -arlt
total 1734
-rwxr-xr-x  1 mailsrv  mail      432843 Jun 28  2004 libbmiclient.so.1
-rwxr-xr-x  1 mailsrv  mail      432843 Jun 28  2004 libbmiclient.so
drwxr-xr-x  3 mailsrv  mail          512 Jun 20  14:44 ..
-rwxr-xr-x  1 mailsrv  mail          745 Jun 30  11:45 bmiconfig_client.xml
drwxr-xr-x  2 mailsrv  mail          512 Jul 10  15:26 .
```

6 Install the Symantec Brightmail server.

```
./install
```

7 Select the following options:

- Brightmail Scanner
- Choose the default folder
- Default Install Folder: `/opt/symantec/sbas/Scanner`
- Log Folder (default: `/var/log/brightmail`)
- Install Set: Brightmail Server only

Tip – Brightmail Server only is not the default.

8 Register Symantec Brightmail server. This step happens automatically as part of the installation.

```
/opt/symantec/sbas/Scanner/sbin/register.sh
```

Specify the valid licence file you got from Step 1.

For example:

```
# /opt/symantec/sbas/Scanner/sbin/register.sh
Please enter the path to a valid license file: /export/brightmail/1425886.7.slf
Connecting to Brightmail. This may take a few minutes.
Verifying Certificate...
Registration Successful.
```

You are now enabled to retrieve Symantec Brightmail rules from Symantec Security Response.

- 9 Change the ownership of cert.pem under the /opt/symantec/sbas/Scanner/etc directory so that the mailwall user can access cert.pem.**

```
# ls -arlt cert.pem
-rw-r--r--  1 root    other      1892 Jul 10 14:19 cert.pem
# chown mailwall:bmi cert.pem
# ls -arlt cert.pem
-rw-r--r--  1 mailwall bmi        1888 Jun 29 16:14 cert.pem
```

- 10 Change the ownership of the directory so that the Messaging Server user (in the following example mailsrv:mail) can access this directory.**

```
chown -R mailsrv:mail /opt/symantec/
```

Note – The IMTA_USER option in the MTA tailor file (typically /opt/SUNWmsgsr/config/imta_tailor) is how the MTA knows who its user is.

- 11 Make backup copies of the bmiconfig.xml (from the scanner= server) and bmiconfig_client.xml (from the SDK) files.**

- 12 Modify the bmiconfig_client.xml file, replacing the HOST and the PORT (where the server is listening). Also, configure the Symantec Brightmail client log file, CLIENT.LOG, which is the path to the Symantec Brightmail client log file. Make sure Messaging Server can write to this file.**

For example, if Symantec Brightmail server is running on a host named host1.red.example.com and it is listening on port 41000, then your modification would look like this:

```
<servers> <server host="host1.red.example.com" port="41000"></server>
```

- 13 Set the LD_LIBRARY_PATH:**

```
LD_LIBRARY_PATH=/opt/SUNWmsgsr/lib:/usr/local/lib:/opt/sun/messaging
/brightmail:/opt/symantec/sbas/Scanner/lib
```

Also, add *base_dir/SDK/lib* to the LD_LIBRARY_PATH on the host running Messaging Server.

- 14 Start the Symantec Brightmail server:**

```
/etc/init.d/mailwall start
```

▼ To Verify the Symantec Brightmail Installation

- 1 Make sure that the Symantec Brightmail server starts without any errors by examining /var/log/syslog output.**

You should see output similar to the following for a functioning server:

```
Jul 10 14:21:39 host1 runner[24856]: [ID 702911 mail.info] starting bmagent.
Jul 10 14:21:39 host1 runner[24856]: [ID 702911 mail.info] starting harvester.
Jul 10 14:21:39 host1 runner[24856]: [ID 702911 mail.info] starting conduit.
Jul 10 14:21:39 host1 runner[24856]: [ID 702911 mail.info] starting bmserver.
```

- 2 **Check logs in the `/var/log/brightmail` directory for errors. Also, check the Symantec Brightmail client log file (configured in the `bmconfig_client.xml`).**
- 3 **Make sure that the Symantec Brightmail server has started successfully by examining the `bmserver` process.**

For example:

```
# ps -eaf | grep sbas
mailwall 16808 16806 0 17:49:12 ? 0:01 /opt/symantec/sbas/Scanner/bin/bmserver -c
/opt/symantec/sbas/Scanner/etc/bmico
mailwall 16806 1 0 17:49:12 ? 0:00 /opt/symantec/sbas/Scanner/sbin/runner
/opt/symantec/sbas/Scanner/etc/runner.cf
mailwall 16807 16806 0 17:49:12 ? 0:00 /opt/symantec/sbas/Scanner/sbin/bmagent -c
/opt/symantec/sbas/Scanner/etc/agent
```

Configuring the Messaging Server MTA for Symantec Brightmail

The Sun Java System Messaging Server MTA supports the use of up to four separate spam/virus filtering packages. Typical usage would be to configure Symantec Brightmail as spam/virus filter package #1 as shown in this section, using a minimal set of `option.dat` options. However, if one or more other spam/virus filter packages are already in use and Symantec Brightmail is to be added as yet another spam/virus filter package, then configure Symantec Brightmail by setting an appropriate pair of (previously unused) `SPAMFILTER n _CONFIG_FILE` and `SPAMFILTER n _LIBRARY` options.

In the following example, Messaging Server has been installed in the `/opt/SUNWmsgsr` directory.

▼ To Modify the `option.dat` and `imta.cnf` Files

- 1 **Modify the `option.dat` file as follows.**

Here the Symantec Brightmail client is located under the `/SYMSDK/BSDK` directory.

```
!
! Brightmail Stuff
!
spamfilter1_config_file=/SYMSDK/BSDK/etc/bmconfig_client.xml
spamfilter1_library=/SYMSDK/BSDK/lib/libbmiclient.so
```

Consider also setting `SPAMFILTER1_OPTIONAL=-2` (or `SPAMFILTER n _OPTIONAL=-2`, as appropriate) in the `option.dat` file. If the MTA encounters an error contacting Symantec Brightmail, then in addition to temporarily rejecting incoming SMTP messages, the MTA will also generate a `syslog` notice. For `syslog` notices to be routed appropriately, you might also need to adjust the `SNDOPR_PRIORITY` `option.dat` option and your `syslog.conf` file.

2 Modify the `imta.cnf` file as follows.

Symantec Brightmail scanning can be selected in the MTA in a variety of ways, including via use of a per-user LDAP attribute, or via use of a per-domain LDAP attribute, or according to source or destination channel. A typical usage is to perform Symantec Brightmail scanning on all messages destined to locally hosted users: that is, on all messages being delivered to users via an `ims-ms` channel, or via `tcp_lmtp*` client channels. For instance, to trigger Symantec Brightmail “spam” filtering on all messages being delivered to the store via the `ims-ms` channel, if Symantec Brightmail is being used as spam/virus filter package # 1, add `destinationspamfilterloptin spam` to the `ims-ms` channel definition in the `imta.cnf` file. Such a channel definition might then look something like the following:

```
! ims-ms
ims-ms defragment subdirs 20 notices 1 7 14 21 28 \
  backoff "pt5m" "pt10m" "pt30m" "pt1h" "pt2h" "pt4h" \
  maxjobs 2 pool IMS_POOL fileinto $U+$S@$D \
  destinationspamfilterloptin spam
ims-ms-daemon
```

3 Compile the MTA configuration.

```
./imsimta cnbuild
```

4 Restart the MTA dispatcher.

```
imsimta restart dispatcher
```

This will cause use of the new compiled configuration (enabling Symantec Brightmail use) by the MTA’s (new) SMTP server processes.

▼ To Verify Messaging Server MTA

Use one of the following steps to verify that the Messaging Server MTA is functioning properly.

1 Run the `imsimta test -rewrite` command on a sample local user address. There should be no errors. For example:

```
# /opt/SUNWmsgsr/sbin/imsimta test -rewrite -debug=level=4 -filter user99@red.example.com
```

```
12:32:29.33: - passed.
12:32:29.33: - send_access mapping check:
l|postmaster@host1.red.example.com|ims-ms|user99@ims-ms-daemon
12:32:29.33: Mapping 4 applied to
|postmaster@host1.red.example.com|ims-ms|user99@ims-ms-daemon
12:32:29.33: Final result
"l|postmaster@host1.red.example.com|ims-ms|user99@ims-ms-daemon"
12:32:29.33: - passed.
12:32:29.33: - adding address user99@ims-ms-daemon to channel ims-ms
12:32:29.33: Closing URL context 1, new type = 7
12:32:29.33: - adding address user99@red.example.com to headers.
12:32:29.33: Copy estimate after address addition is 2
```

Expanded address:

user99@red.example.com

Submitted address list:

ims-ms

user99@ims-ms-daemon (orig

user99@red.example.com, inter

user99@red.example.com, host ims-ms-daemon)

NOTIFY-FAILURES *NOTIFY-DELAYS*

Submitted notifications list:

- 2 **Compose and send an email. Look at the Symantec Brightmail server logs under the `/var/log/brightmail` directory and verify that the `bmserver_logs` file contains information about this message.**

Note – You can also log in to the Control Center and check for statistics.

- 3 **If you set `SPAMFILTER1_OPTIONAL=-2` in the `option.dat` file, as previously explained, then you can check for warning `syslog` messages to verify the MTA/Symantec Brightmail operation.**
- 4 **If you set `LOG_FILTER=1` in the `option.dat` file, you can check that “expected” results are showing up in the filter field in `mail.log*` records. See [“Adding More Information to Message Transaction Records” on page 12](#) for more information.**

Adding More Information to Message Transaction Records

If you are currently logging message transactions (have the `logging` keyword enabled in your `imta.cnf` file), consider also setting `LOG_FILTER=1` in the `option.dat` file.

Note – If you enable “logging,” make sure that you have a method in place to manage the resulting log files. See Chapter 21, “Managing Logging,” in *Sun Java System Messaging Server 6 2005Q4 Administration Guide* for more information.

`LOG_FILTER=1` will cause inclusion of an additional field in the message transaction records in the `mail.log*` files that will record both other sorts of Sieve filter results, as well as Symantec Brightmail results applied to each message recipient. Exactly what will appear in the Symantec Brightmail result portion of this field depends upon what verdict or destination Symantec Brightmail returns, and how the MTA in turn is configured to react to that verdict or destination. But the general form will be:

`spamfiltern:encoded-string Sieve-action(s)-comma-separated`

where in general (when other forms of Sieve filtering are also in use) this is one part (also comma-separated) within the overall filter field. For instance, a message recipient with no general MTA Sieve, no applicable channel Sieve, no applicable domain Sieve, and no personal Sieve, but

where Symantec Brightmail returned a “null destination-data” result (normally configured to be interpreted as a request to discard the message, it having been determined to be spam), where here Symantec Brightmail is assumed to be configured as spam/virus filter package # 1, might show in the filter field as:

```
'spamfilter1:encoded-string , discard;'
```

Or, if Symantec Brightmail has been configured to return a “spam” destination-data (normally configured to be interpreted as a request to file the message to a “spam” folder), in the case of messages determined to be spam, then this might show in the filter field as:

```
'spamfilter1:encoded-string fileinto "spam";'
```

Configuring a Multi-node Symantec Brightmail and Messaging Server Deployment

On a multi-node Symantec Brightmail and Messaging Server installation—where the Symantec Brightmail server is running on one host and the Messaging Server MTA is running on a separate host—in addition to the previous steps, perform the following:

1. Copy the `libbmishareddata.so` file to the Scanner directory, for example:


```
cp libbmishareddata.so /opt/symantec/sbas/Scanner/lib
```
2. Make sure that the Symantec Brightmail Client is installed where your MTA exists.
3. Make sure that the `LD_LIBRARY_PATH` contains `/opt/symantec/sbas/Scanner`.

Using Control Center and Messaging Server MTA

You can use Control Center to manage your Symantec Brightmail scanners, but not the client component running with Messaging Server. Messaging Server is able to understand and act upon the potential responses that you can configure based on setting group policies. For example, you can delete spam for some users, but return it marked up for others. The two configurations, Brightmail and the Sun MTA, aren't “synchronized” in the sense that a change in one would automatically cause a (correct) change in the other. But the two configurations are configured to work in accord in a more manual sense.

Troubleshooting the Configuration

Use the following to troubleshoot problems with your configuration.

- If there is a problem in bringing up Symantec Brightmail server, check the Symantec Brightmail log file for errors. If the log file is not displaying errors, then there is a permission problem (write permission problem to the log file). If necessary, for troubleshooting problems, you can change the log level from the default of 4 to log level 7. Level 7 should be used for debugging only. Leaving the debug level at 7 at all times will decrease performance.

Modify the `bmi config.xml` file under the `/opt/symantec/sbas/Scanner/etc` directory to change the log level from the default value of 4 to 7. Also, modify the `bmi config_client.xml` file in the `/opt/symantec/sbas/Scanner` directory to change the log level from 4 to 7.

- If there is a problem with either Symantec Brightmail itself, or with the integration configuration, check the following:

If the global MTA option (that is, `option.dat option`) `SPAMFILTER n _OPTIONAL` is set to -2 or 2, then trouble getting a result back from the n th spam/virus filter package will result in a `syslog` notice, with `syslog` facility and severity controlled by the `SNDOPR_PRIORITY` global MTA option, with text of the general form:

```
SPAMFILTER $n$ , error-text
```

- When Symantec Brightmail is the spam/virus filter package, there is potentially additional information text. If Symantec Brightmail either error location or type information is also available, then the text takes the form:

```
SPAMFILTER $n$ , error-text [ - error-location ][ - error-type ]
```

where the square bracket characters shown above indicate the optional additional information and are not part of the actual output string. The *error-location* can be any of client, network, or server; the *error-type* can be any of memory, network, time-out, data, module down, type arg, or bad version.

In the case of Symantec Brightmail, the *error-text* always indicates the stage at which processing failed.

- Enable `MM_DEBUG` and `OS_DEBUG` parameters. For example, add the following lines to the `option.dat` file:

```
MM_DEBUG=8
OS_DEBUG=1
```

As with Brightmail and high levels of debugging, leaving this level of MTA debugging on is not intended for normal operation and performance once you have solved the problem. Only use this high level of MTA debugging while resolving a problem.

Further Reading

Refer to the Symantec Brightmail AntiSpam documentation at the following location:

http://www.symantec.com/techsupp/enterprise/products/sba/sba_60x/manuals.html

See the following information in the *Sun Java System Messaging Server 2005Q4 Administration Guide*:

- Chapter 14, “Integrating Spam and Virus Filtering Programs Into Messaging Server,” in *Sun Java System Messaging Server 6 2005Q4 Administration Guide*
- “Using Symantec Brightmail Anti-Spam” in *Sun Java System Messaging Server 6 2005Q4 Administration Guide*

Documentation, Support, and Training

The Sun web site provides information about the following additional resources:

- Documentation (<http://www.sun.com/documentation/>)
- Support (<http://www.sun.com/support/>)
- Training (<http://www.sun.com/training/>)

Third-Party Web Site References

Third-party URLs are referenced in this document and provide additional, related information.

Note – Sun is not responsible for the availability of third-party web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused or alleged to be caused by or in connection with use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. To share your comments, go to <http://docs.sun.com> and click Send Comments. In the online form, provide the full document title and part number. The part number is a 7-digit or 9-digit number that can be found on the book’s title page or in the document’s URL. For example, the part number of this book is 819-5195.

