How to change ssh port on CentOS 7

Recently one of our server has welcomed us with ugly messages like:

> Last failed login: Fri Aug 22 19:31:42 CEST 2014 from xx.xxx.xxx.xx on ssh:notty
> There were 17307 failed login attempts since the last successful login.
> Last login: Wed Aug 13 11:11:55 2014 from yyy-yyy-yyy-yyy

The simplest way to prevent such attacks is to change the ssh port. Mostly this attacks are coming from stupid robots trying to hack an open ssh port (22) with many thousand tries.
Do the following steps to change the ssh server port on your machine:

- Edit /etc/ssh/sshd_config and uncomment the port line to something like: "Port 4444"
- Because CentOS 7 is a Security-Enhanced Linux (SELinux) you have to tell SELinux that running ssh on the new Port 4444 is allowed. This can be done by using the command "semanage".
- On a minimal CentOS 7 System the command "semanage" is missing therefore install it with "sudo yum install policycoreutils-python"
- Afterwards you can use "semanage port -a -t ssh_port_t -p tcp 4444", now SELinux allows sshd to listen on the new port 4444.
- Check the configuration with "semanage port -l | grep ssh" and you should see something like:

> ssh_port_t tcp 4444, 22

- Actually the old port 22 you don't need any longer and you could have the idea to delete it from SELinux with "semanage port -d -t ssh_port_t -p tcp 22" but this isn't possible and you will see the message:

> ValueError: Port tcp/22 ist in der Richtlinie festgelegt und kann nicht gelöscht werden

- Now restart the ssh daemon with "systemctl restart sshd.service". Because CentOS 7 is a systemd-based OS you have to use the systemctl command to start, stop, restart services. In earlier versions you would have used "service sshd restart" for example. Systemd is just another process manager. CentOS 6 have used upstart or older versions have used System V init.
- After the restart check the SELinux log for problems with "tail -f /var/log/secure". Everything should be fine, if you can see something like:

```
Aug 22 22:54:38 xxx sshd[2309]: Server listening on 0.0.0.0 port 4444.
Aug 22 22:54:38 xxx sshd[2309]: Server listening on :: port 4444.
```

- Don't forget the firewall. At this point you would be able to connect to your ssh server with "ssh -p 4444 myuser@x.xx.xxx.xx" if your firewall does not refuse the connection. Just open the port in your firewall to allow access from outside to your sshd. On CentOS 7 iptables was replaced by firewalld. Read in my next blog how to disable firewalld and activate iptables on CentOS 7 again.
- If you want to check whether sshd is really listening on the new port then use netstat. Because on a minimal CentOS 7 System netstat isn't installed by default use: "sudo yum install net-tools" and then use "netstat -tulpn | grep :4444".

```
tcp 0 0 0.0.0.0:4444 0.0.0.0:* LISTEN 2309/sshd
tcp6 0 0 :::4444 :::* LISTEN 2309/sshd
```

My biggest problem to change the ssh port was our firewall iptables on the CentOS 7 system. I tried to open the new port with "iptables -A INPUT -p tcp --dport 4444 -j ACCEPT" and this worked. I could login via ssh on the new port until the machine was restarted. After the restart login on the port 4444 was not possible anymore. I managed to enter "iptables -A INPUT -p tcp --dport 4444 -j ACCEPT" and access was permitted again. Due to the fact that CentOS 7 has a new firewall called firewalld, iptables was not starting on boot time and the rule "iptables -A INPUT -p tcp --dport 4444 -j ACCEPT" was not performed at boot time. After that I decided to uninstall firewalld and installed iptables fully. From now on everything workded as expected. If you have similar problems don't hesitate to contact me. My email can be found on the dropbit website.