centos 7 上配置SELinux允许nginx指定/home/www作为网站根目录

原创 2014年11月19日 23:19:34 标签：SELinux / 配置 / nginx / www 11816

现象:

1 启动nginx成功,使用wget 127.0.0.1得到内容,但是提示是禁止访问(403);

2 查看/var/log/nginx/error.log,提示访问/home/www/l.com/i.html禁止;

3 查看SELinux 是否运行: sestatus -v, enable就是运行了

4查看/var/log/Audit/Audit.log日志,发现有提示到nginx被拒绝了;但是看不明白怎么处理...

它是类似这样的内容

```
[plain]
1. type=AVC msg=audit(1416406823.013:3137): avc:  denied  { search } for  pid=15488 comm="nginx" name="www" dev="dm-
   3" ino=146 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:user_home_dir_t:s0 tclass=dir
```

5 安装人类能看得懂的转化工具:yum install setroubleshoot

6 echo >audit.log来清空这个日志,再刷新浏览器,访问一下这个url,让只生成一个出错日志

7 把出错内容转成可以看得懂的:sealert -a ./audit.log >qq.txt

8查看内容:cat qq.txt:

```
[plain]
1.  [root@l audit]# cat qq.txt
2.  string index out of range
3.  'list' object has no attribute 'split'
4.
5.  found 1 alerts in ./audit.log
6.  --------------------------------------------------------------------------------
7.
8.  SELinux is preventing /usr/sbin/nginx from search access on the directory .
9.
10. *****  Plugin catchall_boolean (47.5 confidence) suggests   ******************
11.
12. If 您要 allow httpd to read user content
13. Then 您必须启用 'httpd_read_user_content' 布尔值告知 SELinux 此情况。
14.
15. Do
16. setsebool -P httpd_read_user_content 1
17.
18. *****  Plugin catchall_boolean (47.5 confidence) suggests   ******************
19.
20. If 您要 allow httpd to enable homedirs
21. Then 您必须启用 'httpd_enable_homedirs' 布尔值告知 SELinux 此情况。
22.
23. Do
24. setsebool -P httpd_enable_homedirs 1
25.
26. *****  Plugin catchall (6.38 confidence) suggests   **************************
27.
28. If 您确定应默认允许 nginx search 访问  directory。
29. Then 您应该将这个情况作为 bug 报告。
30. 您可以生成本地策略模块允许这个访问。
31. Do
32. 请执行以下命令此时允许这个访问:
33. # grep nginx /var/log/audit/audit.log | audit2allow -M mypol
34. # semodule -i mypol.pp
35.
36.
37. Additional Information:
38. Source Context                system_u:system_r:httpd_t:s0
39. Target Context                unconfined_u:object_r:user_home_dir_t:s0
40. Target Objects                [ dir ]
41. Source                        nginx
42. Source Path                   /usr/sbin/nginx
43. Port                          <Unknown>
44. Host                          <Unknown>
45. Source RPM Packages           nginx-1.6.2-4.el7.x86_64
46. Target RPM Packages
47. Policy RPM                    selinux-policy-3.12.1-153.el7_0.11.noarch
48. Selinux Enabled               True
49. Policy Type                   targeted
50. Enforcing Mode                Enforcing
51. Host Name                     l.com
52. Platform                      Linux l.com 3.10.0-123.9.3.el7.x86_64 #1 SMP Thu
53.                               Nov 6 15:06:03 UTC 2014 x86_64 x86_64
54. Alert Count                   13
55. First Seen                    2014-11-19 22:32:40 CST
56. Last Seen                     2014-11-19 22:24:28 CST
57. Local ID                      bb55eec2-48bf-44eb-9722-7ca6f1045a59
58.
59. Raw Audit Messages
60. type=AVC msg=audit(1416407068.287:3141): avc:  denied  { search } for  pid=15488 comm="nginx" name="www" dev="dm-
    3" ino=146 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:user_home_dir_t:s0 tclass=dir
61.
62.
63. type=SYSCALL msg=audit(1416407068.287:3141): arch=x86_64 syscall=open success=no exit=EACCES a0=7f0661e65bc0 a1=800 a2=0
    (none) ses=4294967295 comm=nginx exe=/usr/sbin/nginx subj=system_u:system_r:httpd_t:s0 key=(null)
64.
65. Hash: nginx,httpd_t,user_home_dir_t,dir,search
66.
67. [root@l audit]#
```

9 按提示一步一步处理成功了就可以了.