



freeshell.de
FREE SHELLS FOR A FREE WORLD

User Manual

Table of contents

Author.....	3
Naming.....	3
Server.....	4
Description of base setup.....	5
Backup.....	5
User resources.....	6
Disk space.....	6
Processes and RAM.....	6
Account deletion.....	7
Servername / network addresses.....	8
IPV4.....	8
IPV6.....	8
Connectivity.....	9
System identification / Certificates.....	10
DNSSEC.....	10
SSH-Fingerprints.....	10
SSL certificate.....	11
Authentication and access.....	12
SSH.....	12
Password.....	12
Public Key.....	12
Limited access / censored internet.....	13
Software and services.....	15
OS.....	15
Installation of additional packages.....	15
Firewall.....	15
Mail system.....	16
Postfix.....	16
Domain names for email.....	16
Anti-Spam / Anti-Virus.....	16
Dovecot - Retrieving mail.....	17
ActiveSync – Push-Services.....	19
Owncloud.....	20
Homepage / PHP.....	21
Permissions.....	21
MySQL-Database.....	21
Tor and anonymous surfing.....	22
Support and help.....	22
Link collection.....	23
Disclaimer / Misc.....	23

Author



Contact private:

Sebastian Krajenski

Sulzgrieser Str. 112

73733 Esslingen

Germany

Tel/GSM: +49-162-8741288 (not for tech-support)

E-Mail: postmaster@freeshell.de

Contact business:

mars solutions GmbH

Robert-Bosch-Str. 8

73037 Goeppingen

Germany

Tel: +49-7161-6549250 (Mon-Fri / 8AM-5PM CET)

E-Mail: sk@mars-solutions.de

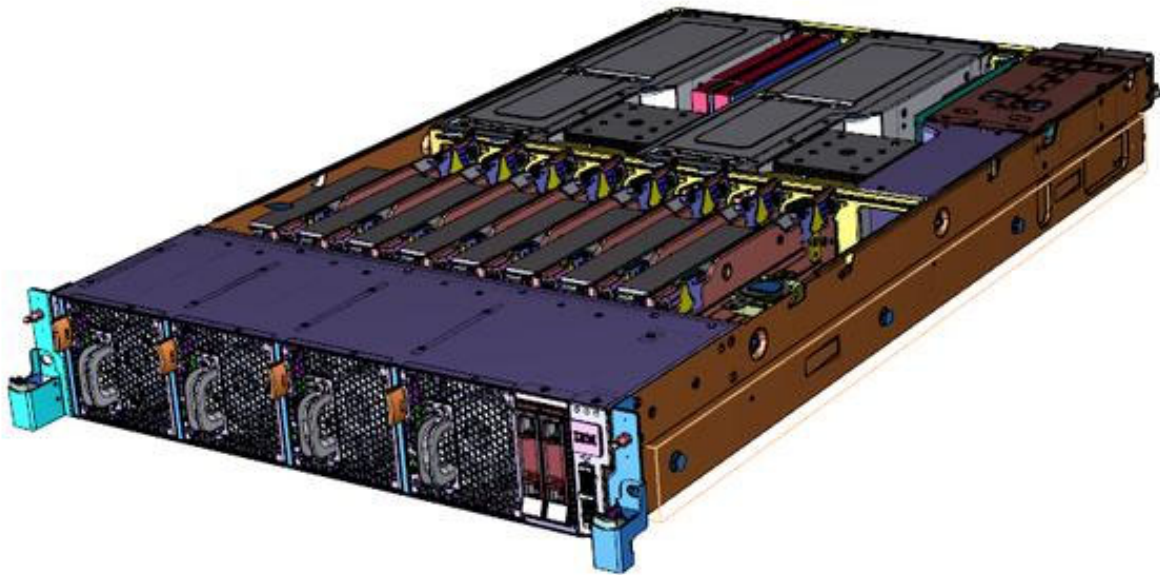
Business proposals welcome.

Naming

The project is called “**freeshell.de**”, like the homepage and main domain name.

The former name “Nic.Nac.Project” is not in use anymore.

Server



Those are the server and services specs in a small table as summary for the impatient:

OS	Ubuntu 20.04 LTS “focal”
Kernel	Linux Kernel 5.4.0
CPU	Intel Xeon (E-2176G)
RAM	64 GB ECC
HDD	8.0 TB RAID
Your quota(s)	20 GB Homedir + 20 GB Owncloud
WAN connectivity	1 Gbit/s guaranteed bandwidth
Database	MySQL 8.0
Server location	Germany
Backup concept	Two separate locations
E-Mail system	MTA is postfix / Mailbox in “Maildir”-Format
Personal crontab	Yes
Background jobs (screen, tmux & Co.)	Yes
Private/Custom TCP/UDP-Ports on request	Yes
Account inactivity period	None. Your files remain as long as system exists
Homepage (with HTML, PHP, CGI, PY)	https://freeshell.de/yourname + .../~yourname
Missing programs in the OS ?	Will be installed on request!

Description of base setup

The setup as such is a single server system. Regarding storage a software RAID 1 is used. Both HDD are monitored using “smartd”. Daily tests (“short-test”) as well as weekly tests (“long-test”) assure that possible SMART-Errors are detected as fast as possible.

Nameservers of “freeshell.de”:

NS1	ns1.nic-nac-project.de
NS2	ns2.nic-nac-project.de

In detail:

ns1.nic-nac-project.de	IP: 116.202.128.144 (the freeshell server itself, the PRIMARY DNS)
ns2.nic-nac-project.de	IP: 3.67.14.200 (an AWS VM used as SECONDARY DNS)

The “legacy domain” nic-nac-project.de above that is served from those nameservers:

nsa5.schlundtech.de	Schlund Technologies GmbH
nsb5.schlundtech.de	Schlund Technologies GmbH
nsc5.schlundtech.de	Schlund Technologies GmbH
nsd5.schlundtech.de	Schlund Technologies GmbH

The MX record points to “freeshell.de”. Backup MX records do not exist at the moment.

The hardware- and software-situation as well as the DNS setup is permanent work-in-progress. There may be regular updates and improvements, which will be documented here.

Backup

The system is saved to two other data centres on a daily/nightly basis using “Veeam Agent for Linux”. The data is stored encrypted. 14 rolling restore points each are kept. An additional local daily “mysqldump”-Job ensures that the integrity of your databases in the backup is kept at all times.

User resources

Disk space

There are different quotas for you, depending on what services we're talking about:

Linux \$HOME directory including your Maildir	20 GB
OwnCloud file sharing service	20 GB
MySQL database	Technically: None (Please don't exceed 20 GB)
Kopano-Groupware mailbox	Technically: None (Please don't exceed 20 GB)

Processes and RAM

Here is an overview on what resources to expect on the shell:

core file size	(blocks, -c) 0
data seg size	(kbytes, -d) unlimited
file size	(blocks, -f) unlimited
pending signals	(-i) 256478
max locked memory	(kbytes, -l) 65536
max memory size	(kbytes, -m) unlimited
open files	(-n) 1024
pipe size	(512 bytes, -p) 8
POSIX message queues	(bytes, -q) 819200
real-time priority	(-r) 0
stack size	(kbytes, -s) 8192
cpu time	(seconds, -t) 900
max user processes	(-u) 50
virtual memory	(kbytes, -v) unlimited
file locks	(-x) unlimited

Account deletion

Basically this is covered in the "terms and conditions".

For short: Misuse of any kind, as well as illegal content, will lead to account deletion.

For your privacy I recommend you to use encryptfs, TrueCrypt, Veracrypt, gpg or similar software.

We want an open Internet.

Can't
~~Don't~~ be evil.

(Welcome to the new internet | Muneeb Ali | TEDxNewYork | YouTube Video)

Servername / network addresses

IPV4

116.202.128.144 – Primary IPV4-IP

DNS-Name: freeshell.de (DNS-Wildcard-Resolution “*.freeshell.de” resolves to this IP)

Legacy DNS-Names, that also resolve here:

- nic-nac-project.de, nic-nac-project.org, nic-nac-project.com, nic-nac-project.net
- freeshell.at, freeshell.ch

Services officially listening on the primary IP on default ports:

- postfix
- dovecot
- sshd
- apache2
- bind9

178.63.180.185 – Secondary IPV4-IP

DNS-Names: ssh.freeshell.de, zarafa.freeshell.de, kopano.freeshell.de

Services officially listening here:

- sshd (on alternative high-port: “32768”)
- sshd (on alternative special-port: “443”)
- kopano-gateway (POP and IMAP service for the Groupware)

IPV6

2a01:4f8:231:482b::2 – Primary IPV6-IP

DNS-Name: freeshell.de

Services listening here:

- postfix
- dovecot
- sshd
- apache2

Connectivity

The server is connected by a 1000 MBit/s-Link to the internet.

In case of a D(D)oS-attack, the system automatically gets disconnected from the internet infrastructure. Likewise it is automatically connected back when attack(s) stop.

System identification / Certificates

DNSSEC

The DNS of the main domain “freeshell.de” is secured with DNSSEC.

I recommend the following URLs to check the zone:

URL: <http://dnssec-debugger.verisignlabs.com/freeshell.de>

At the moment I maintain no extra TLSA-entries.

SSH-Fingerprints

Old-style notation:

MD5: d1:0d:d2:cc:a1:fa:3b:f6:28:cc:c8:c6:49:76:8b:e7 (RSA)

MD5: f0:7a:cd:56:94:a8:41:55:0e:c9:df:91:dd:a6:10:a4 (ED25519)

MD5: 4a:0f:b4:89:c2:8b:3a:86:01:19:83:79:d0:80:c3:50 (ECDSA)

New-style notation:

SHA256: pDFR0atCakVtmZProASRXRGq2aXyKxW6KMx8F6gZtvE (RSA)

SHA256: ZqpqRZyzAnlwjFFbycMVmZVJIUQ7NQVindfsuTLU37A (ECDSA)

SHA256: /uazD/Cfo+SC9/3JgsIWkbKvev0MP5ikNUficvU7KJk (ED25519)

Please always check those when first connecting from a new computer!

Hint: In case of being in an "untrusted" environment or mobile situations like Internet Cafe, hotel etc.: I deeply recommend to print out the fingerprints beforehand on a piece of paper (or your Laptop/GSM) and carry them with you. You prevent "man-in-the-middle" attacks knowing what to trust.

SSL certificate

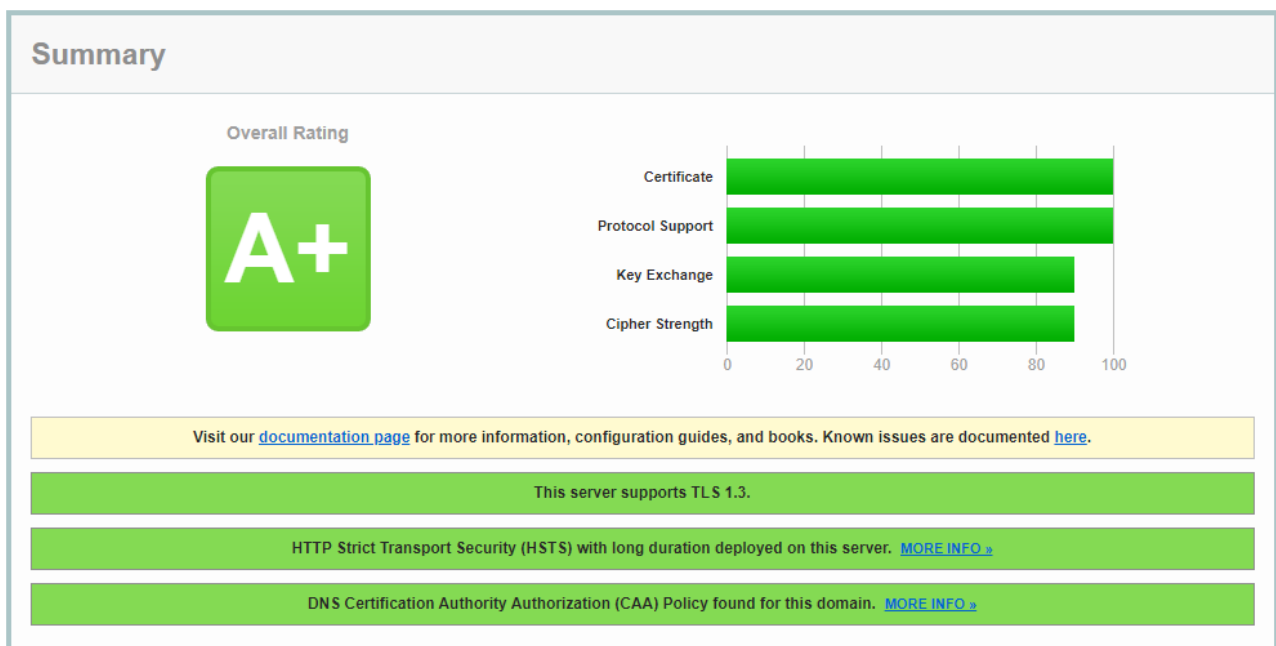
The other services provided here are published using a certificate from Comodo/Sectigo CA. In the DNS a “CAA” entry regarding this is maintained.

The webserver also uses “certificate pinning” aka HPKP.

Technical background info: <https://tools.ietf.org/html/draft-ietf-websec-key-pinning-21>

Implementation hints: https://developer.mozilla.org/en-US/docs/Web/Security/Public_Key_Pinning

If you run “freeshell.de” through “ssllabs.com” it should look about like this:



Authentication and access

SSH

The OpenSSH server here accepts connections to “freeshell.de” on the default port (TCP/22) for interactive sessions. With Linux and MacOS I recommend you use “ssh” on their respective terminal. With MS Windows “putty” is my favoured client:

<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

When you connect from a computer for the first time, please always check the fingerprint!

Password

Your first login will always be password based. After that, there are a couple of possible enhancements or variants:

Public Key

You already have a public key identity for SSH ? Just fill **\$HOME/.ssh/authorized_keys** ...with your public key, to login with a keyfile in the future.

In case you don't, have a look here: <https://help.ubuntu.com/community/SSH/OpenSSH/Keys>

If you additionally like to improve the SSH secrecy, I recommend this article:

<https://stribika.github.io/2015/01/04/secure-secure-shell.html>

Hint: File transfer to the server is only possible using SFTP or SCP.

Classic (unencrypted) FTP is not possible anymore.

Limited access / censored internet

So you are limited in some way regarding your internet connection? It's still likely that you can connect anyway. Let me show you some alternative ways to get into the system.

1) Using one of the alternative TCP ports for SSH here:

```
$ ssh ssh.freeshell.de -p 443  
$ ssh ssh.freeshell.de -p 32768
```

2) If your only limitation is not being able to run SSH-client software, use the browser variant:
→ <https://gateone.freeshell.de>

3) If all else fails, maybe try “DNS2TCP” ?
If you have access to a linux machine, install the package “dns2tcp”.

With this method the TCP packets for SSH are sent out covered in "normal" DNS requests.

Usage:

```
Terminal 1 (starting the tunnel)  
$ dns2tcp -z dns.freeshell.de ssh.freeshell.de -l 12345 -r ssh  
(Tunnels SSH through DNS, and port forwards freeshell SSH traffic to your localhost:12345)
```

```
Terminal 2 (login to freeshell)  
$ ssh <yourname>@localhost -p 12345
```

In case you not want to login to the shell, but like to “proxy surf” through that connection:
\$ ssh -o “CompressionLevel=5” -C -4 -ND localhost:1080 <yourname>@localhost -p12345

Now you got yourself also a SOCKS proxy to freeshell.
Hint: You won't get a shell prompt with that command, that's normal.

If you use Firefox as browser, you hit: Settings → Proxy and enter / choose the following:
- manual proxy configuration
- SOCKS-Host: 127.0.0.1
- Port: 1080

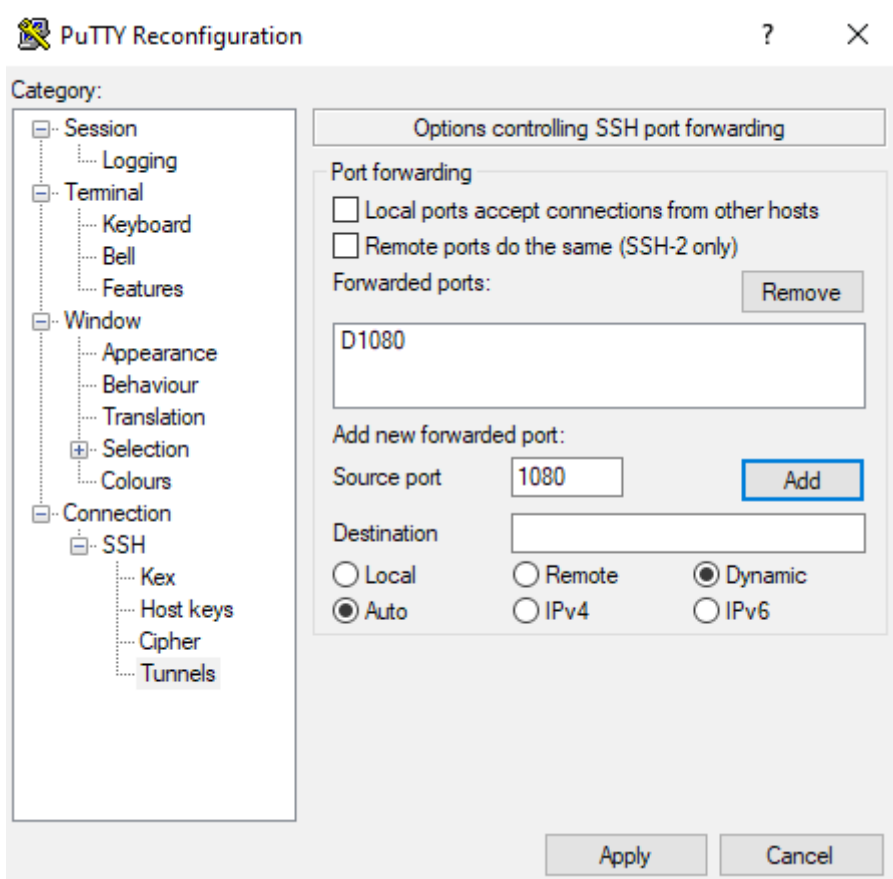
It's imperative to also check the “Remote DNS” box. Otherwise your "evil" ISP might get a clue to where you surf.

This method in general will be really slow because of the DNS2TCP overhead in general.

Hint: Anyway, even if you can connect to freeshell without hazzle, you are welcome to use the socks proxy technique as well!

In the most simple use case, this looks like this (example using Windows this time):

1) Connect to “freeshell.de” using “putty” and setting this extra options:



2) Open your favourite browser and set the proxy settings as follows:

- Type: Manual Proxy configuration
- SOCKS-Host: 127.0.0.1 (Socks v5)
- Port: 1080
- When using SOCKS v5 let the proxy do DNS: YES

3) Test the result by visiting e.g.: <https://whatismyipaddress.com/>

Software and services

OS

ubuntu 

The server runs Ubuntu 20.04 (“focal”) LTS 64-Bit-version. In irregular intervals the distribution gets updated to the latest “stable” or “LTS” release. There are 3rd-party software-dependencies that normally lead to 3-4 months of delay until I’m able to upgrade (after the initial release). Please be patient :)

Installation of additional packages

In case you miss a package just ask for it using the request form on the homepage. I will install almost any package that is available from official channels (in respect to the running release): <https://packages.ubuntu.com/> → “focal”

Firewall

This system uses a packet filtering “iptables” based firewall. All ports (from the outside) to non-standard services are closed. In case you need a private port please let me know through the request form on the homepage.

Mail system

Postfix



The MTA on the server is postfix. The following services are configured.

Servename: freeshell.de

Port 25 (SMTP) sending/receiving email (Relaying) with authentication. Type: STARTTLS

Port 587 (Submission) sending/receiving email with authentication. Type: TLS

Port 465 (SMTPS) sending email with authentication. Type: TLS

The mailbox format used on the system is “Maildir”.

So your e-mails technically reside in:

\$HOME/Maildir/

Domain names for email

You are reachable with the following addresses:

<**your_name@freeshell.de**>

Secondary: @freeshell.ch, @freeshell.at, @nic-nac-project.de

Anti-Spam / Anti-Virus

Email on the system is passed through a couple of techniques (in- and outbound)

- policyd-spf (freeshell.de uses “hard fail” = strict in its own DNS entries)
- policyd-weightd (RBL-list checks)
- DKIM check (OpenDKIM in “safe mode” receiving side, otherwise mailing-lists would break)
- BATV (you get automated BATV-envelope-addresses to your sent mails)

The maximum element size (per single mail element) is 50MB.

Dovecot - Retrieving mail



Dovecot provides you mailbox access through POP3 and IMAP on the following ports:

Servename: freeshell.de

- Port 110 (POP3) STARTTLS
- Port 143 (IMAP) STARTTLS
- Port 995 (POP3S) TLS
- Port 993 (IMAPS) TLS

On the shell you can run preconfigured “mutt” or “pine” to access your mailbox.

There are also webinterfaces in place:

SquirrelMail:



Type: more “classic” and functional

URL: <https://freeshell.de/squirrelmail/>



RoundCube:

URL: <https://freeshell.de/rc/>

Type: modern ui/ux, as well as mobile compatible

Kopano – The alternative Groupware you may use here



In case you want a ‘full collaboration experience’ and simple email is not enough for you. Kopano is a AGPL3 groupware solution that provides (besides basic email services) things like:

- Calendaring (also via ActiveSync aka “Exchange Mailbox Type”, see below)
- Tasks
- Notes
- Contacts (address books)

Kopano is in permanent co-existence with the "normal" mail-system. On the shell you can at any time migrate to Kopano.

You are free to visit the GUI experience here: <https://freeshell.de/webapp>

If you like the system you may proceed with the following steps to receive mail there:

1) Create a .forward file in your home directory that looks like this:

```
"| IFS=' ' && exec /usr/bin/procmail || exit 75"
```

2) Create a .procmailrc that looks like this:

```
LOGFILE=/home/y/yourname/procmail-kopano.log  
:0 w  
| /usr/sbin/kopano-dagent yourname  
EXITCODE=$?
```

The things in bold letters need to be adjusted to fit your login.

3) Optional: Move mails from some former accounts there using “imapsync” if you like.

An example command line would look like this:

```
imapsync --ssl1 --ssl2 --host1 localhost --user1 login --host2 kopano.freeshell.de --user2 login
```

“localhost” may be also any other source you like to move mail in from.

Please consult the documentation before using it: <https://github.com/imapsync/imapsync>

Classic IMAP or POP to the Kopano Groupware account works as follows:

Servername: zarafa.freeshell.de (aka 'kopano.freeshell.de')

→ Port 995 (POP3S) TLS

→ Port 993 (IMAPS) TLS

Sending email (SMTP) with a mailclient of your choice:

Servername: kopano.freeshell.de

Kopano WebApp:

URL: <https://freeshell.de/webapp>

Of course there is always a way back. In case the Kopano account doesn't fit your needs:

Simply delete your \$HOME/.forward and .procmailrc file

Now, new mail will arrive in your classic "Maildir" mailbox" again.

Mail from the Kopano account can be moved back using a mail client (or "imapsync") of your choice.

ActiveSync – Push-Services

In case you use your Kopano account, you can configure your mobile devices to sync with it. Choose "Exchange account" as type and sync contacts, tasks, calendar and mail with it.

Servername: freeshell.de

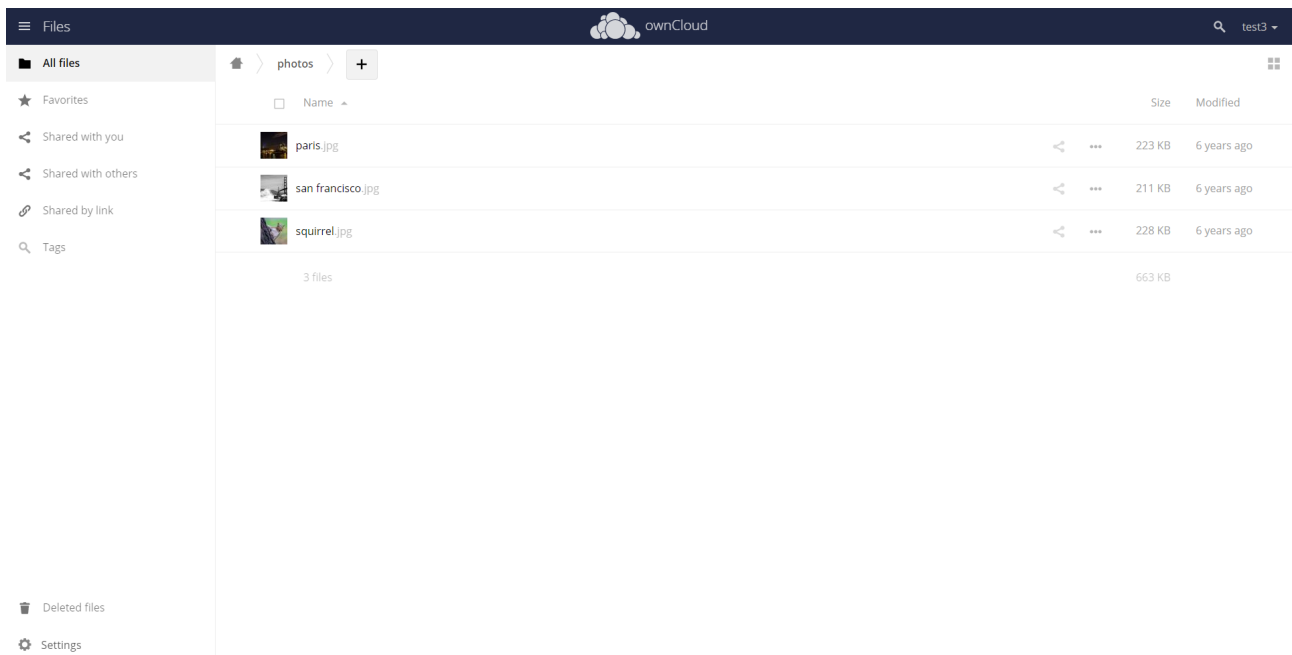
Login and password: as known

Domain field: (leave empty!)

Owncloud

URL: <https://freeshell.de/owncloud/>

Your account here is automatically equipped with owncloud file sharing storage. It's usable by browser or the native client(s). By the way: I only support the file-sharing features. Other owncloud features or plugins are officially unsupported by me.



Homepage / PHP

Your account automatically provides a directory where you can publish your homepage.

The URL is as follows:

`https://freeshell.de/yourlogin/`

as well as:

`https://freeshell.de/~yourlogin/`

To put content into it that should be reachable from the outside, put it into this directory:

`$HOME/public_html/`

This is so to say your “document root”.

Script languages:

PHP 7.4 is installed and available, Perl, SSI and Python as well.

Permissions

Your home directory (and “public_html” directory below that folder) are equipped with the correct minimal permissions per default:

“0711” aka “drwx—x—x” !

More won't work – less won't work !

File permissions: PHP files need exactly “chmod 644” in order to be executed here.

“777” files for example will not be executed for security reasons.

MySQL-Database

In case you also need a mysql database, just ask using the request form on the homepage.

PHPMyAdmin is installed here: <https://freeshell.de/phpmyadmin/>

Tor and anonymous surfing

This project supports and promotes anonymous surfing. “Tor” is installed and running in the server. It is accessible through the local privoxy-proxy service as well as with “tsocks”.

Set the proxy variables as follows:

```
$ export http_proxy="http://127.0.0.1:8118"  
$ export https_proxy="http://127.0.0.1:8118"
```

Privoxy of course keeps no log files here.

Here is an example for "tsocks" usage:

```
$ tsocks ssh login@where_ever.com
```

Many other programs like lynx, links and alike use those variables.

Support and help

In case of difficulties that are not covered by the manual, please leave me a message through the request form on the homepage.

Hint: Most login problems derive from “fail2ban” . The server blocks any attempts to the system from your source-IP when a attempted login fails 5 times in a row. The block lasts for one hour. This slows down brute-force-attacks and is in place to protect your account.

Link collection

Links to "freeshell.de" services

- HTML5-SSH-Client: <https://gateone.freeshell.de/>
- SquirrelMail Webmail: <https://freeshell.de/squirrelmail/>
- Roundcube Webmail: <https://freeshell.de/rc/>
- PHPMyadmin: <https://freeshell.de/phpmyadmin/>
- Zarafa WebApp: <https://freeshell.de/webapp/>
- Etherpad Text pad collaboration: <https://pad.freeshell.de/>

External useful links

- Mailserver-Crypto check: <https://ssl-tools.net/mailservers>
- Webserver-Crypto check: <https://www.ssllabs.com/>
- "Tails" Privacy-Live-Distro: <https://tails.boum.org/>
- DANE-SMTP-Validator: <https://dane.sys4.de/>
- DNSSEC-Zone-Analyzer: <http://dnssec-debugger.verisignlabs.com/>
- DNSSEC-Browser-Plugin: <https://www.dnssec-validator.cz/>
- Secure E-Mail Test Tools: <http://checktls.com/>
- Meta-RBL-Check-Seite: <http://multirbl.valli.org/>
- Test-Mailaddress for various Checks: test@allaboutspam.com
- Test-Mailaddress for various Checks: check-auth@verifier.port25.com
- Mail-Tester: <https://www.mail-tester.com/>

Disclaimer / Misc.

The terms and conditions as well as the data protection statement are available through the homepage www.freeshell.de on menu item "Contact".

All documents are updated regularly. Please make sure you always use the most recent version.

Remember, this is a "shared system". Over 2600 people from literally all over the world share the server. Please treat persons with respect and use the available resources wisely.