author	Liu Shixin <liushixin2@huawei.com>	2022-11-03 16:33:01 +0800
committer	Greg Kroah-Hartman <gregkh@linuxfoundation.org>	2022-11-16 09:58:27 +0100
commit	c9fe4719c662e0af17eea723cf345e37719fd3c9 (patch)	
tree	eb8d22ca28d5b31956a3537a5d78c79a3c43d135	
parent	f96fd36936310cefe0ea1370a9ae30e6746e6f62 (diff)	
download	linux-c9fe4719c662e0af17eea723cf345e37719fd3c9.tar.gz	

diff options

context: 3

space: include

mode: unified

btrfs: fix match incorrectly in dev_args_match_device

```
commit 0fca385d6ebc3cabb20f67bcf8a71f1448bdc001 upstream.

syzkaller found a failed assertion:

  assertion failed: (args->devid != (u64)-1) || args->missing, in fs/btrfs/volumes.c:6921

This can be triggered when we set devid to (u64)-1 by ioctl. In this
case, the match of devid will be skipped and the match of device may
succeed incorrectly.

Patch 562d7b1512f7 introduced this function which is used to match device.
This function contains two matching scenarios, we can distinguish them by
checking the value of args->missing rather than check whether args->devid
and args->uuid is default value.

Reported-by: syzbot+031687116258450f9853@syzkaller.appspotmail.com
Fixes: 562d7b1512f7 ("btrfs: handle device lookup with btrfs_dev_lookup_args")
CC: stable@vger.kernel.org # 5.16+
Reviewed-by: Nikolay Borisov <nborisov@suse.com>
Signed-off-by: Liu Shixin <liushixin2@huawei.com>
Signed-off-by: David Sterba <dsterba@suse.com>
Signed-off-by: Greg Kroah-Hartman <gregkh@linuxfoundation.org>
```

Diffstat

-rw-r--r-- fs/btrfs/volumes.c 16

1 files changed, 8 insertions, 8 deletions

```
diff --git a/fs/btrfs/volumes.c b/fs/btrfs/volumes.c
index 0f22d91e239273..b8d5d341b5810d 100644
--- a/fs/btrfs/volumes.c
+++ b/fs/btrfs/volumes.c
@@ -6841,18 +6841,18 @@ static bool dev_args_match_fs_devices(const struct btrfs_dev_lookup_args *args,
 static bool dev_args_match_device(const struct btrfs_dev_lookup_args *args,
                                   const struct btrfs_device *device)
 {
-       ASSERT((args->devid != (u64)-1) || args->missing);
+       if (args->missing) {
+               if (test_bit(BTRFS_DEV_STATE_IN_FS_METADATA, &device->dev_state) &&
+                   !device->bdev)
+                       return true;
+               return false;
+       }

-       if ((args->devid != (u64)-1) && device->devid != args->devid)
+       if (device->devid != args->devid)
```

```
                return false;
        if (args->uuid && memcmp(device->uuid, args->uuid, BTRFS_UUID_SIZE) != 0)
                return false;
-       if (!args->missing)
-               return true;
-       if (test_bit(BTRFS_DEV_STATE_IN_FS_METADATA, &device->dev_state) &&
-           !device->bdev)
-               return true;
-       return false;
+       return true;
 }

 /*
```