文件系统的 nodev 挂载选项有什么用?

nodev挂载选项有什么用?

一些安全策略会要求，除了根目录(/)，其他目录如果挂载了单独的分区，应该添加 nodev 挂载选项。
所以 nodev 有什么用呢？ mount 的 man 手册如此解释：

nodev Do not interpret character or block special devices on the file system.
好吧，看完我还是没理解这个选项到底是干嘛的。网上搜索到了几个回答[2][3]。如果在挂载时，添加了nodev选项，那么系统不会把该文件系统里面的 block/character 文件当作是 block/character 文件来处理。

举个例子，一位别有用心的用户，在他有权限的机器上（比如他的笔记本），在U盘上创建了一个 block 文件，指向 sd* 之类的数据盘，这么巧他有权限把U盘插到服务器上，这么巧服务器自动挂载了这个U盘且没有 nodev 挂载选项，那么这位用户就能通过这个 block 文件读取到服务器上相应磁盘的数据。

验证nodev挂载选项

1. 在系统上，使用 root 用户，验证通过 mknod 创建的 block 文件能够访问相应 block 的数据。

光盘 sr0 的 major,minor 号是 11,0
[root@build ~]# ls -l /dev/sr0
brw-rw----. 1 root cdrom 11, 0 Sep 11 14:15 /dev/sr0

在 /tmp 创建一个伪 sr0 设备
[root@build tmp]# mknod new-sr0 b 11 0

从正常sr0设备和伪sr0设备中提取相同数量的数据
[root@build tmp]# dd if=/tmp/new-sr0 of=/tmp/new_one bs=20M count=1
[root@build tmp]# dd if=/dev/sr0 of=/tmp/ori_one bs=20M count=1

MD5 值是一样的
[root@build tmp]# md5sum /tmp/new_one
30e67ca36a3cb120c88a18587570bac6 /tmp/new_one
[root@build tmp]# md5sum /tmp/ori_one
30e67ca36a3cb120c88a18587570bac6 /tmp/ori_one
</pre>
2. 正常情况下，普通用户是无法调用 mknod 命令的。所以不外挂文件系统（比如U盘）的话，没有 nodev 还比较安全。

[feichashao@build tmp]$ mknod new-sr0 b 11 0
mknod: ‘new-sr0’: Operation not permitted
3. 比较有 nodev 挂载选项和没有 nodev 挂载选项的效果。可以看到，加上 nodev 挂载选项之后，尽管这个文件系统存在 block 文件，但也无法从中提取中数据，从而保障了数据安全。

不添加nodev挂载选项的情况：

创建一个 ext4 文件系统用于挂载
[root@build tmp]# dd if=/dev/zero of=/tmp/diskfile bs=10M count=10
[root@build tmp]# mkfs.ext4 /tmp/diskfile

使用默认的挂载选项，挂载该文件系统到 /testdir/
[root@build tmp]# mount -o loop /tmp/diskfile /testdir/

在这个文件系统中，创建伪sr0文件
[root@build tmp]# mknod /testdir/new-sr0 b 11 0
[root@build tmp]# ls -l /testdir/new-sr0
brw-r--r--. 1 root root 11, 0 Sep 21 20:31 /testdir/new-sr0

能够从中读取数据
[root@build tmp]# dd if=/testdir/new-sr0 of=/tmp/new_one bs=20M count=1
[root@build tmp]# md5sum /tmp/new_one

30e67ca36a3cb120c88a18587570bac6 /tmp/new_one

[root@build tmp]# umount /testdir/
添加nodev挂载选项的情况：

使用 nodev 挂载选项挂载同一文件系统
[root@build tmp]# mount -o loop,nodev /tmp/diskfile /testdir/

无法从伪sr0中读取数据
[root@build tmp]# dd if=/testdir/new-sr0 of=/tmp/new_one bs=20M count=1
dd: failed to open ‘/testdir/new-sr0’: Permission denied

参考资料

[1] https://access.redhat.com/solutions/60728
[2] https://superuser.com/questions/538550/understanding-mount-option-nodev-and-its-use-with-usb-flash-drives
[3] https://serverfault.com/questions/547237/explanation-of-nodev-and-nosuid-in-fstab