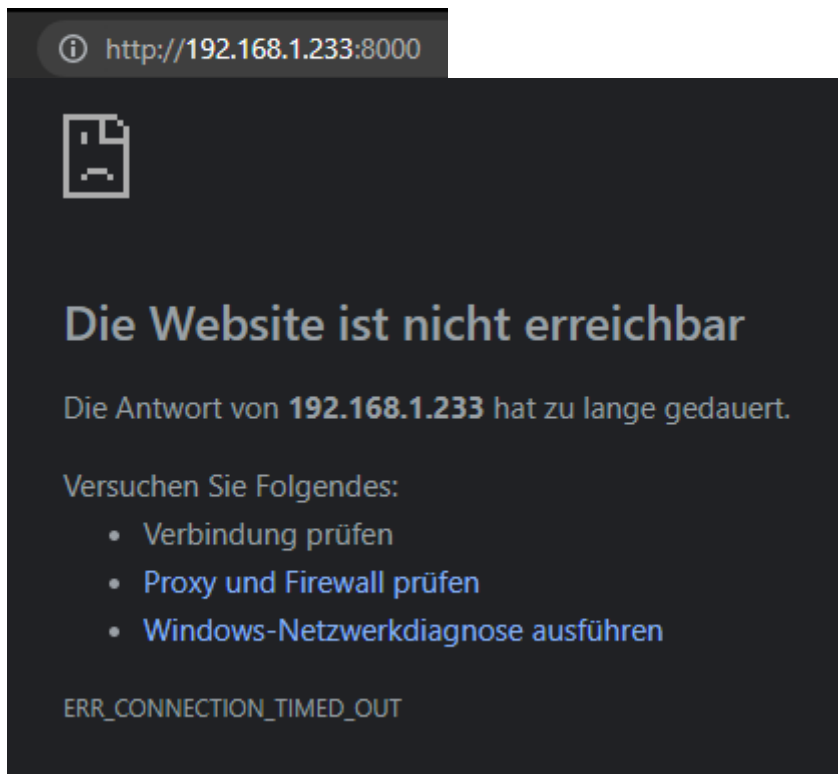


Configure Firewall & Splunk

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.

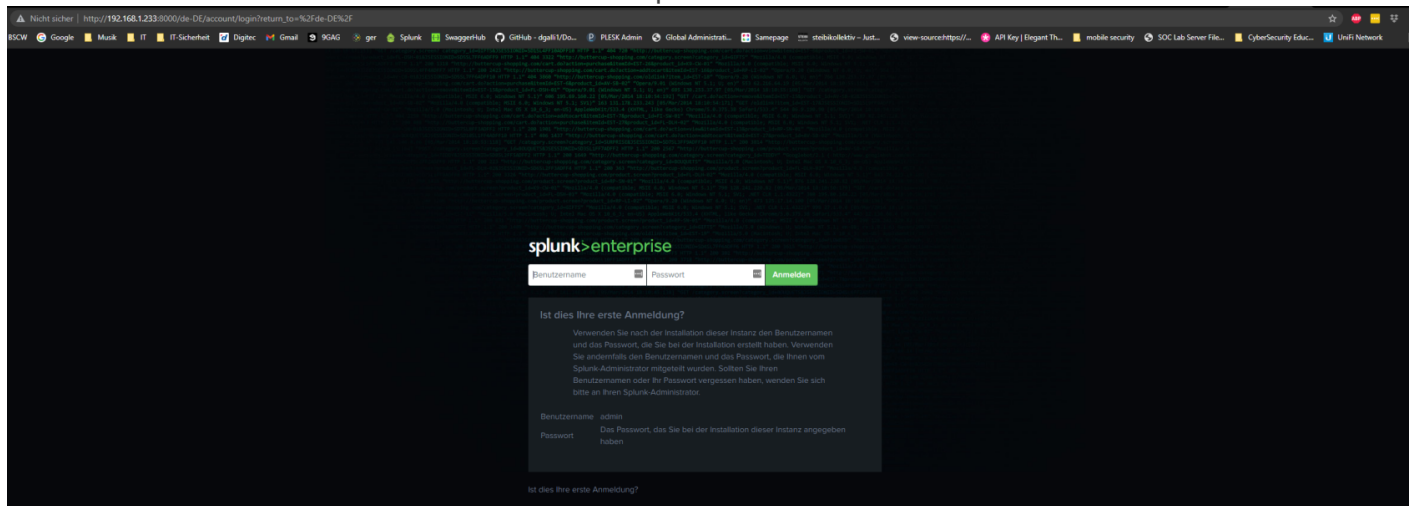
The guide how to change firewall rules can be found here:

<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.



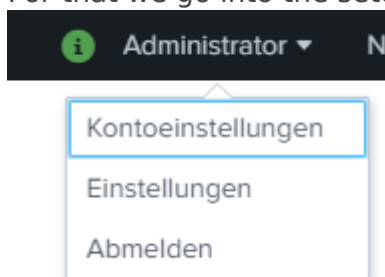
Configure Splunk

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

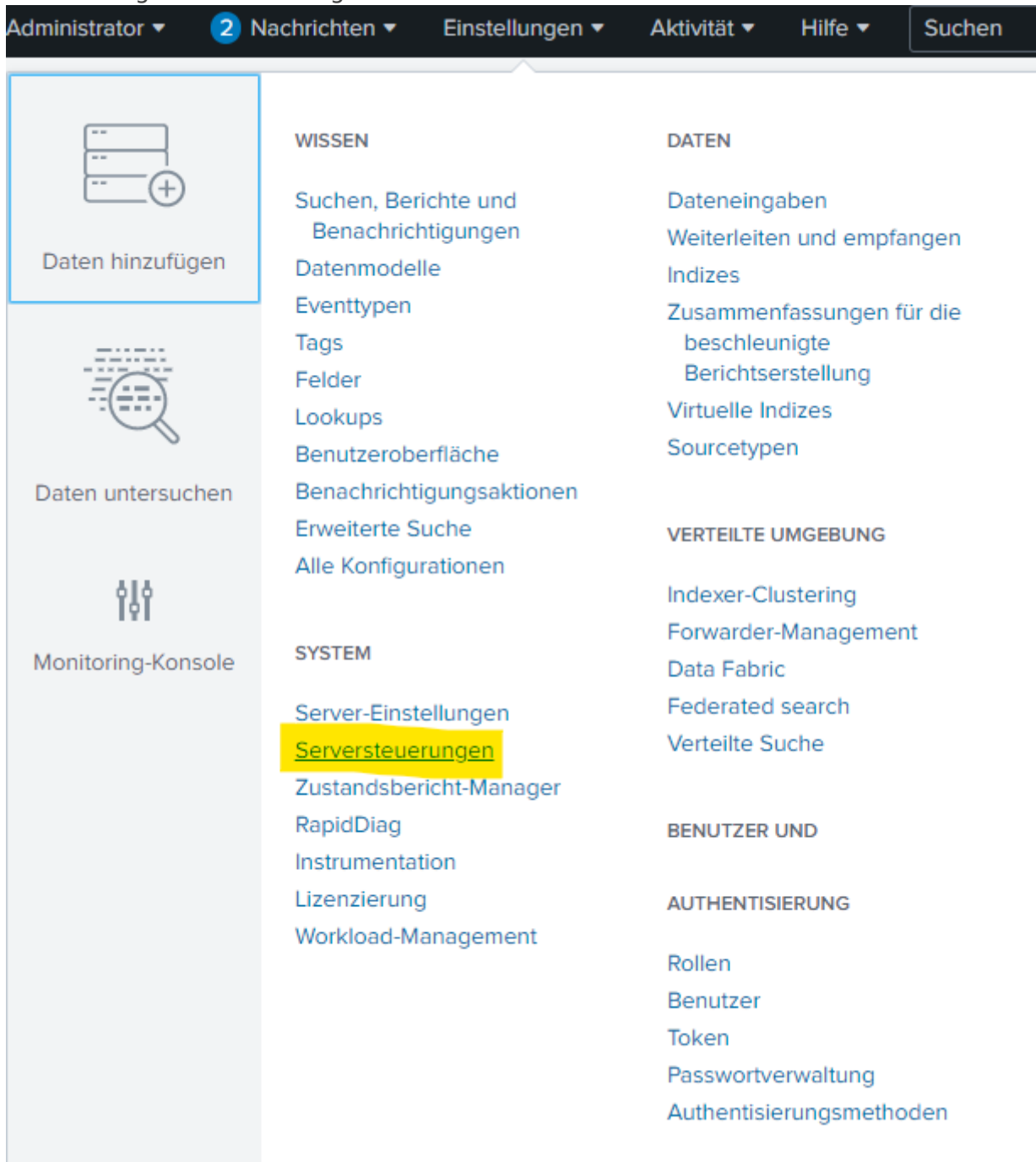
Then we access the general settings

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

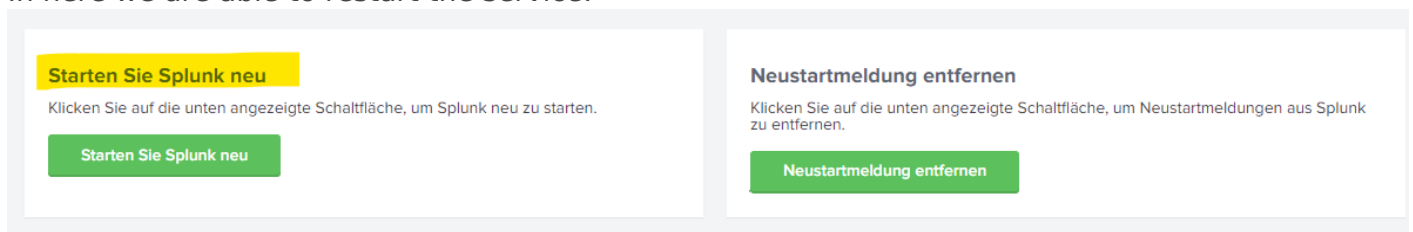
In the general setting we choose "enable HTTPS in Splunk Web":

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.	

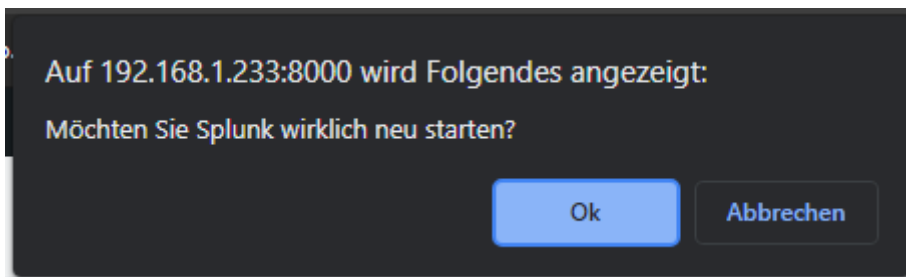
After the HTTPS box is checked we need to perform a restart of the Splunk service. To initiate a restart we go to the "Settings" tab and choose Server-Control:



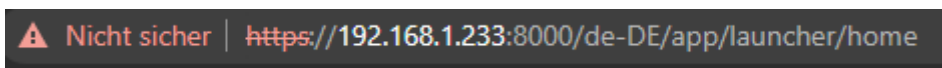
In here we are able to restart the service:



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

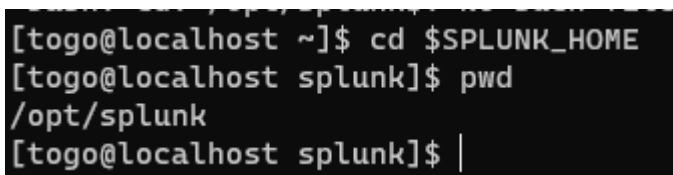


Click on the URL and you'll get redirected to the HTTPS login



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)

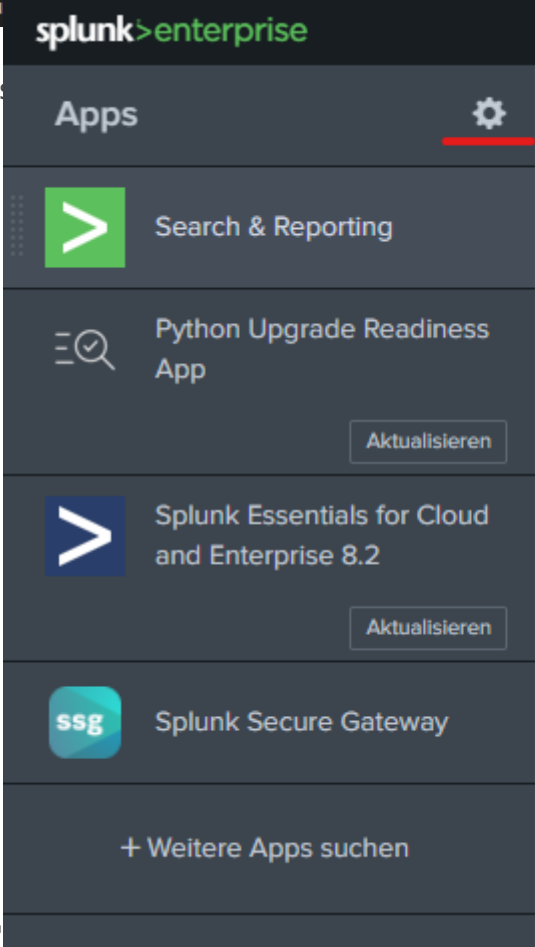
[Simple Timeseries Custom Visualization](#) (Note: Tested with version 1.0)

[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

Anzeigt 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	5.61	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

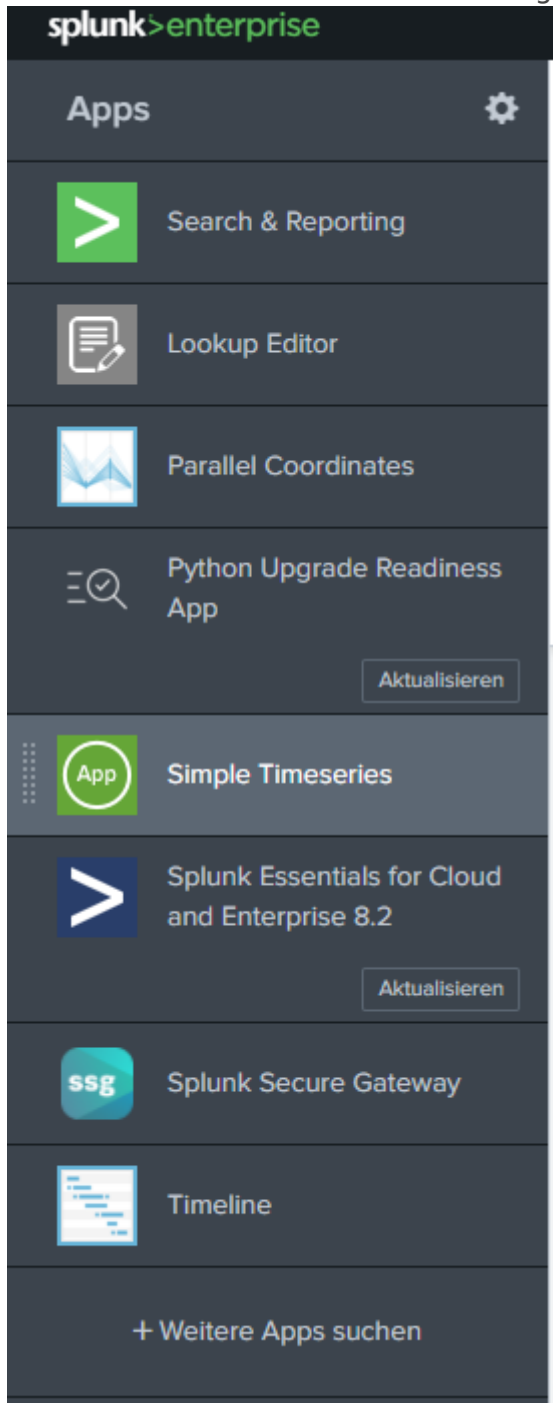
☐ App-Upgrade. Bei Auswahl dieser Option wird die App überschrieben, falls sie bereits vorhanden ist.

Abbrechen

Hochladen

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
```

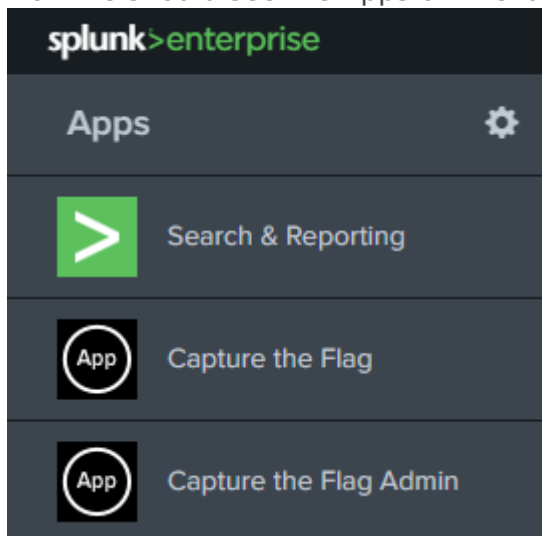
```
[togo@localhost apps]$ sudo git clone https://github.com/splunk/SA-ctf_scoreboard_admin
Cloning into 'SA-ctf_scoreboard_admin'...
remote: Enumerating objects: 459, done.
remote: Counting objects: 100% (17/17), done.
remote: Compressing objects: 100% (14/14), done.
remote: Total 459 (delta 3), reused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

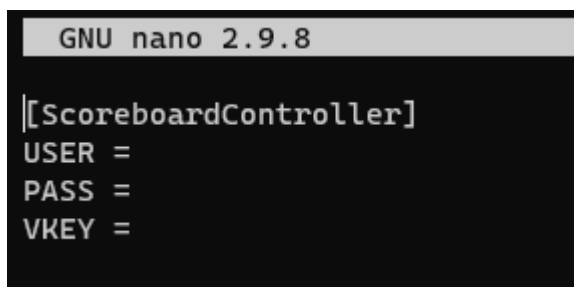
Access the log directory

```
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/>

Revision #3

Created 9 July 2022 07:59:10 by Togoboi

Updated 10 July 2022 08:33:14 by Togoboi