Whitepaper

Using LISTSERV® with Security-Enhanced Linux (SELinux)

January 13, 2011

Information in this document is subject to change without notice. Companies, names, and data used for example herein are fictitious unless otherwise noted. Some screen captures have been cropped and/or edited for emphasis or descriptive purposes.

L-Soft invites comments on its documentation. Please feel free to send your comments by email to: manuals@lsoft.com

Introduction

Security-Enhanced Linux (SELinux) is an increasingly popular addition to many Linux distributions. While it does contribute additional security mechanisms to LISTSERV's operating environment, it can also prevent LISTSERV from working without some additional configuration. This document will outline how to add custom SELinux rules to allow LISTSERV to operate correctly on a server with SELinux enabled.

Am I Using SELinux?

Some Linux distributions ship with SELinux enabled; others do not. Less experienced Linux administrators may not even be aware of whether or not their Linux distribution comes with SELinux enabled. To find out, check the /etc/selinux/config file. There should be a line like this:

```
SELINUX=enforcing
```

If the SELINUX variable is set to 'enforcing', then SELinux rules are being enforced on the server, and those rules probably need to be configured for LISTSERV. If the setting is 'permissive', then SELinux warnings are logged, but policies are not enforced. If the setting is 'disabled', then SELinux is disabled on the server.

If SELinux is in 'enforcing' mode, it's likely that the default policies will keep the LISTSERV Mail and Web Interfaces from working correctly. To fix that, we need to create special SELinux policies for LISTSERV.

Creating SELinux Policies for LISTSERV

There are usually two places where SELinux requires adjustment for LISTSERV to work properly – Inbound Mail and the Web Interface. Both LISTSERV's inbound mail processor (lsv_amin) and its web archive executable (wa) typically run with permissions 4755 and are owned by the 'listserv' user. SELinux needs to be told to allow those executables to run as that user.

The easiest way to create the necessary rules is to first allow the operations to fail, and then to check the audit logs on the system. The audit logs are typically in /var/log/audit/audit.log, but the location may vary depending on your logging configuration. Sending mail to the command address (LISTSERV@LISTSERV.EXAMPLE.ORG) should produce entries similar to the following in the audit log if the inbound mail is denied by the SELinux configuration:

```
type=AVC msg=audit(1274130421.913:65): avc:  denied  { signal } for  pid=4526
comm="lsv_amin" scontext=user_u:system_r:postfix_local_t:s0
tcontext=user_u:system_r:unconfined_t:s0 tclass=process
```

```
type=SYSCALL msg=audit(1274130421.913:65): arch=40000003 syscall=37 success=no
exit=-13 a0=1087 a1=a a2=9e4d518 a3=bff280cb items=0 ppid=4525 pid=4526
auid=500 uid=99 gid=99 euid=501 suid=501 fsuid=501 egid=99 sgid=99 fsgid=99
tty=(none) ses=2 comm="lsv_amin" exe="/usr/local/bin/lsv_amin"
subj=user_u:system_r:postfix_local_t:s0 key=(null)
```

Accessing the Web Interface at http://listserv.example.org/cgi-bin/wa may produce log errors similar to the following:

```
type=SYSCALL msg=audit(1274130658.383:66): arch=40000003 syscall=102
success=no exit=-13 a0=3 a1=bfd94be0 a2=0 a3=3 items=0 ppid=4560 pid=4601
```

```
auid=500 uid=48 gid=48 euid=501 suid=501 fsuid=501 egid=48 sgid=48 fsgid=48
tty=(none) ses=2 comm="wa" exe="/var/www/cgi-bin/wa"
subj=user_u:system_r:httpd_sys_script_t:s0 key=(null)
```

You can collect these log failures into a separate log file to use to create new SELinux policy exceptions:

```
# grep lsv_amin /var/log/audit/audit.log >> /tmp/listserv-policy.log
```

```
# grep /var/www/cgi-bin/wa /var/log/audit/audit.log >> /tmp/listserv-
policy.log
```

Creating SELinux Policy Files

Now that we've collected the audit log failures for lsv_amin and wa, we need to tell SELinux to permit those operations. First, create the policy:

```
# audit2allow -M listserv < /tmp/listserv-audit.log
```

```
******************** IMPORTANT ***********************
To make this policy package active, execute:
semodule -i listserv.pp
and then make the policy active:
# semodule -i listserv.pp
```

Then, test the failing operation again. If it still fails, check the audit log again. It may be that the first blocked operation was permitted, but a follow-up operation failed. If so, then grep the audit log again, run audit2allow a second time, and activate the new (revised) module with the semodule command. Since SELinux performs several different tests in sequence, it may be necessary to run audit2allow multiple times to create all of the necessary exceptions.

References

SELinux: http://www.nsa.gov/research/selinux/index.shtml

CentOS SELinux HowTo Page: http://wiki.centos.org/HowTos/SELinux

LISTSERV for UNIX installation Guide: http://www.lsoft.com/resources/manuals.asp