Checking whether Auditing is Enabled

Describes how to verify whether auditing is enabled for a directory, file, or stream.

When you enable the auditing of a particular directory, file, table, or stream, you set the *audit bit* to "on" that object. You can tell whether auditing is enabled for a directory, file, or table by checking the status of the object's audit bit.

For example,the volume, as shown in the first tree diagram below, consists of the root directory, the two directories `dir1` and `dir2` , and two files in directory `dir1` . Every directory, file, table, and stream in a volume has an "audit bit" associated with it. You can tell whether, say, `dir1` has its audit bit on and is therefore enabled for auditing by running the `hadoop mfs -ls` command. The output of the command might look like this:

```
drwxrwxrwx Z U U 3 root root 100 2015-05-20 21:09 192473738 /dir1
```

The second `U` indicates that auditing is not enabled on the directory.

However, an `A` in place of that `U` indicates that auditing is enabled on the directory:

```
drwxrwxrwx Z U A 3 root root 100 2015-05-20 23:41 192473738 /dir1
```

In the first diagram, as well as in the next two diagrams, `U` indicates that the audit bit is turned off for a filesystem object and `A` indicates that the audit bit is on for that object. After you run `maprcli volume audit` on the volume, none of the audit bits are on:

```
/              U
-/dir1          U
 -file1         U
 -file2         U
-/dir2          U
```

Suppose you enable auditing on the root directory by running this command:

```
hadoop mfs -setaudit on /
```

Then, you create the file `file3` in `dir2` and you create the directory `dir3` and the file `file4` in it. The tree diagram now looks like this:

```
/           A
-/dir1          U
 -file1         U
 -file2         U
-/dir2          U
 -file3         U
-/dir3          A
 -file4         A
```

The audit bit is still `U` on `dir1` , the files in `dir1` , and `dir2` . The new file `file3` in `dir2` inherits the audit bit from `dir2` .

`dir3` inherits the audit bit from the root folder, so the audit bit for `dir3` is `A` . Moreover, `file4` inherits the audit bit from `dir3` , so its audit bit is `A` , as well.

Next, you run this command to enable auditing in `dir1` :

```
hadoop mfs -setaudit on /dir1
```

Then, you create the file `file5` . The new file inherits the audit bit from its parent folder, so it is enabled for auditing immediately upon being created. However, `file1` and `file2` still have the audit bit turned off.

```
/         A
-/dir1          A
 -file1         U
 -file2         U
 -file5         A
-/dir2          U
 -file3         U
-/dir3          A
 -file4         A
```

Because file1 and file2 existed before you turned on the audit bit for their parent folder, you need to enable auditing for them like this:

```
hadoop mfs -setaudit on /dir1/file1
```

```
hadoop mfs -setaudit on /dir1/file2
```