The Nautilus security team performed an audit on all servers present in Stratos DC. During the audit some critical data/files were identified which were having the wrong permissions as per security standards. Once the report was shared with the production support team, they started fixing the issues one by one. It has been identified that one of the files named /etc/hosts on Nautilus App 2 server has wrong permissions, so that needs to be fixed and the correct ACLs needs to be set.

1. The user owner and group owner of the file should be root user.  
  
2. Others must have read only permissions on the file.  
  
3. User kareem must not have any permission on the file.  
  
4. User garrett should have read only permission on the file.

[root@stapp02 etc]# id kareem

uid=1002(kareem) gid=1002(kareem) groups=1002(kareem)

[root@stapp02 etc]# id garrett

uid=1003(garrett) gid=1003(garrett) groups=1003(garrett)

[root@stapp02 etc]# cat /etc/passwd | grep kareem

kareem:x:1002:1002::/home/kareem:/bin/bash

[root@stapp02 etc]# cat hosts

127.0.0.1 localhost

::1 localhost ip6-localhost ip6-loopback

fe00::0 ip6-localnet

ff00::0 ip6-mcastprefix

ff02::1 ip6-allnodes

ff02::2 ip6-allrouters

172.16.238.10 stapp01

172.16.238.11 stapp02

172.16.238.12 stapp03

172.16.238.11 stapp02.stratos.xfusioncorp.com stapp02

172.16.239.5 stapp02.stratos.xfusioncorp.com stapp02

172.17.0.5 stapp02.stratos.xfusioncorp.com stapp02

[root@stapp02 etc]# setfacl -x u:kareem hosts.txt

setfacl: hosts.txt: No such file or directory

[root@stapp02 etc]# setfacl -x u:kareem hosts [ As per requirement not correct the command for kareem, the command is only while removing the current file permision]

[root@stapp02 etc]# setfacl -m u:garrett:r hosts [ user garrett only read condition]

[root@stapp02 etc]# setfacl -m u:kareem:--- hosts [user kareem has no permission]

[root@stapp02 etc]# getfacl hosts

# file: hosts

# owner: root

# group: root

user::rw-

user:kareem:---

user:garrett:r--

group::r--

mask::r--

other::r--

[root@stapp02 etc]#