LTTng-modules - Bug #1280

_IOR should be _IOW for a few commands in lttng-modules ABI

08/11/2020 04:14 PM - Mathieu Desnoyers

Status:	New	**Start date:**	08/11/2020
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			

Description

Recently added commands are passing data from user-space to the kernel. According to Documentation/userspace-api/ioctl/ioctl-number.rst, this means:

```
    _IO    an ioctl with no parameters
    _IOW   an ioctl with write parameters (copy_from_user)
    _IOR   an ioctl with read parameters  (copy_to_user)
    _IOWR  an ioctl with both write and read parameters.
```

those should use _IOW, rather than _IOR. A quick review comes up with this list of offenders:

- LTTNG_KERNEL_SESSION_SET_NAME
- LTTNG_KERNEL_SESSION_SET_CREATION_TIME
- LTTNG_KERNEL_SESSION_TRACK_ID
- LTTNG_KERNEL_SESSION_UNTRACK_ID
- LTTNG_KERNEL_SESSION_LIST_TRACKER_IDS

Another weird one is this:

- LTTNG_KERNEL_SESSION_TRACK_PID
- LTTNG_KERNEL_SESSION_UNTRACK_PID

Which takes a int32_t as _IOR, which it receives by directly casting the argument as int32_t, rather than using it as a pointer as we could expect.

Fixing this without introducing an ABI break is non-trivial, because changing _IOR to _IOW really changes the ioctl number AFAIU. So we need to be smart about fixing this without introducing an ABI break.