

1.1 Filesystem Configuration

List of content

- 1.1.1 Disable unused filesystems
 - 1.1.1.1 Ensure mounting of cramfs filesystems is disabled (Scored)
 - 1.1.1.2 Ensure mounting of freevxfs filesystems is disabled (Scored)
 - 1.1.1.3 Ensure mounting of jffs2 filesystems is disabled (Scored)
 - 1.1.1.4 Ensure mounting of hfs filesystems is disabled (Scored)
 - 1.1.1.5 Ensure mounting of hfsplus filesystems is disabled (Scored)
 - 1.1.1.6 Ensure mounting of squashfs filesystems is disabled (Scored)
 - 1.1.1.7 Ensure mounting of udf filesystems is disabled (Scored)
 - 1.1.1.8 Ensure mounting of FAT filesystems is disabled (Scored)
- 1.1.2 Ensure separate partition exists for /tmp (Scored)
- 1.1.3 Ensure nodev option set on /tmp partition (Scored)
- 1.1.4 Ensure nosuid option set on /tmp partition (Scored)
- 1.1.5 Ensure noexec option set on /tmp partition (Scored)
- 1.1.6 Ensure separate partition exists for /var (Scored)
- 1.1.7 Ensure separate partition exists for /var/tmp (Scored)
- 1.1.8 Ensure nodev option set on /var/tmp partition (Scored)
- 1.1.9 Ensure nosuid option set on /var/tmp partition (Scored)
- 1.1.10 Ensure noexec option set on /var/tmp partition (Scored)
- 1.1.11 Ensure separate partition exists for /var/log (Scored)
- 1.1.12 Ensure separate partition exists for /var/log/audit (Scored)
- 1.1.13 Ensure separate partition exists for /home (Scored)
- 1.1.14 Ensure nodev option set on /home partition (Scored)
- 1.1.15 Ensure nodev option set on /dev/shm partition (Scored)
- 1.1.16 Ensure nosuid option set on /dev/shm partition (Scored)
- 1.1.17 Ensure noexec option set on /dev/shm partition (Scored)
- 1.1.18 Ensure nodev option set on removable media partitions (Not Scored)
- 1.1.19 Ensure nosuid option set on removable media partitions (Not Scored)
- 1.1.20 Ensure noexec option set on removable media partitions (Not Scored)
- 1.1.21 Ensure sticky bit is set on all world-writable directories (Scored)
- 1.1.22 Disable Automounting (Scored)

Description

Directories that are used for system-wide functions can be further protected by placing them on separate partitions. This provides protection for resource exhaustion and enables the use of mounting options that are applicable to the directory's intended use. Users' data can be stored on separate partitions and have stricter mount options. A user partition is a filesystem that has been established for use by the users and does not contain software for system operations.

The recommendations in this section are easier to perform during initial system installation. If the system is already installed, it is recommended that a full backup be performed before repartitioning the system.

Notes

If you are repartitioning a system that has already been installed, make sure the data has been copied over to the new partition, unmount it and then remove the data from the directory that was in the old partition. Otherwise it will still consume space in the old partition that will be masked when the new filesystem is mounted. For example, if a system is in single-user mode with no filesystems mounted and the administrator adds a lot of data to the /tmp directory, this data will still consume space in / once the /tmp filesystem is mounted unless it is removed first.

From:

<https://secscan.acron.pl/> - **SecScan**

Permanent link:

<https://secscan.acron.pl/centos7/1/1>

Last update: **2017/05/06 14:26**

