1.1.10 Ensure separate partition exists for /var/log (Scored)

Profile Applicability

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

Description

The `/var/log` directory is used by system services to store log data .

Rationale

There are two important reasons to ensure that system logs are stored on a separate partition: protection against resource exhaustion (since logs can grow quite large) and protection of audit data.

Audit

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

```
# mount | grep /var/log
/dev/xvdh1 on /var/log 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`.
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/