1.1.11 Ensure separate partition exists for /var/log/audit (Scored)

Profile Applicability

```
Level 2 - Server
Level 2 - Workstation
```

Description

The auditing daemon, `auditd`, stores log data in the `/var/log/audit` directory.

Rationale

There are two important reasons to ensure that data gathered by `auditd` is stored on a separate partition: protection against resource exhaustion (since the `audit.log` file can grow quite large) and protection of audit data. The audit daemon calculates how much free space is left and performs actions based on the results. If other processes (such as `syslog`) consume space in the same partition as `auditd`, it may not perform as desired.

Audit

Run the following command and verify output shows `/var/log/audit` is mounted:

```
# mount | grep /var/log/audit
/dev/xvdi1 on /var/log/audit type ext4 (rw,relatime,data=ordered)
```

Remediation

For new installations, during installation create a custom partition setup and specify a separate partition for `/var/log/audit`. For systems that were previously installed, create a new partition and configure `/etc/fstab` as appropriate.

Impact

Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may

prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

References

AJ Lewis, “LVM HOWTO”, http://tldp.org/HOWTO/LVM-HOWTO/