Restoring a file system on a Nebula instance that has gone read-only

How to restore a read-only file system

- Reboot the instance
- Log into the instance as root
- Run fsck
- Reboot the instance

Why does it happen?

The default behavior on many Linux operating systems is to set a file system to read-only if critical information can't be written to disk. If this happens the file system is corrupt and fsck has to be run to fix it. The default behavior can be changed but it is not advisable. If it is changed to "continue" errors can accumulate and corrupt the file system. If it is changed to "panic" the system will halt and fsck will need to be run on the file system before it can be restarted.

How can I detect when the file system has been changed to read-only?

The following command can be run to find read-only file systems in your instance.

```
grep "\sro[\s,]" /proc/mounts
```

Details

Reboot the instance through the OpenStack Horizon dashboard.

Browse to the Nebula dashboard at nebula.ncsa.illinois.edu.

In the drop-down "Actions" menu to the right of your instance select "Hard Reboot Instance". A soft reboot tries to shut down the instance gracefully and normally would be preferable to a hard reboot, which halts the instance immediately. However, in this case, the soft reboot will try shutting down services and writing to disk and at this point the disk is read-only.

Confirm the instance has rebooted.

Logging in as root

To log in as root you must previously have set a password for root in the instance.

Browse to the Nebula dashboard at nebula.ncsa.illinois.edu.

In the drop-down "Actions" menu to the right of your instance select "Console".

You will be given a login prompt.

Running fsck

There is no guaranteed way to restore an instance with disk corruption. Good backups are the only way to avoid losing data.

The `fsck` command can recover your disk partition but there is no guarantee that it will work correctly. The `fsck` operation can occasionally cause data corruption on active disks. For this reason, the `fsck` procedure should only be performed on unmounted or read-only file systems to minimize this risk. Problems can still occur in cases of severe damage.

Use the "mount" command to verify the file system you wish to fix is read-only.

```
/dev/vdb1 on /tmp/newdir type ext4 (ro,relatime,seclabel,data=ordered)
```

Run fsck on the file device you wish to check.

```
fsck /dev/vdb1
```

Normally, the file system is consistent, and the fsck command merely reports on the number of files, used blocks, and free blocks in the file system. If the file system is inconsistent, the fsck command displays information about the inconsistencies found and prompts you for permission to repair them.

After fsck has been run it is important to check the `/lost+found` directory in the checked file system. This is where fsck puts partially recovered files. Sometimes, fsck is able to recover file data, but it cannot find a reference to the file on the filesystem.When this happens, fsck places the files in the `/lost+found` directory so that you can manually try to figure out what the file is. If there are files in this directory check to see if you can identify them. Often these are files that were previously deleted but were still being used when the system crashed. It is worth checking them though to be sure.

Contact "nebula@ncsa.illinois.edu" with any questions.