

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.

Name und Betriebssystem

Bitte wählen Sie einen angemessenen Namen und Speicherort für die neue virtuelle Maschine. Dann wählen Sie den Typ des Betriebssystems, das Sie installieren möchten. Der gewählte Name wird zur Identifizierung dieser Maschine verwendet.

Name:

Ordner der virtuellen Maschine:

Typ:

Version:

Set the RAM to ca. 4GB:

Speichergöße

Wählen Sie die Größe des Hauptspeichers (RAM) der virtuellen Maschine in Megabyte.

Die empfohlene Größe beträgt **1024 MB**.

MB

4 MB 32768 MB

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

Dateiname und Größe

Bitte geben Sie den Namen der neuen Festplatte an oder wählen Sie das Ordner-Icon, um einen anderen Ordner für die Datei zu wählen.

Wählen Sie die Größe der virtuellen Festplatte in Megabyte. Dies ist die maximal nutzbare Größe der virtuellen Festplatte.

4.00 MB 2.00 TB

Now the VM is ready to start but we need to specify some settings.

First we set the clipboard to bidirectional mode:

Allgemein

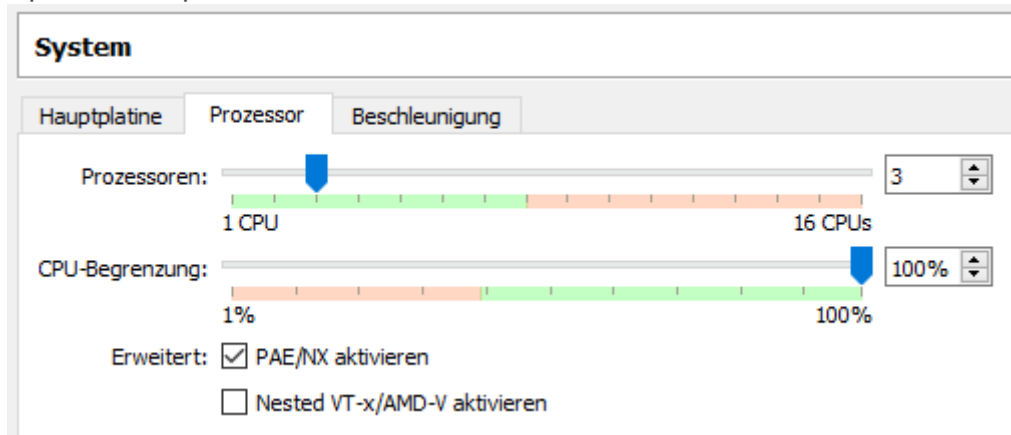
Basis | Erweitert | Beschreibung | Festplattenverschlüsselung

Ordner Sicherungspunkte:

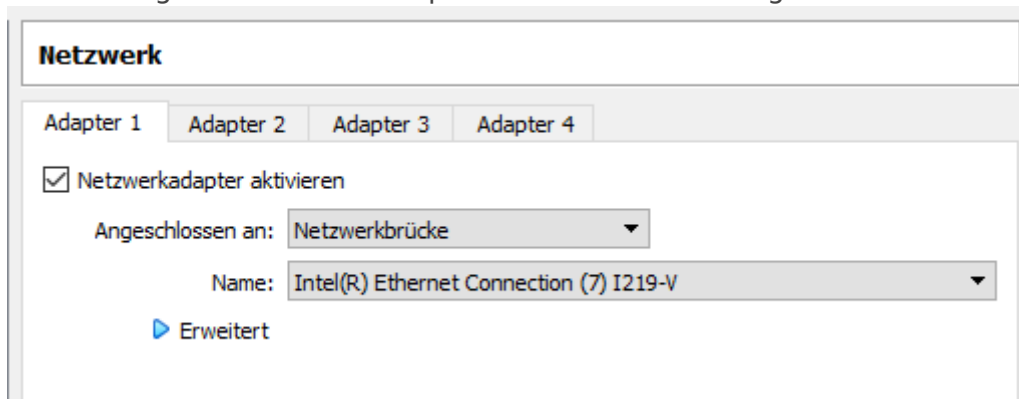
Gemeinsame Zwischenablage:

Drag'n'Drop:

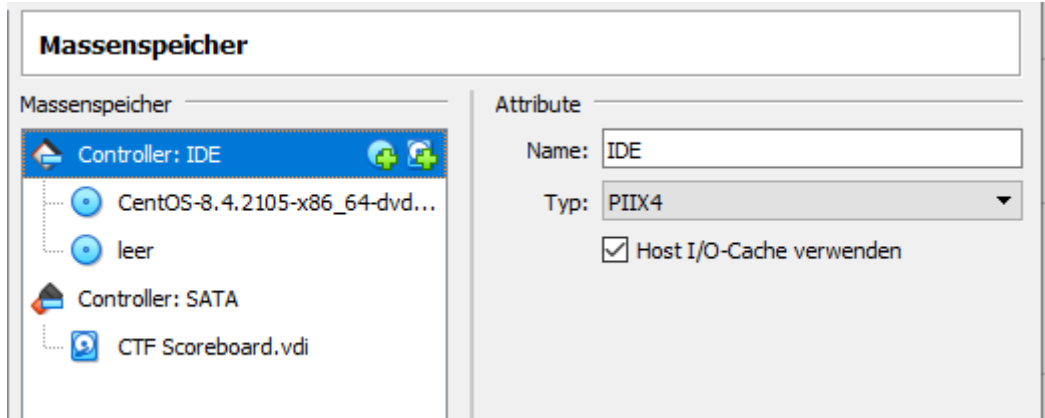
Upscale the processor to minimum 2 cores:



Then change the network adapter to the Network bridge:



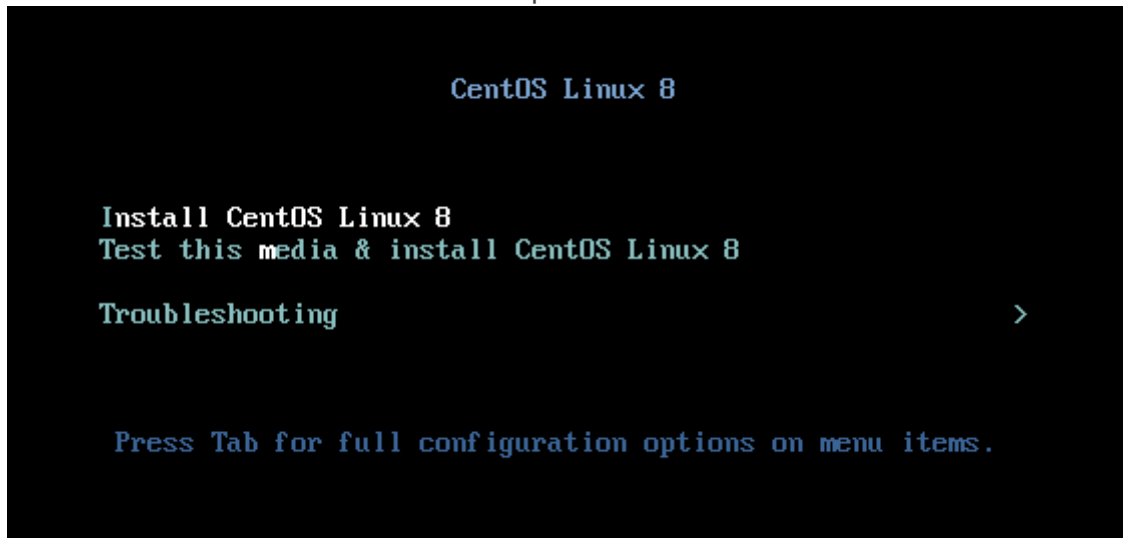
And finally add the ISO File to the storage:



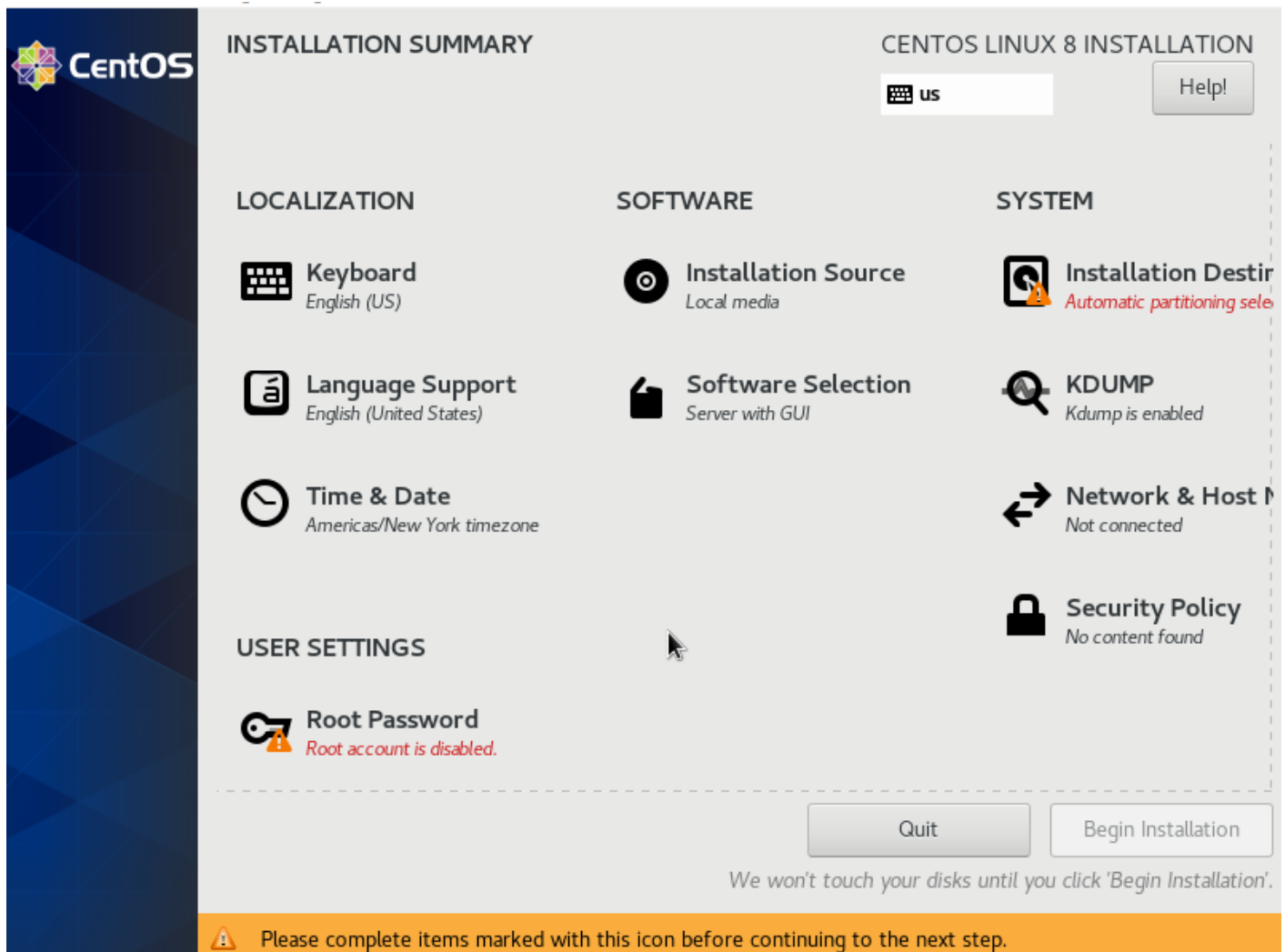
Now we can start the machine and configure the setup.

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:

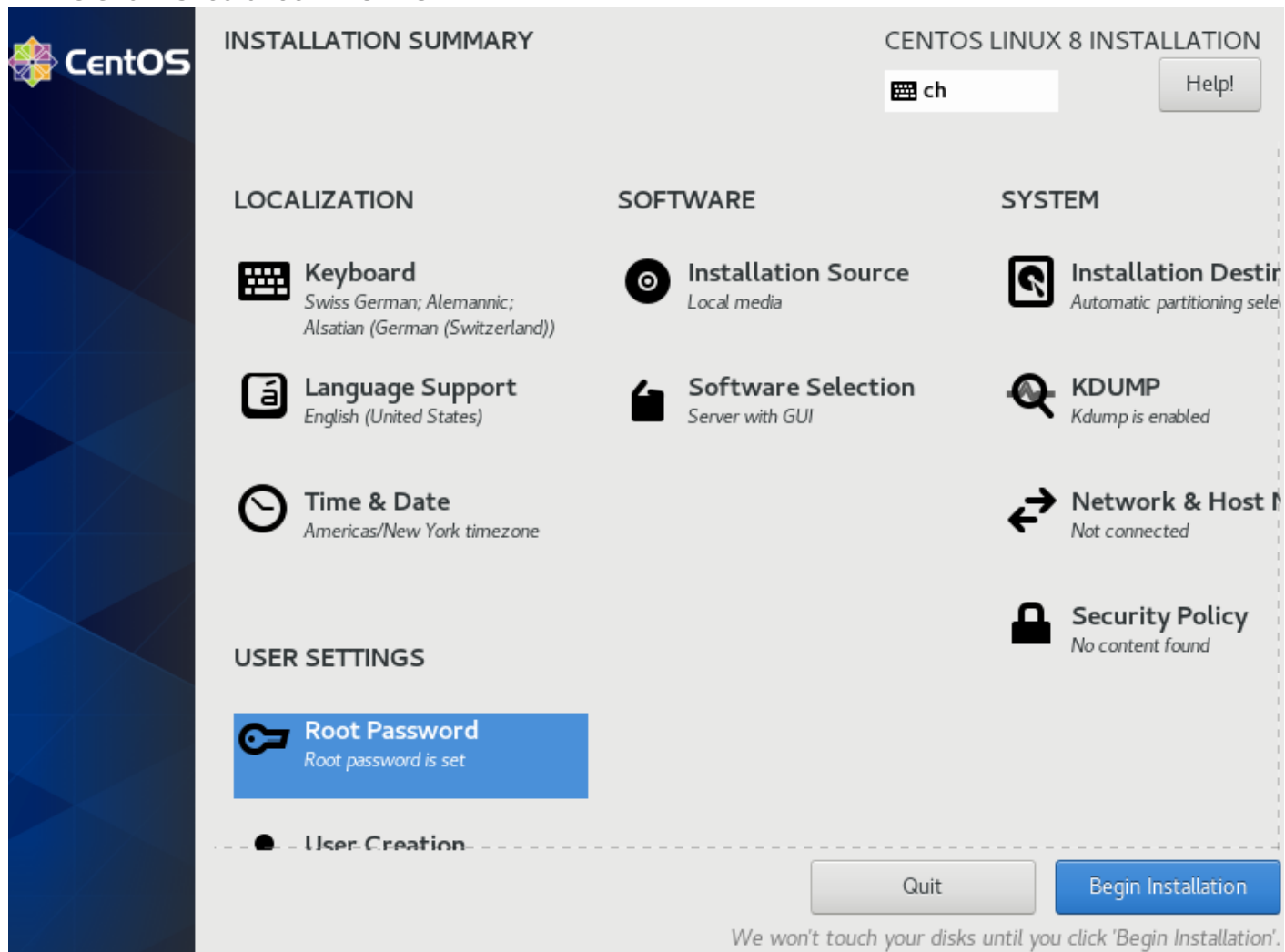


Set the Keyboard to Swissgerman.

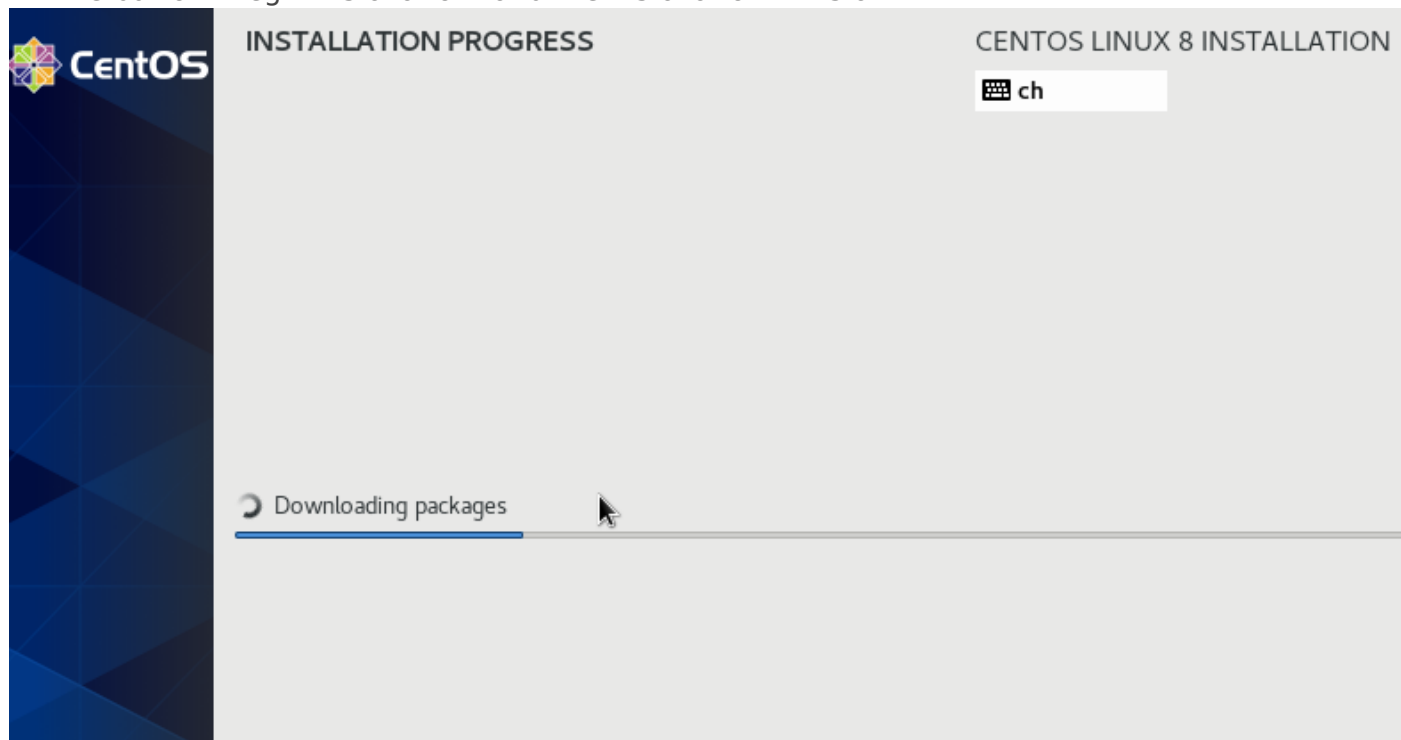
Change the root password.

Define the partition to install the OS. Usually I choose automatic and use the whole disk.

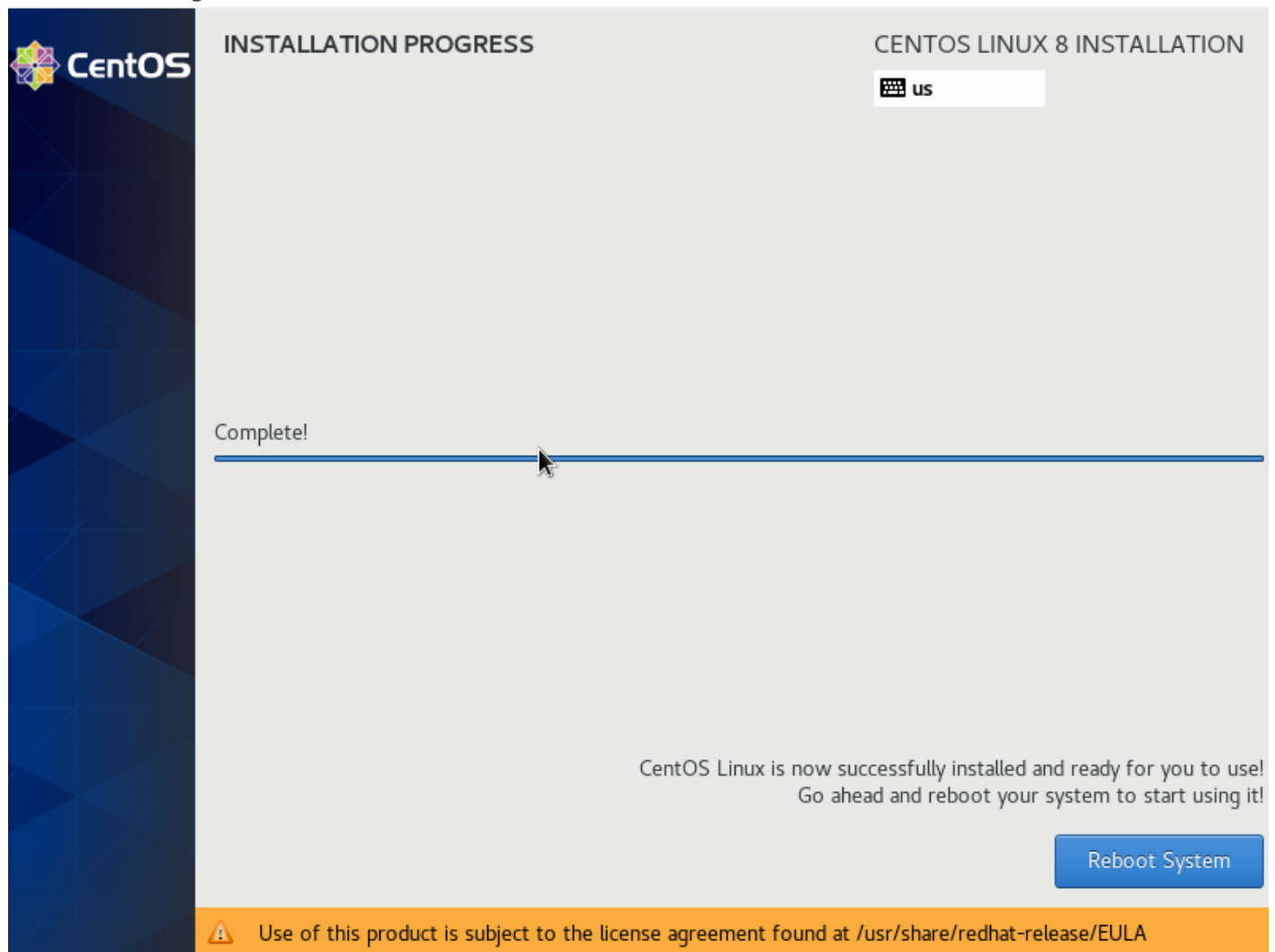
At the end it should look like this:



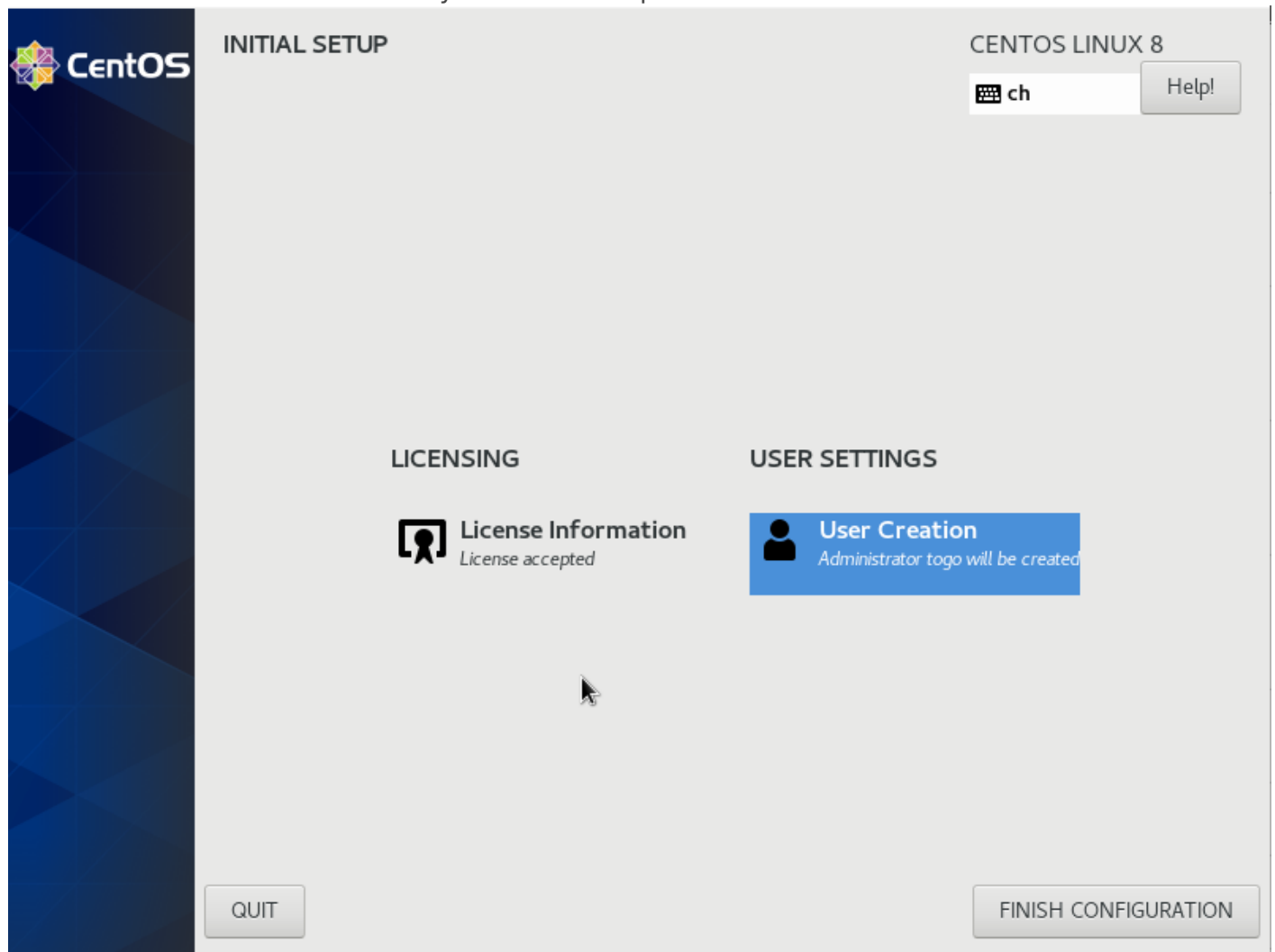
Hit the button "Begin Installation" and the installation will start:



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

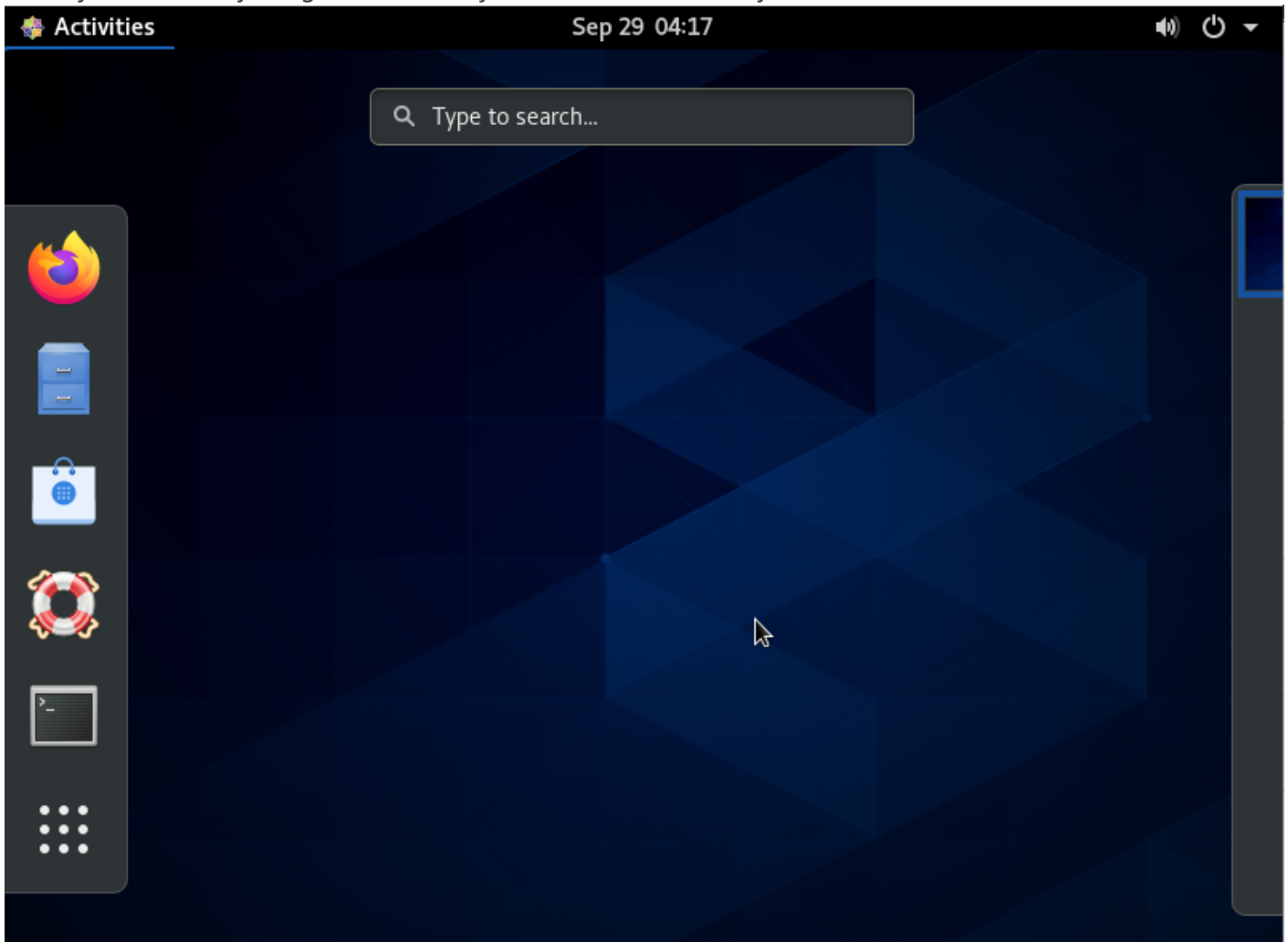


Once rebooted set a user on the system and accept the EULA disclaimer:



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 inactive
```

```
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.

 Windows	 Linux	 Mac OS
64-bit	2.6+, 3.x+, 4.x+, or 5.4.x kernel Linux distributions	
	.tgz	542.94 MB
		Download Now 
	.rpm	543.74 MB
		Download Now 
	.deb	414.12 MB
		Download Now 

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  
[togo@localhost Downloads]$
```

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  
[root@localhost Downloads]#
```

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 ]

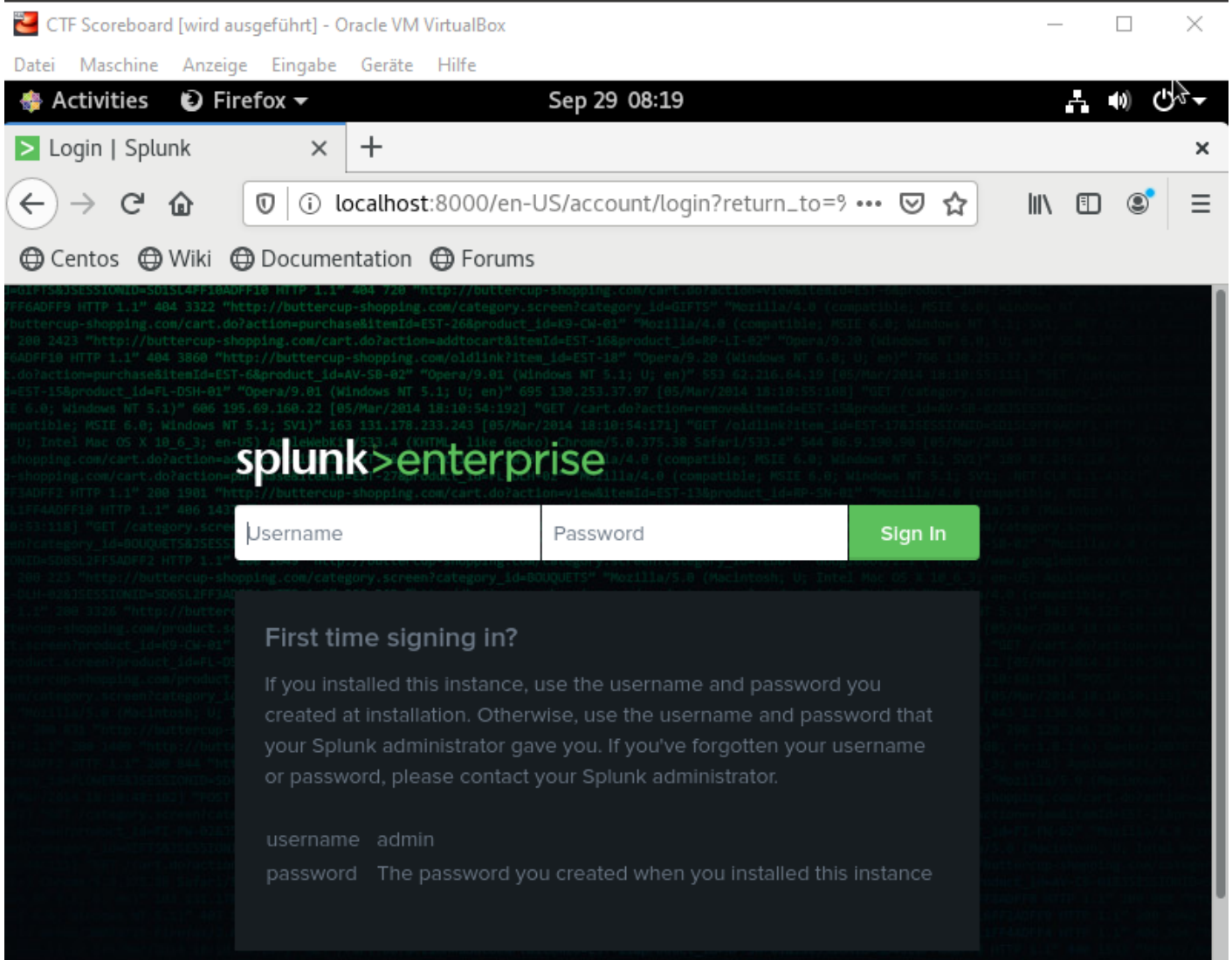
Waiting for web server at http://127.0.0.1:8000 to be available..... Done

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]$
```

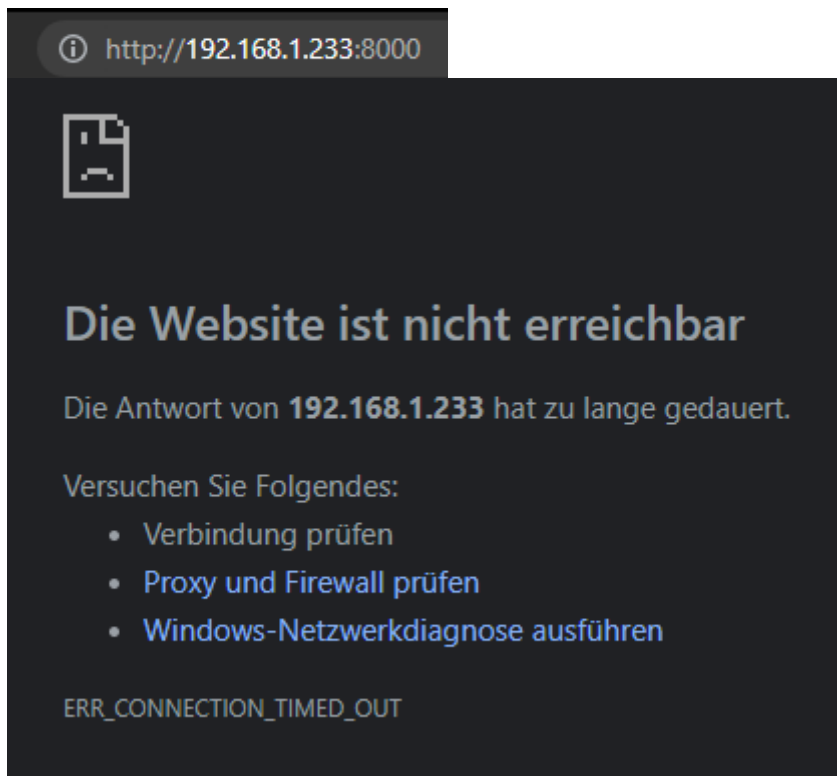
By checking on the browser in the CentOS VM localhost:8000 we should see a Splunk login screen:



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.

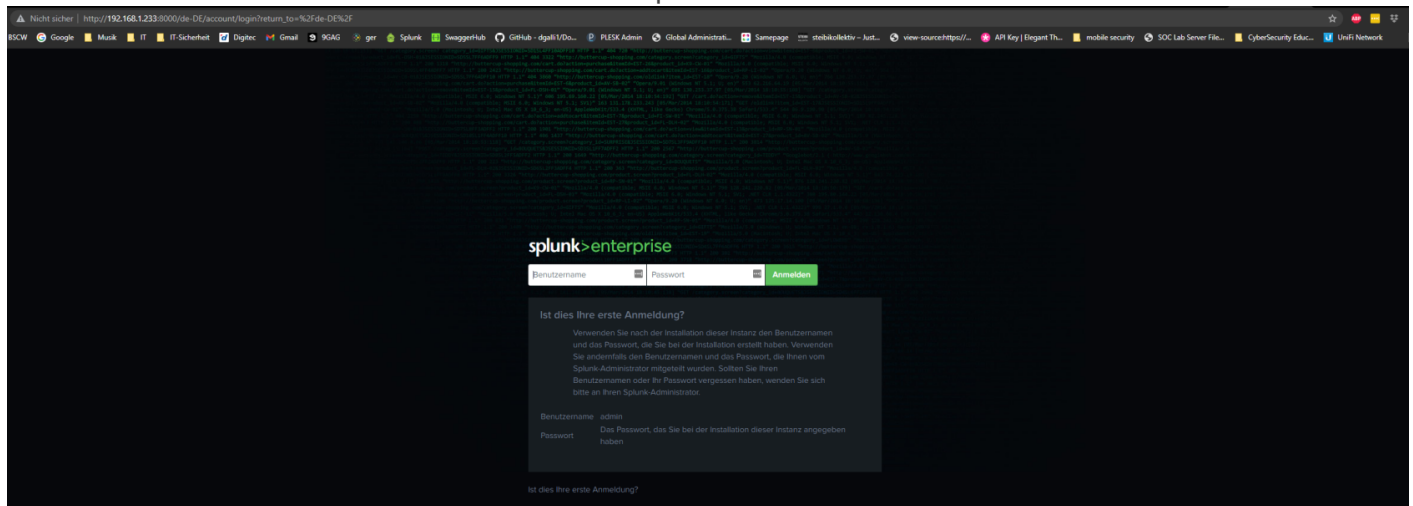
The guide how to change firewall rules can be found here:

<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.



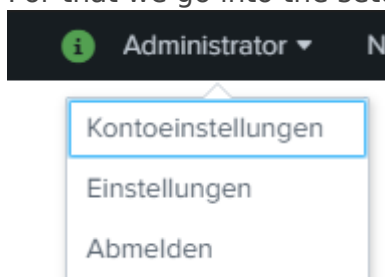
Configure Splunk

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.



Einstellungen


Global


SPL-Editor

Verwenden Sie diese Eigenschaften, um Zeitzone, Standardanwendung und standardmäßige Suchzeitpannenauswahl festzulegen. Sie können auch angeben, ob Hintergrundaufräge bei einem Neustart der Splunk-Software neu gestartet werden sollen.

Zeitzone

(GMT+01:00) Amsterdam, Berlin, Bern, Rom, Stockh... ▾

Legen Sie eine Zeitzone für diesen Benutzer fest.

Standardanwendung

Home ▾

Diese Einstellung überschreibt jede Standardanwendung.

Hintergrundaufträge neu starten

☐

Starten Sie Hintergrundaufräge neu, wenn die Splunk-Software neu gestartet wird.

Abbrechen

Anwenden

Easy!

Next thing to do is enable HTTPS.

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

Administrator ▾

Nachrichten ▾

Einstellungen ▾

Aktivität ▾

Hilfe ▾

Suchen



Daten hinzufügen



Daten untersuchen



Monitoring-Konsole

WISSEN

Suchen, Berichte und Benachrichtigungen

Datenmodelle

Eventtypen

Tags

Felder

Lookups

Benutzeroberfläche

Benachrichtigungsaktionen

Erweiterte Suche

Alle Konfigurationen

SYSTEM

Server-Einstellungen

Serversteuerungen

Zustandsbericht-Manager

RapidDiag

Instrumentation

Lizenzierung

Workload-Management

DATEN

Dateneingaben

Weiterleiten und empfangen

Indizes

Zusammenfassungen für die beschleunigte Berichtserstellung

Virtuelle Indizes

Sourcetypen

VERTEILTE UMGEBUNG

Indexer-Clustering

Forwarder-Management

Data Fabric

Federated search

Verteilte Suche

BENUTZER UND

AUTHENTISIERUNG

Rollen

Benutzer

Token

Passwortverwaltung

Authentisierungsmethoden

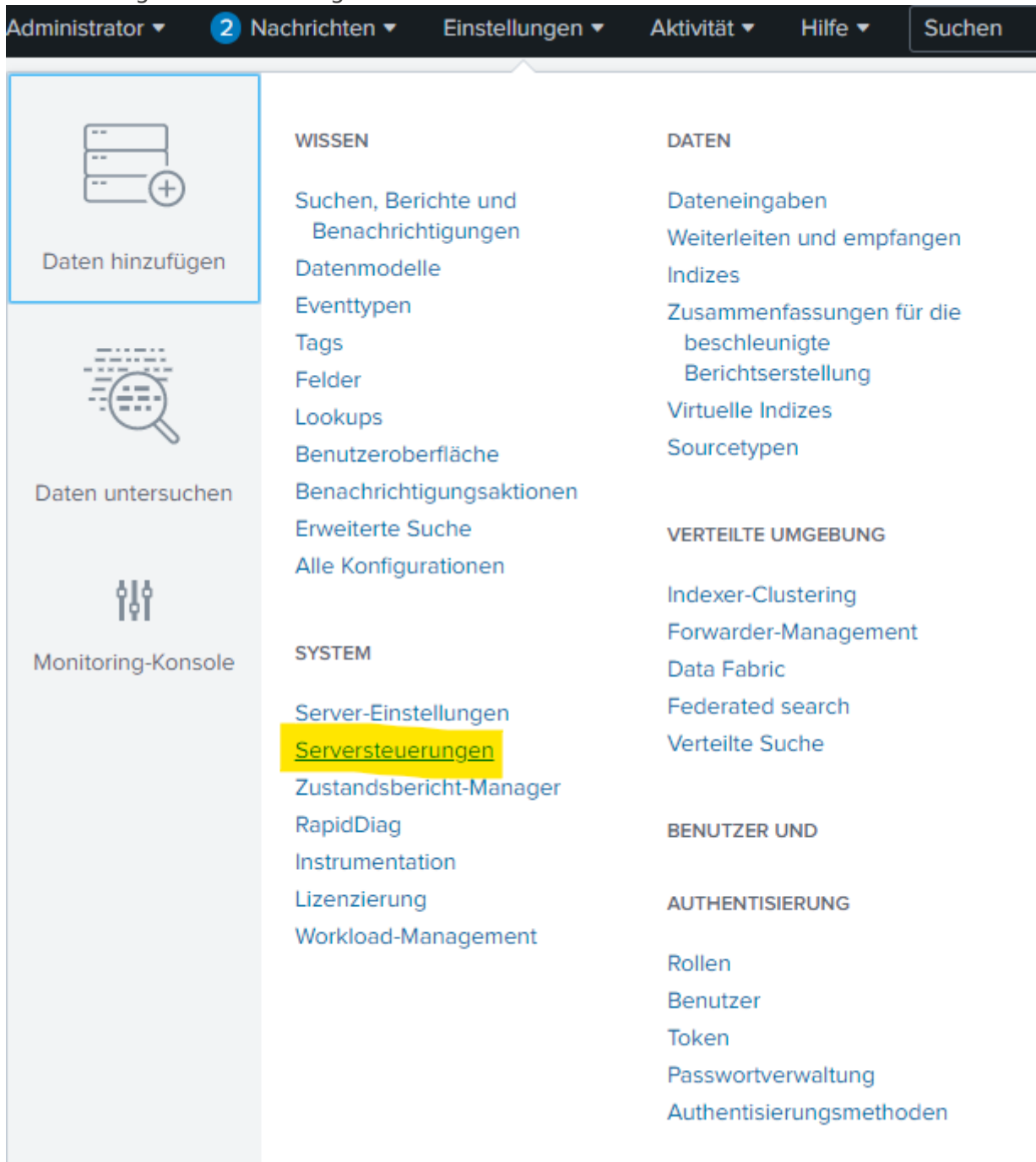
Then we access the general settings

Allgemeine Einstellungen
Hintergrund der Anmeldung
Globales Banner
E-Mail-Einstellungen
Server-Protokollierung
Verteilungs-Client
Sucheinstellungen

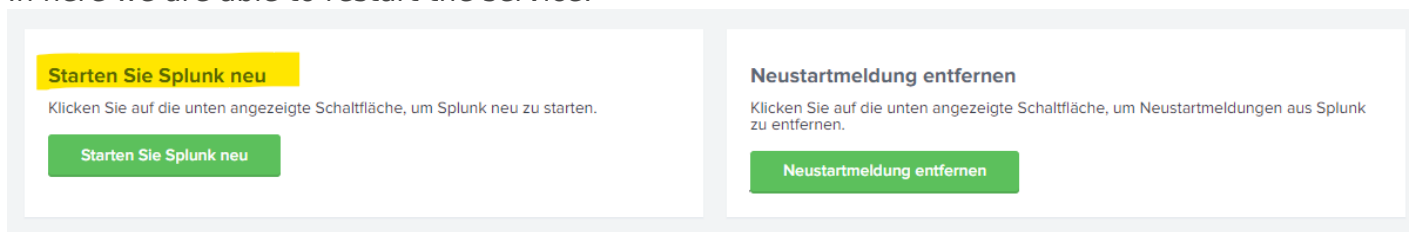
In the general setting we choose "enable HTTPS in Splunk Web":

Splunk-Server-Name *	localhost.localdomain
Installationspfad	/opt/splunk
Verwaltungs-Port *	8089
Port, der von Splunk Web zur Kommunikation mit dem splunkd-Prozess verwendet wird. Dieser Port wird auch für die verteilte Suche verwendet.	
Vertrauenswürdige SSO-IP	
Die IP-Adresse, über die vertrauenswürdige Anmeldungen akzeptiert werden. Legen Sie diese Option nur bei Verwendung von SSO (Single Sign-On) mit einem Proxy-Server für die Authentifizierung fest.	
Splunk Web	
Splunk Web ausführen	☒ Ja ☐ Nein
SSL (HTTPS) in Splunk Web aktivieren?	☒ Ja ☐ Nein
Web-Port *	8000
Anwendungsserver-Ports	8065
Port-Nummer(n) für den Python-basierten Anwendungsserver, der bzw. die überwacht werden soll(en). Zur Angabe mehrerer Port-Nummern trennen Sie diese durch Kommas.	
Sitzungs-Timeout *	1h
Legen Sie das Timeout für die Splunk Web-Sitzung fest. Verwenden Sie dieselbe Notation wie zugehörige Zeitmodifizierer, zum Beispiel 3h, 100s, 6d.	

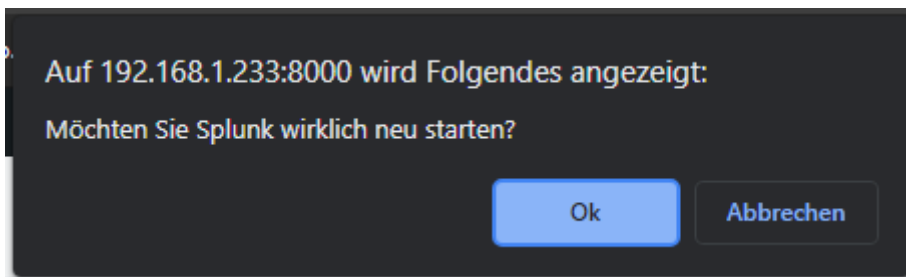
After the HTTPS box is checked we need to perform a restart of the Splunk service. To initiate a restart we go to the "Settings" tab and choose Server-Control:



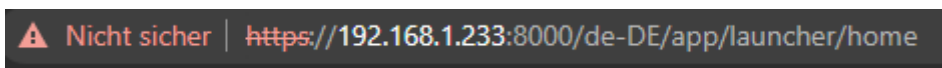
In here we are able to restart the service:



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

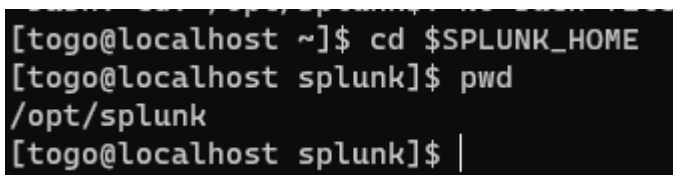


Click on the URL and you'll get redirected to the HTTPS login



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)

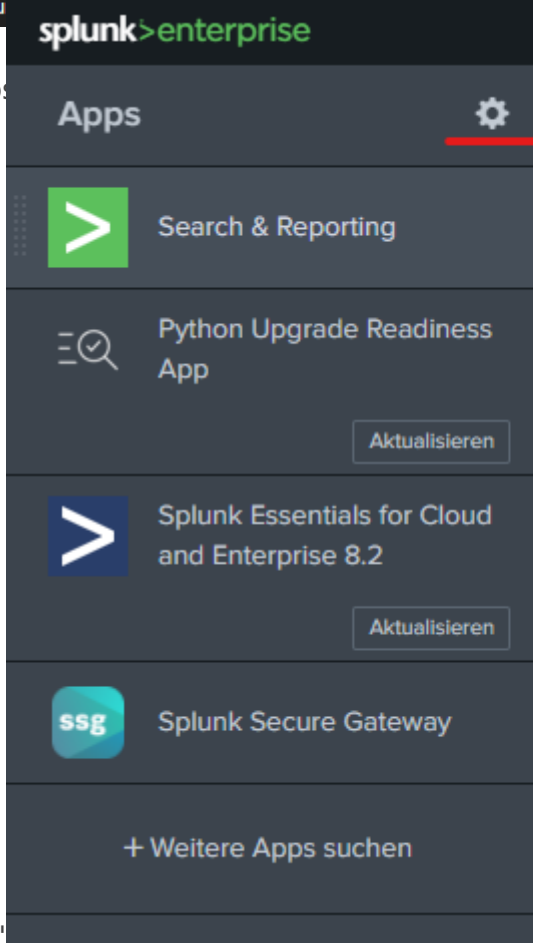
[Simple Timeseries Custom Visualization](#) (Note: Tested with version 1.0)

[Timeline Custom Visualization](#) (Note: Tested with version 1.2.0)

lookup-file-editor_350.tgz	28.09.2021 16:02
parallel-coordinates-custom-visualization_150.tgz	28.09.2021 16:02
simple-timeseries-custom-visualization_10.tgz	28.09.2021 16:03
splunk_..._...	-----

All apps

On the



Splunk Enterprise untersuchen

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:

Apps							
Angezeigt werden 1-24 von 24 Elementen							
Filter Q Weitere Apps durchsuchen App aus Datei installieren App erstellen 25 pro Seite							
Name	Ordnername	Version	Suchen nach Updates	Sichtbar	Freigabe	Status	Aktionen
SplunkForwarder	SplunkForwarder		Yes	No	App Berechtigungen	Deaktiviert Aktivieren	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App Berechtigungen	Deaktiviert Aktivieren	
Log Event Alert Action	alert_logevent	8.2.21	Yes	No	App Berechtigungen	Aktiviert Deaktivieren	Eigenschaften bearbeiten Objekte anzeigen
Webhook Alert Action	alert_webhook	8.2.21	Yes	No	App Berechtigungen	Aktiviert Deaktivieren	Eigenschaften bearbeiten Objekte anzeigen
Apps Browser	appstrower	8.2.21	Yes	No	App Berechtigungen	Aktiviert	Eigenschaften bearbeiten Objekte anzeigen
Introspection_generator_addon	introspection_generator_addon	8.2.21	Yes	No	App Berechtigungen	Aktiviert Deaktivieren	Eigenschaften bearbeiten Objekte anzeigen
Journald_input	journald_input		Yes	No	App Berechtigungen	Aktiviert Deaktivieren	Eigenschaften bearbeiten Objekte anzeigen
Home	launcher		Yes	Yes	App Berechtigungen	Aktiviert	App starten Eigenschaften bearbeiten Objekte anzeigen
learned	learned		Yes	No	App Berechtigungen	Aktiviert Deaktivieren	Eigenschaften bearbeiten Objekte anzeigen
legacy	legacy		Yes	No	App Berechtigungen	Deaktiviert Aktivieren	
Python Upgrade Readiness App	python_upgrade_readiness_app	1.0.0 Aktualisieren auf 3.01	Yes	Yes	App Berechtigungen	Aktiviert Deaktivieren	App starten Eigenschaften bearbeiten Objekte anzeigen Details aus Splunkbase anzeigen
sample data	sample_app		Yes	No	App Berechtigungen	Deaktiviert Aktivieren	
Search & Reporting	search	8.2.21	Yes	Yes	App Berechtigungen	Aktiviert	App starten Eigenschaften bearbeiten Objekte anzeigen
Splunk Dashboard Studio	splunk-dashboard-studio	11.0	Yes	Yes	App Berechtigungen	Aktiviert Deaktivieren	App starten Eigenschaften bearbeiten Objekte anzeigen
Splunk Archiver App	splunk_archiver	1.0	Yes	No	App Berechtigungen	Aktiviert Deaktivieren	Eigenschaften bearbeiten Objekte anzeigen Details aus Splunkbase anzeigen
Splunk Essentials for Cloud and Enterprise 8.2	splunk_essentials_8_2	0.3.0 Aktualisieren auf 1.0.0	Yes	Yes	App Berechtigungen	Aktiviert Deaktivieren	App starten Eigenschaften bearbeiten Objekte anzeigen Details aus Splunkbase anzeigen
Splunk Get Data In	splunk_gdi	1.0.4	Yes	No	App Berechtigungen	Aktiviert	Eigenschaften bearbeiten Objekte anzeigen
splunk_httpinput	splunk_httpinput		Yes	No	App Berechtigungen	Aktiviert Deaktivieren	Eigenschaften bearbeiten Objekte anzeigen
Instrumentation	splunk_instrumentation	5.6.1	Yes	Yes	App Berechtigungen	Aktiviert	App starten Eigenschaften bearbeiten Objekte anzeigen
Clone Internal Metrics into Metrics Index	splunk_internal_metrics		Yes	No	App Berechtigungen	Aktiviert Deaktivieren	Eigenschaften bearbeiten Objekte anzeigen
Splunk Analytics Workspace	splunk_metrics_workspace	1.4.15	Yes	Yes	App Berechtigungen	Aktiviert Deaktivieren	App starten Eigenschaften bearbeiten Objekte anzeigen
Monitoring Console	splunk_monitoring_console	8.2.21	Yes	Yes	App Berechtigungen	Aktiviert Deaktivieren	App starten Eigenschaften bearbeiten Objekte anzeigen
Splunk RapidDiag	splunk_rapid_diag	1.4.0	Yes	Yes	App Berechtigungen	Aktiviert Deaktivieren	App starten Eigenschaften bearbeiten Objekte anzeigen
Splunk Secure Gateway	splunk_secure_gateway	2.7.4	Yes	Yes	App Berechtigungen	Aktiviert Deaktivieren	App starten Eigenschaften bearbeiten Objekte anzeigen Details aus Splunkbase anzeigen

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

App aus Datei installieren

Wenn Ihnen eine App-Datei mit der Erweiterung '.spl' oder '.tar.gz' vorliegt, die Sie installieren möchten, dann können Sie diese unter Verwendung dieses Formulars hochladen.

Sie können eine vorhandene App über die Splunk-Befehlszeile ersetzen. [Erfahren Sie mehr.](#)

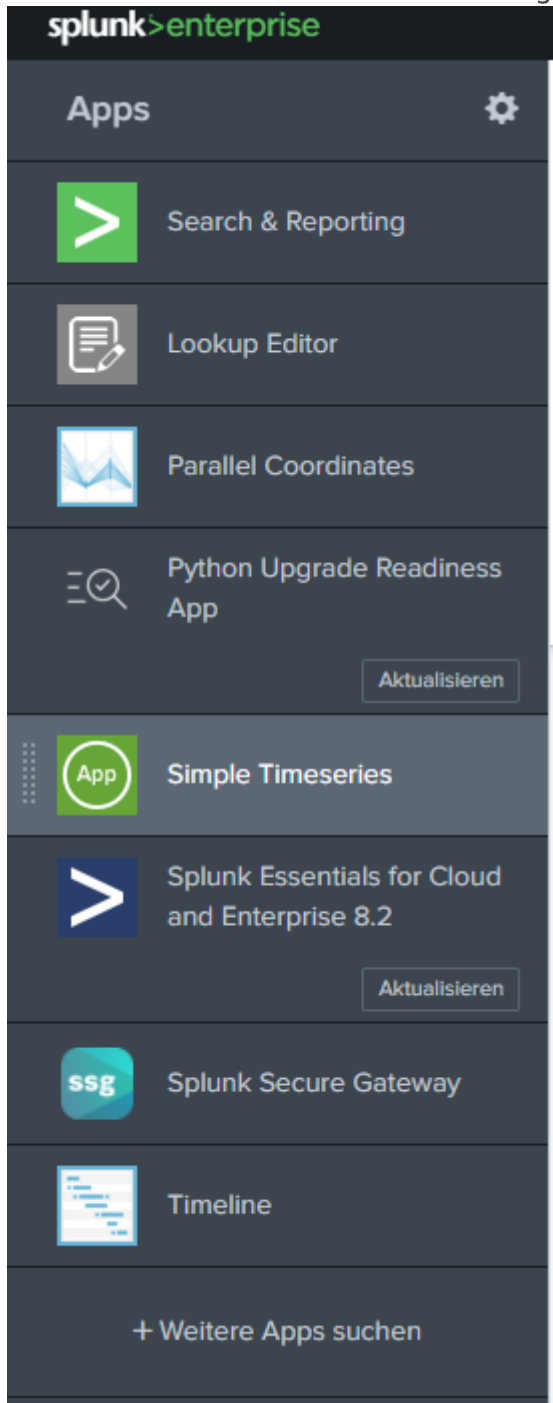
Datei

Keine ausgewählt

☐ App-Upgrade. Bei Auswahl dieser Option wird die App überschrieben, falls sie bereits vorhanden ist.

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
```

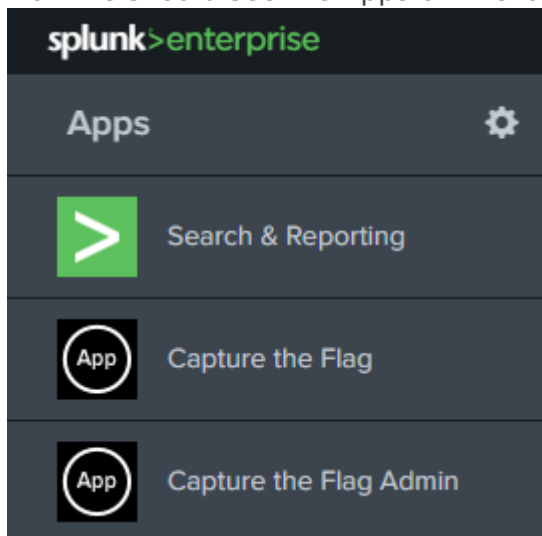
```
[togo@localhost apps]$ sudo git clone https://github.com/splunk/SA-ctf_scoreboard_admin
Cloning into 'SA-ctf_scoreboard_admin'...
remote: Enumerating objects: 459, done.
remote: Counting objects: 100% (17/17), done.
remote: Compressing objects: 100% (14/14), done.
remote: Total 459 (delta 3), reused 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

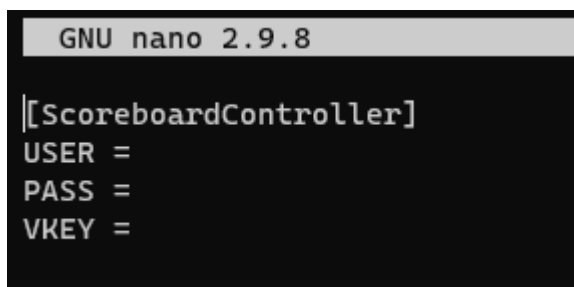
Access the log directory

```
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

A screenshot of a terminal window with a black background. At the top, a grey header bar reads "GNU nano 2.9.8". Below it, the text "[ScoreboardController]" is displayed. Underneath, there are three lines of configuration: "USER =", "PASS =", and "VKEY =", each followed by a blank line for input.

User: cabanaboy

Pass: *****

VKey: randomstringbytogo

need 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/>