4.2.3 Ensure rsyslog or syslog-ng is installed (Scored)

Profile Applicability

```
Level 1 - Server
Level 1 - Workstation
```

Description

The `rsyslog` and `syslog-ng` software are recommended replacements to the original `syslogd` daemon which provide improvements over `syslogd`, such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server.

Rationale

The security enhancements of `rsyslog` and `syslog-ng` such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server) justify installing and configuring the package.

Audit

Verify either rsyslog or syslog-ng is installed. Depending on the package management in use one of the following command groups may provide the needed information:

```
# rpm -q rsyslog
# rpm -q syslog-ng
```

Remediation

Install `rsyslog` or `syslog-ng` using one of the following commands:

```
# yum install rsyslog
# yum install syslog-ng
```

Notes

The syslog-ng package requires the EPEL7 and Optional repositories be enabled. See https://czanik.blogs.balabit.com/2015/09/installing-syslog-ng-ose-3-7-1-on-rhel6-and-centos6/ for more information.