the disk at a time when all the data is written to the disk, meanwhile the superblock information on the cache will be flashed to the disk.

2.7 Process for recovering data

The system is restarted after power is restored, then make a decision whether or not to write data by reading the flag of the superblock in the partition of system disk. The data recovery process should be started if the flag means the system is powered off. Firstly, the description information of the page is read, which keeps a record of which position on the disk the corresponding data block should be written to; Secondly, the page offset is calculated according to the index of the descriptor. In order to search the corresponding file pointer for writing, a linked list should be saved, which records the correspondence between the block device and the file, because there are more than one back-end disk will be written. Thirdly, the corresponding page data is read form system partition, then the data will be written to the specified position on the JBOD according to the device number of the descriptor and the index on the block device. Finally, when all the page data is flushed into the back-end JBOD, the flag of the superblock is cleared and another flag is set, which indicates the recovering is finished. A kind of transformation is mainly performed here, the block address on partition will be transformed into the one in the back-end JBOD. The process of writing data to the back-end JBOD is illustrated in figure 7.

3 System test

What's important is that the data in the cache can be stably and reliably protected in the case of power break by applying cache power-down protection, meanwhile, the data was stably and accurately recovered after the power is restored. Therefore, test was as follows.

The hardware configuration of the test system was as follows.

Controller: CPU: E5620 *2; memory: 16GB; system disk: 500GB; JBOD: 500GJ; SAS card: LSI 3801E; network card: gigabit NIC; UPS: Delta GES-N7K.

Client-server: CPU: E5504; memory: 6GB; network card: gigabit NIC; operating system: Redhat Enterprise 5.4 x86_64; services protocol: iscsi.

After copying all the different size of data from or to the disk, which mapped from the ISCSI device (first check the MD5 value of the source data), we removed Commercial power immediately. The data was written to the specified partition on the system disk by the power-down protection module, till the commercial power was recovered. We verified the MD5 value of the recovered data and compared it with the one of the source data. The result of the experiment is shown in Table 1. From Table 1, we can see the cache data at the controller can be well protected by the cache power-down protection module in the case of power break, and the MD5 value of the recovered data is equal to the one of the source data. Therefore, the consistency of the data can be ensured.

Table 1 the result of the test

items	size	The MD5 of source data	The MD5 of data removed
1	4K	620f0b67a91f7f74151bc5be745b7110	620f0b67a91f7f74151bc5be745b7110
2	4M	b5cfa9d6c8febd618f91ac2843d50a1c	b5cfa9d6c8febd618f91ac2843d50a1c
3	40M	ec8bb3b24d5b0f1b5bdf8c8f0f541ee6	ec8bb3b24d5b0f1b5bdf8c8f0f541ee6
4	400M	61eabaf2bf278703738b433ff884c91f	61eabaf2bf278703738b433ff884c91f
5	4000M	ffe3915bd77fde9dd5dc8077ced09c10	ffe3915bd77fde9dd5dc8077ced09c10

4. Conclusion

In this paper, a technical solution based on UPS cache power-down protection is proposed and implemented to solve the problem that the cache data at the controller will be lost in the case of power break. The result indicates that the cache data can be stably and reliably protected by the cache power-down protection in the case of power break, and the recovered data is same to the source data. It is meaningful for this cache power-down protection to improve the reliability and the availability of the storage service.