

Dokumentation Deployment einer Rest API

Autor: Gerrit Koppe

Ausbildungsberuf: Fachinformatiker für Anwendungsentwicklung

Klasse: IFA12

Lernfeld 9: Netzwerke und Dienste bereitstellen

11. Juni 2023

Anmerkungen

Aus Gründen der Leserlichkeit wird in dieser Dokumentation das Wort „Server“ verwendet, wann immer vom Raspberry Pi die Rede ist.

Alle ausgeführten Befehle werden im laufenden Text der Dokumentation angegeben. Während des gesamten Prozesses, welcher in dieser Dokumentation beschrieben wird, wurden des Weiteren Screenshots gemacht, welche in den Anlagen in Kapitel 9.1 beigefügt sind. Auf diese wird an den entsprechenden Stellen der Dokumentation verwiesen.

Inhaltsverzeichnis

1	Einleitung	1
2	Vorbereitungen	1
3	Konfiguration der User	1
3.1	Anlage neuer User	1
4	Konfiguration des Netzwerks	2
5	Konfiguration der Firewall	2
6	Installation Apache2	3
7	Inbetriebnahme Rest API	3
8	Veröffentlichung Swagger Dokumentation auf Webserver	3
9	Anlagen	4
9.1	Bilder	4
9.1.1	Konfiguration User	4
9.1.2	Konfiguration Netzwerk	6
9.1.3	Konfiguration Firewall	6
9.2	Quellen	7

1 Einleitung

In dieser Dokumentation

2 Vorbereitungen

3 Konfiguration der User

Nachdem das Betriebssystem des Servers installiert, der Server in das Netzwerk eingebunden und überprüft wurde, ob eine SSH Verbindung zum Server möglich ist, wurden zwei neue User angelegt, um den Server abzusichern, da der User „Pi“ der Standarduser des Betriebssystems ist und somit allgemein bekannt.

Es wurden insgesamt zwei neue User angelegt. Ein User „benutzer72“ mit grundlegenden Nutzungsrechten und ein Benutzer „fernzugriff“ mit administrativen Rechten. Des Weiteren kann der Benutzer „fernzugriff“ verwendet werden, um eine SSH-Verbindung zum Server aufzubauen.

3.1 Anlage neuer User

Zunächst wurde der user „benutzer72“ mit folgenden Befehlen angelegt:

```
pi@raspberrypi:~$ sudo useradd -m benutzer72
pi@raspberrypi:~$ sudo passwd benutzer72
New password:
Retype new password:
passwd: password updated successfully
```

Der Befehl `useradd` dient dazu, den neuen Benutzer anzulegen. Mit dem flag `-m` wird außerdem automatisch ein Home-Verzeichnis für den neuen Benutzer erzeugt. Des Weiteren wurde dem neuen Benutzer mittels des `passwd` Befehls ein neues Passwort zugewiesen¹.

Nachdem der Benutzer `benutzer72` konfiguriert wurde, wurde ein neuer administrativer Nutzer „fernzugriff“ angelegt. Die Vorgehensweise war hier zunächst identisch zu der der Neuanlage von `benutzer72`²:

```
pi@raspberrypi:~$ sudo useradd -m fernzugriff
pi@raspberrypi:~$ sudo passwd fernzugriff
New password:
Retype new password:
passwd: password updated successfully
```

¹Vgl. Abbildung 1 in Kapitel 9.1.1

²Vgl. Abbildung 2 in Kapitel 9.1.1

Da dieser Benutzer administrative Rechte auf dem Server erhalten sollte, wurde er anschließend in die Gruppe „sudo“ aufgenommen³:

```
pi@raspberrypi:~$ sudo usermod -aG sudo fernzugriff
```

Hier dient der Befehl `usermod` allgemein dazu, einen User zu modifizieren. Der Flag `-aG` gibt an, dass der User einer Gruppe hinzugefügt werden soll, welche wiederum direkt hinter dem Flag definiert ist (in diesem Fall „sudo“).

Abschließend wurde dem Benutzer „fernzugriff“ noch das Recht gewährt, sich per SSH mit dem Server zu verbinden. Dafür wurde die Einstellung `AllowUsers` in der Datei `/etc/ssh/sshd_config` angepasst⁴:

```
pi@raspberrypi:~$ sudo nano /etc/ssh/sshd_config
```

```
$OpenBSD: sshd_config,v 1.103 2018/04/09 2041:22 tj Exp $
```

```
#Port 22
#AddressFamily any
AllowUsers      fernzugriff
#...
```

Nun besitzt der Benutzer „fernzugriff“ alle notwendigen Rechte, um ihn für administrative Tätigkeiten zu verwenden. Fortan wird der Benutzer „pi“ nicht mehr verwendet und alle Umsetzungen werden mit dem Benutzer „fernzugriff“ durchgeführt.

4 Konfiguration des Netzwerks

Bislang nutzte der Server die IP-Adresse, welche ihm vom DHCP-Server des Netzwerks zugewiesen wurde.

5 Konfiguration der Firewall

```
fernzugriff@raspberrypi ~$
```

³Vgl. Abbildung 3 in Kapitel 9.1.1.

⁴Vgl. Abbildung 4 in Kapitel 9.1.1

6 Installation Apache2

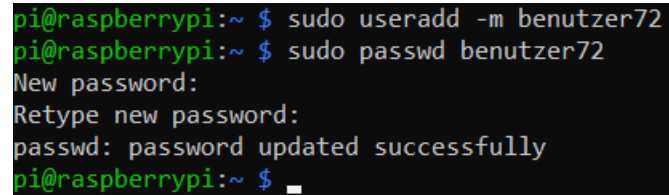
7 Inbetriebnahme Rest API

8 Veröffentlichung Swagger Dokumentation auf Webserver

9 Anlagen

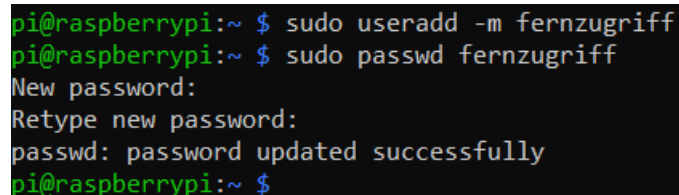
9.1 Bilder

9.1.1 Konfiguration User



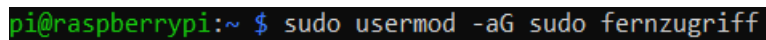
```
pi@raspberrypi:~ $ sudo useradd -m benutzer72
pi@raspberrypi:~ $ sudo passwd benutzer72
New password:
Retype new password:
passwd: password updated successfully
pi@raspberrypi:~ $
```

Abbildung 1: Anlage und Konfiguration des Benutzers „benutzer72“



```
pi@raspberrypi:~ $ sudo useradd -m fernzugriff
pi@raspberrypi:~ $ sudo passwd fernzugriff
New password:
Retype new password:
passwd: password updated successfully
pi@raspberrypi:~ $
```

Abbildung 2: Anlage und Konfiguration des Benutzers „fernzugriff“



```
pi@raspberrypi:~ $ sudo usermod -aG sudo fernzugriff
```

Abbildung 3: Benutzer „fernzugriff“ in die Gruppe sudo aufnehmen

```
# $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
AllowUsers      fernzugriff

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none
```

Abbildung 4: Benutzer „fernzugriff“ SSH-Rechte gewähren

9.1.2 Konfiguration Netzwerk

9.1.3 Konfiguration Firewall

```
fernzugriff@raspberrypi:~$ sudo apt install ufw
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done: 100%
The following package was automatically installed and is no longer required:
  libfuse2
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  ufw
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 167 kB of archives.
After this operation, 857 kB of additional disk space will be used.
Get:1 http://mirror.netzwerke.de/raspbian/raspbian bullseye/main armhf ufw all 0.36-7.1 [167 kB]
Fetched 167 kB in 0s (497 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 109573 files and directories currently installed.)
Preparing to unpack .../archives/ufw_0.36-7.1_all.deb ...
Unpacking ufw (0.36-7.1) ...
Setting up ufw (0.36-7.1) ...

Creating config file /etc/ufw/before.rules with new version
Creating config file /etc/ufw/before6.rules with new version
Creating config file /etc/ufw/after.rules with new version
Creating config file /etc/ufw/after6.rules with new version
Created symlink /etc/systemd/system/multi-user.target.wants/ufw.service → /lib/systemd/system/ufw.service.
Processing triggers for rsyslog (8.2102.0-2+deb11u1) ...
Processing triggers for man-db (2.9.4-2) ...
```

Abbildung 5: Installation der UFW Firewall

```
fernzugriff@raspberrypi:/etc/ufw$ sudo ufw allow from 192.168.24.0/24 proto tcp to any port 22
Rules updated
```

Abbildung 6: SSH Port für gleiches Netzwerk öffnen

```
fernzugriff@raspberrypi:/etc/ufw$ sudo ufw allow 13376
Rules updated
Rules updated (v6)
```

Abbildung 7: Port der API für alle Netzwerke freischalten

```
fernzugriff@raspberrypi:/etc/ufw$ sudo ufw allow out to any port 53
Rule added
Rules updated (v6)
```

Abbildung 8: Ausgehende DNS Anfragen erlauben

```
fernzugriff@raspberrypi:/etc/ufw $ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
```

Abbildung 9: Alle eingehenden Pakete ohne Regel verbieten

```
fernzugriff@raspberrypi:/etc/ufw $ sudo ufw status numbered
Status: active
```

	To	Action	From	
	--	-----	----	
[1]	13376	ALLOW IN	Anywhere	
[2]	22/tcp	ALLOW IN	192.168.24.0/24	
[3]	53	ALLOW OUT	Anywhere	(out)
[4]	13376 (v6)	ALLOW IN	Anywhere (v6)	
[5]	53 (v6)	ALLOW OUT	Anywhere (v6)	(out)

Abbildung 10: Übersicht aller angelegten Regeln

9.2 Quellen