Splunk CTF

Splunk CTF setup guide.

- Installation guide CentOS
- Splunk Installation
- Configure Firewall & Splunk

Installation guide CentOS

At my workplace I'm managing a course for apprentices inside the organization. As we are working in the IT Security we are presenting how the work is done in several teams.

Splunk is an well known application and is needed everyday. Splunk is logging everything what happens in the network. In my course for the event we are playing a CTF with Splunk.

Preparation and Information

CTF Scoreboard:

https://github.com/splunk/SA-ctf_scoreboard

Splunk Dataset:

https://github.com/splunk/botsv1

Splunk installation:

https://docs.splunk.com/Documentation/Splunk/7.0.3/Installation/InstallonLinux

Splunk Download:

https://www.splunk.com/de_de/download/splunk-enterprise.html

CentOS Download:

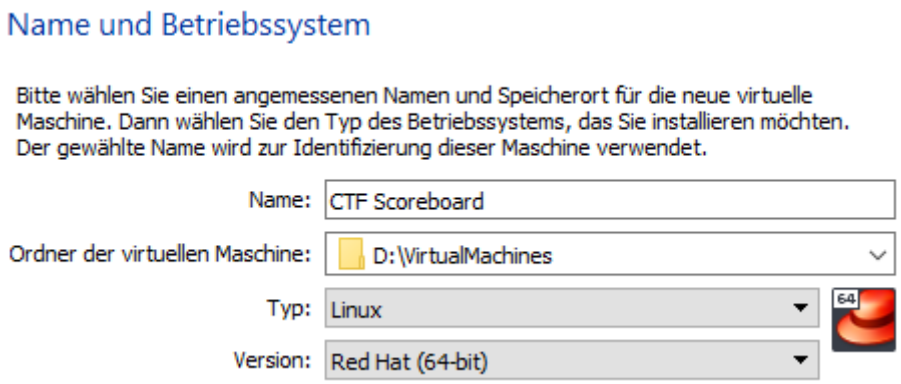
https://www.centos.org/download/

Setting up VM

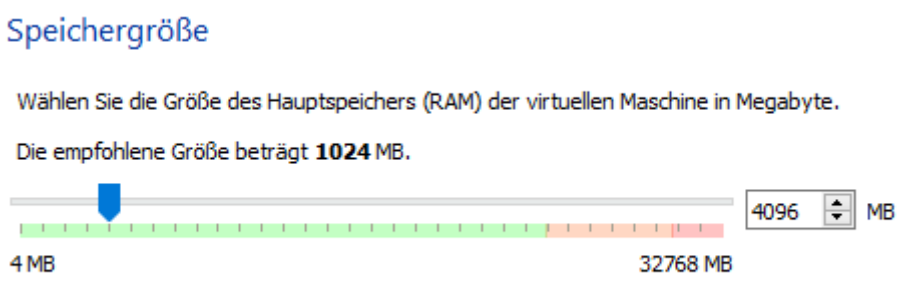
First download the CentOS 8 iso file so we can start setup a VM.

http://mirror.init7.net/centos/8.4.2105/isos/x86_64/CentOS-8.4.2105-x86_64-dvd1.iso

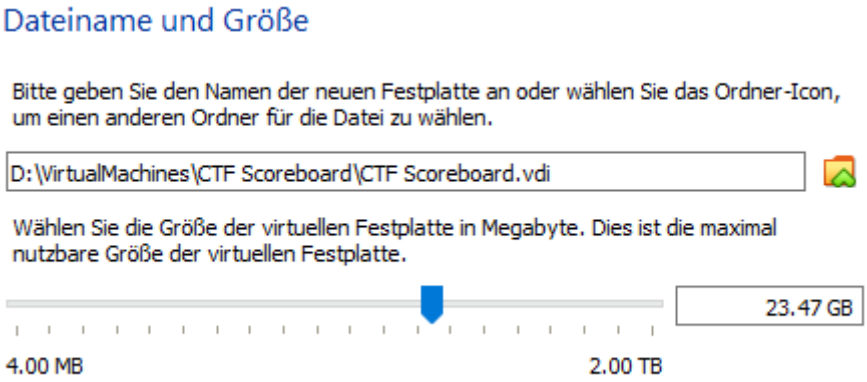
As soon you downloaded the iso we can start with VirtualBox.



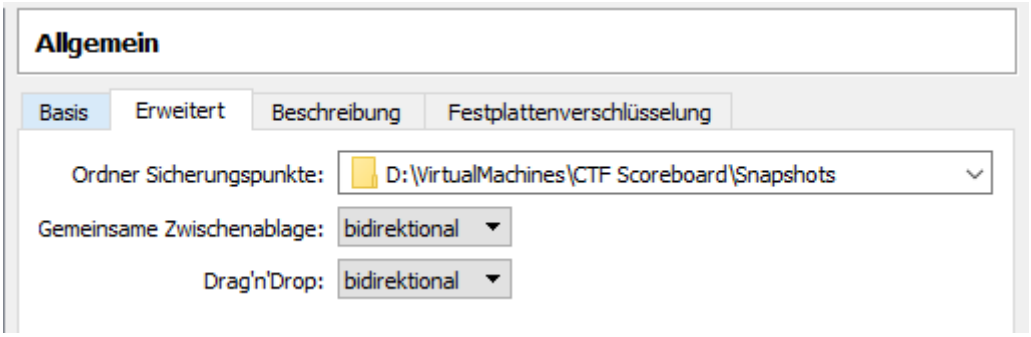
Set the RAM to ca. 4GB:



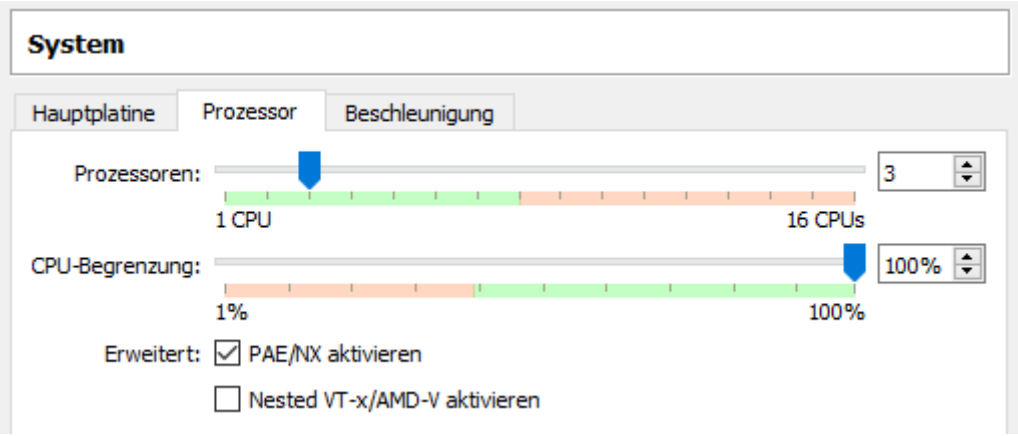
Create a dynamic VDI Disk with ca. 20-25 GB:



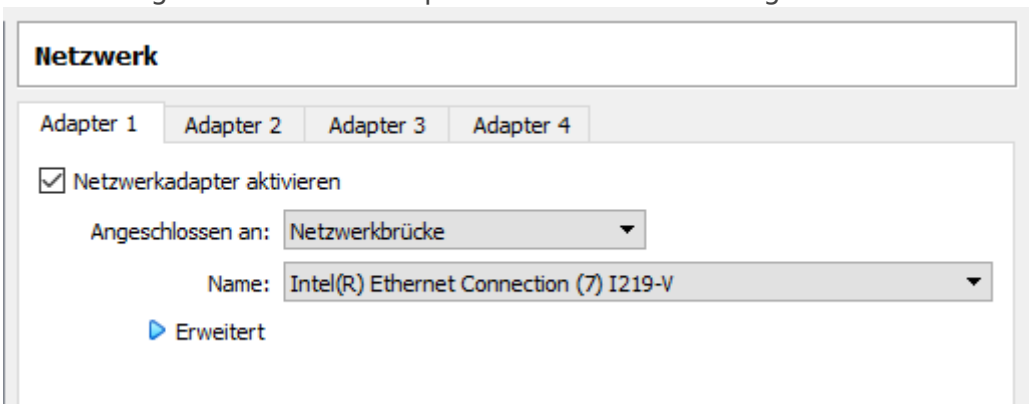
Now the VM is ready to start but we need to specify some settings.
First we set the clipboard to bidirectional mode:



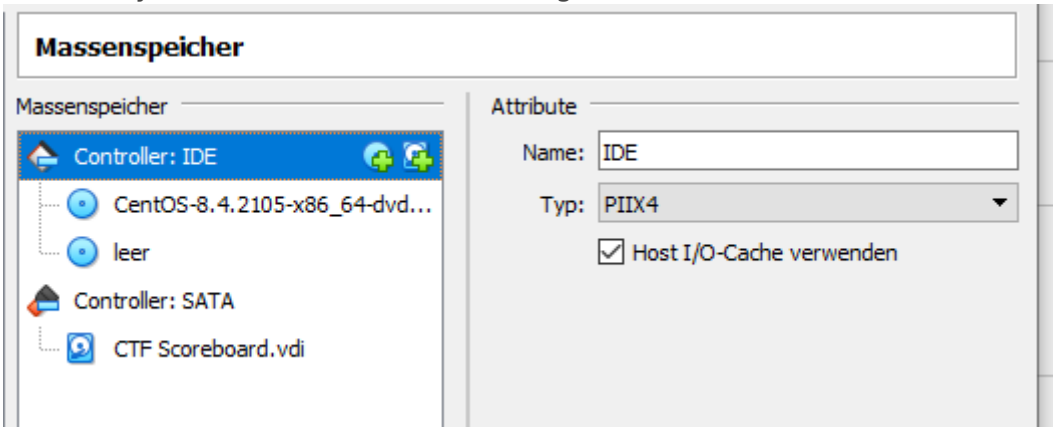
Upscale the processor to minimum 2 cores:



Then change the network adapter to the Network bridge:



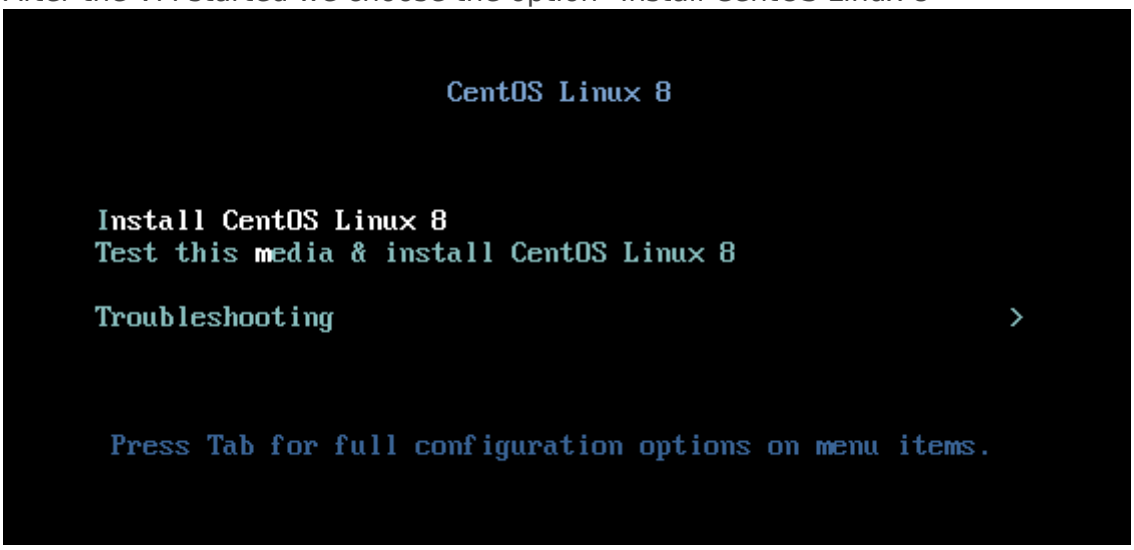
And finally add the ISO File to the storage:



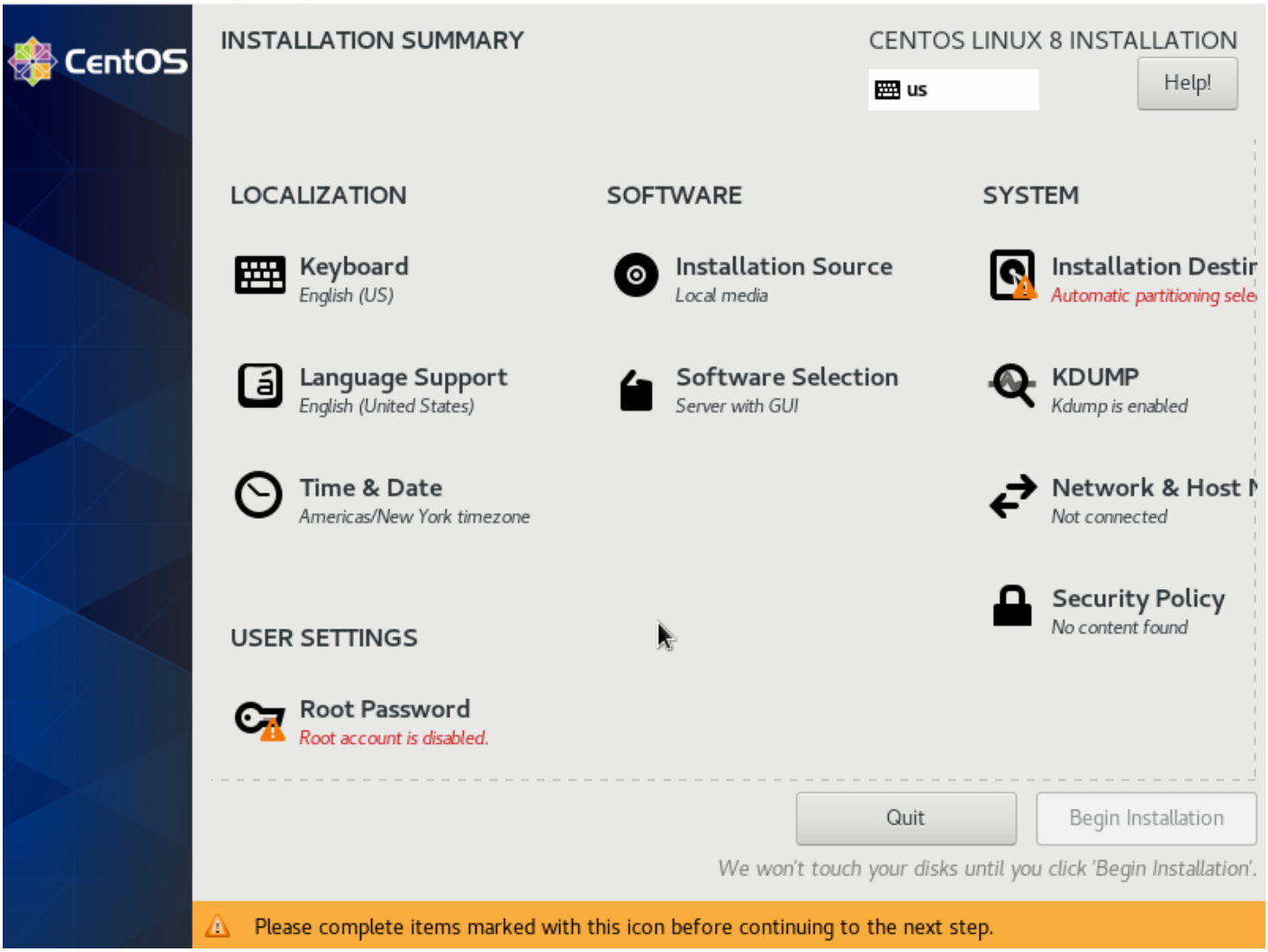
Now we can start the machine and configure the setup.

Setting up Operating System

After the VM started we choose the option "Install CentOS Linux 8"

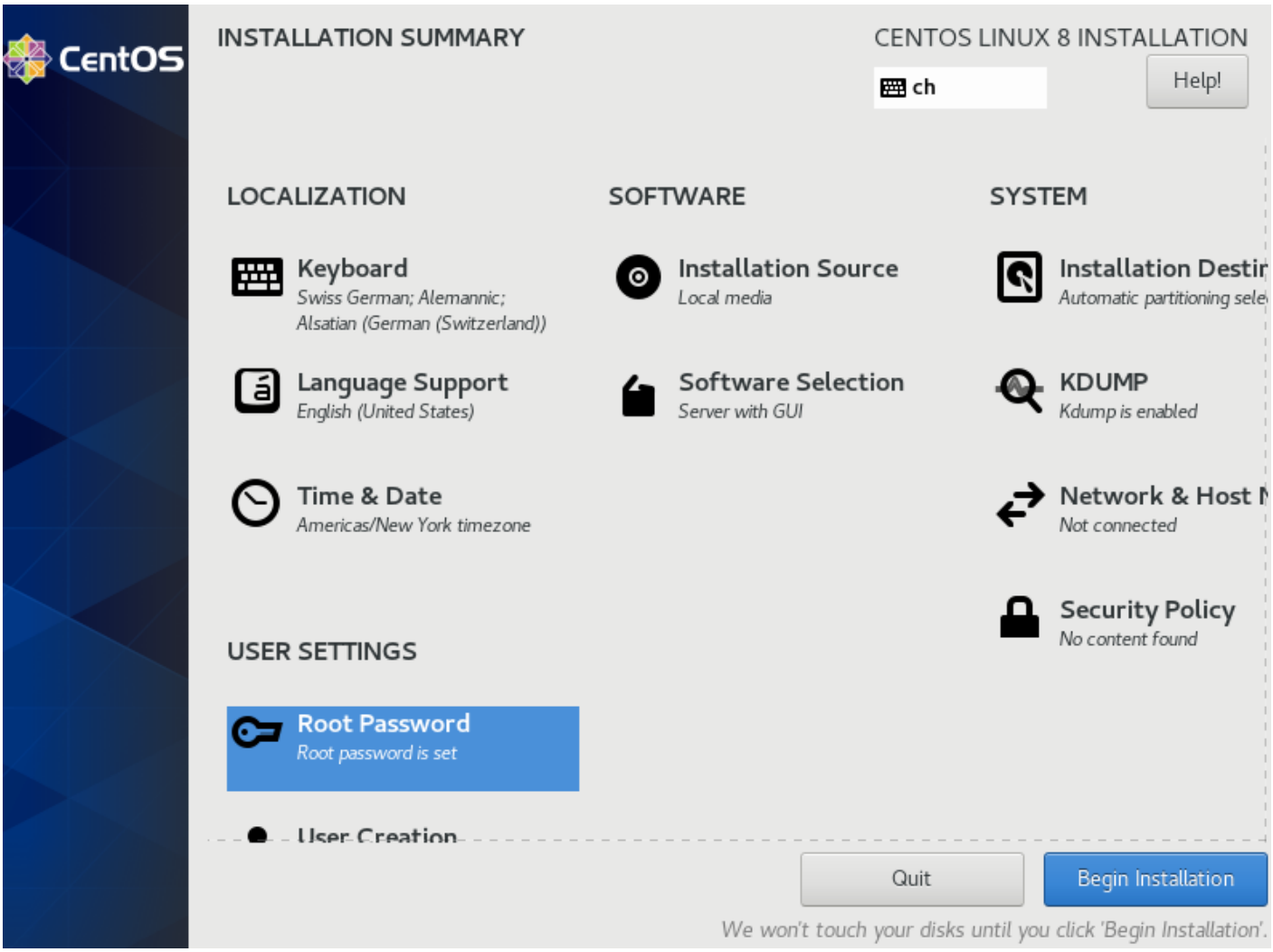


First we land on a page where we need to specify some settings before we can go for the actual setup:



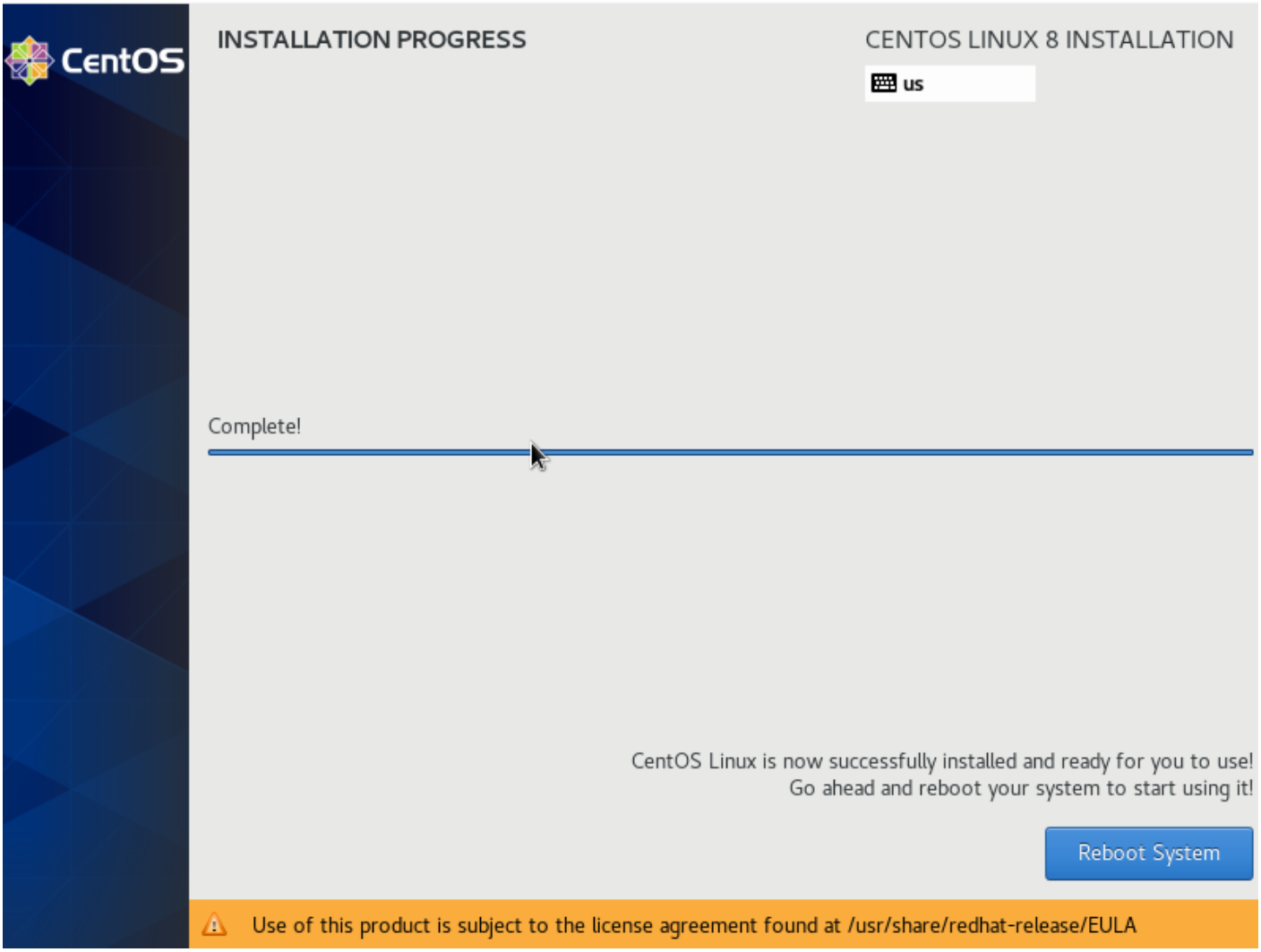
Set the Keyboard to Swissgerman.
Change the root password.
Define the partition to install the OS. Usually I choose automatic and use the whole disk.

At the end it should look like this:

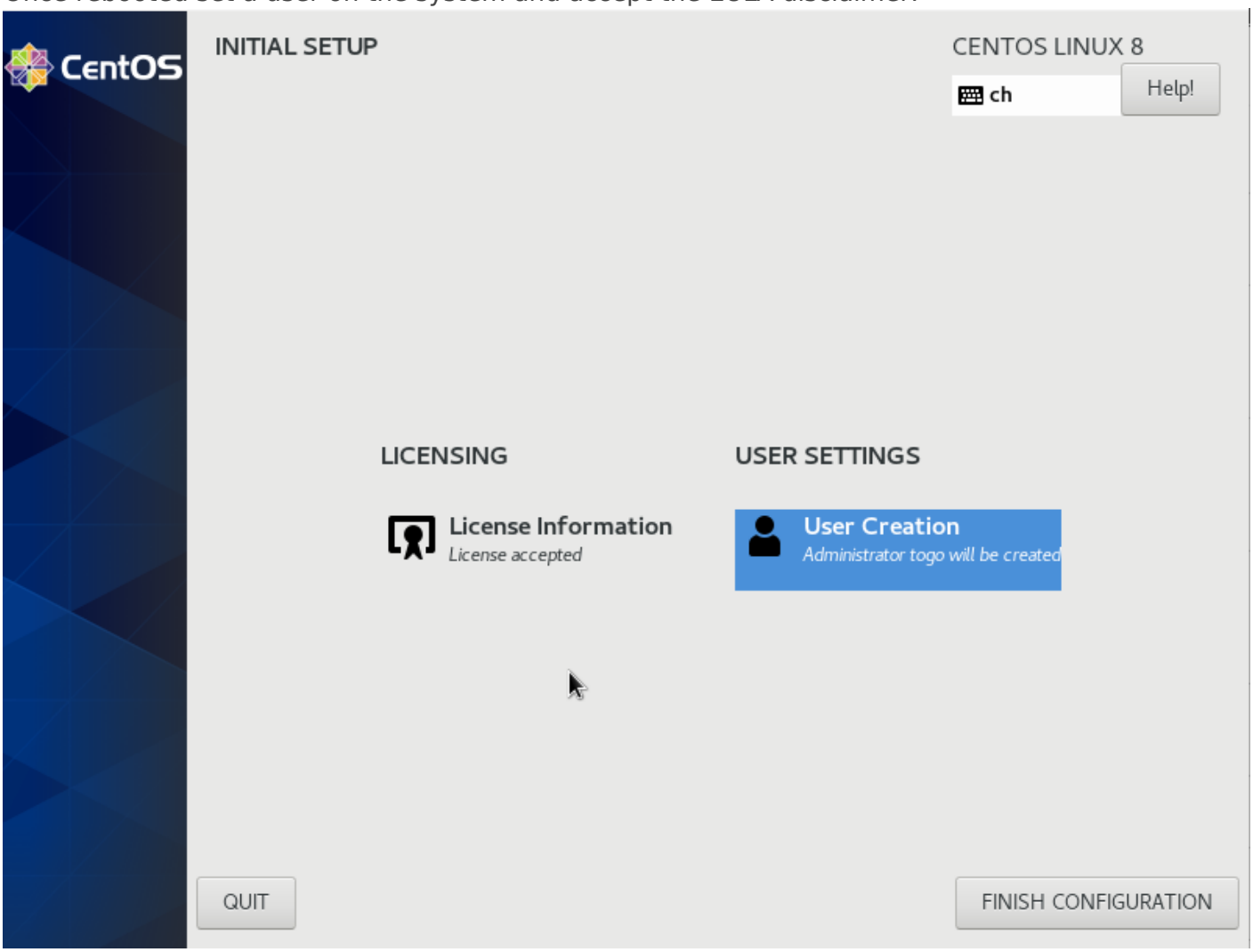


Hit the button "Begin Installation" and the installation will start:

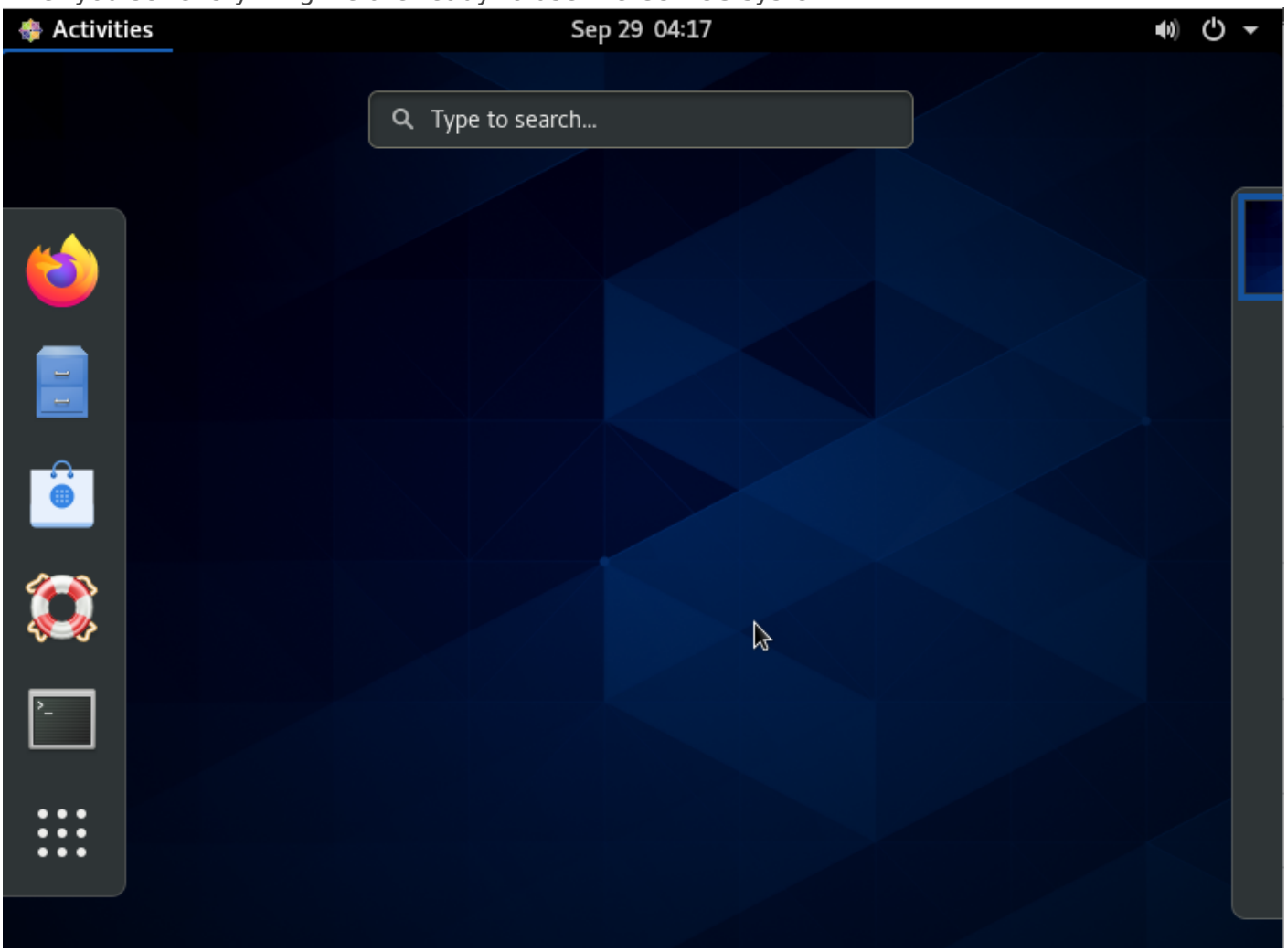
Once the installation is complete we need to perform a reboot. IMPORTANT: Remove the ISO file from the storage.



Once rebooted set a user on the system and accept the EULA disclaimer:



Click on "Finish Configuration" and login with you recent created user account. Once you are logged in you are getting asked to define your system language, keyboard and some privacy settings.
After you set everything we are ready to use the CentOS system:



Don't forget to turn on the Internet on top right corner by selecting "Choose wired".

Splunk Installation

Before we install splunk we need to change some settings.

First we remove the "virbr0" network interface as it's useless for our project. Virbr0 is used for virtualization purposes and acts as a switch you can connect your guests and your host if you are virtualizing.

```
virbr0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 192.168.122.1  netmask 255.255.255.0  broadcast 192.168.122.255
        ether 52:54:00:d1:2f:c2  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

To do this enter following commands:

`systemctl stop libvirtd.service`

`systemctl status libvirtd.service -> make sure service is innactive`

`systemctl disable libvirtd.service`

`reboot`

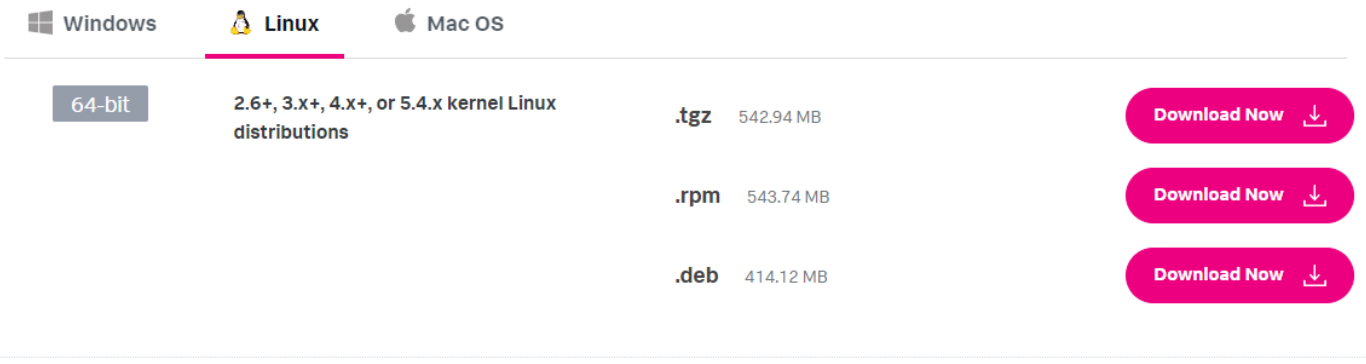
After reboot the interface is removed.

```
[togo@localhost ~]$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.233  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe7b:c4fd  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:7b:c4:fd  txqueuelen 1000  (Ethernet)
        RX packets 344  bytes 32416 (31.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 95  bytes 12671 (12.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[togo@localhost ~]$
```

Install Splunk

Now we are one step closer to the Splunk CTF. First we need to install Splunk Enterprise.

Splunk Enterprise is free for 60 days and afterwards you'll need to provide a license anyway we download Splunk enterprise from the homepage https://www.splunk.com/de_de/download/splunk-enterprise.html
Probably you need to log in yourself to have access.



I followed the guide of Splunk
https://docs.splunk.com/Documentation/Splunk/7.0.3/Installation/InstallonLinux

We are downloading the RPM package. Once downloaded we can start with the installation.

```
[togo@localhost ~]$ cd Downloads/
[togo@localhost Downloads]$ ls
splunk-8.2.2.1-ae6821b7c64b-linux-2.6-x86_64.rpm
```

Confirm that the RPM package you want is available locally on the target host.

Verify that the Splunk Enterprise user account that will run the Splunk services can read and access the file.

If needed, change permissions on the file.

`chmod 744 splunk_splunk-8.2.2.1-ae6821b7c64b-linux-2.6-x86_64.rpm`

```
[root@localhost Downloads]# ls
splunk-8.2.2.1-ae6821b7c64b-linux-2.6-x86_64.rpm
```

Invoke the following command to install the Splunk Enterprise RPM in the default directory /opt/splunk.

`rpm -i splunk-8.2.2.1-ae6821b7c64b-linux-2.6-x86_64.rpm`

```
[togo@localhost Downloads]$ sudo rpm -i splunk-8.2.2.1-ae6821b7c64b-linux-2.6-x86_64.rpm
warning: splunk-8.2.2.1-ae6821b7c64b-linux-2.6-x86_64.rpm: Header V4 RSA/SHA512 Signature, key ID b3cd4420: NOKEY
useradd: cannot create directory /opt/splunk
complete
[togo@localhost Downloads]$
```

```
[togo@localhost opt]$ pwd
/opt
[togo@localhost opt]$ ls
splunk
[togo@localhost opt]$
```

Now as Splunk is installed we need to set the admin password.

Go to the directory: /opt/splunk/bin

```
[togo@localhost bin]$ sudo ./splunk start
[sudo] password for togo:
```

Afterwards you are prompted to accept the license. Accept it and go on.

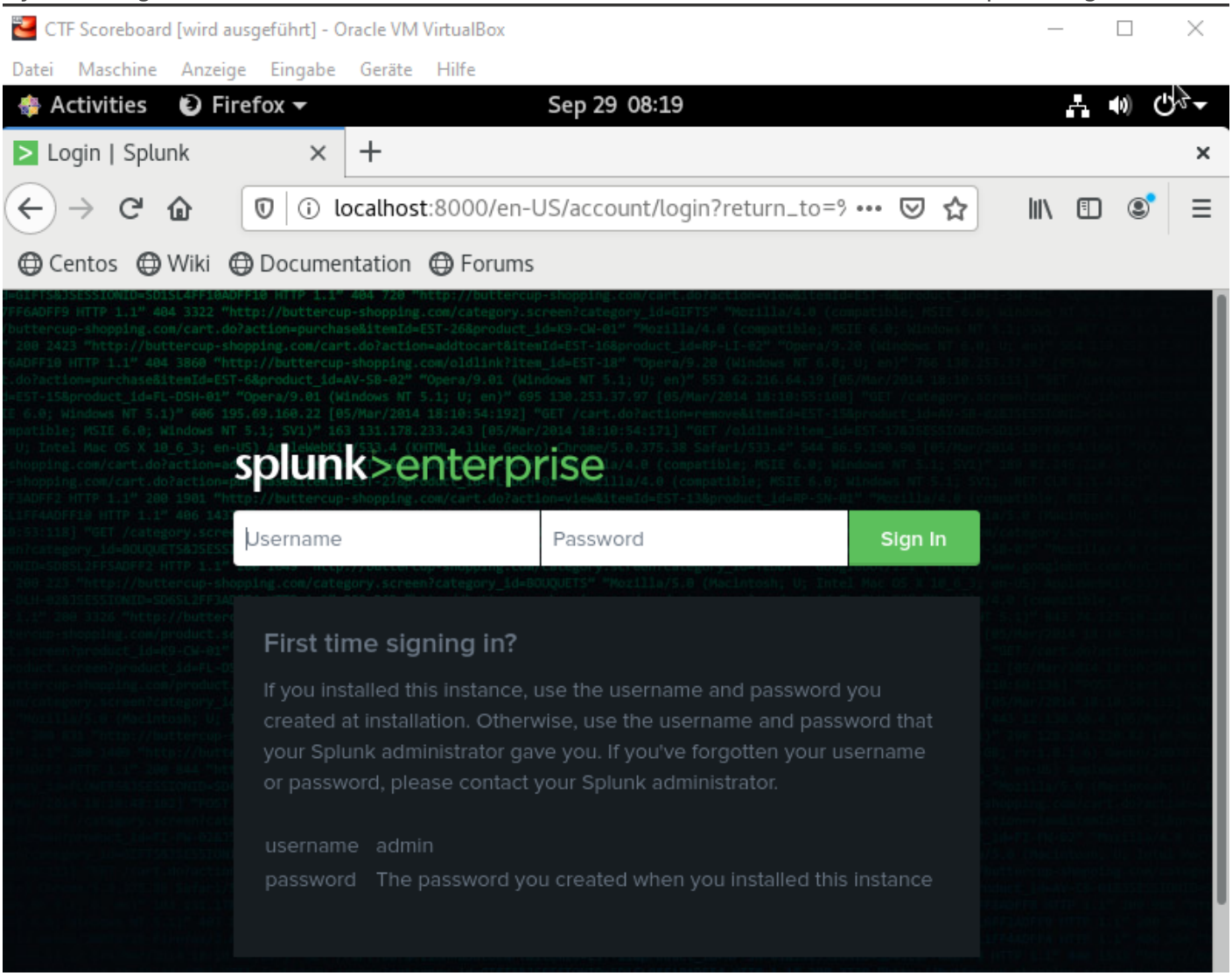
Choose and administrator username:

```
This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: admin
```

Provide a password and splunk will get started.

```
Signature ok
subject=/CN=localhost.localdomain/O=SplunkUser
Getting CA Private Key
writing RSA key
Done
                                                        [  OK  ]

Waiting for web server at http://127.0.0.1:8000 to be available..... Done


If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://127.0.0.1:8000

[togo@localhost bin]$
```

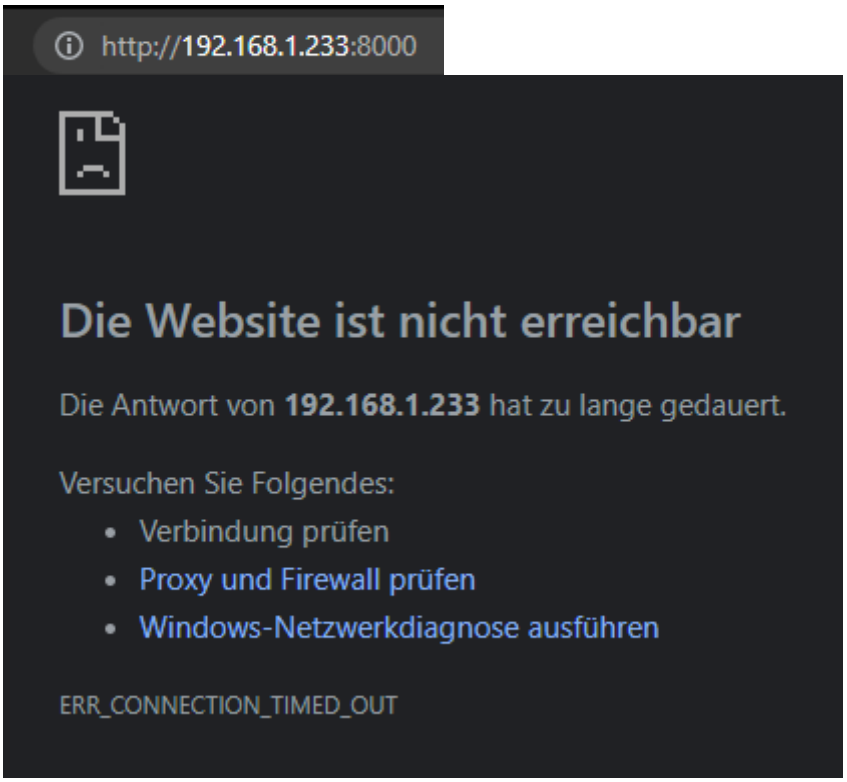
By checking on the browser in the CentOS VM localhost:8000 we should see a Splunk login screen:



Configure Firewall & Splunk

Open Firewall

When we try to access the login via internal network we won't be able to establish a connection.



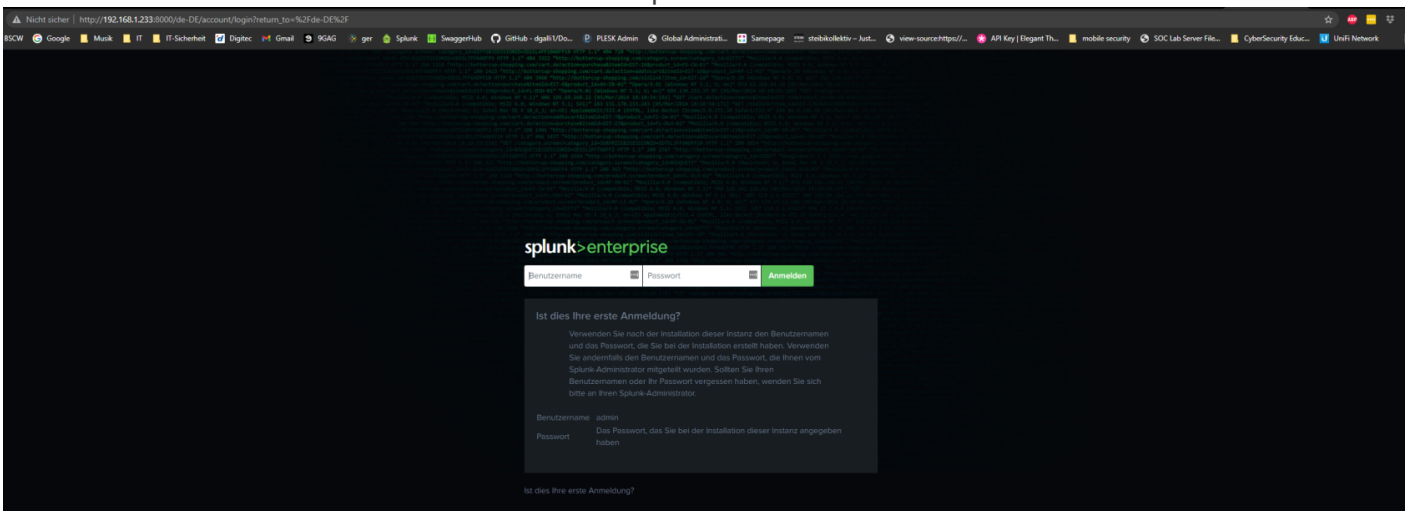
The problem is that our machine is refusing connections from outside via port 8000. We need to open the port on the firewall.

The guide how to change firewall rules can be found here:
https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-using-firewalld-on-centos-8-de

With a simple oneliner we have opened the port:

```
sudo firewall-cmd --zone=public --permanent --add-port=8000/tcp
```

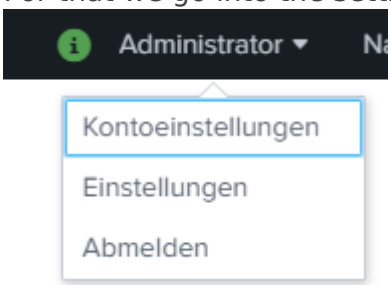
That's it now we need to reboot once and the port is accessible via the network.

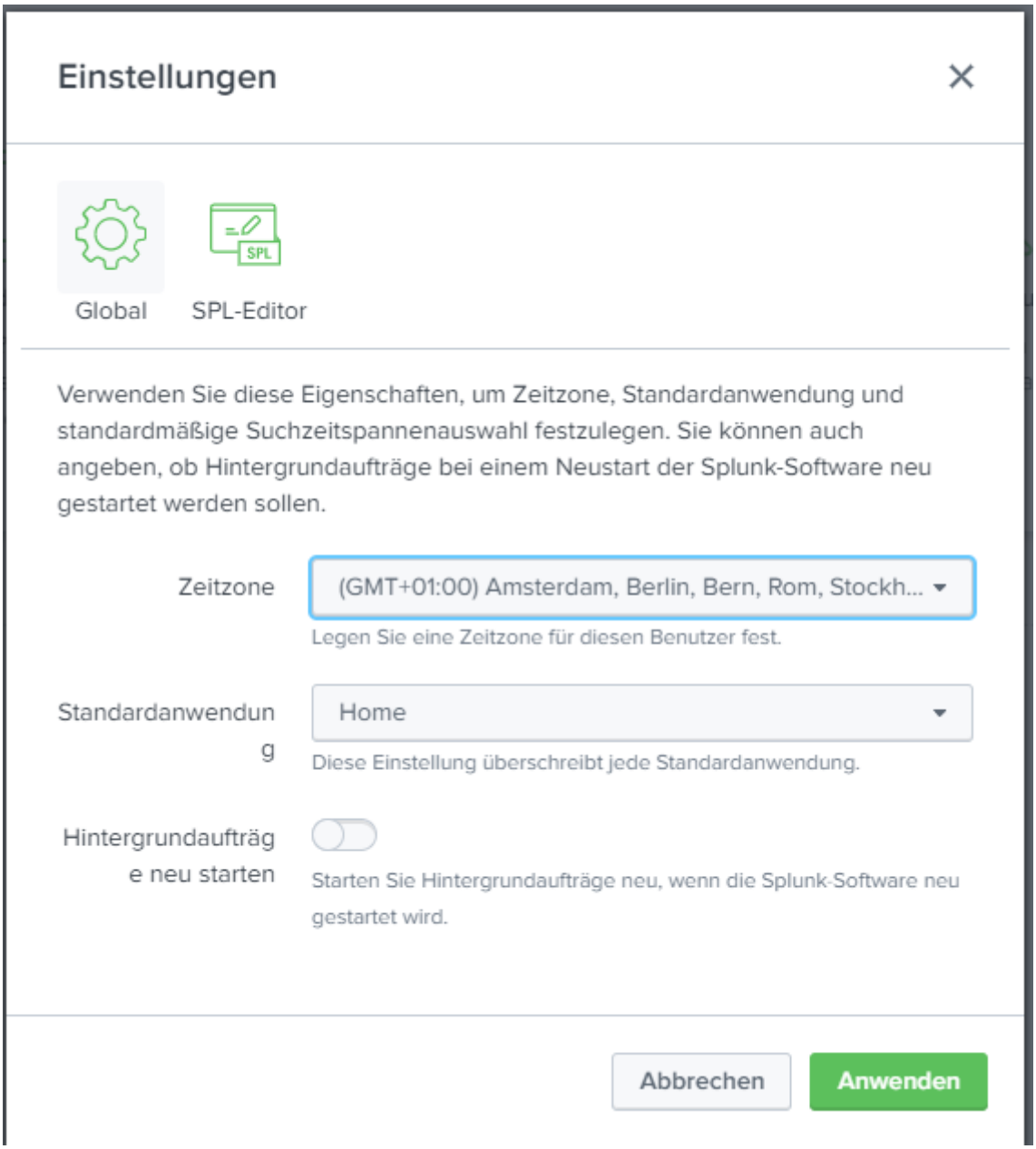


Configure Splunk

Now as Splunk is running we can log in with the defined credentials.

Next step we set the correct timezone and enable HTTPS.
For that we go into the settings below the Administrator Tab.

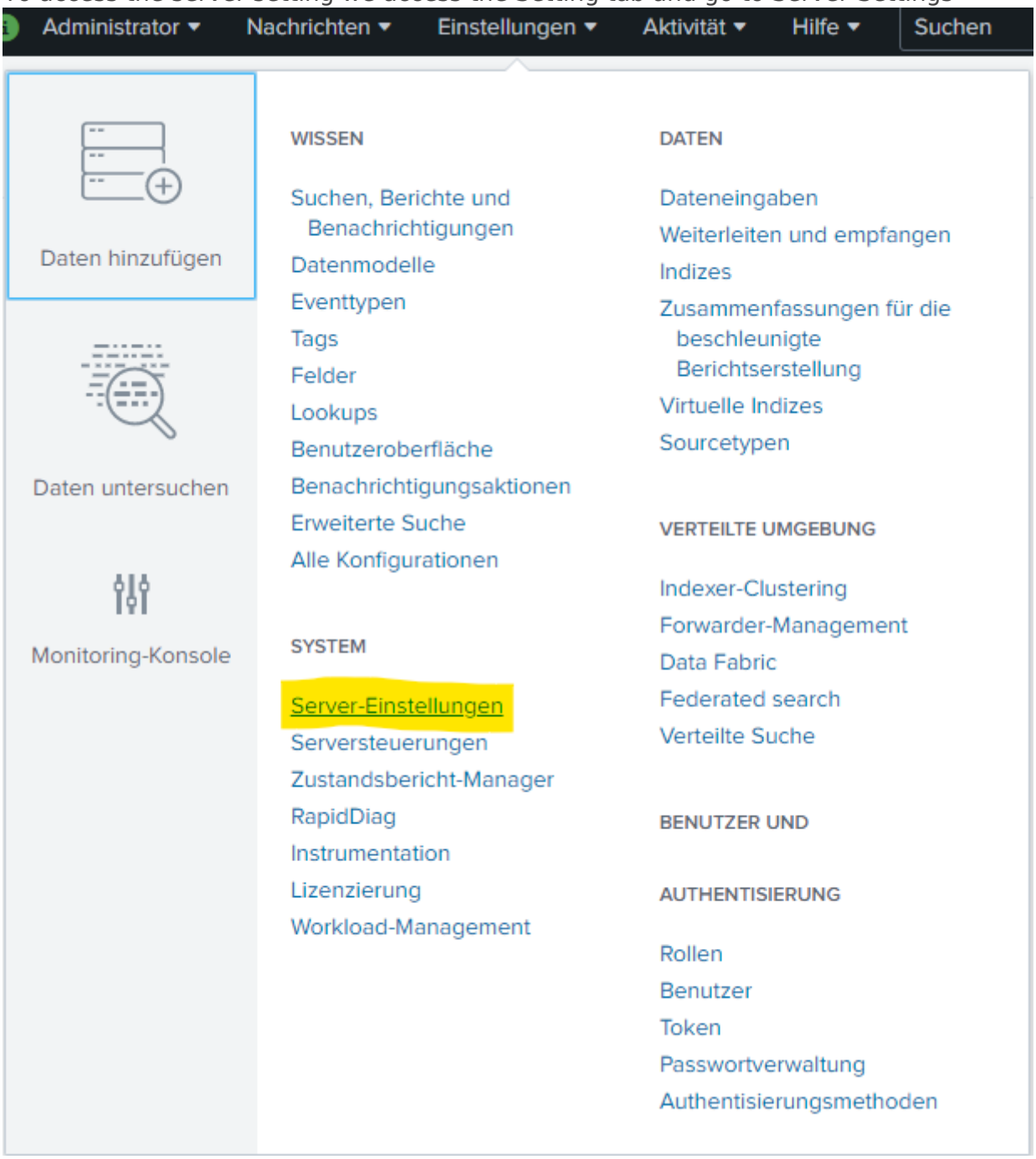




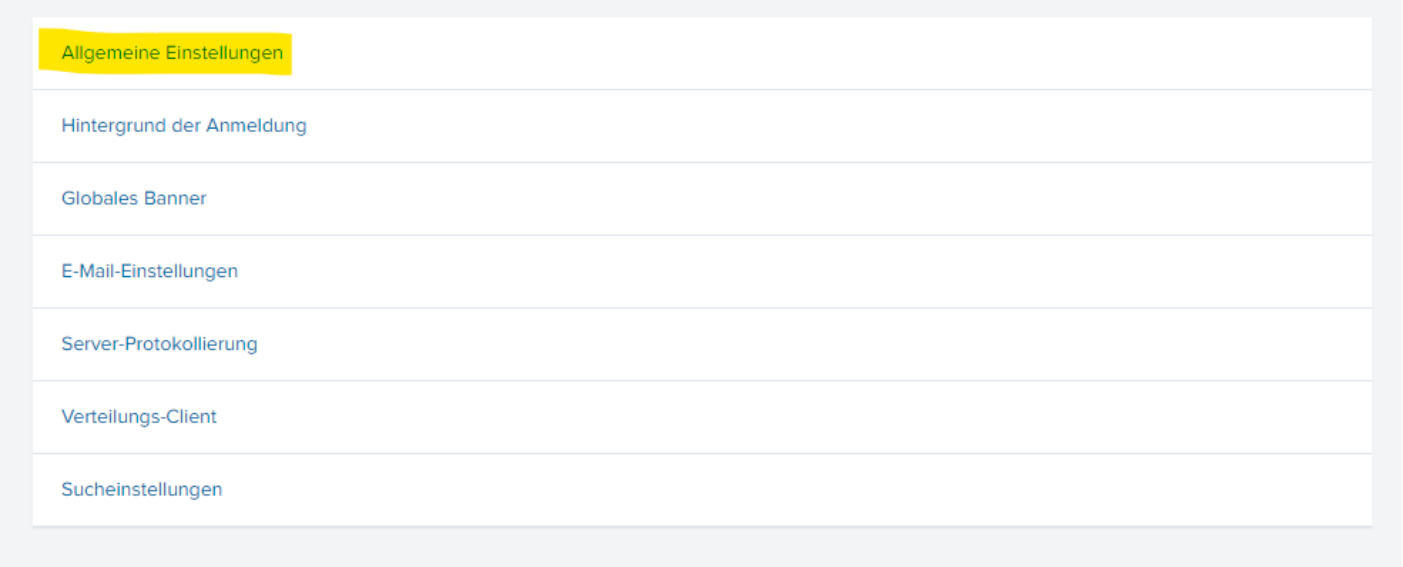
Easy!

Next thing to do is enable HTTPS.

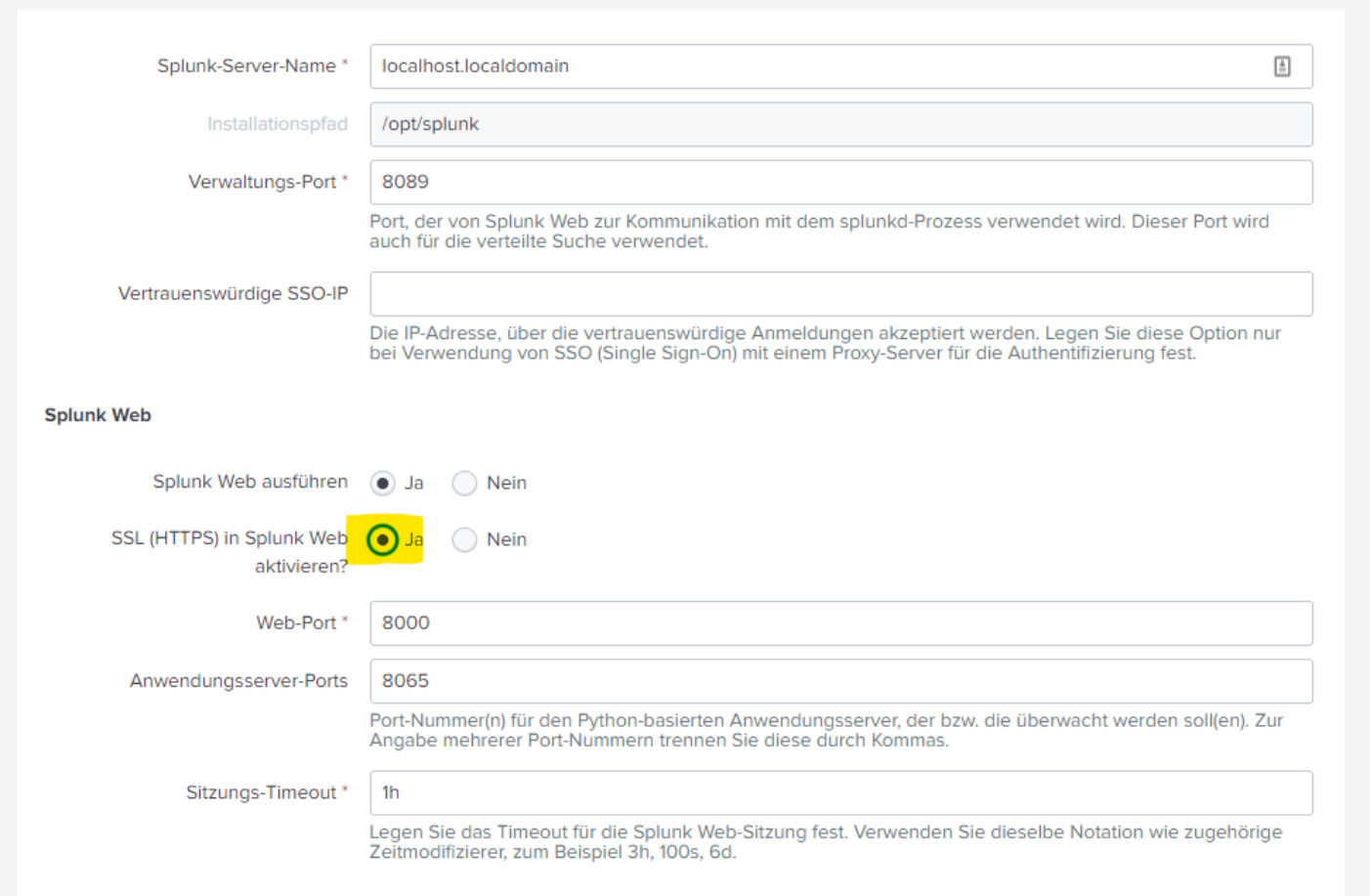
To access the server setting we access the Setting tab and go to Server-Settings



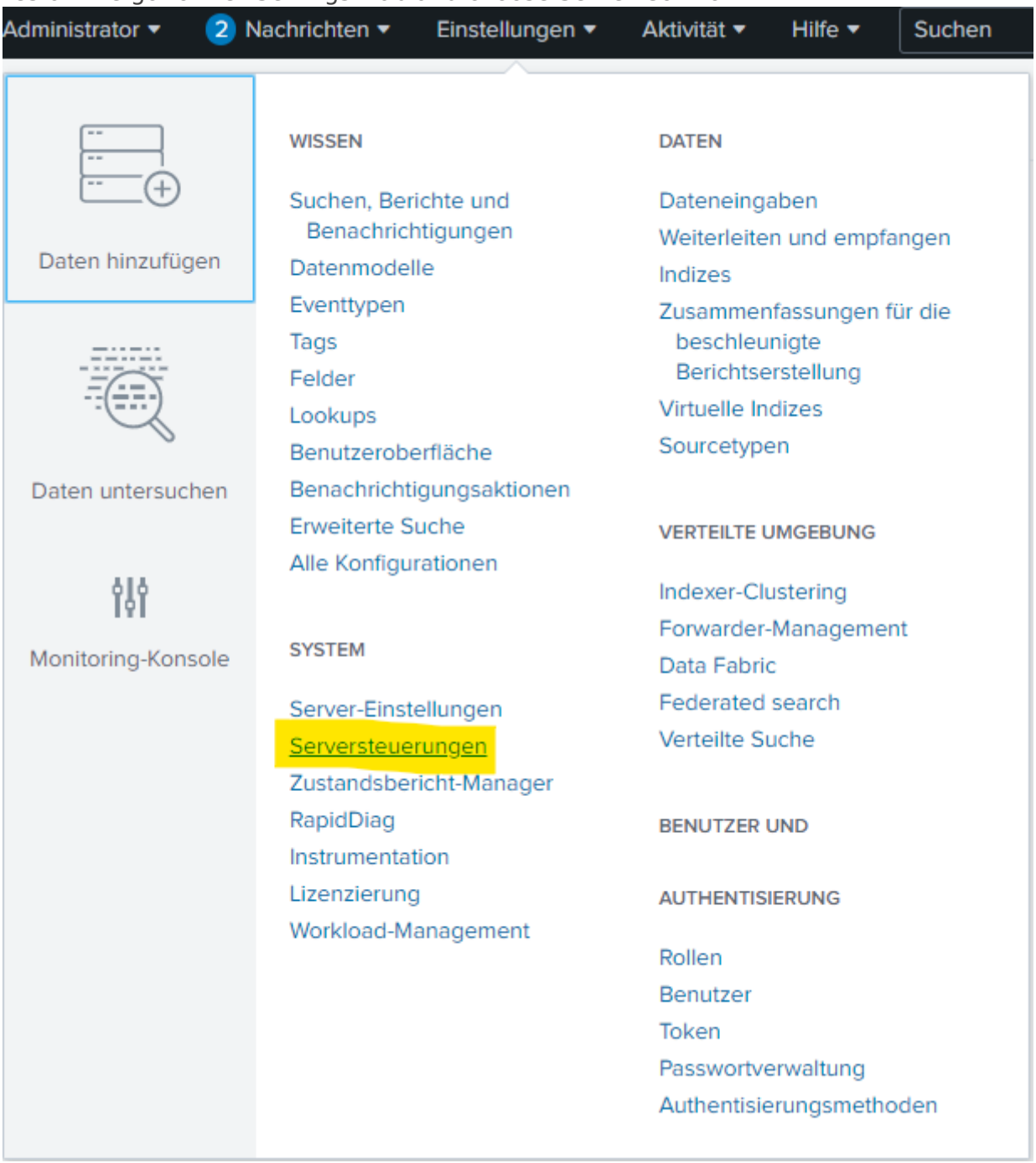
Then we access the general settings



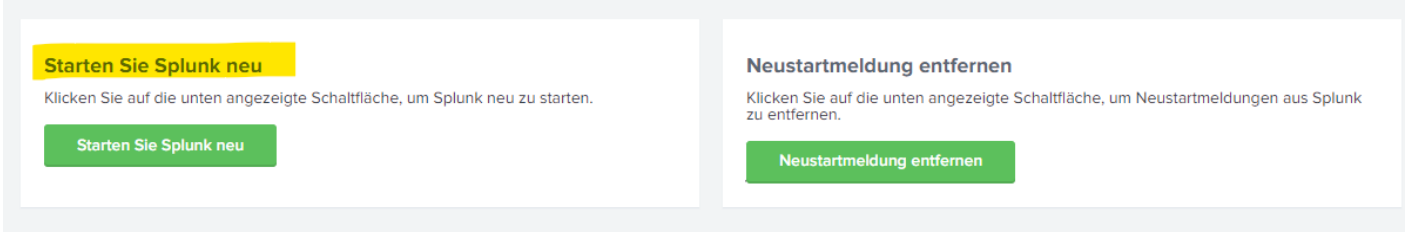
In the general setting we choose "enable HTTPS in Splunk Web":



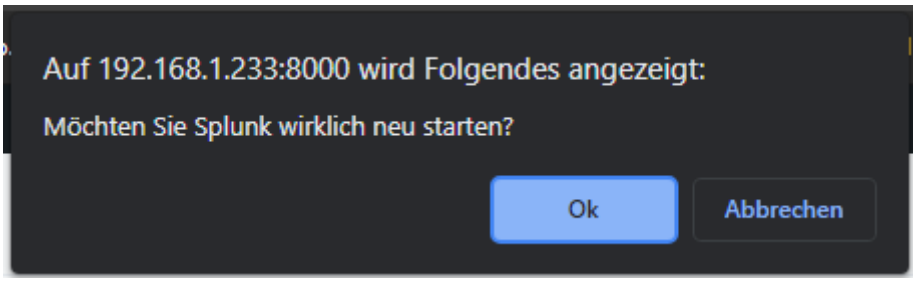
After the HTTPS box is checked we need to perform a restart of the Splunk service. To initiate a restart we go to the "Settings" tab and choose Server-Control:



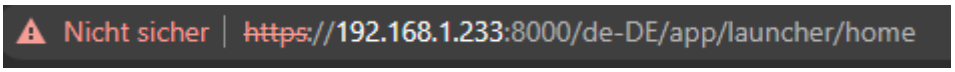
In here we are able to restart the service:



You'll get asked if you really want to restart. Press OK

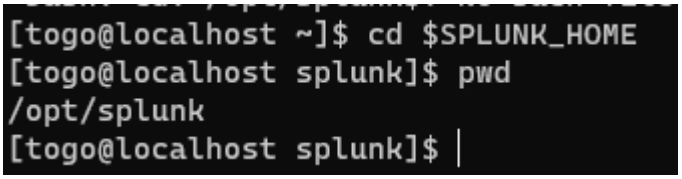


Click on the URL and you'll get redirected to the HTTPS login



Now we are going back to the shell and set the $SPLUNK_HOME environment variable.

```
export SPLUNK_HOME=/opt/splunk
```



Install Apps and Addons

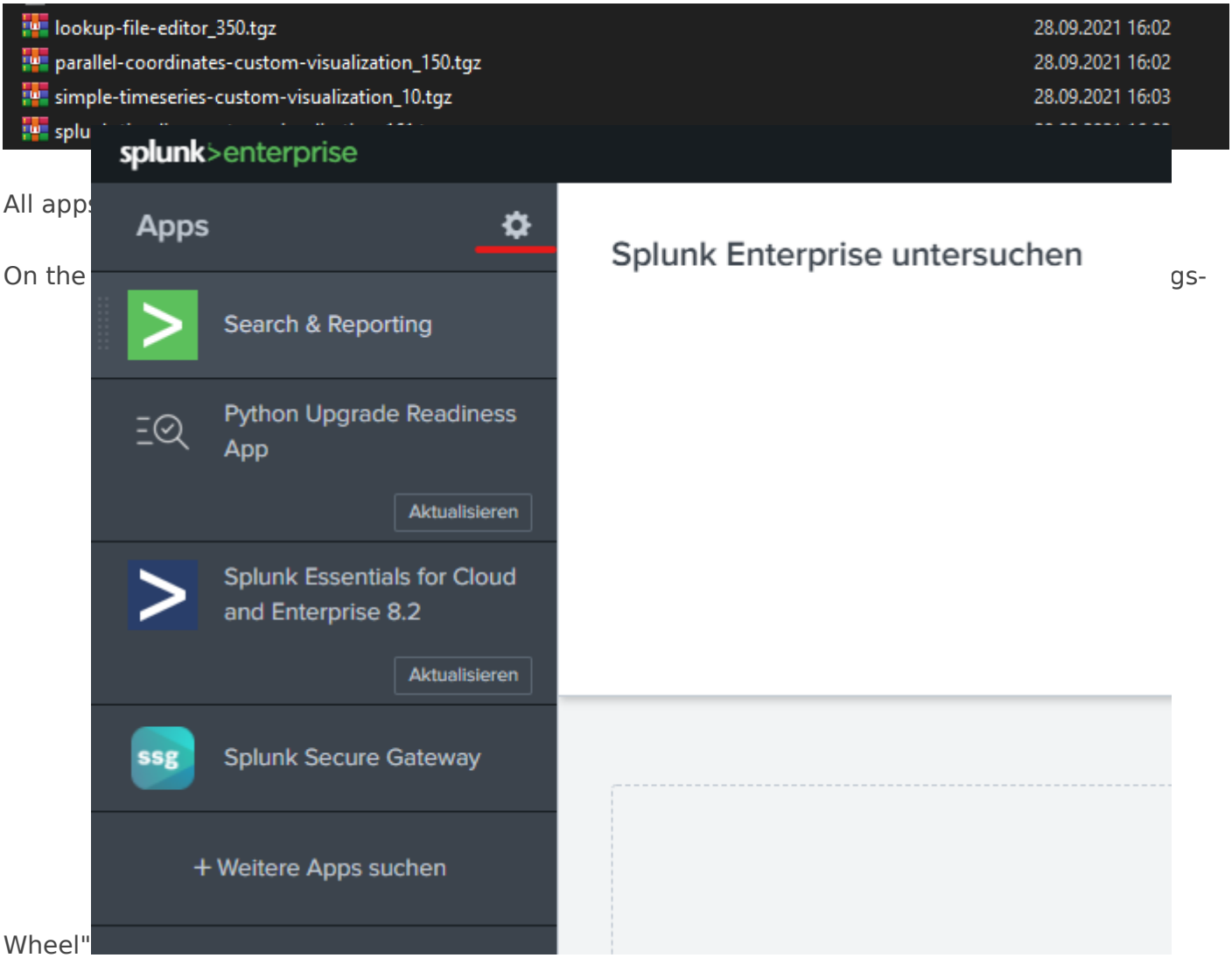
Download following Apps:

Lookup File Editor app (Note: Tested with version 3.0.3)

Parallel Coordinates Custom Visualization (Note: Tested with version 1.2.0)

Simple Timeseries Custom Visualization (Note: Tested with version 1.0)

Timeline Custom Visualization (Note: Tested with version 1.2.0)

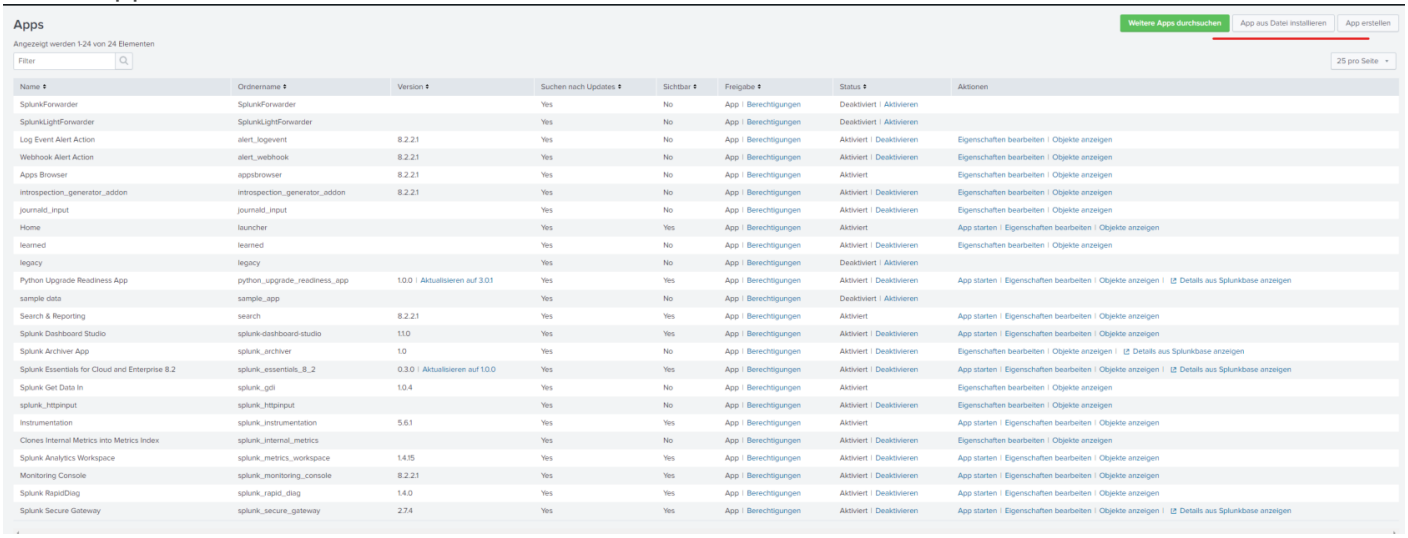


All apps

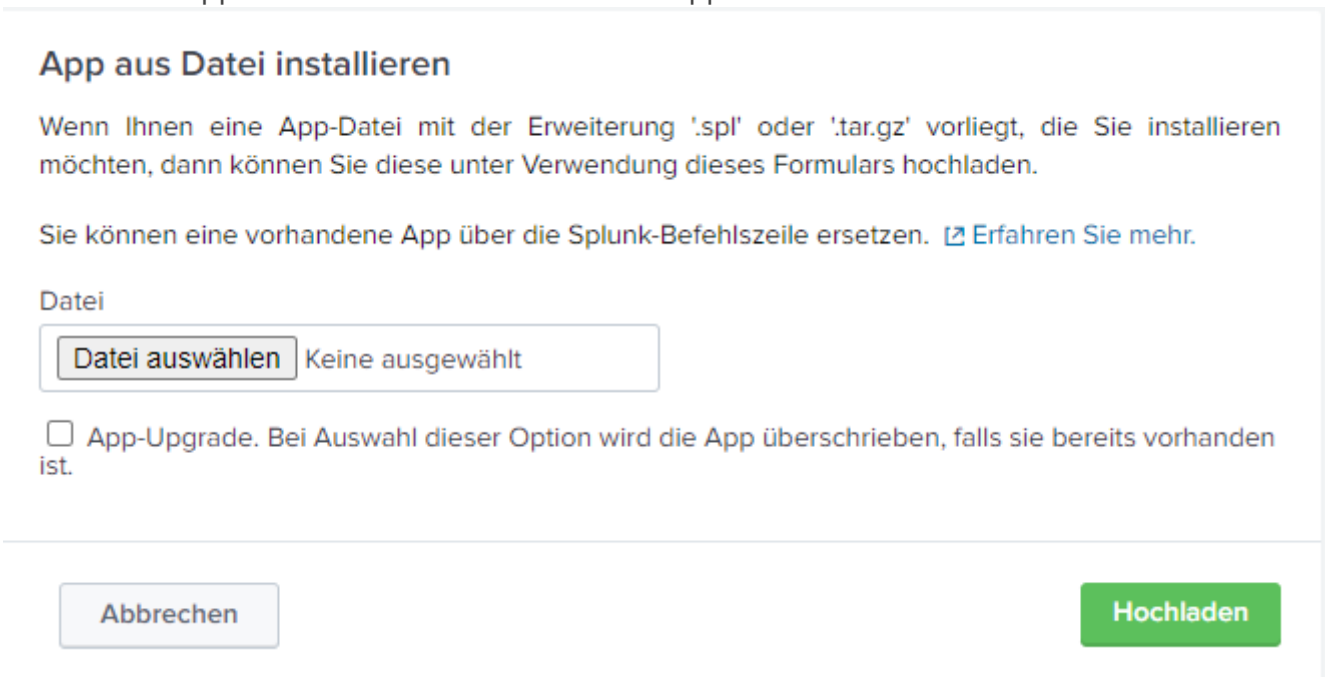
On the gs-

Wheel"

We are getting redirected to the main Apps and Addons page. Top right corner we are able to install apps of a file:

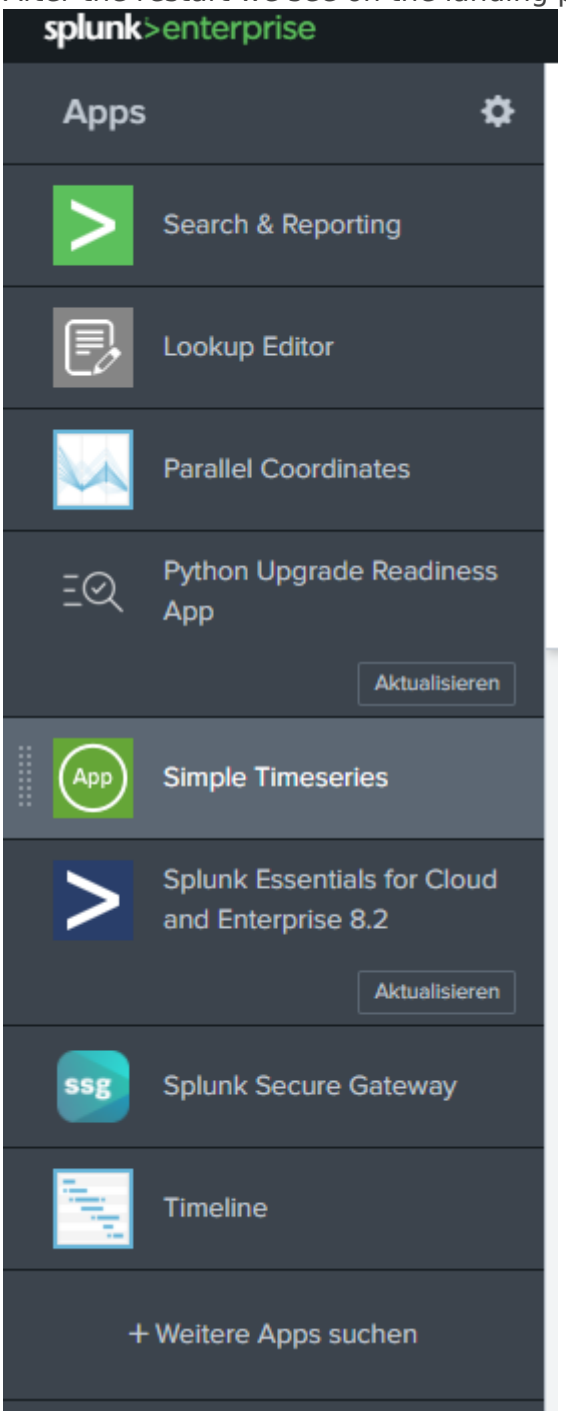


To install an app we click on the button "install app out of file":



Install all apps and restart the service.

After the restart we see on the landing page the newly added apps.



Install CTF Scoreboard

Now we install the CTF Scoreboard. Enter the directory of the apps and clone the repository:

> cd $SPLUNK_HOME/etc/apps

> sudo git clone https://github.com/splunk/SA-ctf_scoreboard

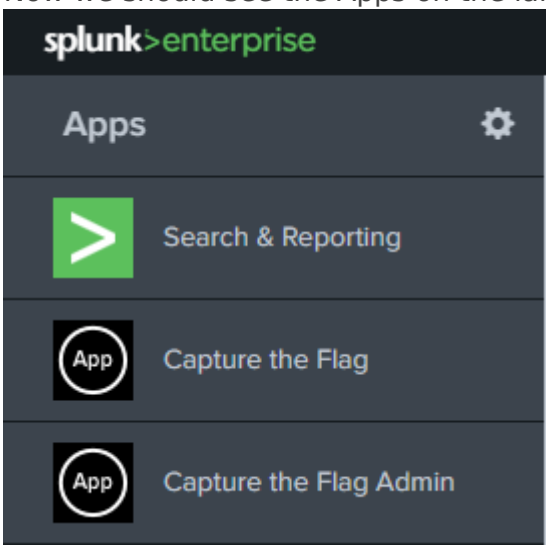
```
[togo@localhost apps]$ sudo git clone https://github.com/splunk/SA-ctf_scoreboard_admin
Cloning into 'SA-ctf_scoreboard_admin'...
remote: Enumerating objects: 459, done.
remote: Counting objects: 100% (17/17), done.
remote: Compressing objects: 100% (14/14), done.
remote: Total 459 (delta 3), reused 6 (delta 0), pack-reused 442
Receiving objects: 100% (459/459), 738.59 KiB | 9.72 MiB/s, done.
Resolving deltas: 100% (113/113), done.
[togo@localhost apps]$ ls
SA-ctf_scoreboard        journald_input              search                  sp
SA-ctf_scoreboard_admin  launcher                    simpletimeseries_app    sp
```

sudo git clone https://github.com/splunk/SA-ctf_scoreboard_admin

After you installed the Scoreboards we need to restart the service

> sudo $SPLUNK_HOME/bin/splunk restart

Now we should see the Apps on the landing page



Next we create the log folder for the scoreboard:

```
sudo mkdir $SPLUNK_HOME/var/log/scoreboard
```

Create CTF Answers service account cabanaboy

By convention this user is called cabanaboy because that’s what any rational person would pick while sitting next to Ryan Kovar

Pick a good strong password, and record it. You will need it again soon. The good news is that it does not need to be easily memorized by a human.

Assign the cabanaboy user to role ctf_answers_service

This can all be accomplished from the command line as follows:

```
sudo  $SPLUNK_HOME/bin/splunk add user cabanaboy -password <password> -role ctf_answers_service -auth admin:<admin_password>
```

Configure Scoreboard controller

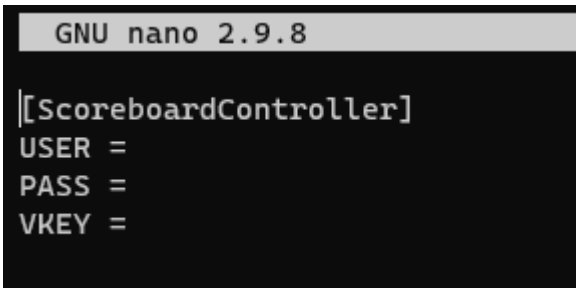
Access the log directory

```
cd $SPLUNK_HOME/etc/apps/SA-ctf_scoreboard/appserver/controllers
```

```
cp scoreboard_controller.config.example scoreboard_controller.config
```

Edit scoreboard_controller.config to reflect the following:

- The CTF Answers service account username (probably cabanaboy)
- The CTF Answers service account password you chose above
- A vkey parameter which should just be a random string, 10-20 characters in length



User: cabanaboy
Pass: **********
VKey: randomstringbytogo

neeed to write from here:

example file is included in the repository.

10. Restart Splunk to recognize the changes to the controller configuration file.

```
$SPLUNK_HOME/bin/splunk restart
```

11. Confirm the custom controller came up properly:

```
ls -l $SPLUNK_HOME/var/log/scoreboard
-rw------- 1 splunk staff 59 Sep 2 14:26 scoreboard.log
-rw------- 1 splunk staff 59 Sep 2 14:26 scoreboard_admin.log
```

12. Set up an admin user

- It does not need to be *the* Splunk admin user, but it can be and often is
- In Splunk Web ensure the admin user has been assigned the following roles:
- admin
- ctf_admin
- can_delete

13. Load sample data

- Log in as the admin user created above
- Navigate to Capture the Flag Admin app
- Click each of the following menu items in turn:
    - Data Management...->Load SAMPLE data (DANGER)->Load sample users/teams
    - Data Management...->Load SAMPLE data (DANGER)->Load sample questions
    - Data Management...->Load SAMPLE data (DANGER)->Load sample answers
    - Data Management...->Load SAMPLE data (DANGER)->Load sample hints
    - Data Management...->Load SAMPLE data (DANGER)->Load sample hint entitlements
    - Data Management...->Load SAMPLE data (DANGER)->Load sample badges
    - Data Management...->Load SAMPLE data (DANGER)->Load sample badge entitlements
    - Data Management...->Load SAMPLE data (DANGER)->Load sample user agreements
- It's not *really* dangerous, but it will overwrite the data you currently have loaded in the game.

https://run-as-root.com/2021/06/08/splunk-botsv3-install-and-configuration/