

CentOS SELinux Settings

Page Tags

SELinux

security

Security-Enhanced Linux (SELinux) settings

```
[root@biskinler.com ~]# setsebool -P antivirus_can_scan_system 1
```

```
[root@biskinler.com ~]# getsebool named_disable_trans
named_disable_trans --> off
```

```
[root@biskinler.com ~]# setsebool named_disable_trans 1
```

```
[root@biskinler.com ~]# getsebool named_disable_trans
named_disable_trans --> on
```

If you get

```
#2016/04/01 19:20:45 [error] 16415#0: *16 connect() failed (111: Connection refused) while connecting
```

Running this fixed my problem:

```
[root@biskinler.com ~]# setsebool -P httpd_can_network_connect 1
```

```
[root@biskinler.com:~/]# getenforce
Enforcing
[root@biskinler.com:~/]# setenforce 0
[root@biskinler.com:~/]# getenforce
Permissive
```

```
[root@biskinler.com:~/]# cat /etc/selinux/config
```

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
#SELINUX=enforcing
SELINUX=disabled
# SELINUXTYPE= can take one of three two values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

To get all settings

```
[root@biskinler.com:~/]# getsebool -a
```

```
# antivirus_can_scan_system --> on
# antivirus_use_32bit --> off
# authlogin_passwd_check --> off
# authlogin_radius --> off
# authlogin_yubikey --> off
```

Created Wed, Aug 3, 2016 8:30 PM by Ahmet Faruk Biskinler

Last Updated Mon, Aug 15, 2016 12:30 PM by Ahmet Faruk Biskinler