|  |
| --- |
| **JDN Standards – Synology SHA** |

Rack mounting 1

Connectivity 2

Configuration 2

Create a new Volume 23

Set up scheduled SMART Testing 27

Create a new shared folder “VEEAM” 29

Disable auto update 30

Set NTP server 31

Create a backup group 32

Create a Backup user 34

Set up monitoring (SNMP) 37

Enable SSH 37

Boot after power failure 38

Disable disk hibernation 38

Enable Monthy Raid Scrub 39

Disable MAC File Service 40

Enable Notifications (Control Panel\Notification) 41

Adjust Notifications 42

# Rack mounting

The Synology rack mount kit rails do not lock the NAS in place when slid into the rack. Due to a ship’s movement, this could cause the NAS to move. To prevent this, we advise to use a long rack mounting screw (not supplied in the rail kit) through the NAS’s front bracket to secure it in place. This should be done on only one side of the unit, as it will be sufficient to lock it firmly in place. The other side of the unit can use the standard Synology recommended mounting method.



*Synology recommended mounting procedure, using the supplied screws.*



*JDN ship mount procedure for Synology, using a long rack mounting screw.*

# Connectivity



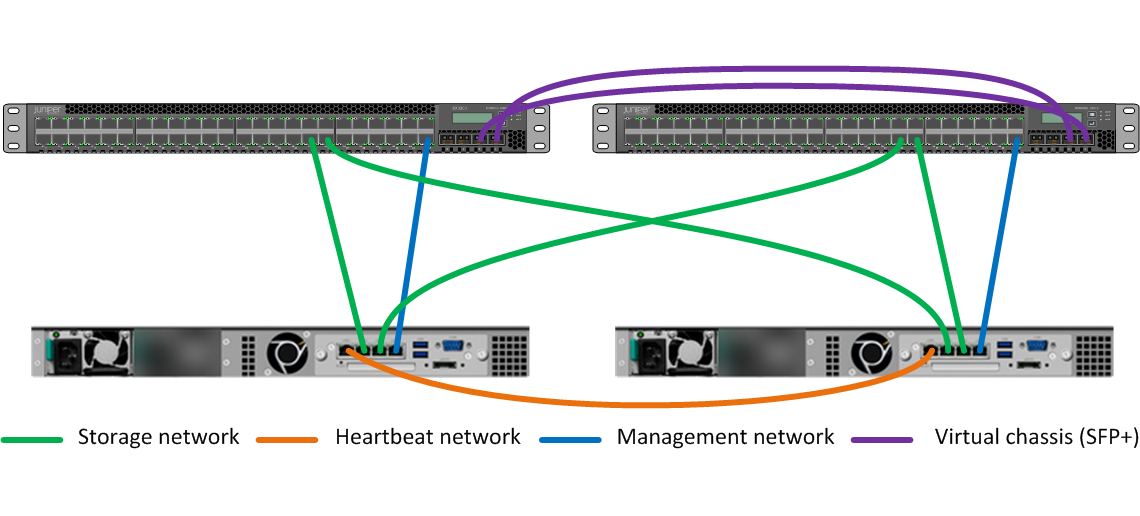
The Synology RS814+ & RS815+ have 4 available network ports:

**NIC1**: Heartbeat (directly connected between Synologies)

**NIC2**: Backup/storage network (connected to the switch on Backup, not VLAN tagged)

**NIC3**: Backup/storage network (connected to the switch on Backup, not VLAN tagged)

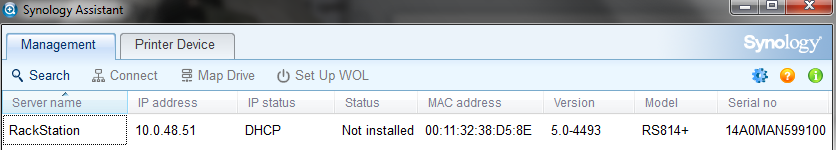
**NIC4**: Management (connecto to the switch on Admin\_Trust, not VLAN tagged)



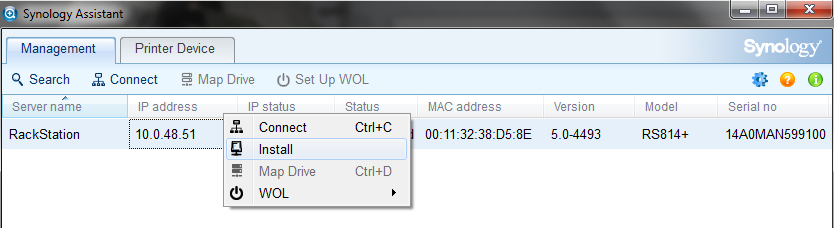
During initial configuration it is easiest to only connect NIC4.

# Configuration

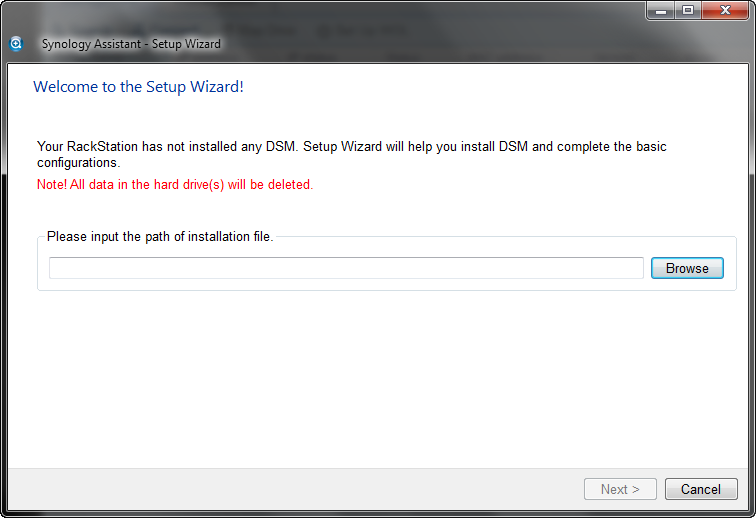
Use Synology assistant to discover your first NAS on the network

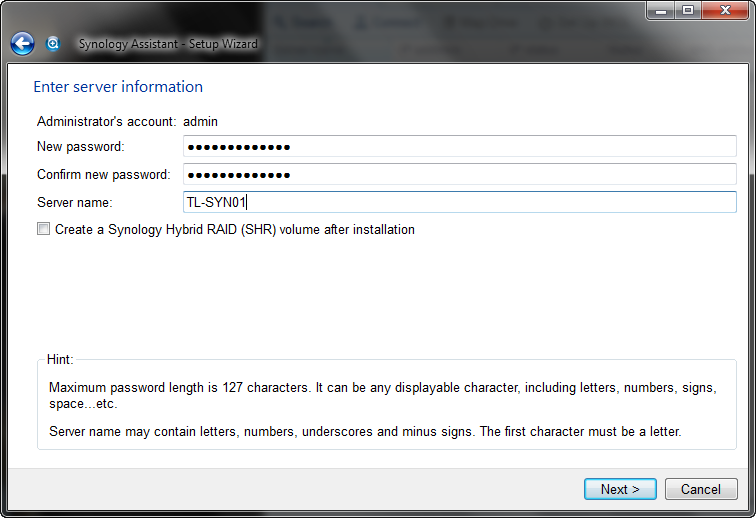
Right click the NAS and select install



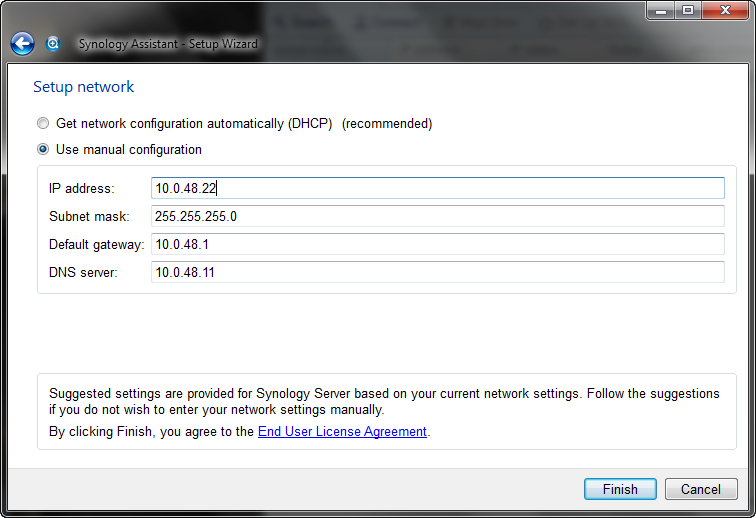
Upload the DSM software onto the NAS



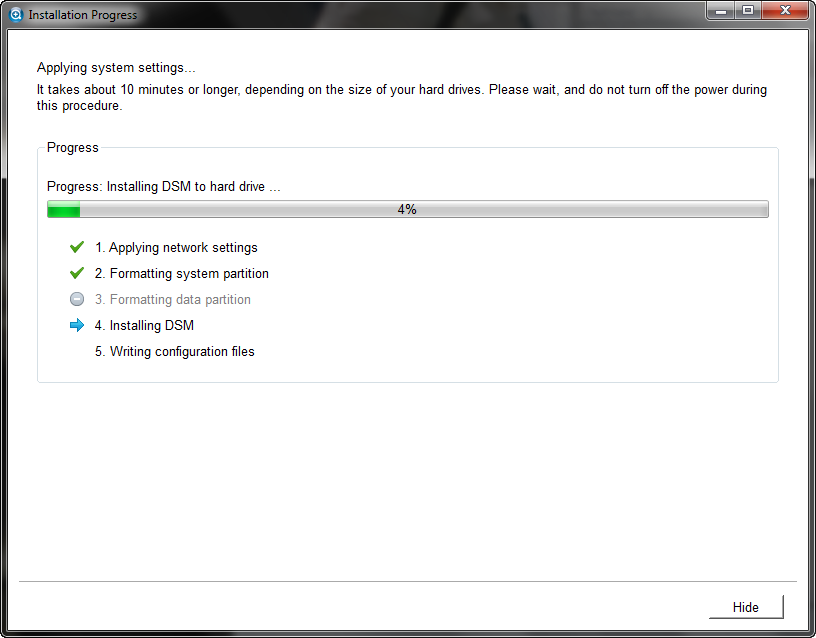
Enter the server information **and disable the creation of SHR**



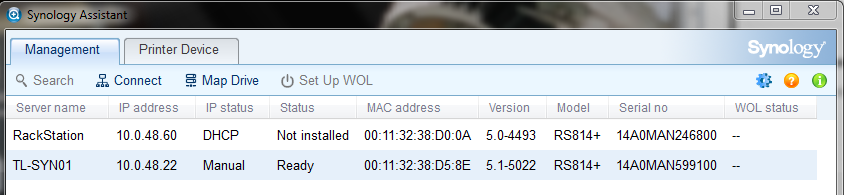
Configure the network in the admin trust range

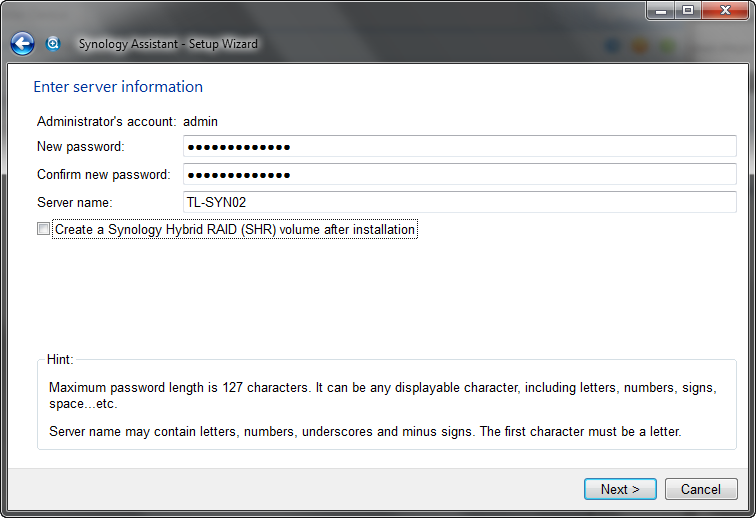


Grab something to drink

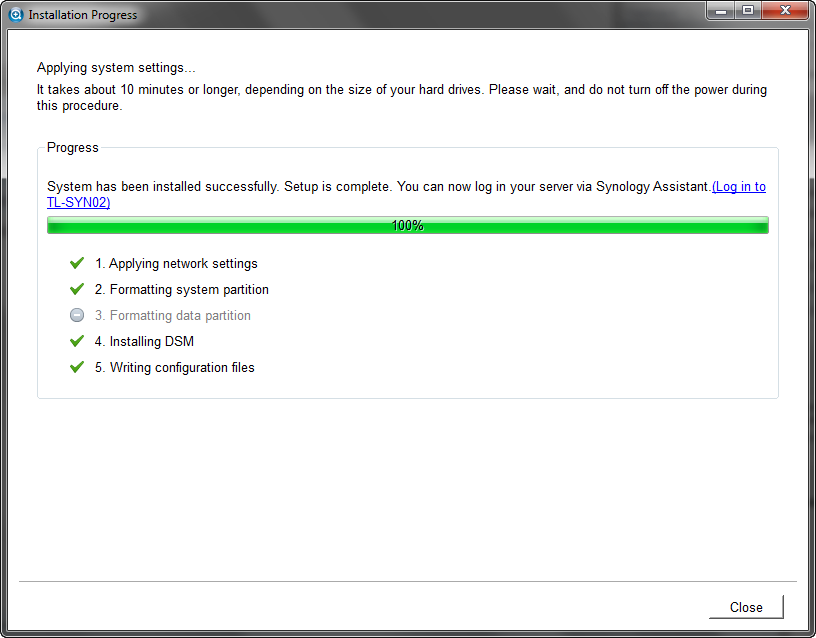


Repeat all the previous steps for NAS02

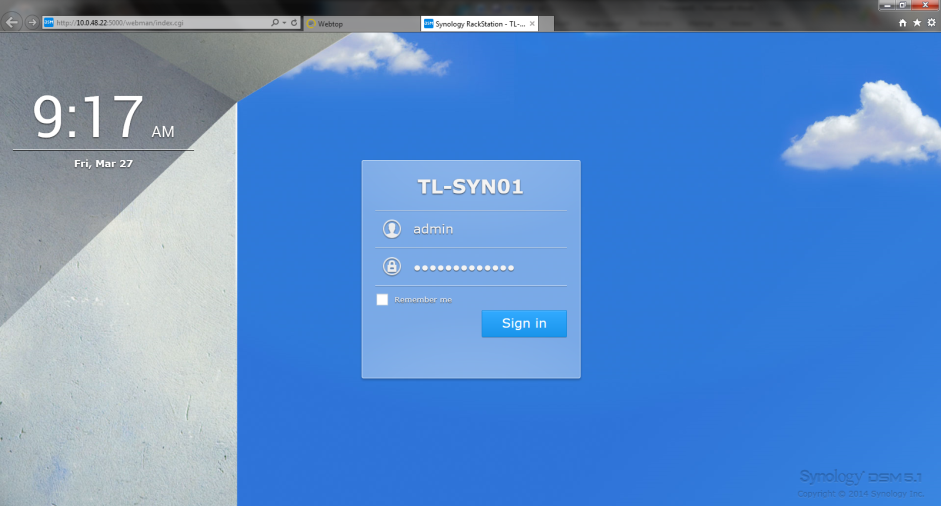




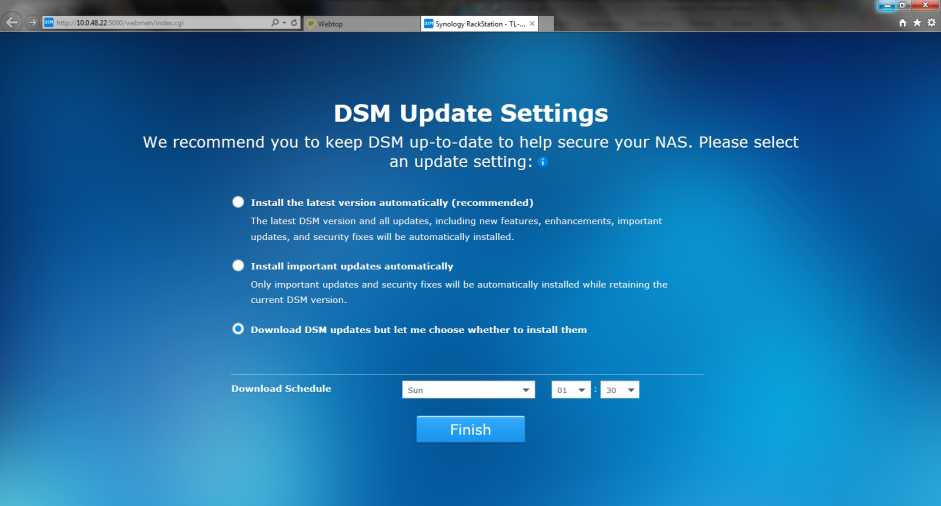




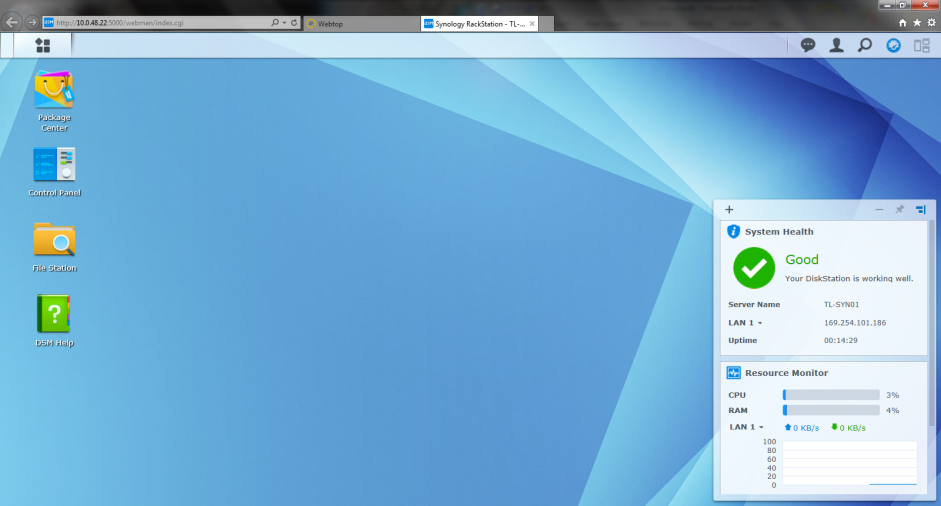
Log in into the first NAS



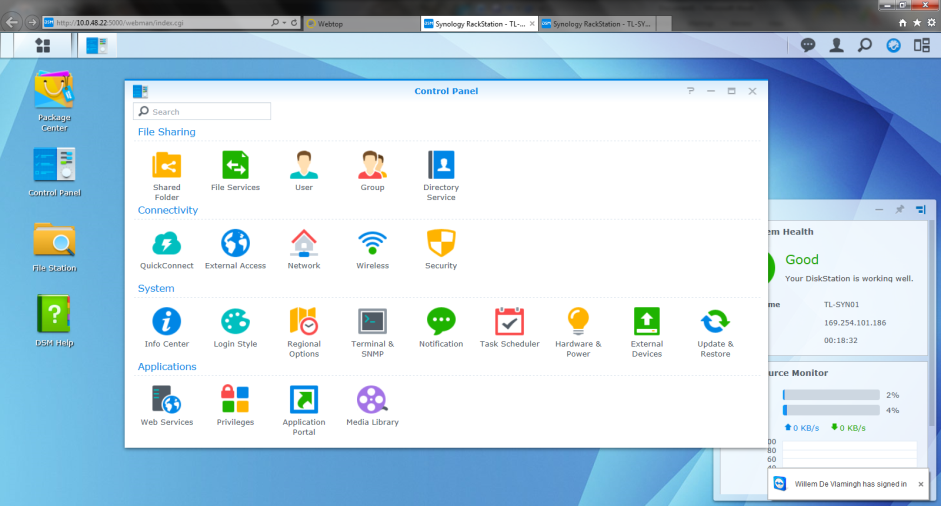
Select download DSM updates but let me chose whether to install them and click finish



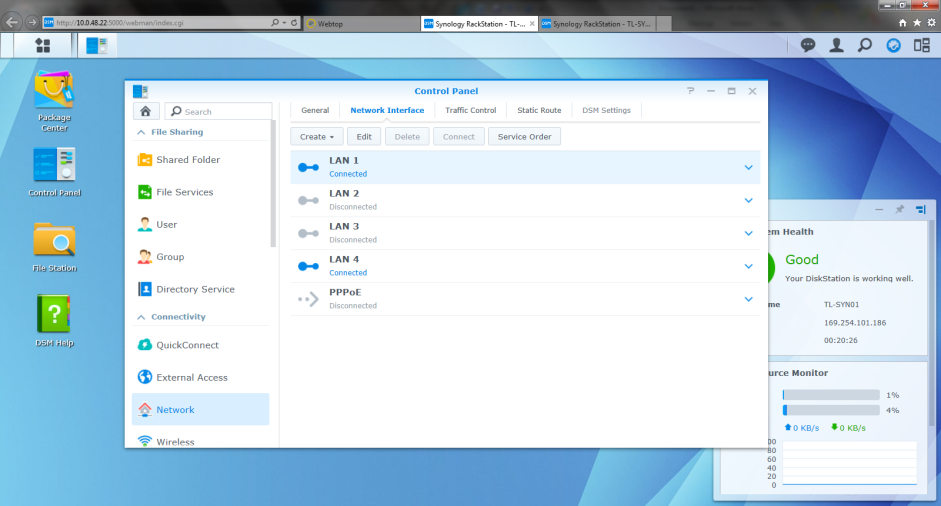
The NAS is now ready for configuration.



Open the control panel on SYN01 and select network

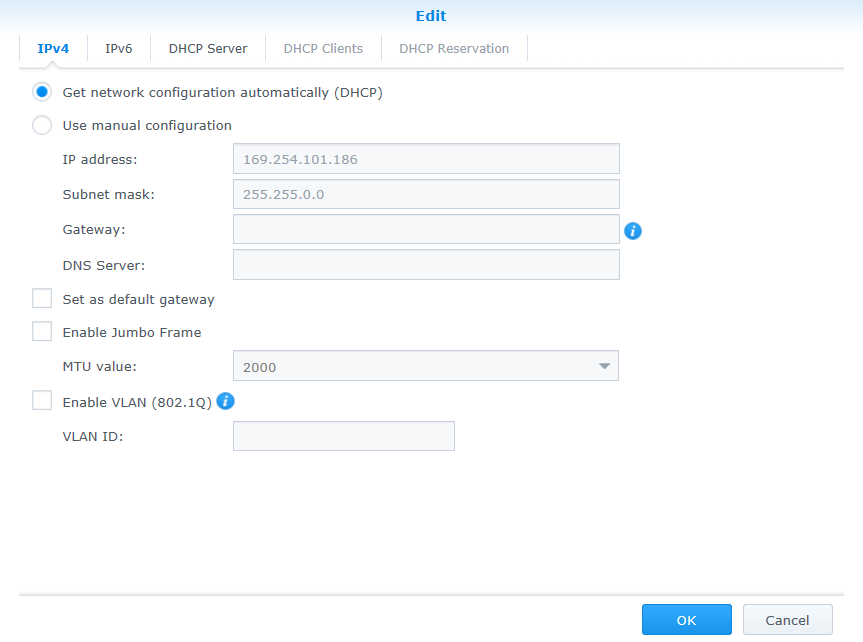


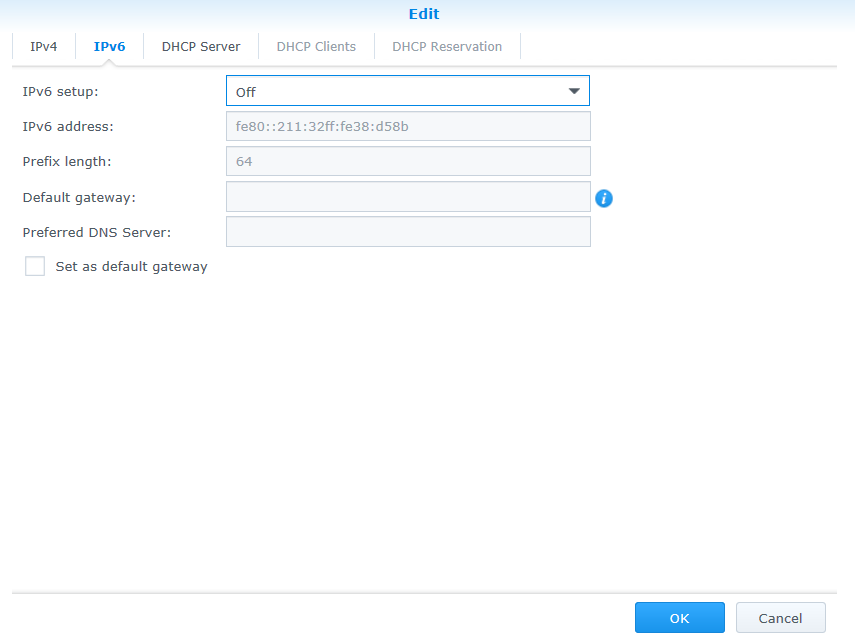
Go to the 2nd tab interfaces and select the interface you would like to edit



Press the edit button and adjust the interface IP settings for LAN1

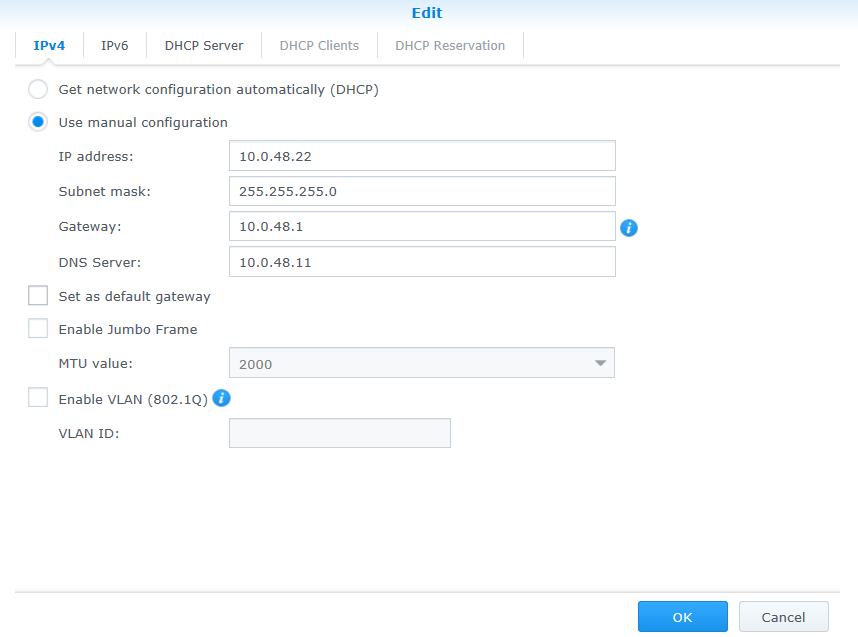
* IPv4 can stay on DHCP since this interface will link the 2 NAS and will be used as heartbeat.
* Disable IPv6

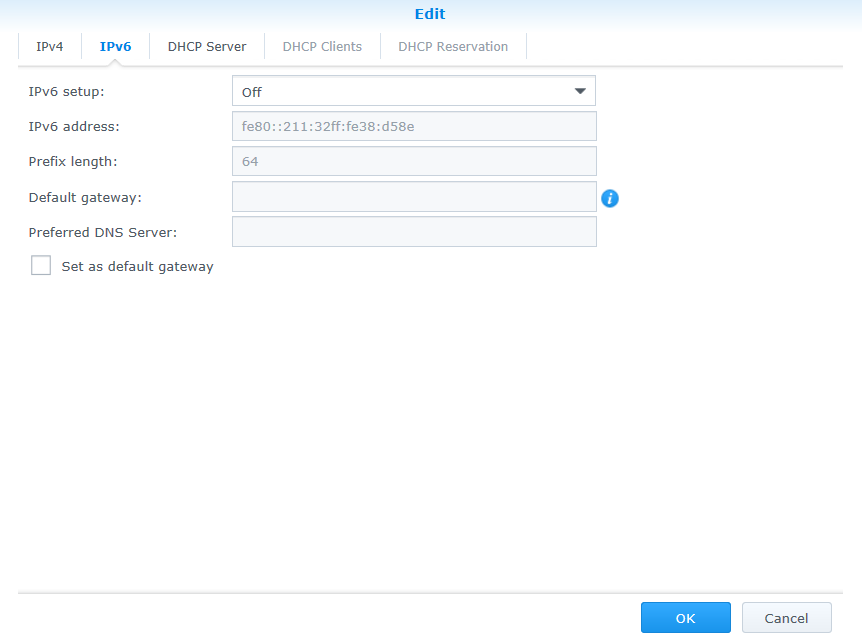




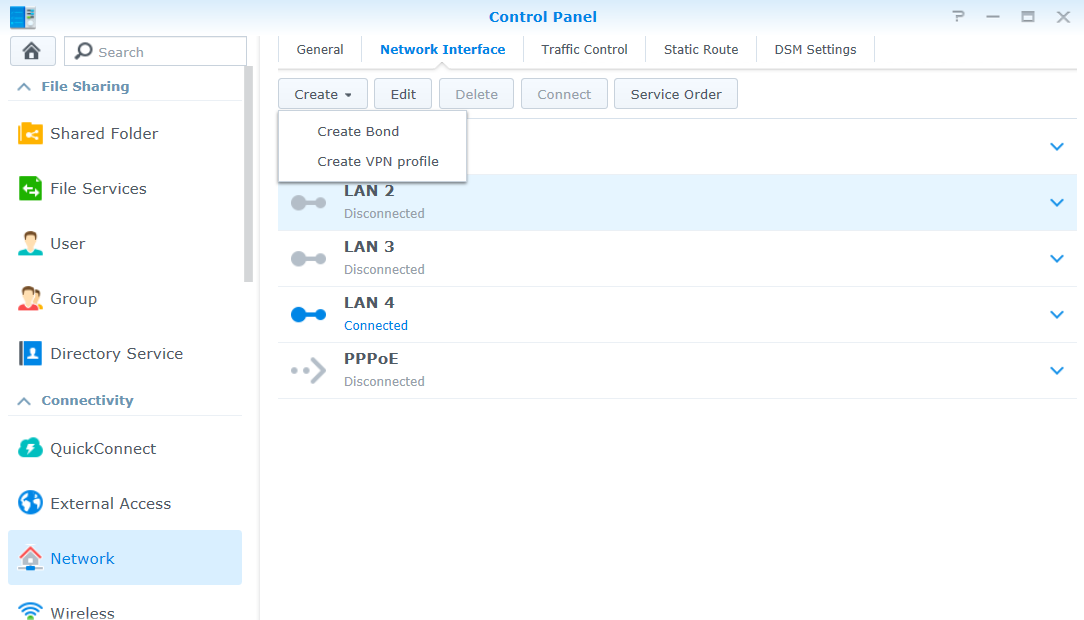
Press OK and edit LAN4 which will be used for MGMT (ADMIN-TRUST)

* IP address should already be in place
* Enable “Set as default gateway”
* Disable IPv6

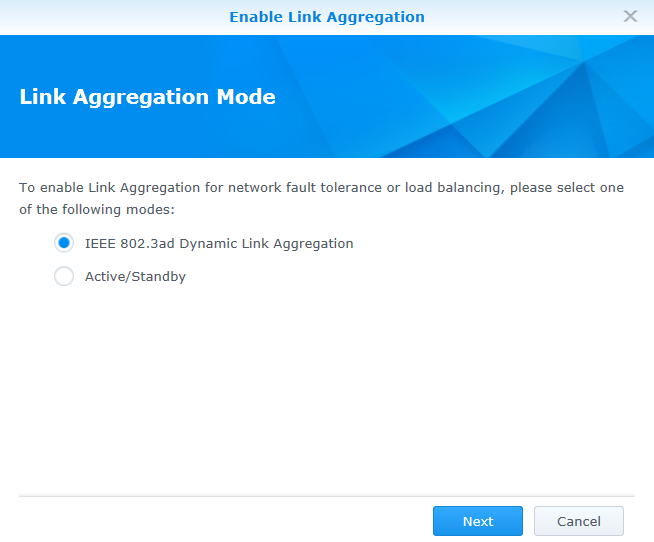




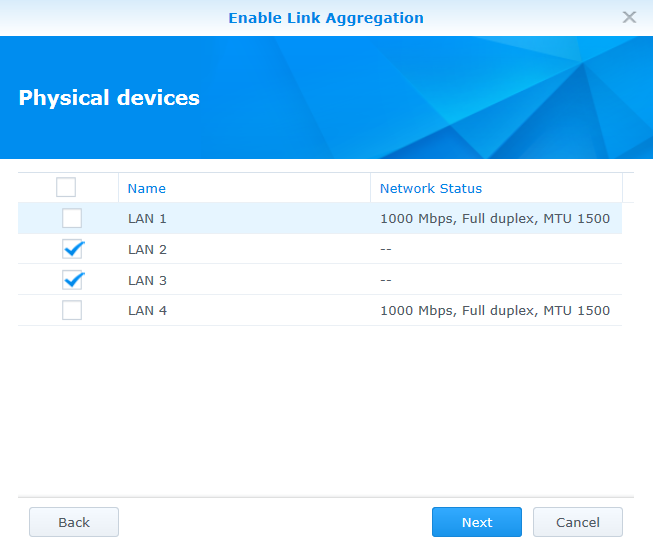
Select LAN2 and click “Create” > “Create Bond”



Select IEEE802.3ad



Select LAN2 and LAN3



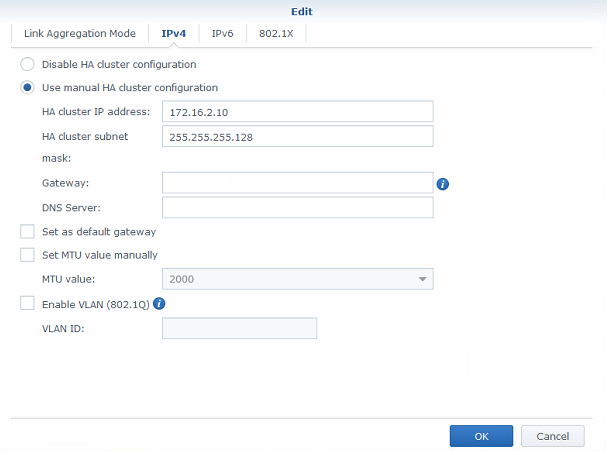
Select manual IP configuration and configure the network

Click apply

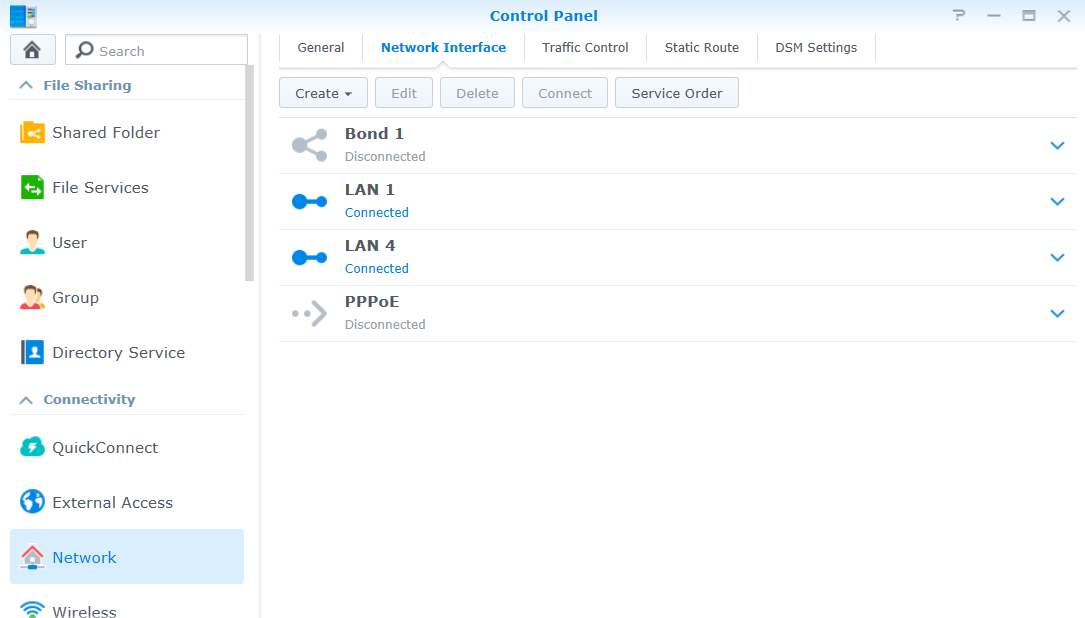
Make sure default gateway is unchecked.

The IP address should be 172.16.2.11 on both hosts (instead of the 172.16.2.10 in the screenshot)

No Gateway!

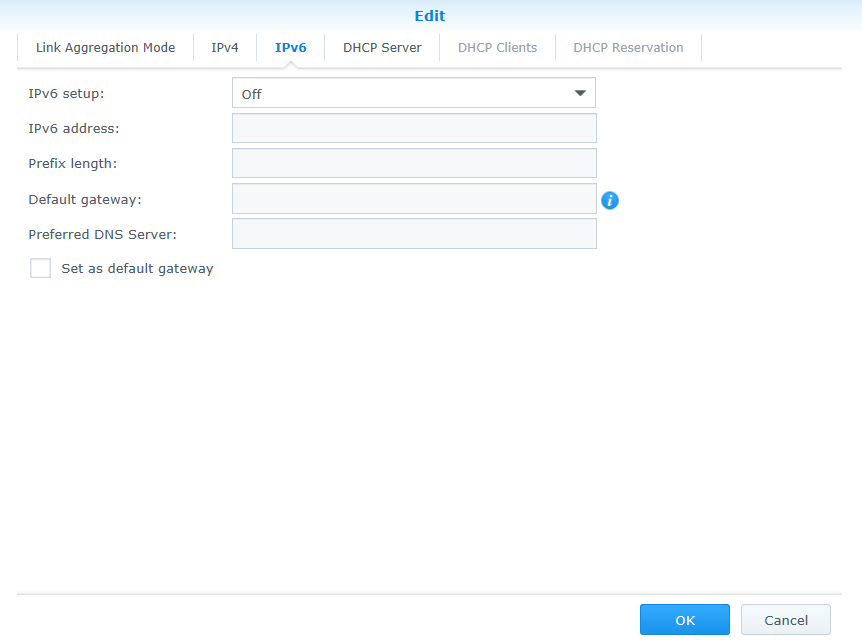


After configuring the Bond interface the network tab should look like this.

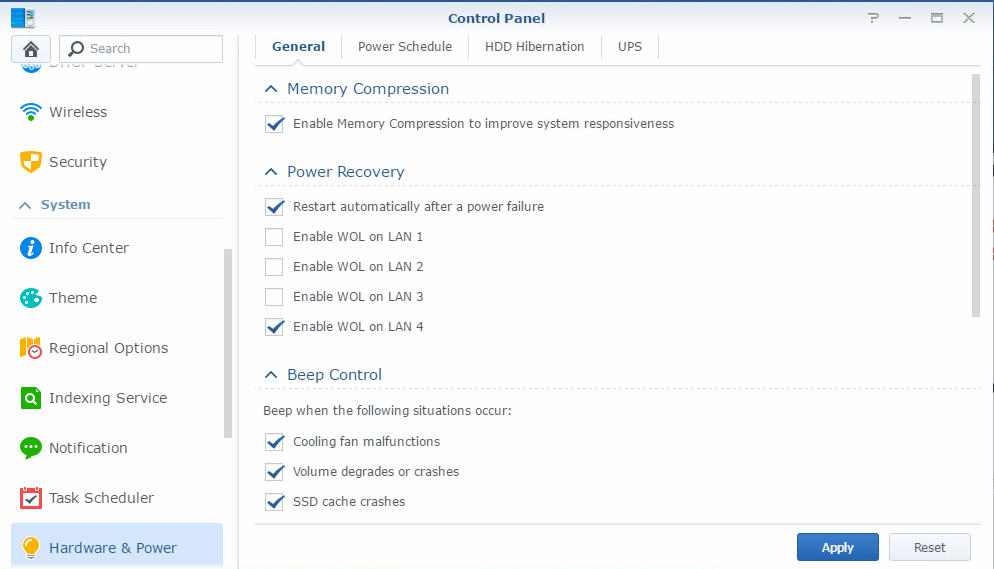


Disable IPv6 on “Bond 1”

Disable “Set as default gateway”

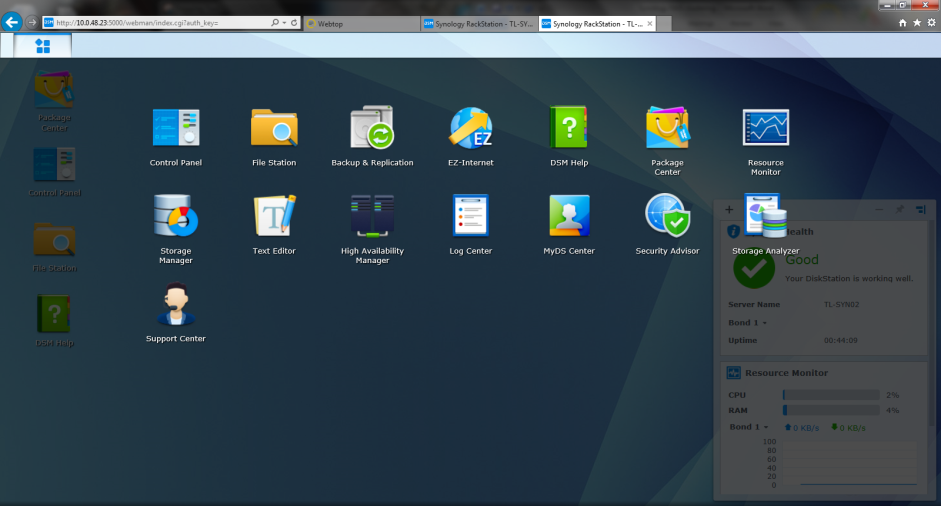


Enable Wake on LAN for LAN4

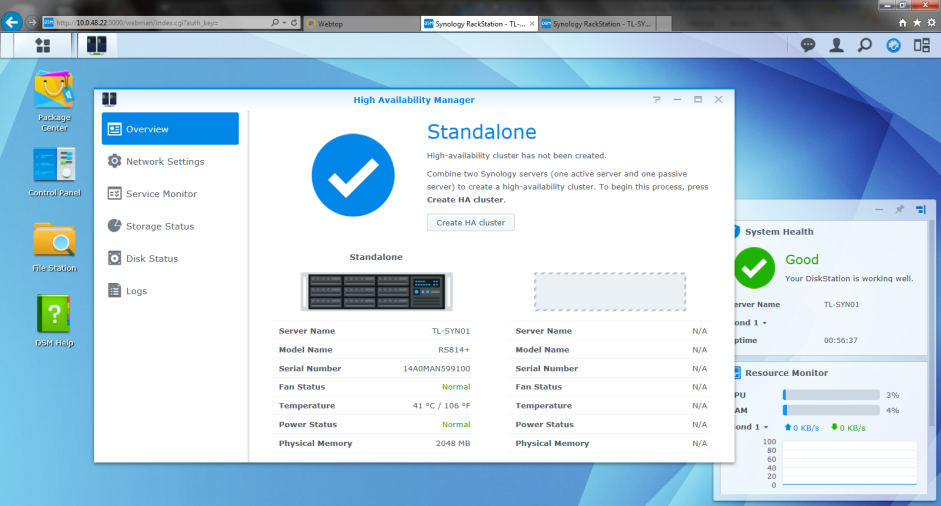


**Repeat these steps onto the 2nd NAS**

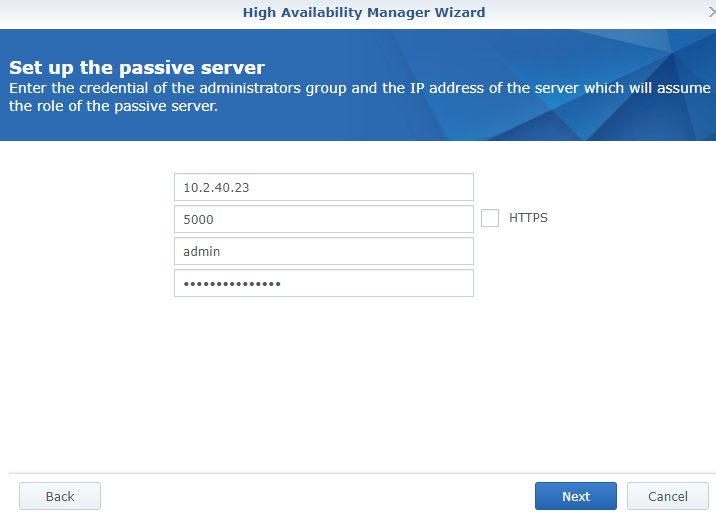
If the 2nd NAS is configured, return to the “Main menu” of the 1st NAS and select the High Availability Manager



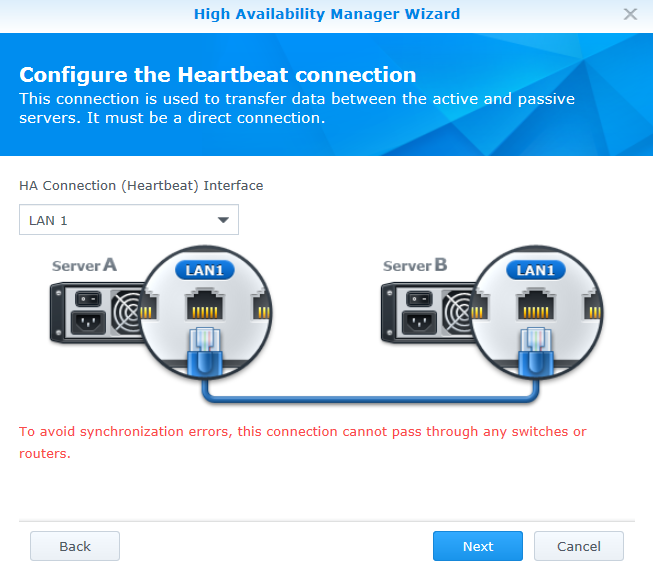
Click the “Create HA Cluster” button



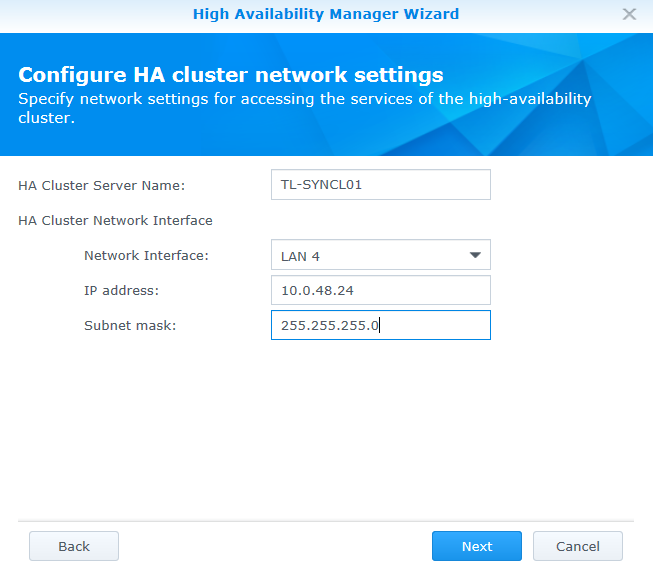
Set up the Passive server by entering the SYN02 network address and logon credentials



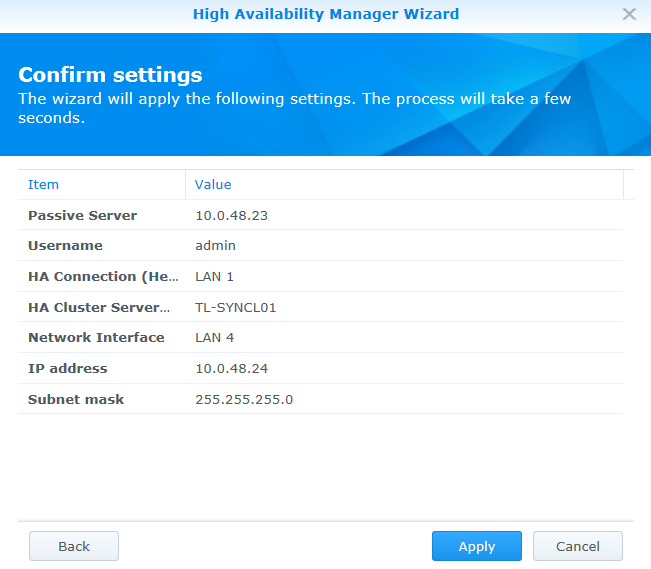
Select the LAN1 interface as the interface of the heartbeat (used for data transfer)



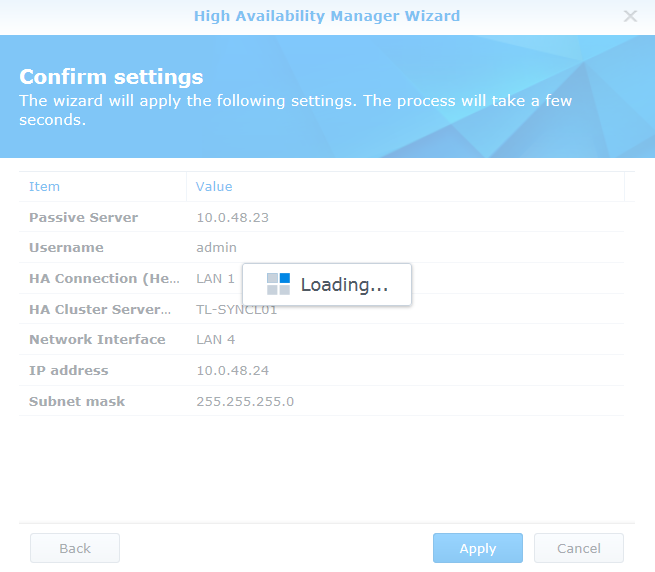
Select a Name and a virtual IP address for the cluster (use LAN4)

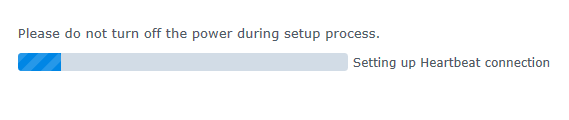


Select Apply to create the Cluster

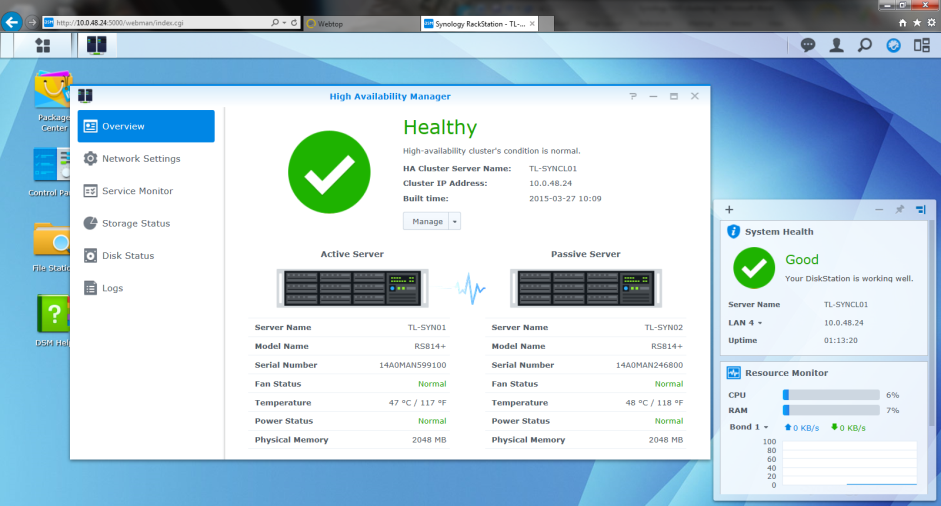


This will take a while





The cluster is ready when the following screen appears



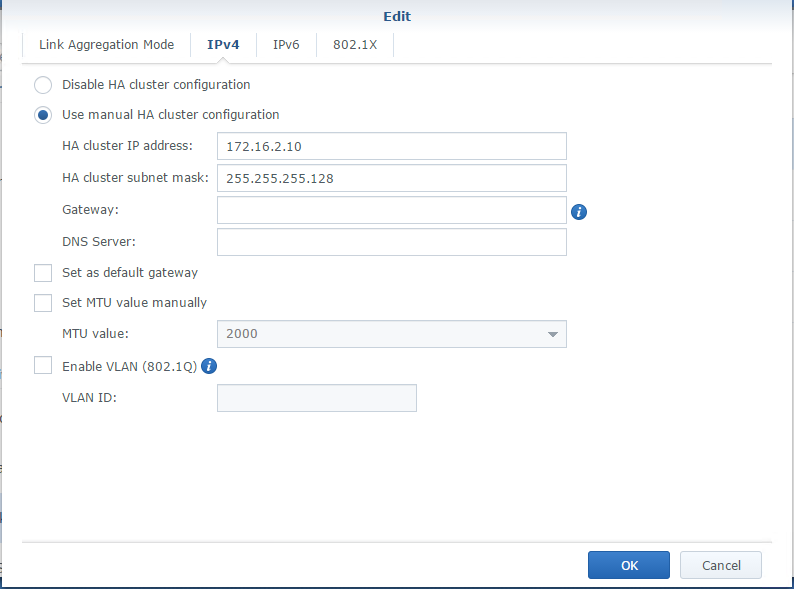
Go in the HA Availability Manager to the “Network Settings” tab and press the “Change network settings” button.



Make sure that bond 1 is up on Both NAS and Edit the Bond 1 network settings.



No Gateway!



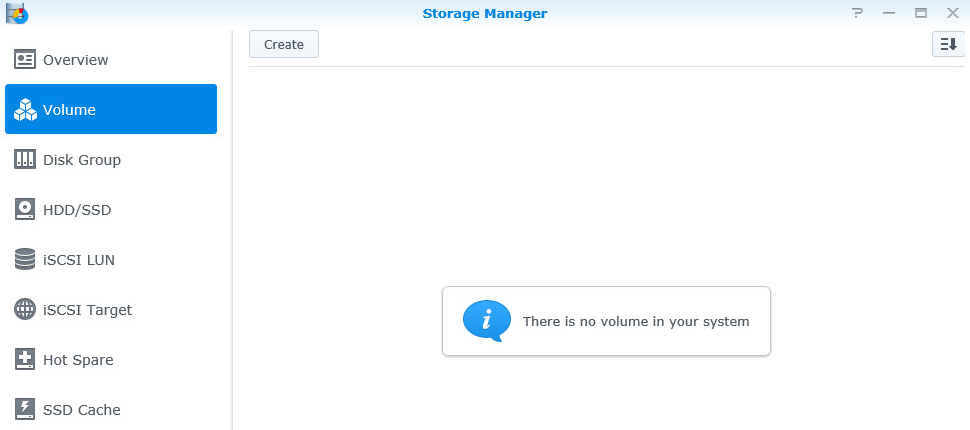
After configuration the cluster should be reachable on the additional cluster IP address.

## Create a new Volume

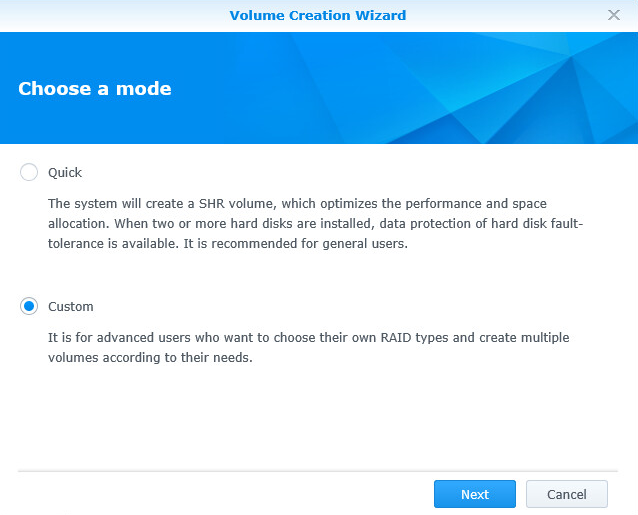
Open the Synology storage manager



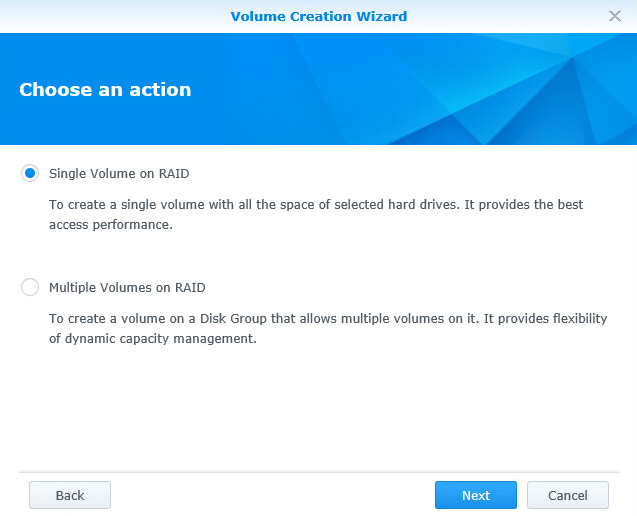
Select volume and click create



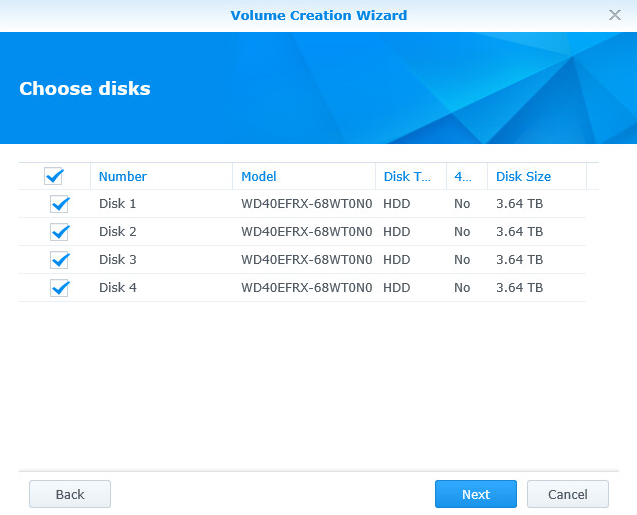
Select custom instead of SHR and press next



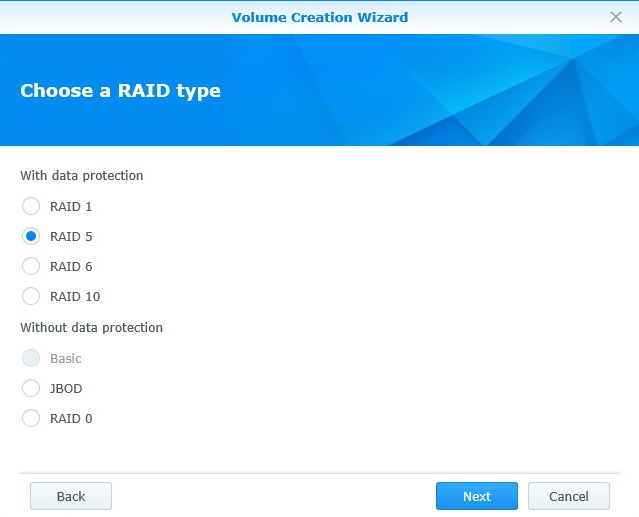
Select a single volume



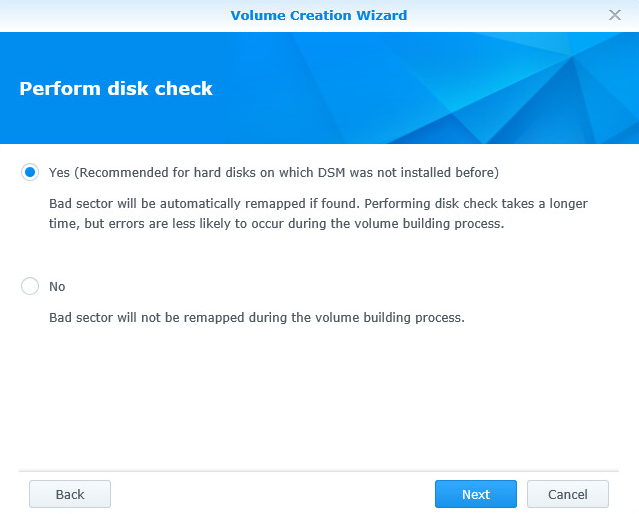
Select all disks



Select RAID5



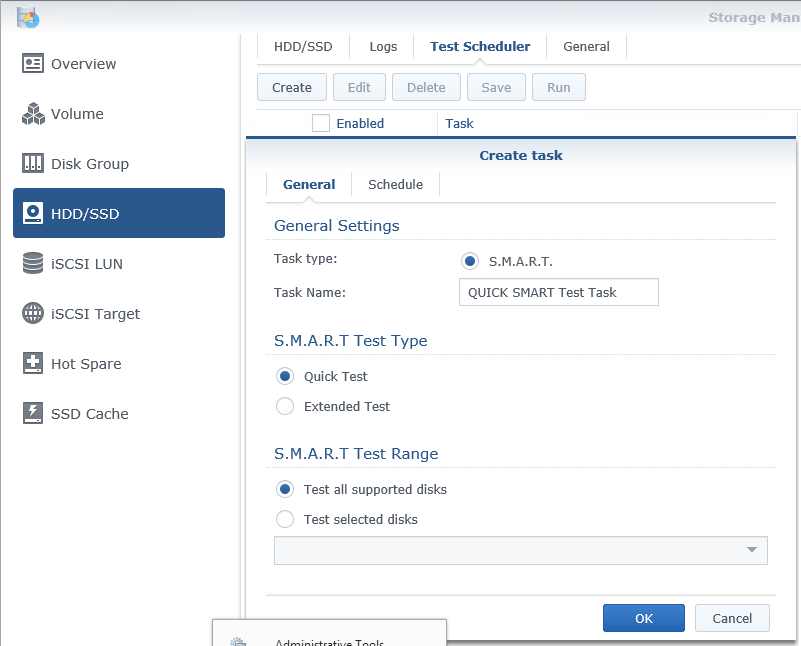
And always perform a disk check (this can take more than 24h!!!)



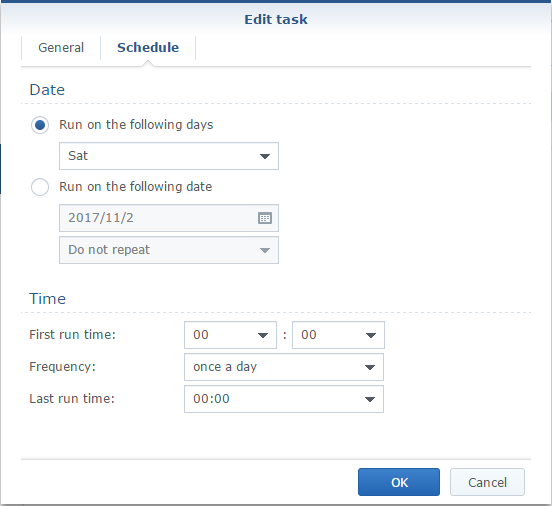
## Set up scheduled SMART Testing

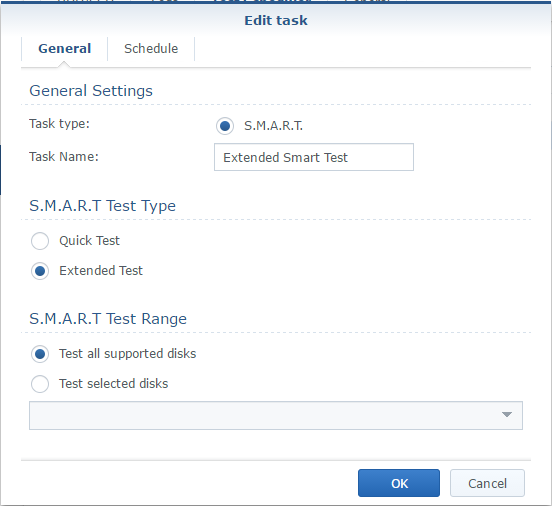
In the Storage manager > HDD/SSD > Test Scheduler section, create 2 new rules.

1 quick SMART test that runs weekly and 1 extended SMART test that runs monthly

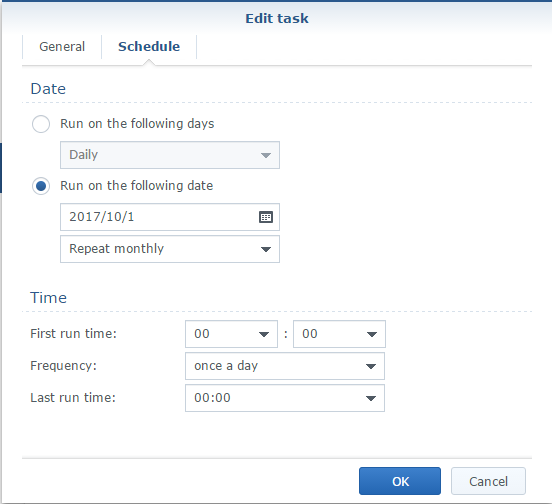


Select a day to run the quick test weekly.

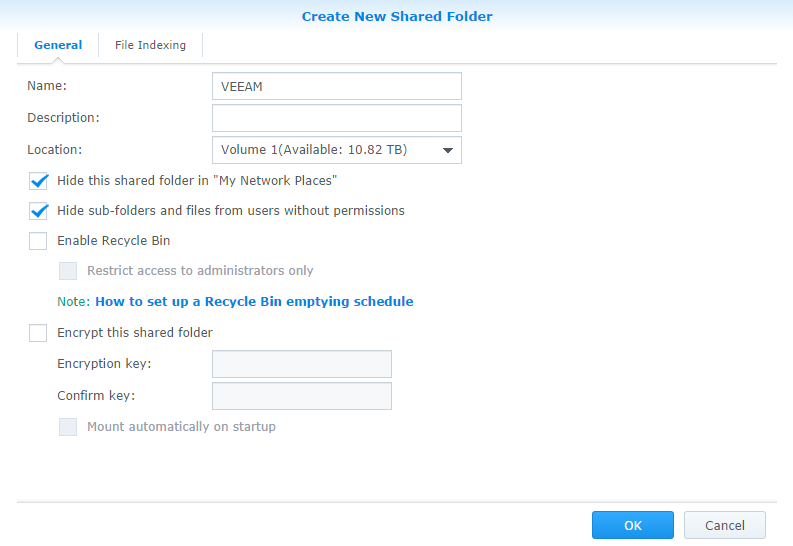


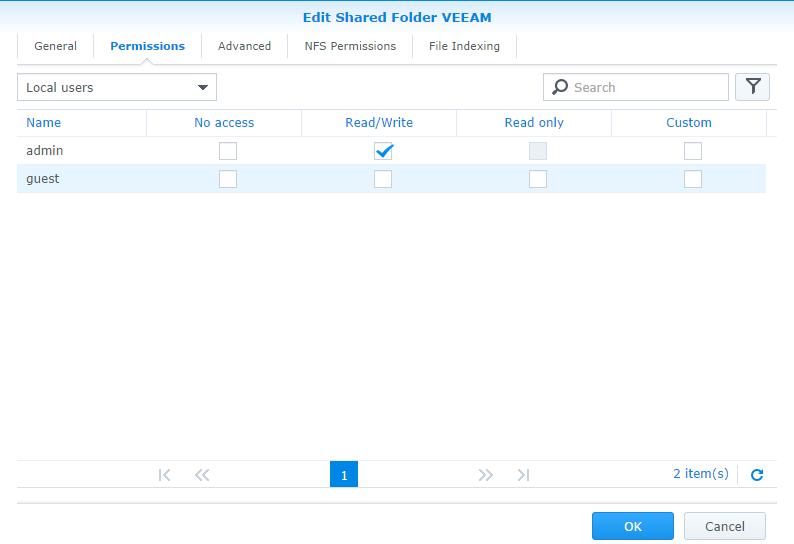


Select a start date and select repeat monthly for extended.



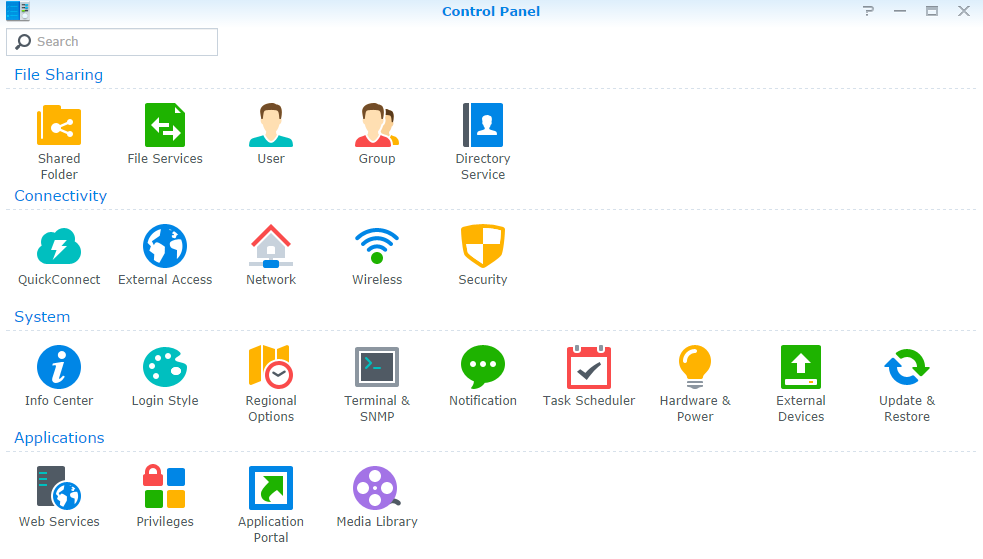
## Create a new shared folder “VEEAM”



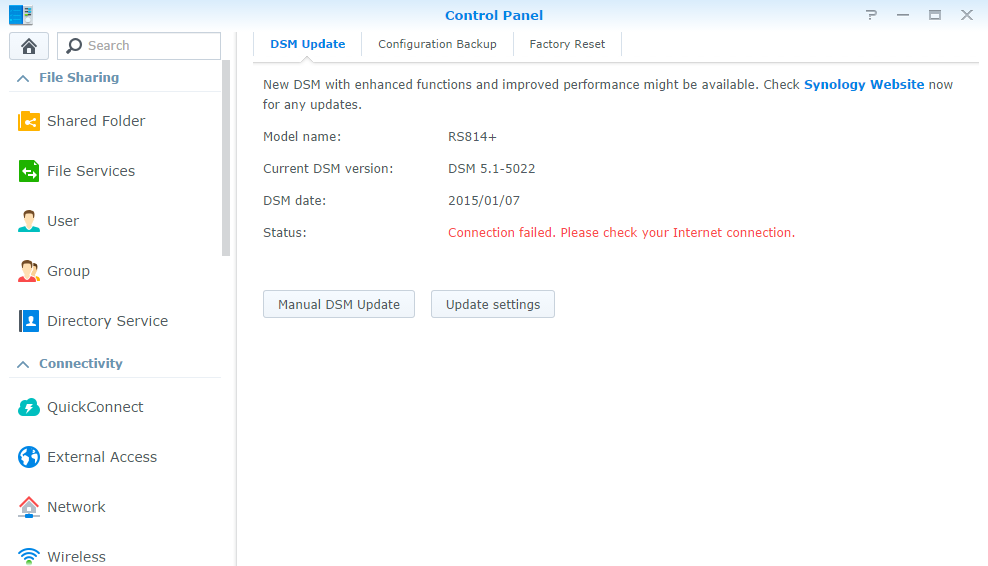


## Disable auto update

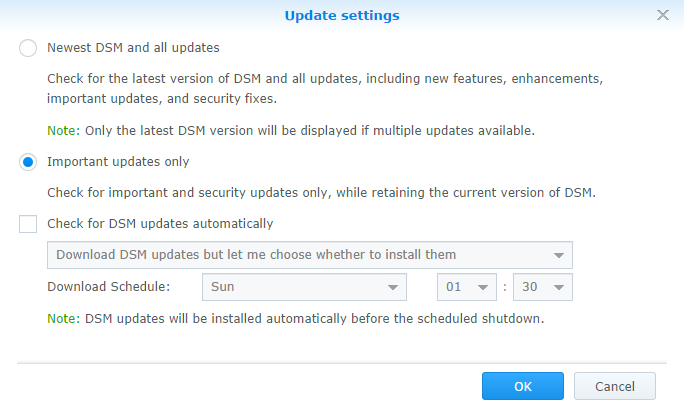
In the configuration panel select “Update & Restore”



Select Update settings

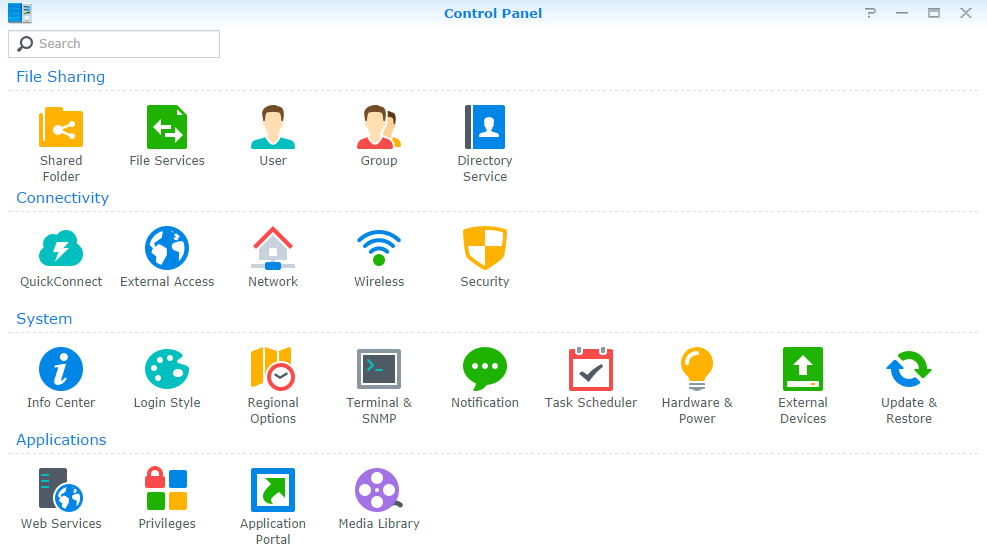


Uncheck “Check for DSM updates automatically” and press “Ok”

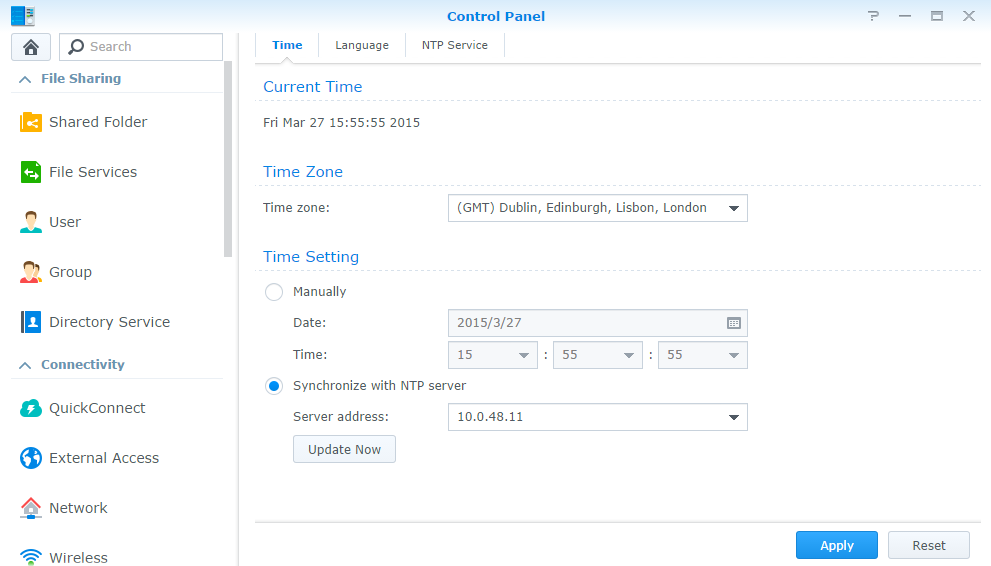


## Set NTP server

Select “regional options” in the “control panel”.



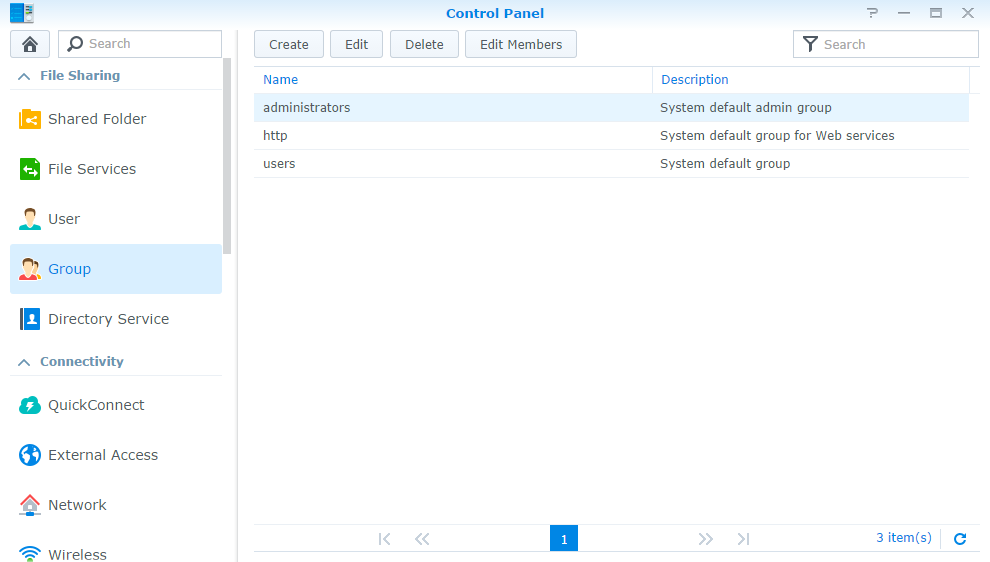
Set the Time zone to UTC and fill in the IP address of the domain controller in the server address bar



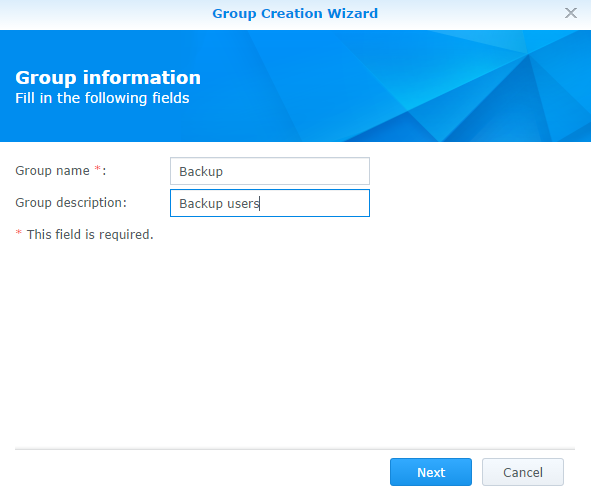
Press update now to make sure the device is synchronized

## Create a backup group

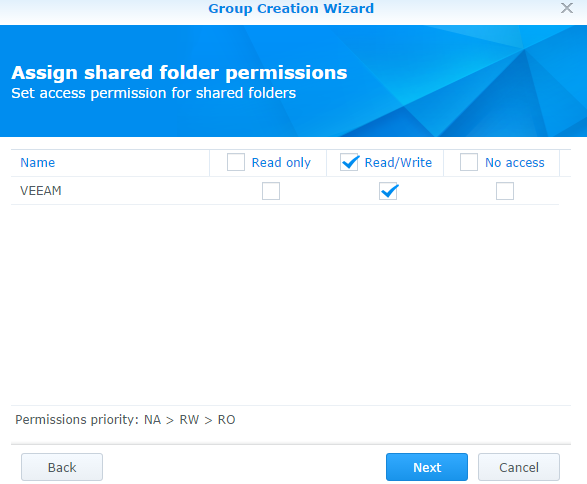
Select group in the control panel and click on the create button



Create a new group named “Backup” and press “Next”



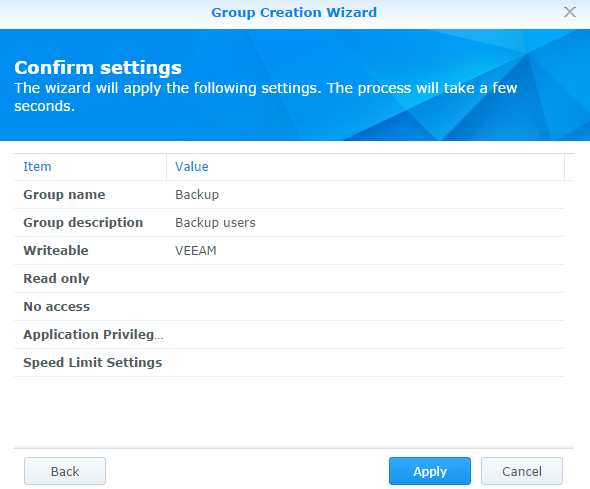
Give the backup group RW rights to the Veeam backup share



Don’t assign application permissions

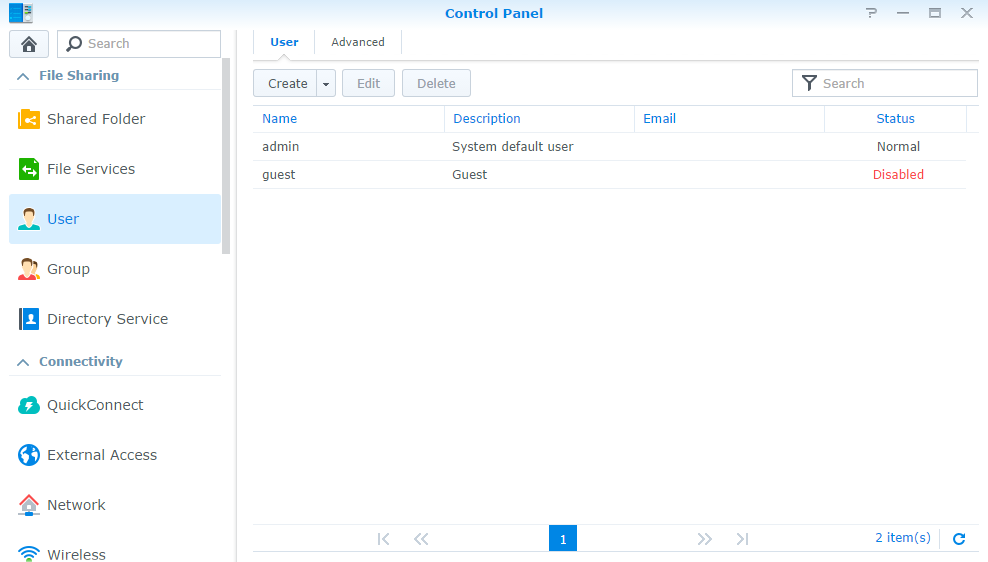
Don’t set speed settings

Apply the configured settings

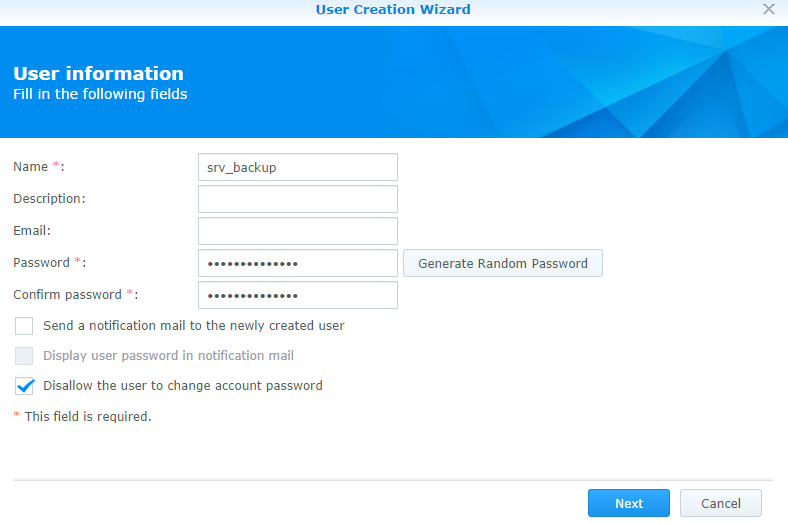


## Create a Backup user

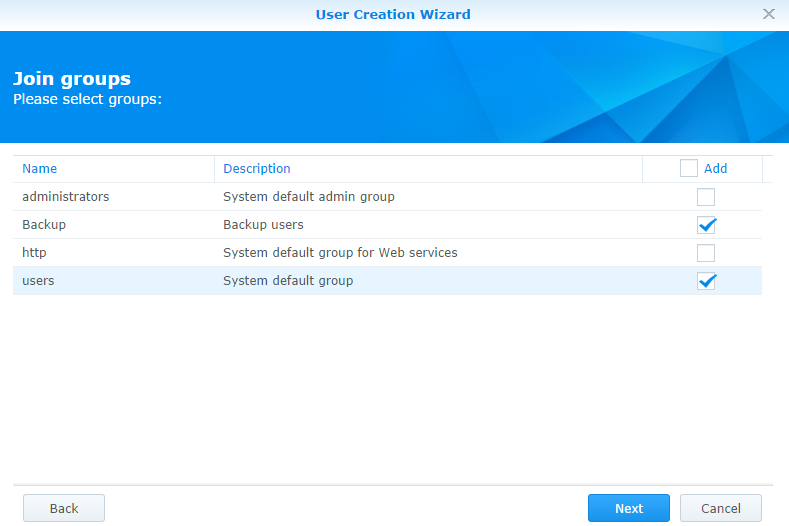
Select “User” in the control panel and click on the create button

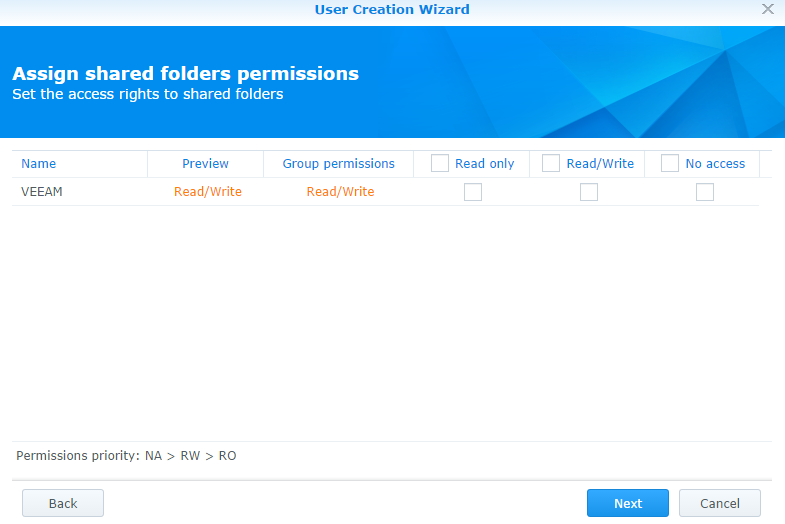


Create a “srv\_backup” user, including password and select that the user is not allowed to change his password

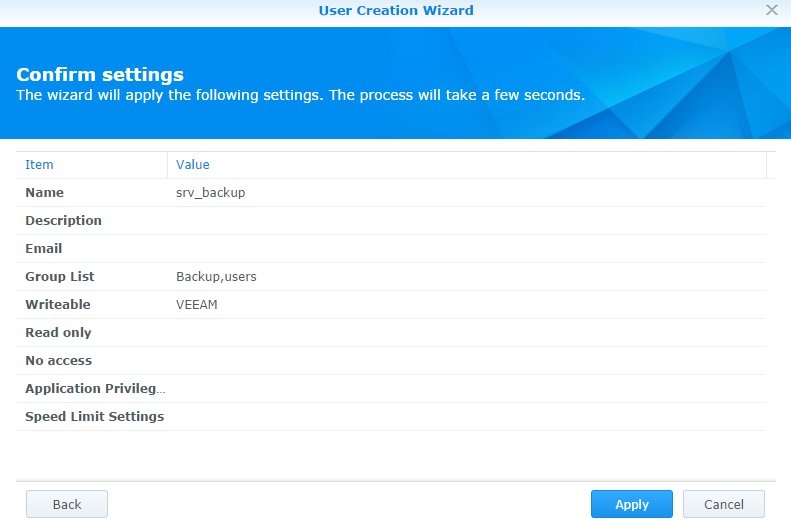


Add the user to the backup group





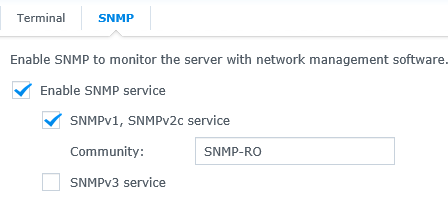
* Don’t set usage quota
* Don’t assign application perissions
* Don’t assign speed limits



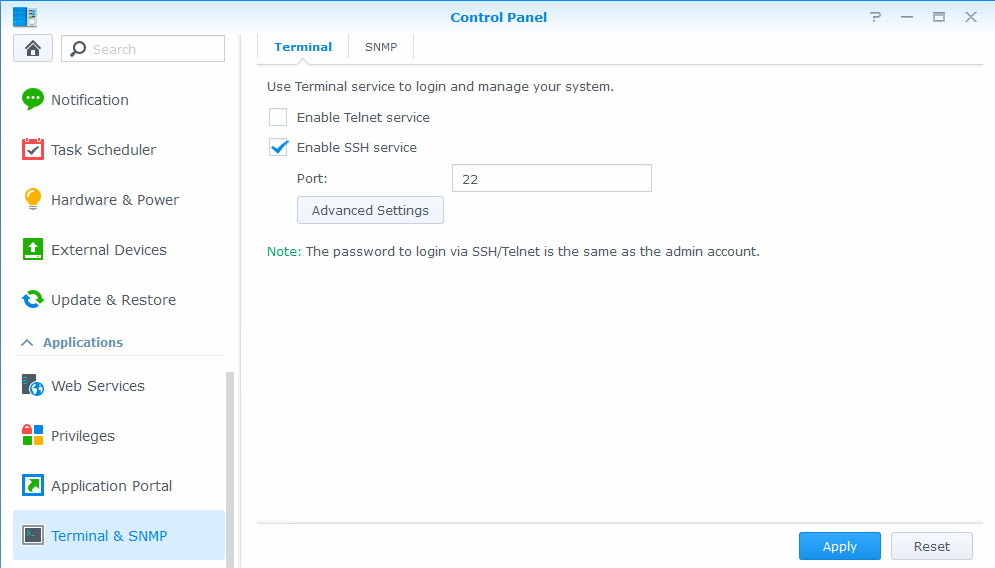
## Set up monitoring (SNMP)

Select “Terminal & SNMP” in the “Control Panel” and go to the SNMP tab.

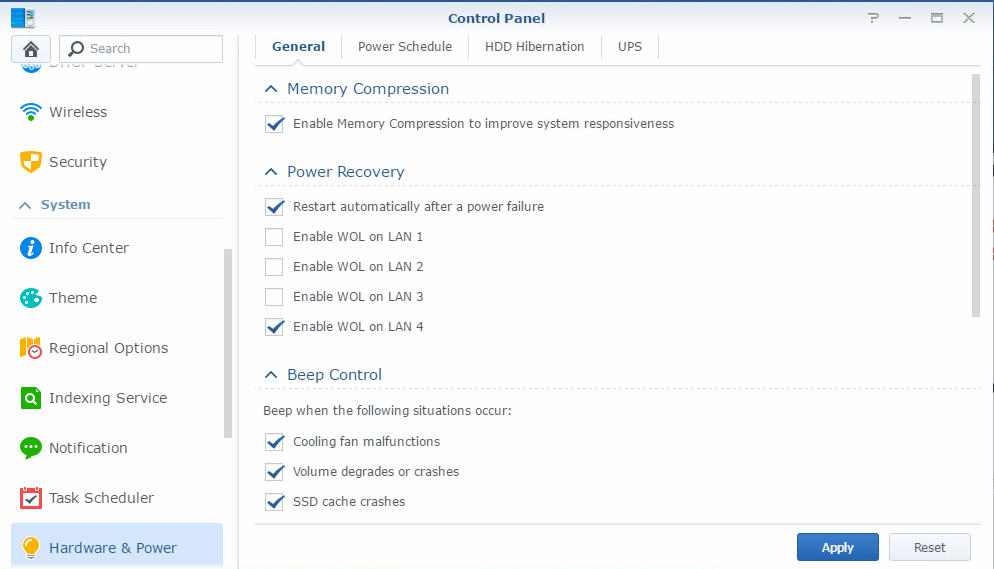
Community: SNMP-RO



## Enable SSH

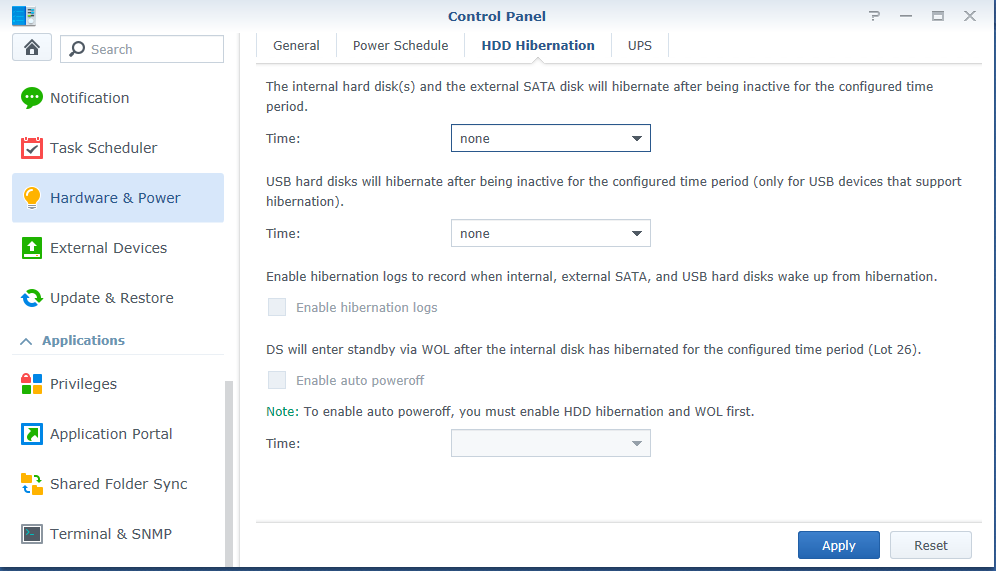


## Boot after power failure



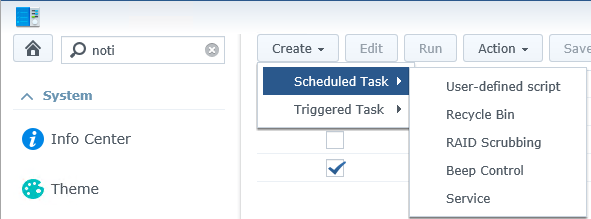
## Disable disk hibernation

Set Time to ‘none’

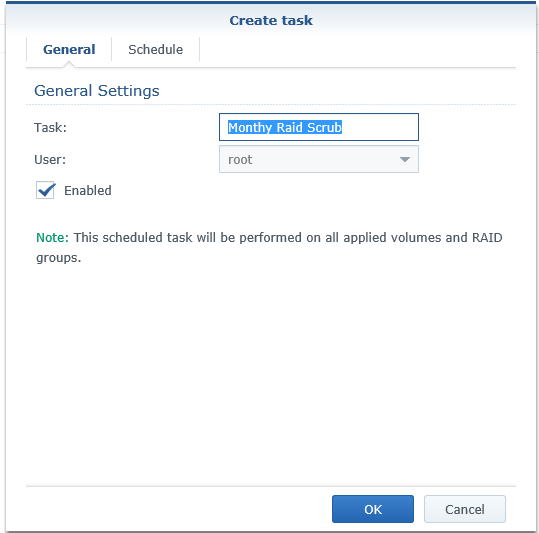


## Enable Monthy Raid Scrub

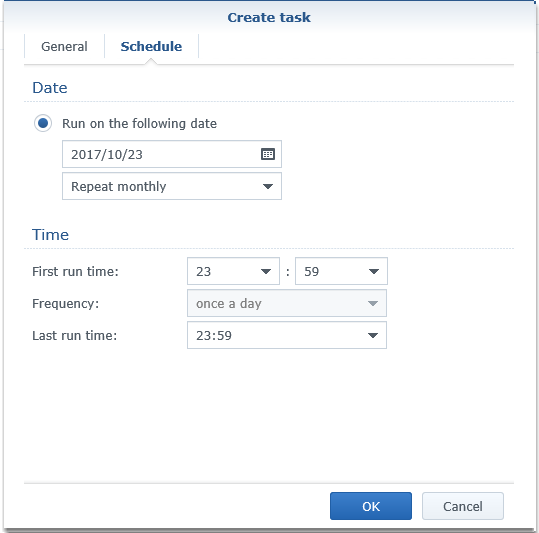
In control panel > Task scheduler: create scheduled Task and select ‘RAID Scrubbing’.



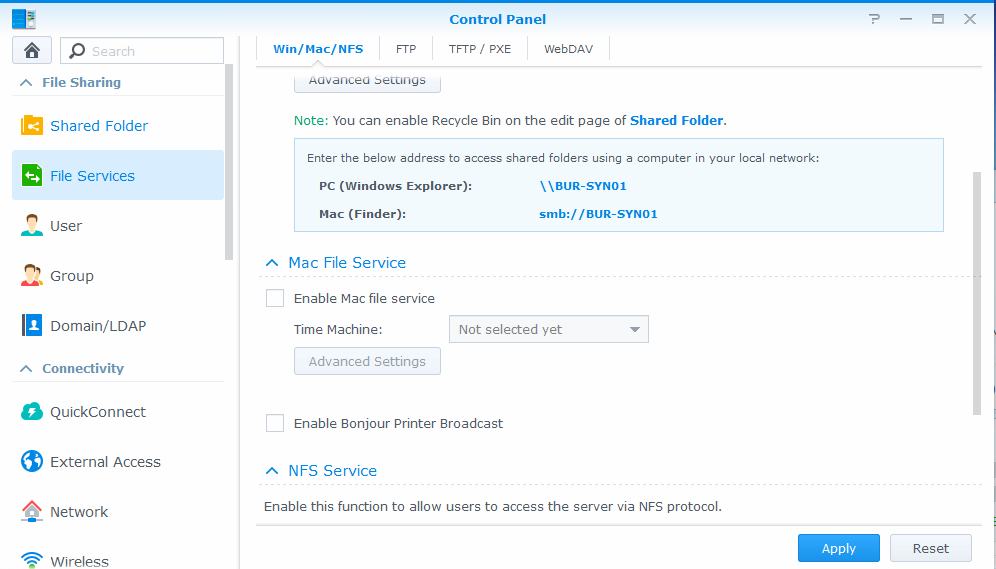
Use following settings



Set to repeat monthy

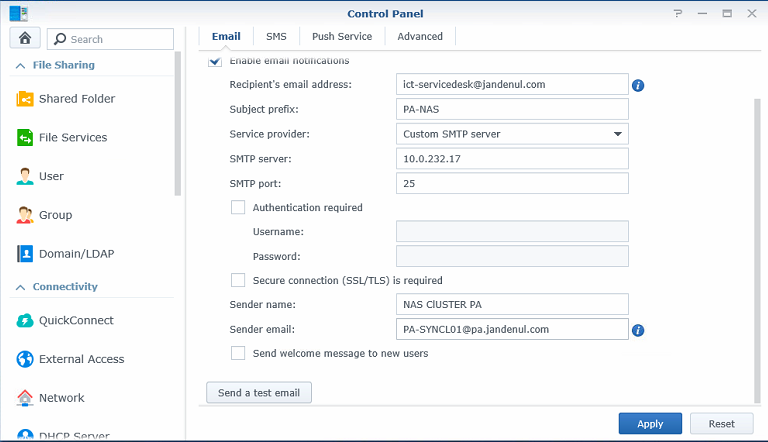


## Disable MAC File Service

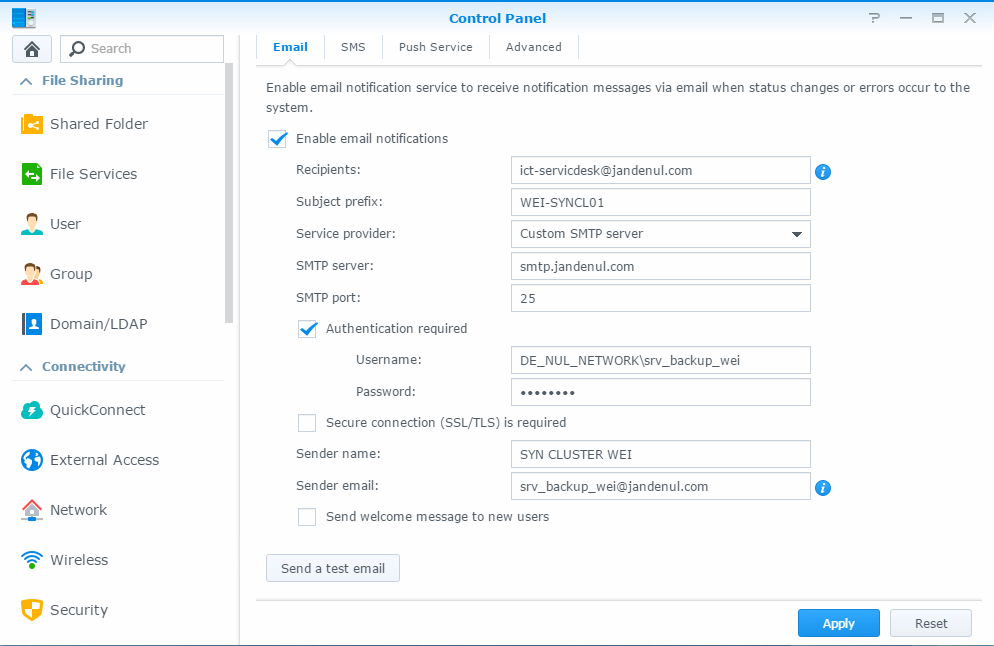


## Enable Notifications (Control Panel\Notification)

For ships: no authentication required as Commbox is being used.



For sites: authentication is required.



## Adjust Notifications

Copy script folder SetNotifications from below location to the MGMT.

[\\Jdn-file01\ict\_new\_standard\_sites\_vessels\Scripted Install\Synology (1.1)](file:///\\Jdn-file01\ict_new_standard_sites_vessels\Scripted%20Install\Synology%20(1.1))

Run the script; enter the Admin password and Synology IP.

The script will now enable and disable the required Notification messages.