

# Linux – Securing your important files with XFS extendend attributes

Article Number: 327 | Rating: Unrated | Last Updated: Wed, Jul 25, 2018 1:44 PM

Let's say, the tnsnames.ora is a quite important file on your system, and you want to make sure that you notice when someone changes the file. Taking a look at the modification time of that file would be good idea, or not?

Per default, the `ls -l` command show only the (mtime) modification time. In my case, I know that the tnsnames.ora was changed on “Feb 9 11:24”.

```
1
2
oracle@dbidg03:/u01/app/oracle/network/admin/
[rdbsms112] ls -l tnsnames.ora

-rw-r--r-- 1 oracle oinstall 1791 Feb  9 11:24
tnsnames.ora
```

But in reality, more time stamps are stored. The atime, the ctime and the mtime.

- atime is the access time (only stored in filesystem is not mounted with the noatime option)
- ctime is the change time, meaning the inode was change, e.g. with the chmod command
- mtime is the modification time, meaning the content changed

The ctime is often misinterpreted as “creation time”, but this is not the case. The creation time of a file is not recorded with XFS. There are other file systems that can do it, like ZFS, but XFS does not support “creation time”. You can use the stat command to see all time stamps in one shot.

---

```
1
2 oracle@dbidg03:/u01/app/oracle/network/admin/
3 [rdbms112] stat tnsnames.ora
4
5 File: 'tnsnames.ora'
6
7 Size: 2137      Blocks: 8      IO Block: 4096
8 regular file
9
10 Device: fb02h/64258d  Inode: 163094097  Links:
11 1
12
13 Access: (0644/-rw-r--r--)  Uid: (54321/ oracle)
14 Gid: (54321/oinstall)
15
16 Access: 2017-02-09 11:24:00.243281419 +0100
17
18 Modify: 2017-02-09 11:24:00.243281419 +0100
19
20 Change: 2017-02-09 11:24:00.254281404 +0100
21
22 Birth: -
```

Ok. Now someone comes along and changes the tnsnames.ora

```
1
2 oracle@dbidg03:/u01/app/oracle/network/admin/
3 [rdbms112] vi tnsnames.ora
```

A change was done, and the modification time of that file changed immediately.

```
1 oracle@dbidg03:/u01/app/oracle/network/admin/  
2 [rdbms112] ls -l tnsnames.ora  
  
-rw-r--r-- 1 oracle oinstall 2136 Feb  9 11:31  
tnsnames.ora
```

And also other timestamps might have changed like the atime and ctime.

```
1 oracle@dbidg03:/u01/app/oracle/network/admin/  
2 [rdbms112] stat tnsnames.ora  
  
3 File: 'tnsnames.ora'  
  
4 Size: 2136      Blocks: 8      IO Block: 4096  
regular file  
  
5 Device: fb02h/64258d  Inode: 161521017  Links:  
6 1  
  
7 Access: (0644/-rw-r--r--)  Uid: (54321/ oracle)  
Gid: (54321/oinstall)  
  
8 Access: 2017-02-09 11:31:06.733673663 +0100  
  
9 Modify: 2017-02-09 11:31:06.733673663 +0100  
  
Change: 2017-02-09 11:31:06.738673656 +0100  
  
Birth: -
```

Cool, now I know that the file was changed at “Feb 9 11:31”. But how reliable is that information? With the touch command, I can easily change the modification time to any value I like. e.g. I can set it to the same date as beforehand.

```
1
2 oracle@dbidg03:/u01/app/oracle/network/admin/
3 [rdbms112] touch -m --date="Feb 9 11:24"
4 tnsnames.ora
5
6 oracle@dbidg03:/u01/app/oracle/network/admin/
7 [rdbms112] ls -l tnsnames.ora
8
9 -rw-r--r-- 1 oracle oinstall 2136 Feb 9 11:24
10 tnsnames.ora
```

Now I have set the modification time to almost the same value, as it was beforehand. (Almost, because the microseconds are different) Besides that, the access and the change time are different.

```
1
2 oracle@dbidg03:/u01/app/oracle/network/admin/
3 [rdbms112] stat tnsnames.ora
4
5 File: 'tnsnames.ora'
6
7 Size: 2136      Blocks: 8      IO Block: 4096
8 regular file
9
10 Device: fb02h/64258d  Inode: 161521017  Links:
11 1
12
13 Access: (0644/-rw-r--r--)  Uid: (54321/ oracle)
14 Gid: (54321/oinstall)
```

```
8 Access: 2017-02-09 11:31:06.733673663 +0100
9 Modify: 2017-02-09 11:24:00.000000000 +0100
Change: 2017-02-09 11:36:51.631671612 +0100
Birth: -
```

No problem, I can make it even more precise by specifying the whole date format including microseconds and time zone.

```
1 oracle@dbidg03:/u01/app/oracle/network/admin/
2 [rdbms112] touch -m --date="2017-02-09
3 11:24:00.243281419 +0100" tnsnames.ora
4
5 oracle@dbidg03:/u01/app/oracle/network/admin/
6 [rdbms112] stat tnsnames.ora
7
8 File: 'tnsnames.ora'
9
10 Size: 2136      Blocks: 8      IO Block: 4096
11 regular file
12
13 Device: fb02h/64258d Inode: 161521017 Links:
14 1
15
16 Access: (0644/-rw-r--r--) Uid: (54321/ oracle)
17 Gid: (54321/oinstall)
18
19 Access: 2017-02-09 11:31:06.733673663 +0100
```

Modify: 2017-02-09 11:24:00.243281419 +0100

Change: 2017-02-09 11:39:41.775993054 +0100

Birth: -

And if I want to, I can even change the access time.

```
1
2 oracle@dbidg03:/u01/app/oracle/network/admin/
3 [rdbms112] touch -a --date="2017-02-09
4 11:24:00.243281419 +0100" tnsnames.ora
5
6 oracle@dbidg03:/u01/app/oracle/network/admin/
7 [rdbms112] stat tnsnames.ora
8
9 File: 'tnsnames.ora'
10
11 Size: 2136      Blocks: 8      IO Block: 4096
regular file
Device: fb02h/64258d  Inode: 161521017  Links:
1
Access: (0644/-rw-r--r--)  Uid: (54321/ oracle)
Gid: (54321/oinstall)
Access: 2017-02-09 11:24:00.243281419 +0100
Modify: 2017-02-09 11:24:00.243281419 +0100
Change: 2017-02-09 11:42:22.935350329 +0100
```

Birth: -

Only the ctime (change time) is not so easy to change. At least not with the touch command. For changing the ctime you need to invoke the file system debugger or stuff like that. In the end, monitoring my tnsnames.ora file changes by time is not so precise. So why not using the XFS extend attribute feature to help me. e.g. I could create md5 check sums and when the check sum differs, I know that the content was changed. Let's do it with the root user.

```
1
2
3
4
5
6
7
8
9
10
11
12
13
```

```
As root:

[root@dbidg03 admin]# getfattr -d tnsnames.ora

[root@dbidg03 admin]#

[root@dbidg03 admin]# md5sum tnsnames.ora
d135c0ebf51f68feda895dac8631a999 tnsnames.ora

[root@dbidg03 admin]# setfattr -n user.md5sum -v
d135c0ebf51f68feda895dac8631a999 tnsnames.ora

[root@dbidg03 admin]#

[root@dbidg03 admin]# getfattr -d tnsnames.ora

# file: tnsnames.ora
```

```
user.md5sum="d135c0ebf51f68feda895dac8631a999"
```

But this is also not so secure. Even if done with root, it can easily be removed by the oracle user.

```
1
2
3
4
5
6
oracle@dbidg03:/u01/app/oracle/network/admin/
[rdbms112] getfattr -d tnsnames.ora

# file: tnsnames.ora

user.md5sum="d135c0ebf51f68feda895dac8631a999"

oracle@dbidg03:/u01/app/oracle/network/admin/
[rdbms112] setfattr -x user.md5sum tnsnames.ora

oracle@dbidg03:/u01/app/oracle/network/admin/
[rdbms112] getfattr -d tnsnames.ora
```

To overcome this issue, XFS uses 2 disjoint attribute name spaces associated with every filesystem object. They are the root (or trusted) and user address spaces. The root address space is accessible only to the superuser, and then only by specifying a flag argument to the function call. Other users (like the oracle user in my case) will not see or be able to modify attributes in the root address space. The user address space is protected by the normal file permissions mechanism, so the owner of the file can decide who is able to see and/or modify the value of attributes on any particular file.

Ok. So let's do it again by using the root (trusted) address space.



```
2 [root@dbidg03 admin]# setfattr -n
trusted.md5sumtime -v "09.02.2018 13:00:00"
3 tnsnames.ora

4 [root@dbidg03 admin]# getfattr -n
trusted.md5sumtime tnsnames.ora

5
6 # file: tnsnames.ora
7
8 trusted.md5sumtime="09.02.2018 13:00:00"

9
10 [root@dbidg03 admin]# getfattr -n trusted.md5sum
tnsnames.ora

11
12 # file: tnsnames.ora

13
14 trusted.md5sum="d135c0ebf51f68feda895dac8631
15 a999"
```

Now you have a good chance to find out if the file content was changed or not, by simply checking if the file has a different check sum.

## Conclusion

XFS extended attributes are quite powerful features and you can use them in a lot of scenarios. Take care that you have a backup solution that support extended attributes, else you will lose all the information once you restore your data.

Posted - Wed, Jul 25, 2018 1:44 PM. This article has been viewed 8246 times.

Online URL: <http://kb.ictbanking.net/article.php?id=327>