NAS Installation - Synology DSM 6.1 (Hermes)

Hua Hin cloud server 2017 on Synology DS716+.

Specification

- Intel Celeron N3160 quad core
- 2 HGST Deskstar NAS 6TB HDD
- 2 GB RAM

Setup

1. Find the DS through http://find.synology.com.
2. Create a volume in *Storage Manager*
3. Configure Network settings in *Control Panel*. Select the 2nd LAN and click *Create Bond*.
4. Enable user home service in *Control Panel –> User –> Advanced*.
5. Set disk full warning setting in *Control Panel –> Notification –> Advanced –> Internal Storage –> Volume Full*.
6. Enable the widgets you want to use on your home screen.
7. To setup SSL, import server.key, domain.crt, and domain.intermediate.crt through *Control Panel –> Security –> Certificate –> Add*. Right click on the new certificate, “Edit” to make it default, “Configure” to assign it to services. Detailed instructions see Secure your Synology NAS, install a SSL certificate and How to Move or Copy an SSL Certificate from one Server to Another.
8. Add Two-factor-authentication to your admin user. Select **Options → Personal** on the top right of the DSM window. Settings are saved in

```
/usr/syno/etc/preference/username/google_authenticator
```

Certificates

If you are running a Synology NAS to handle cloud and mail, but another webserver to handle https sites, you will end up with some certificate issues. I solve those by updating the certificate on the web server and then copy the renewed certificate over to the NAS.

1. Check the path to rsync:

```
which rsync
```

2. First, allow rsync to be executed as root on both machines. Add the following line to file 'rsync' under 'sudoers.d':

```
user ALL=(root) NOPASSWD:/path/to/rsync
```

3. As a user on your NAS you can suck the data from your source server like this:

```
sudo rsync -aPLe 'ssh -l user -i /volume1/homes/user/.ssh/id_rsa' --
rsync-path='sudo rsync'
pandora:/etc/letsencrypt/live/cloud.domain.tld/fullchain.pem
/usr/syno/etc/certificate/_archive/<dir>/cert.pem
```

4. You can find the directory where your default certificate is stored in on your NAS with the following command:

```
cat /usr/syno/etc/certificate/_archive/DEFAULT
```

5. Copy the rsync commands into a batch file on the NAS and add the batch file to the task scheduler:

```
sudo -u bco sh /volume1/homes/bco/batch/copycert
```

6. Content of “copycert”:

```
#!/bin/sh
#
# Copy certificates from web server to NAS
#  you must add user to be able to run cksum with sudo without password
on the remote machine
# (c) 2019-08-06, 2019-11-27, 2020-02-21, Bernard Condrau
#
# CERTDIR must be hardcoded and is different in every server instance
#  see https://github.com/Neilpang/acme.sh/wiki/Synology-NAS-Guide
#  if you used the normal method the certificate will be installed in
the "system/default" directory
#  if you used the alternative method it is copied to an unknown path,
you can find it in file "_archive/DEFAULT"
# CERTDIR="system/default"
CERTDIR="_archive/4LSLbi"
CERTROOTDIR="/usr/syno/etc/certificate"
PACKAGECERTROOTDIR="/usr/local/etc/certificate"
FULLCERTDIR="$CERTROOTDIR/$CERTDIR"

# compare cksums first to decide whether certificates need to be copied
REM_CERT=$(ssh -i /volume1/homes/bco/.ssh/id_rsa bco@pandora sudo cksum
/etc/letsencrypt/live/cloud.condrau.com/cert.pem | cut -d' ' -f 1)
REM_FULL=$(ssh -i /volume1/homes/bco/.ssh/id_rsa bco@pandora sudo cksum
/etc/letsencrypt/live/cloud.condrau.com/fullchain.pem | cut -d' ' -f 1)
REM_PRIV=$(ssh -i /volume1/homes/bco/.ssh/id_rsa bco@pandora sudo cksum
/etc/letsencrypt/live/cloud.condrau.com/privkey.pem | cut -d' ' -f 1)
LOC_CERT=$(cksum /usr/syno/etc/certificate/$CERTDIR/cert.pem | cut -d'
' -f 1)
LOC_FULL=$(cksum /usr/syno/etc/certificate/$CERTDIR/fullchain.pem | cut
-d' ' -f 1)
LOC_PRIV=$(cksum /usr/syno/etc/certificate/$CERTDIR/privkey.pem | cut -
d' ' -f 1)
```

```
if [[ $LOC_CERT -ne $REM_CERT ]] || [[ $LOC_FULL -ne $REM_FULL ]] || [[
$LOC_PRIV -ne $REM_PRIV ]]; then

    # copy certificates from web server
    sudo rsync -aPLe 'ssh -l bco -i /volume1/homes/bco/.ssh/id_rsa' --
rsync-path='sudo rsync'
pandora:/etc/letsencrypt/live/cloud.condrau.com/cert.pem
$FULLCERTDIR/cert.pem
    sudo rsync -aPLe 'ssh -l bco -i /volume1/homes/bco/.ssh/id_rsa' --
rsync-path='sudo rsync'
pandora:/etc/letsencrypt/live/cloud.condrau.com/fullchain.pem
$FULLCERTDIR/fullchain.pem
    sudo rsync -aPLe 'ssh -l bco -i /volume1/homes/bco/.ssh/id_rsa' --
rsync-path='sudo rsync'
pandora:/etc/letsencrypt/live/cloud.condrau.com/privkey.pem
$FULLCERTDIR/privkey.pem

    # find all subdirectories containing cert.pem files
    PEMFILES=$(find $CERTROOTDIR -name cert.pem)
    if [ ! -z "$PEMFILES" ]; then
        for DIR in $PEMFILES; do
            # replace the certificates, but never the ones in the
_archive folders as those are all the unique certificates on the
system.
            if [[ $DIR != *"/_archive/"* ]]; then
                rsync -avh "$FULLCERTDIR/" "$(dirname $DIR)/"
            fi
        done
    fi

    # reload
    /usr/syno/sbin/synoservicectl --reload nginx

    # update and restart all installed packages
    PEMFILES=$(find $PACKAGECERTROOTDIR -name cert.pem)
    if [ ! -z "$PEMFILES" ]; then
        for DIR in $PEMFILES; do
            #active directory has it's own certificate so we do not
update that package
            if [[ $DIR != *"/ActiveDirectoryServer/"* ]]; then
                rsync -avh "$FULLCERTDIR/" "$(dirname $DIR)/"
                /usr/syno/bin/synopkg restart $(echo $DIR | awk -F/
'{print $6}')
            fi
        done
    fi
    echo "certificates updated"
else
    echo "nothing to update"
fi
```

```
exit 0
```

7. You must add the following line at the end of the sudoers file with 'visudo' for the above script to work

```
user  ALL=(ALL)  NOPASSWD: /usr/bin/cksum
```

Links

- Create, import, export, and renew certificates
- Two Step Authentication
- Rsync over ssh with root access on both sides
- Version: 6.2.2-24922 Update 4 is out - fixes certificate renewal bug
- HTTPS certificates for your Synology NAS using acme.sh

Shared Folders

- Security
- How to use SFTP on synology NAS server
- Fixing Permissions
- How to migrate between Synology NAS (DSM 5.x)

MailPlus Server

- Copy DKIM Settings following
  MailPlus Server Admin Guide
  page 72 to your DNS.

Contacts

1. Install Synology Contacts
2. Click the **+** behind PERSONAL ADDRESS BOOK and select “Import Address Book” to import your address book from an existing CardDAV server or from a vCard file (extension .vcf) and name it something like *user_CardDAV*.
3. If you want to keep an archive of all your contacts before deleting unused contacts, import the same address book again into PERSONAL or GROUP ADDRESS BOOK and name it something like *archive_user_CardDAV*. Do not sync this address book, keep it as archived backup, and it can be exported to a vCard file later if required.
4. Click the 3 dots to the right of your new address book and check the URL which you need for setting up DAVx[5] below, the URL you need is the one under **iOS** (not CardDAV client!)
5. Install DAVx[5]. Add a new account as “Login with URL and user name”, then enter the CardDAV base URL taken from the web interface explained in the step before. It should look like this:

```
http://diskstation.name:5000/carddav/<user>/ # local network
```

```
https://domain.name.tld:5001/carddav/<user>/ # internet
```

- Note: ContactSync for Android is another CardDAV, it is not freee, but has an automated setup for Synology DSM.
- DAVx⁵ has been successfully tested with Synology DSM

Calendar

1. Install Synology Calendar
2. Click the **v** behind your calendar in the right pane, select *CalDAV Account*, and check the URL which you need for setting up DAVx⁵ below, the URL you need is the one under **macOS / iOS** (not Thunderbird!)
3. Install DAVx⁵. Add a new account as “Login with URL and user name”, name it with your main email address, then enter the CalDAV base URL taken from the web interface explained in the step before. It should look like this:

```
http://diskstation.name:5000/caldav/<user>/ # local network
https://domain.name.tld:5001/caldav/<user>/ # internet
```

- Note: CalendarSync for Android is another CalDAV client, it is not freee, but has an automated setup for Synology DSM.
- DAVx⁵ has been successfully tested with Synology DSM

Customization

- Find all Synology package icons in /var/cache/pkglist.tmp/icon/AVAIL/SYNO

Replace Harddisks

DSM 6

1. Shut down the NAS and replace the first disk. Numbering of disks is from left to right.
2. Boot the NAS and add the new disk to the Raid. It takes about 20 hours to rebuild the Raid.
3. Repeat steps 1 and 2 for the other disk.
4. Expand the Raid volume if the new disks are higher capacity than the replaced ones.

Command Line

Since DSM 6 the Synology NAS features a linux kernel, so Raid management can also be done on the command line. Since the Diskstation 212+ and 213+ do not support HGST Deskstar 10TB drives, I started to look into this to find a way how to make it work. Here is what I found:

1. I replaced a failed HGST 6TB with a new HGST 10TB and rebuilt the Raid through the DSM GUI.
2. I then replaced the other HGST 6TB with a new HGST 10TB and rebuilt the Raid through the

DSM GUI.
3. Extending the Raid volume through the GUI did not work.
4. After rebooting the NAS the data volume Raid degraded. Interestingly, the other 2 Raids (boot, swap) did not degrade

```
# cat /proc/mdstat
Personalities : [linear] [raid0] [raid1] [raid10] [raid6] [raid5]
[raid4]
md2 : active raid1 sda3[2]
      5855800416 blocks super 1.2 [2/1] [U_]
md1 : active raid1 sda2[0] sdb2[1]
      2097088 blocks [2/2] [UU]
md0 : active raid1 sda1[0] sdb1[1]
      2490176 blocks [2/2] [UU]
unused devices: <none>
```

5. I then rebuilt the Raid from the command line and created a conf file

```
# mdadm --add /dev/md2 /dev/sdb3
# mdadm --detail --scan > /etc/mdadm.conf
```

6. I now can boot the NAS without problems.

Remove IPKG/Optware

1. comment out every reference to optware in /etc/rc.local
2. restart DS
3. check that optware has not been loaded, e.g. /opt is empty, and sudo will work without change of path
4. rm -R /opt
5. rm -R /volume1/opt or rm -R /volume1/@optware (depends on where you installed your IPKG)
6. delete every reference to optware in /etc/rc.local
7. delete /etc/rc.optware

- remove ipkg
- How to uninstall IPKG / Optware?

SSH Access

1. Copy the private key into .ssh/authorized_keys
2. Make sure the homes/user directory, .ssh, and the authorized_keys file are accessible by the owner/user only

```
cd /var/services/homes/user
sudo chmod 700 .
sudo chmod 700 .ssh
sudo chmod 600 authorized_keys
```

- Logging into Synology SSH using a key instead of a password

Rsync

1. Enable Rsync in Control Panel –> File Services. Do not enable rsync account.
2. Give user r/w permissions for shared folder “homes”
3. Give user rsync application permission
4. Make sure user has SSH access to the box with key file
5. rsync command example:

```
rsync -av -e ssh sample.file user@machine:/var/services/homes/user/
```

BackupPC Integration

Follow this guide: Configuration on Synology DSM6 Hosts

Encrypted Shared Folders with auto-mount

Follow this guide: Encrypted partitions/folders with auto-mount

Links

- SSL Checker
- Ports for Synology DSM
- Linux Raid Growing
- Mdadm Cheat Sheet
- How To Manage RAID Arrays with mdadm on Ubuntu 16.04
- How to run fsck on a Synology NAS

Services and Packet Installation

- SSH Access
- FTP Access
- NFS Access
- Command Line
- Cloud Station Server
- Note Station
- CardDAV - Address Book
- CalDAV - Calendar
- Sync with Thunderbird - CardDAV & CalDAV
- Surveillance Station
- Photo Station
- MailPlus Server