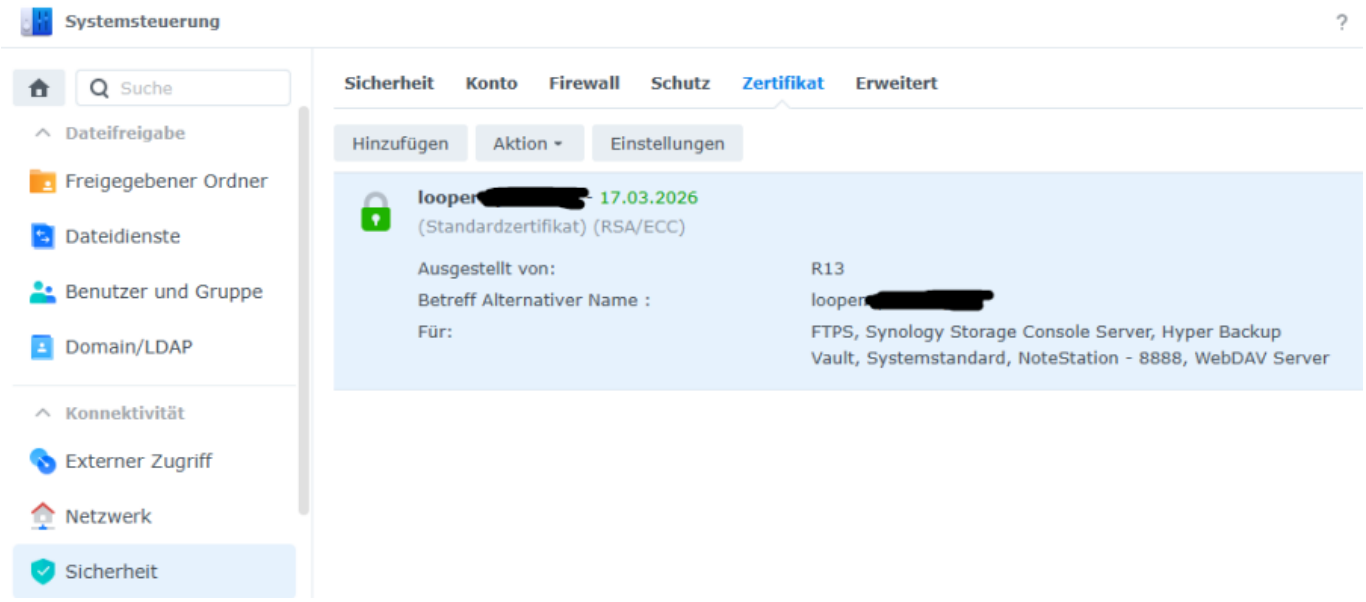
Let's-Encrypt-Zertifikat

Die Synology NAS unterstützt die Einbindung von Let's-Encrypt-SSL-Zertifikaten. Die entsprechende Konfiguration dazu ist in derSystemsteuerung unter „`Sicherheit`“ »> „`Zertifikat`“ zu finden:



Erneuern

Sollte das Zertifikat abgelaufen sein (die Haltbarkeit beträgt 6 Monate), kann es unter dem Menüpunkt „`Aktion`“ mit klick auf „`Zertifikat erneuern`“ erneuert werden. Es wird vorausgesetzt, dass Let's Encrypt einen Zugriff auf die NAS über Port 80 oder 443 besitzt (sollte die NAS normalerweise nicht über die Adresse erreichbar sein, reicht eine temporäre Freischaltung in der FritzBox).

SSH-Zugriff mit Schlüssel

Nachfolgend soll die Methode beschrieben werden, wie mittels eines SSH-Schlüssels auf die NAS zugegriffen werden kann.

SSH-Schlüssel erstellen

Als erstes muss ein SSH-Schlüssel auf dem System erstellt werden, welches sich später mit der NAS verbinden will. Unter Linux kann das wie folgt durchgeführt werden:

```
~$ ssh-keygen -a 128 -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/repo/.ssh/id_ed25519):
Enter passphrase for "/home/repo/.ssh/id_ed25519" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/repo/.ssh/id_ed25519
Your public key has been saved in /home/repo/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:k+vjKzaeLEVYbyg4VHncPyiNar5hja5iYJJP+lQbIUk repo@slxrepo
The key's randomart image is:
+--[ED25519 256]--+
|  E..o .         |
| .... + .        |
| .o..+ = o       |
|  o.o.= =.o      |
| . .o+ oS  .     |
|+...o=.  o       |
|++.o=.. .        |
|oo.ooo+o.        |
|.oo.o=+++o       |
+----[SHA256]-----+
~$
```

Schlüssel kopieren

Jetzt kann der erstellte Schlüssel auf die NAS kopiert werden:

```
~$ ssh-copy-id -p <NAS-Port> -i .ssh/id_ed25519.pub <NAS-Benutzer>@<NAS-
URL>\
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed:
".ssh/id_ed25519.pub"\
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to
filter out any that are already installed\
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are
prompted now it is to install the new keys\
repo@nas's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh -i .ssh/id_ed25519 -p <NAS-
Port> '<NAS-Benutzer>@<NAS-URL>'"\
and check to make sure that only the key(s) you wanted were added.

~$
```

Rechte anpassen

Bevor jetzt ein Versuch gestartet werden kann, müssen noch die Datei- und Verzeichnis-Rechte auf der NAS angepasst werden:

```
~# chmod 755 /volume1/homes/<NAS-Benutzer> && chmod 755 /volume1/homes/<NAS-Benutzer>/.ssh && chmod 644 /volume1/homes/<NAS-Benutzer>/.ssh/authorized_keys
```

Verbindungsversuch

Jetzt kann auf dem Ausgangsssystem ein Verbindungsversuch gestartet werden:

```
~$ ssh <NAS-Benutzer>@<NAS-URL> -p <NAS-Port> -o "IdentitiesOnly=yes" -i .ssh/id_ed25519

Synology strongly advises you not to run commands as the root user, who has\
the highest privileges on the system. Doing so may cause major damages\
to the system. Please note that if you choose to proceed, all consequences are\
at your own risk.

[nas]~$
```

.Ende des Dokuments