Postfix and Dovecot Modifications

8 December, 2014

Introduction

Postfix and Dovecot have been modified to operate in a Multilevel Secure (MLS) environment. This document outlines details that system administrators need to know and describes the new configuration options introduced by these modifications.

Throughout, the name "PBFD-Postfix" will be used to indicate specifically this MLS-aware version of Postfix, to avoid confusion with unmodified, vanilla Postfix. Likewise for Dovecot.

This document assumes that a working DNS resolver is present and that the network's netrules and firewall are configured appropriately to allow the desired communication within the network.

PBFD-Postfix is based on Postfix 2.6.6.
PBFD-Dovecot is based on Dovecot 2.0.9.

General Functionality

Postfix is a mail transfer and delivery agent. It sends and receives mail, and delivers mail locally for storage. PBFD-Postfix will deliver mail into Maildir directories at the sensitivity label at which they were received. Mail will be stored in Maildir format. Maildir directories and subdirectories will be configured to store files across the label range SLSL:SHSL. Individual mail files will be stored at the label at which they were received, as specified by the banner line in the email. If no banner line is present, one will be injected reflecting the label of the connection by PBFD-Postfix.

Dovecot is an IMAP server. It reads mail inside of a Maildir directory and provides it to IMAP clients. PBFD-Dovecot will only deliver mail that a given IMAP client is cleared to read, governed by the label of its connection. For example, if the asg_mail_lookdown setting is enabled, IMAP clients will be allowed to read only mail AT or BELOW the label of their connection.

Note that because Maildir subdirectories can store mail at any label, the subdirectories will be visible to IMAP clients running at any label. However, because the mail files are stored with their own labels, only the expected individual mails will be visible. Users should avoid creating IMAP directories with sensitive names.

Installation Considerations

Installing and configuring PBFD-Postfix and PBFD-Dovecot should be similar to installing their vanilla versions. Full documentation for their configuration is provided by Red Hat. **This document assumes that the reader has read the relevant Red Hat documentation on Postfix and Dovecot**. Here we document some PitBull-specific considerations that administrators should be aware of in addition to the information provided by the vanilla projects.

To take advantage of PitBull's MLS filesystem features, use of the Maildir storage format is required. Both PBFD-Postfix and PBFD-Dovecot have been configured to use Maildir as their default storage mechanism. However, it's possible another mail delivery program has already created mbox storage files in </var/spool/mail>. It's especially common for system users like root to already have mail files. These must be deleted or converted to Maildir before PBFD-Postfix and PBFD-Dovecot can deliver and read mail locally.

Common Postfix (SMTP) errors if a user already has a non-Maildir storage in </var/spool/mail> are:

```
  postfix/local: status=bounced (maildir delivery failed: create
maildir file /var/spool/mail/user/tmp/1234: Not a directory)
```

Common Dovecot (IMAP) errors if a user already has a non-Maildir storage in </var/spool/mail> are:

```
[SERVERBUG] Internal error occured. Refer to server log for more
information.
```

```
imap(user): Error: stat(/var/spool/mail/issouser/dovecot/.INBOX)
failed:Not a directory
```

Users allowed to receive mail must belong to the "mail" group.

By default, mail will be stored in </var/spool/mail>, although this is configurable. The Maildir layout for a user looks like this:

```
/var/spool/mail/  -- Mail storage base directory, configurable
    user01/  -- Maildir directory for user01
        new/,tmp/,cur/  -- Actual mail storage locations,
                           described by Maildir standard
        dovecot/  -- Dovecot control and index
                     cache directory, partitioned directory
```

Both PBFD-Dovecot and PBFD-Postfix should be able to create missing Maildirs for users that belong to the "mail" group. No administrator intervention is required.

PBFD-Postfix provides a filter to verify or inject a banner line into mail. This filter will parse incoming and outgoing emails to ensure they contain a banner line at the top of the mail with a valid classification label that is AT or BELOW the label of the connection.

After processing, the mail will be treated by the mail system for storage and retransmission as if it were received from a connection AT the label given in the mail. This default filter is written in Python and provided at </usr/libexec/postfix/ASGfilter.py>.

This filter is implemented similar to the "Advanced content filter example" described by the Postfix documentation: <http://www.postfix.org/FILTER_README.html#advanced_filter>. By default it is configured to use ports 10025 and 10026. These ports are configurable in </etc/postfix/main.cf> and </etc/postfix/master.cf>. These ports are only accessed by the postfix daemon running on localhost, and they should not be accessible to users. Accessing port 10026 directly will circumvent the banner line filter. Disallowing shell access to users and configuring a firewall should be sufficient.

New Configuration Options

Several new configuration options are provided for administers to further refine the MLS behavior of PBFD-Dovecot and PBFD-Postfix.

Dovecot

asg_label_range: Colon-separated [low,high] label range across which to listen for and service connections. Lookdown will be capped by the lower bound of this range, if enabled. Default is "SLSL:SHSL". This should be specified in </etc/dovecot/dovecot.conf>.

asg_mail_lookdown: Enable or disable lookdown. Lookdown means a user can see emails that are AT or BELOW their connection's security label. If lookdown is disabled, users can only see mail AT the label of the connection. Default is "yes". This should be specified in </etc/dovecot/conf.d/10-mail.conf>.

Postfix

asg_label_range: Colon-separated [low,high] label range across which to listen for and service connections. Default is "SLSL:SHSL". This should be specified in </etc/postfix/main.cf>.