

# Synology Terminal Commands

```
sudo -i

synoservicecfg --list
synoservicecfg --hard-stop <service>
synoservicecfg -stop <service>
synoservicecfg --hard-start <service>
synoservicecfg -start <service>
synoservice -status
synoservice -restart <service>
synoservicectl -restart <service>
```

Apache webserver:

```
stop pkg-apache22
start pkg-apache22
reload pkg-apache22
```

Sonarr/Radarr service:

```
stop pkgctl-nzbdrone
start pkgctl-nzbdrone
stop pkgctl-radarr
start pkgctl-radarr
```

restart DSM Webapplication:

```
restart synoscgi
```

Uninstall Universal Search:

```
synopkg uninstall SynoFinder
```

Synology provides additional tools to diagnose a system. These tools only need to be installed as root. Log in as root or as user and then use `sudo su` to become root. To install:

```
synogear install
```

Installation takes a little while.

The list of tools can be obtained using the command:

```
synogear list
```

```
All tools:
addr2line          eu-unstrip        name2addr         sadf
addr2name          file              ncat              sar
```

```
ar          fio          ndisc6        sh
arping      fio2gnuplot    nethogs      sid2ugid.sh
as          fio-btrace2fio  nfsiostat-sysstat size
ash         fio-dedupe     nm            slabtop
autojump    fio_generate_plots nmap         sockstat
avahi-browse  fio-genzipf    nping        speedtest-cli.py
avahi-publish  fio_latency2csv.py nslookup     strace
avahi-resolve  fiologparser.py  objcopy      strings
bash        fio-verify-state  objdump      strip
c++filt     fix_idmap.sh    perf-check.py  sysctl
cifsiostat  free           pgrep         sysstat
clockdiff   gcore          pidof         tcpdump_wrapper
dig         gdb            pidstat       tcpspray
domain_test.sh  gdbserver     ping          tcpspray6
elfedit     genfio        ping6         tcptraceroute6
eu-addr2line  gprof        pkill         telnet
eu-ar        iftop         pmap          tload
eu-elfcmp    iostat        ps            tmux
eu-elfcompress  iotop        pstree        top
eu-elflint   iperf         pwdx          tracepath
eu-findtextrel  iperf3       ranlib        traceroute6
eu-make-debug-archive  kill         rarpd         tracert6
eu-nm        killall       rdisc         uptime
eu-objdump   ld            rdisc6        vmstat
eu-ranlib    ld.bfd        readelf       w
eu-readelf   ldd           rltraceroute6 watch
eu-size      log-analyzer.sh  run           zblacklist
eu-stack     lsof          sa1           zmap
eu-strings   ltrace        sa2           ztee
eu-strip     mpstat        sadc
```

From now on, these commands can be used directly in the command line. In package center this is now listed as "Diagnosis Tool" and can be removed from there. An installation via package center is not possible though.

## SSH no matching cipher found

When trying to ssh into synology, the following error message may be displayed:

```
Unable to negotiate with x.x.x.x port 22: no matching cipher found. Their offer: aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc
```

Logging in by specifically using one of the offered ciphers works:

```
ssh -c aes256-cbc admin@x.x.x.x
```

This can be changed via the DSM interface: DSM control panel → Terminal → advanced settings →

“high” profile

Alternatively, the `sshd_config` can be changed from the command line with the desired ciphers:

```
sudo vi /etc/ssh/sshd_config
```

and replacing the ciphers `aes256-ctr,aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc` with

```
Ciphers aes128-ctr, aes128-gcm, aes192*, aes256*, dhge-sha256, curve25519-  
sha256, hmac-sha2-256
```

Restart the synology for the changes to take effect.

From:

<http://wuff.dyndns.org/> - **Wulf's Various Things**

Permanent link:

<http://wuff.dyndns.org/doku.php?id=synology:synology-terminal&rev=1552506918>

Last update: **2023/05/29 11:54**

