

How to monitor the status of
Western Digital
My Cloud PR4100
NAS server drives using
Hard Disk Sentinel
and a Windows PC

Illustrated guide



This guide explains how to monitor the status of Western Digital My Cloud PR4100 NAS server drives using Hard Disk Sentinel software and a Windows PC.

The description applies to the PR4100 server with OS5 version 5.31.102.

I. Warning.

Making a mistake when configuring the NAS may cause permanent damage to the My Cloud PR4100 operating system and render the NAS unusable.

If you are not sure what you are doing, don't do it. You act at your own risk.

You have been warned.

II. What you will need

1. Hard Disk Sentinel Professional for Windows:

https://www.hdsentinel.com/hard_disk_sentinel_professional.php

2. Hard Disk Sentinel for Linux:

https://www.hdsentinel.com/hard_disk_sentinel_linux.php

Since the PR4100 is equipped with an Intel Pentium N3710 processor and has a 64-bit version of Linux installed, you should download the program described as „Hard Disk Sentinel 64-bit Linux console version - **executable, zip-compressed**”

3. SSH client, e.g., PuTTY: <https://www.chiark.greenend.org.uk/~sgtatham/putty/>

4. SFTP client, e.g., WinSCP: <https://winscp.net>

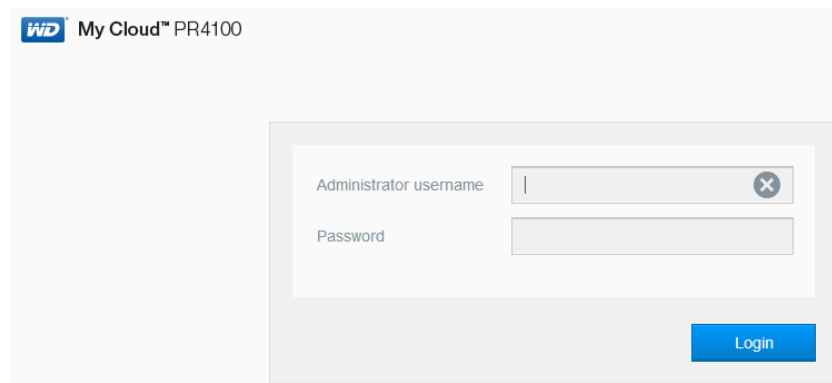
III. Install Hard Disk Sentinel for Linux on your NAS server

1. Download „Hard Disk Sentinel 64-bit Linux console version - **executable, zip-compressed**” (see section II.2).

Today, as I write this guide, the downloadable file is named „hdsentinel-020c-x64.zip”.

2. The downloaded ZIP archive contains one file: „HDSentinel” – extract it. This is a program that you will need to upload to your NAS server (we will do this in section III.6).

3. Log in to the PR4100 GUI as an administrator:



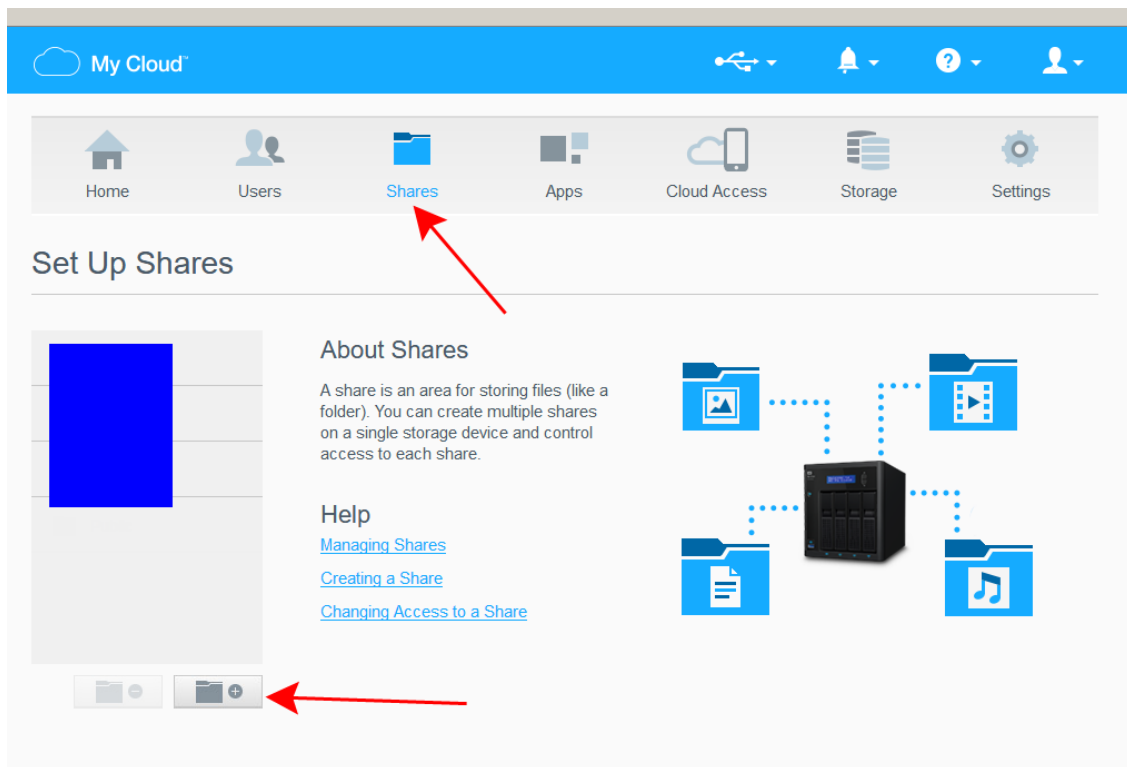
WD My Cloud™ PR4100

Administrator username

Password

Login

4. Go to „Shares” and create a new share called „HDS”:



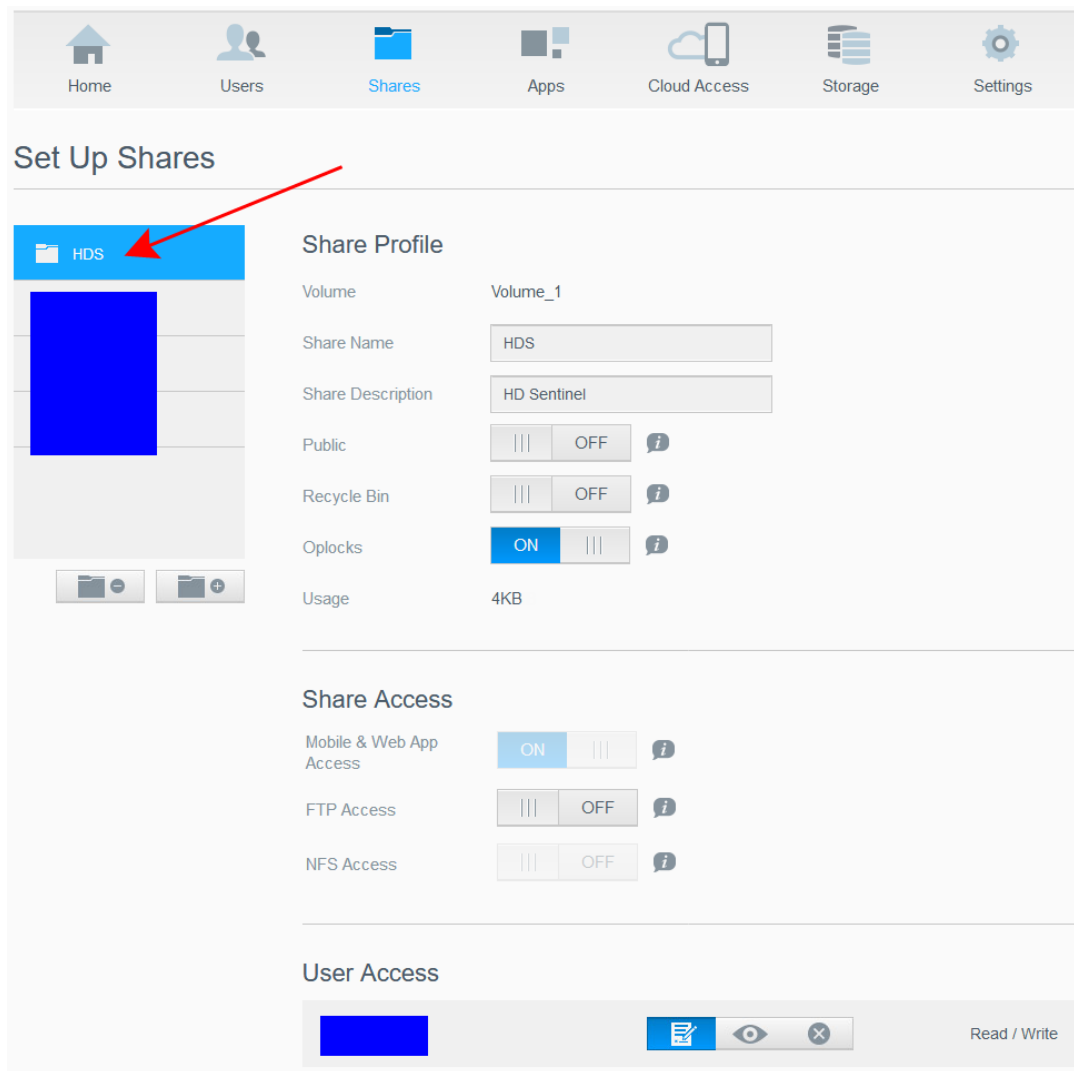
Add Share

Volume	Volume_1
Share Name	HDS
Share Description	

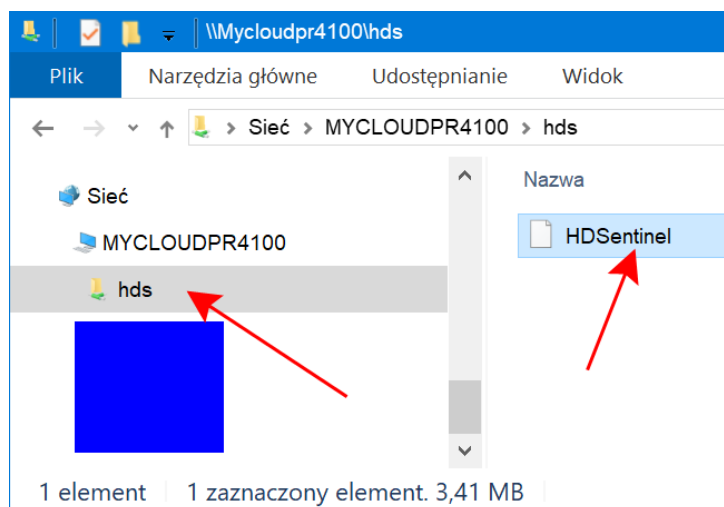
Cancel Apply

5. Configure the „HDS” share.

Note: you can configure this share as „Public”, but I prefer to create private shares and regulate access to them with permissions.



6. Copy the „HDSentinel” file (see section III.2) to the NAS server, to the „HDS” share.



IV. Configure CRONTAB

Note: in this guide, I limit myself to describing „what to do”. For more details and additional explanations, see [3] - I encourage you to read it.

1. In the NAS server GUI, go to „Settings” → „Network” and enable SSH:

The screenshot shows the NAS server GUI. At the top, there is a navigation bar with icons for Home, Users, Shares, Apps, Cloud Access, Storage, and Settings. The Settings icon is highlighted with a red arrow. Below the navigation bar, the 'Settings' page is displayed. On the left, there is a sidebar menu with options: General, Network (highlighted with a red arrow), Utilities, Notifications, and Firmware Update. The main content area is divided into two sections: 'Network Profile' and 'Network Services'. The 'Network Profile' section shows 'Internet access' status, Mac Address, IPv4 IP Address (192...), IPv4 DNS Server, IPv6 IP Address (-), and IPv6 DNS Server (-). The 'Network Services' section includes: IPv4 Network Mode (Static/DHCP), IPv6 Network Mode (Auto/DHCP/Static/Off), Link Aggregation (Active Backup), Link Speed (Auto), Jumbo Frame (OFF(1500)), FTP Access (ON), NFS Service (OFF), SNMP (All/v2c/v3/Off), and SSH (ON). The SSH toggle is highlighted with a red arrow.

2. Read and accept the warnings and information:

The screenshot shows a dialog box titled 'SSH'. It contains the following text:

Please note that modifying or attempting to modify this system outside the normal operation of the product voids your WD warranty.

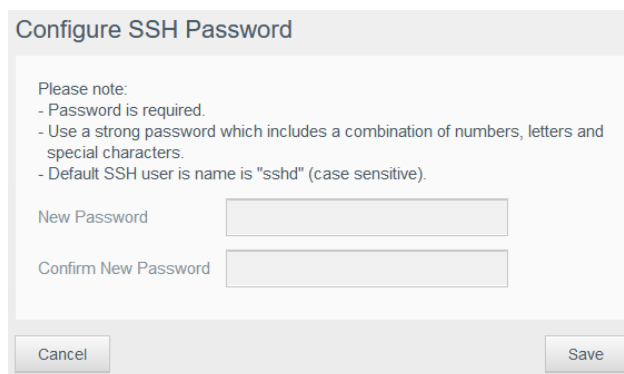
When enabling SSH:

- Password is required.
- Use a strong password which includes a combination of numbers, letters and special characters.
- Default SSH user is name is "sshd" (case sensitive).
- Turn OFF SSH access when not in use.
- Enabling SSH of a device in a DMZ is not recommended.

I accept

Buttons: Cancel, OK

3. Set an SSH password:



The dialog box is titled "Configure SSH Password". It contains a "Please note:" section with three bullet points: "- Password is required.", "- Use a strong password which includes a combination of numbers, letters and special characters.", and "- Default SSH user is name is 'sshd' (case sensitive)". Below the notes are two input fields: "New Password" and "Confirm New Password". At the bottom, there are "Cancel" and "Save" buttons.

4. Start PuTTY and log in to the NAS server using the password from section IV.3:

```
192.168.1.100 - PuTTY
login as: sshd
sshd@192.168.1.100's password:

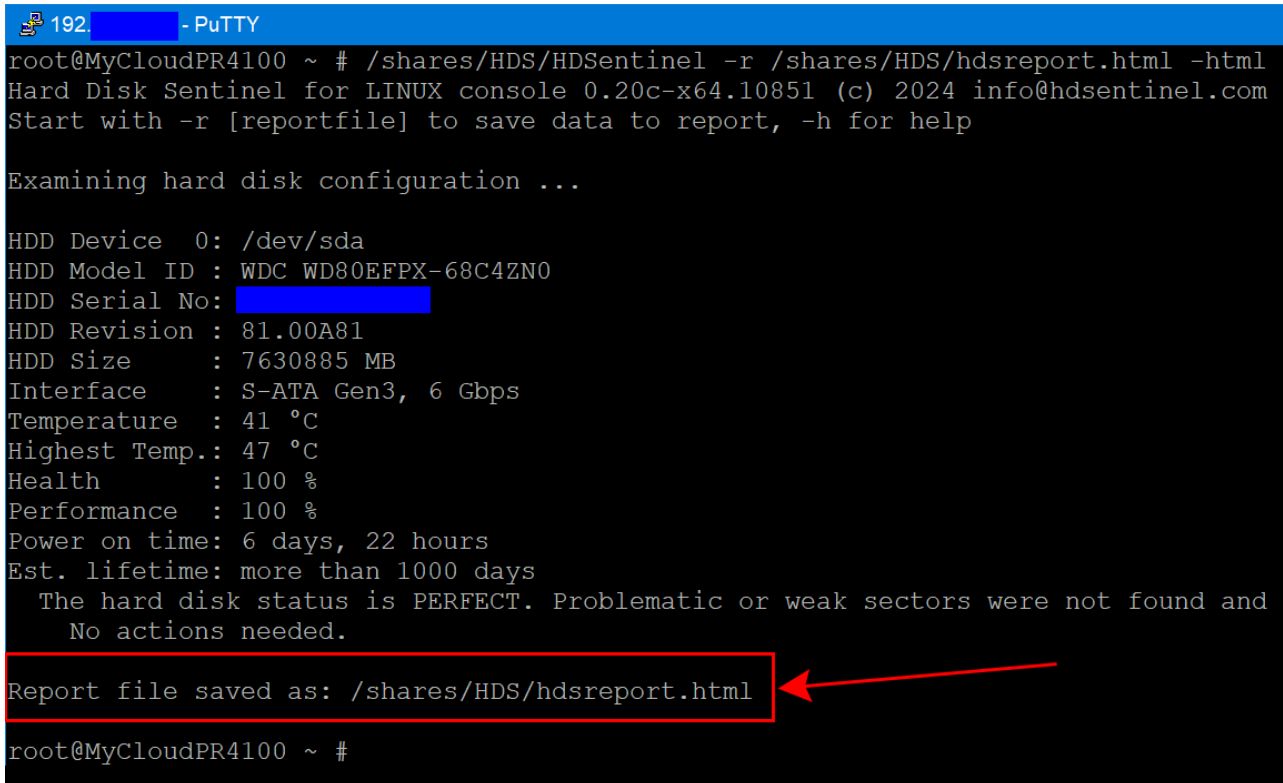
BusyBox v1.30.1 (2023-01-16 13:49:52 UTC) built-in shell (ash)
Enter 'help' for a list of built-in commands.

root@MyCloudPR4100 ~ #
```

5. Check whether the „HDSentinel” program copied to the server in section III.6 is working.
To do this, execute the command:

```
/shares/HDS/HDSentinel -r /shares/HDS/hdsreport.html -html
```

This command should launch the „HDSentinel” program, which should generate a report on the status of the disks and save it in HTML format in the „HDS” share.



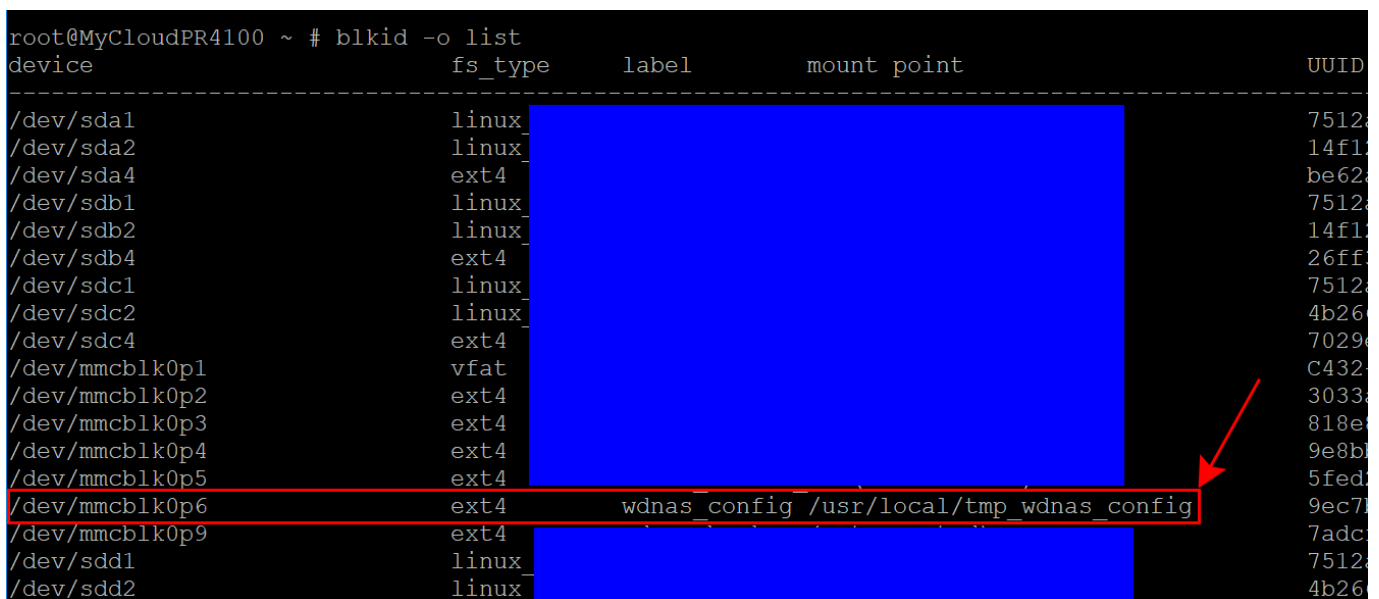
```
192. [redacted] - PuTTY
root@MyCloudPR4100 ~ # /shares/HDS/HDSentinel -r /shares/HDS/hdsreport.html -html
Hard Disk Sentinel for LINUX console 0.20c-x64.10851 (c) 2024 info@hdsentinel.com
Start with -r [reportfile] to save data to report, -h for help

Examining hard disk configuration ...

HDD Device 0: /dev/sda
HDD Model ID : WDC WD80EFPX-68C4ZNO
HDD Serial No: [redacted]
HDD Revision : 81.00A81
HDD Size : 7630885 MB
Interface : S-ATA Gen3, 6 Gbps
Temperature : 41 °C
Highest Temp.: 47 °C
Health : 100 %
Performance : 100 %
Power on time: 6 days, 22 hours
Est. lifetime: more than 1000 days
The hard disk status is PERFECT. Problematic or weak sectors were not found and
No actions needed.

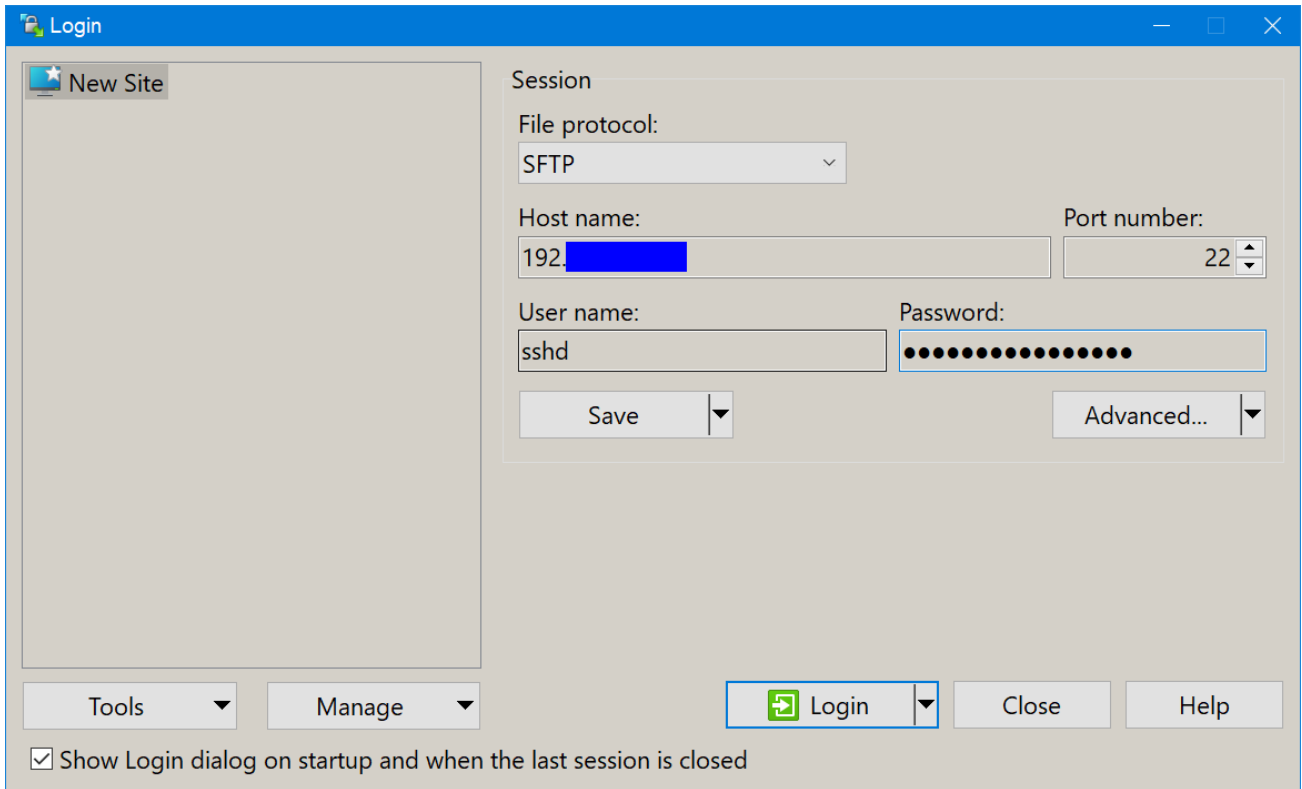
Report file saved as: /shares/HDS/hdsreport.html
root@MyCloudPR4100 ~ #
```

6. Execute the command: `blkid -o list`
Find the partition „mmcblk0p6” („wdnas_config”) in the list displayed. Remember its mount point.

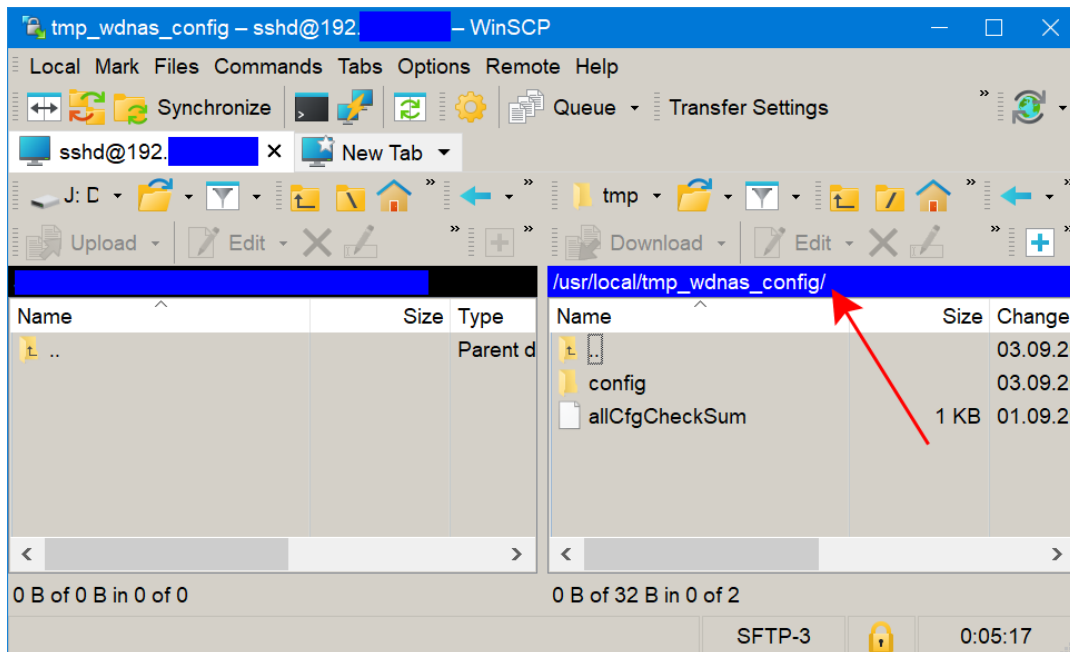


```
root@MyCloudPR4100 ~ # blkid -o list
device          fs_type  label          mount point          UUID
-----
/dev/sda1       linux   [redacted]          [redacted]          7512
/dev/sda2       linux   [redacted]          [redacted]          14f1
/dev/sda4       ext4    [redacted]          [redacted]          be62
/dev/sdb1       linux   [redacted]          [redacted]          7512
/dev/sdb2       linux   [redacted]          [redacted]          14f1
/dev/sdb4       ext4    [redacted]          [redacted]          26ff
/dev/sdc1       linux   [redacted]          [redacted]          7512
/dev/sdc2       linux   [redacted]          [redacted]          4b26
/dev/sdc4       ext4    [redacted]          [redacted]          7029
/dev/mmcblk0p1  vfat    [redacted]          [redacted]          C432
/dev/mmcblk0p2  ext4    [redacted]          [redacted]          3033
/dev/mmcblk0p3  ext4    [redacted]          [redacted]          818e
/dev/mmcblk0p4  ext4    [redacted]          [redacted]          9e8b
/dev/mmcblk0p5  ext4    [redacted]          [redacted]          5fed
/dev/mmcblk0p6  ext4    wdnas_config  /usr/local/tmp_wdnas_config  9ec7
/dev/mmcblk0p9  ext4    [redacted]          [redacted]          7adc
/dev/sdd1       linux   [redacted]          [redacted]          7512
/dev/sdd2       linux   [redacted]          [redacted]          4b26
```

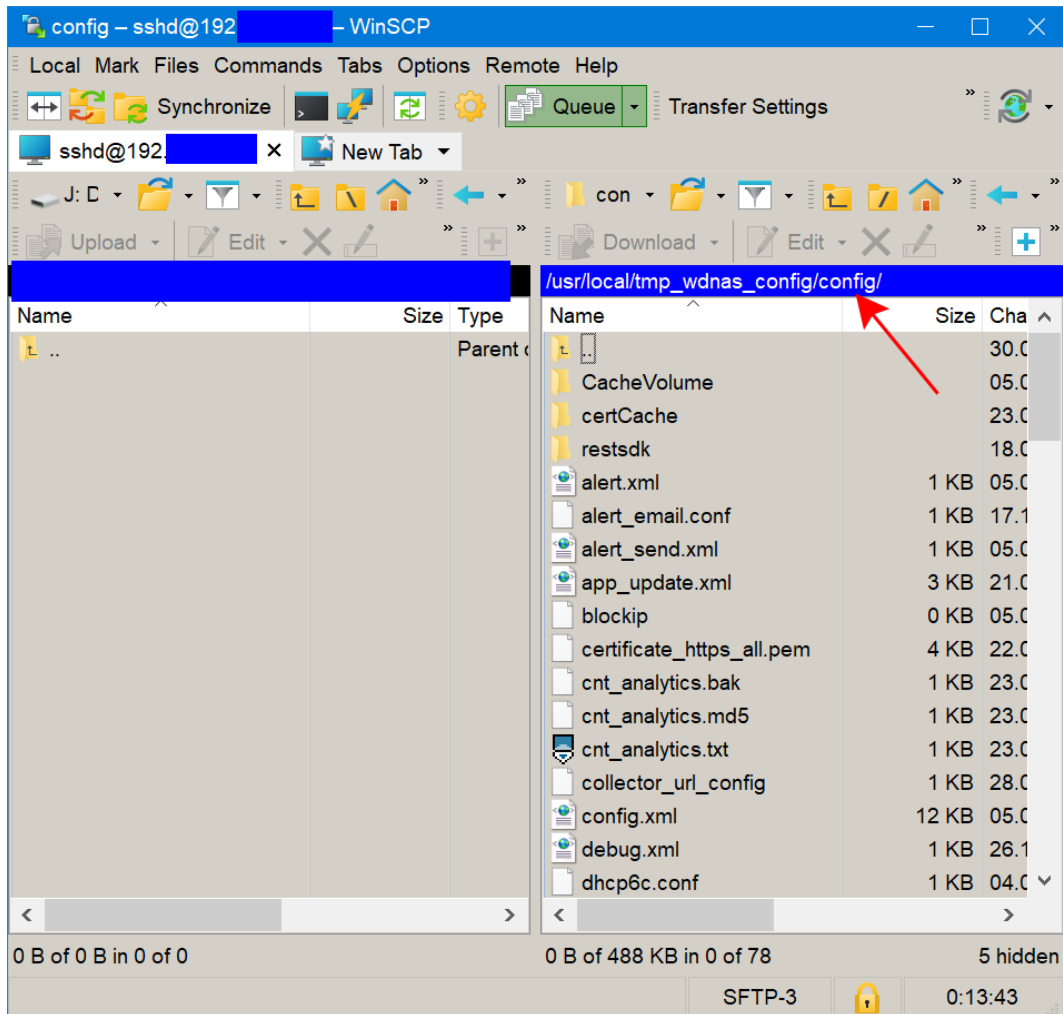
7. Start WinSCP and log in to the NAS server using the password from section IV.3:



8. In WinSCP, in the NAS server window, navigate to the directory (folder) read in section IV.6:

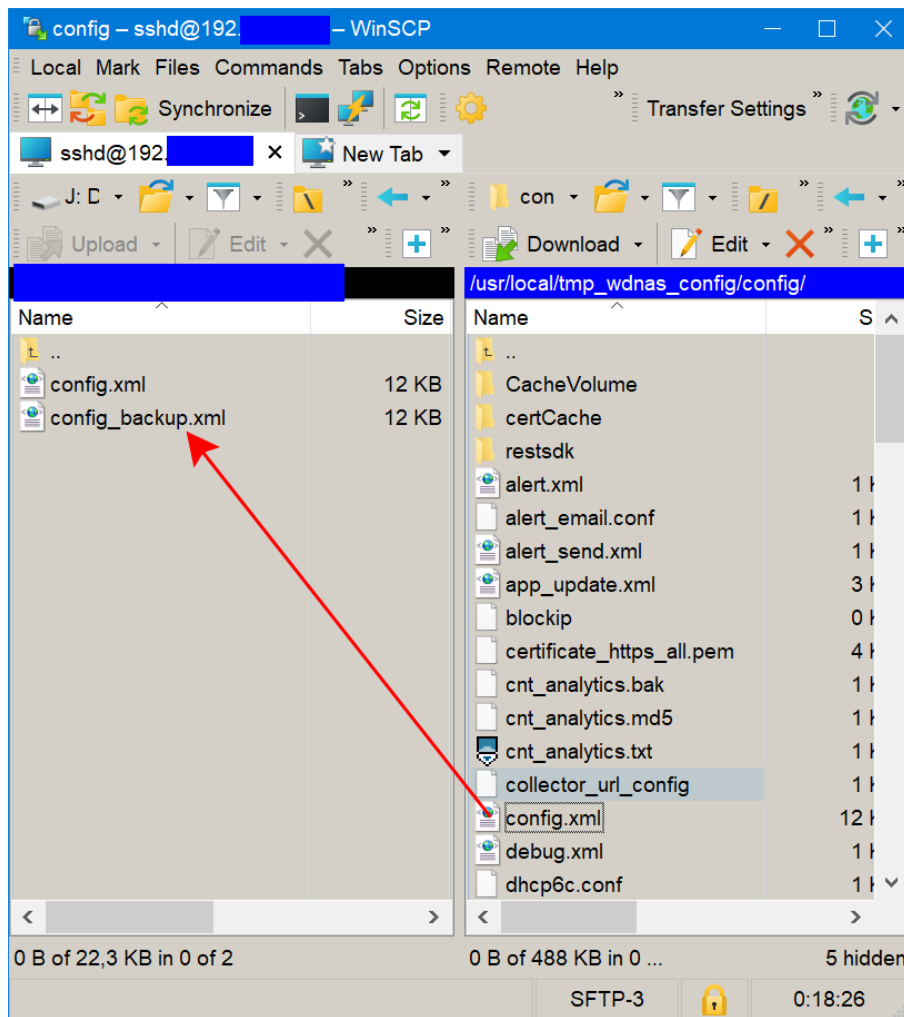


9. Go to the „config” subdirectory (subfolder):



10. Copy the „config.xml” file to your PC and create a backup copy.

You will make changes in the „config.xml” file, and you will need a backup copy of it in case you need to restore the original version of the file.



11. Open the „config.xml” file in a TXT editor (I used PSPad).

12. In the „config.xml” file, find the section „<crond>...</crond>”.

13. At the beginning of the section „<crond>...</crond>”, find the subsection „<list>...</list>”.

Add the name of the next cron job to this subsection: „hdsentinel”.

Please note that the value of „count” should match the number of entries in the „<list>...</list>” subsection.

```
<crond>
  <list>
    <count>10</count>
    <name id="1">stime</name>
    <name id="2">wd_crontab</name>
    <name id="3">app_get_info</name>
    <name id="4">recycle_bin_clear</name>
    <name id="5">chk_wfs_download</name>
    <name id="6">random_check</name>
    <name id="7">fw_available</name>
    <name id="8">user_expire_chk</name>
    <name id="9">pull wdlog config</name>
    <name id="10">hdsentinel</name>
  </list>
```

14. At the end of the section „<crond>...</crond>”, add the cron job „hdsentinel”.

Important: the name of the cron job used here must be identical to the name defined in the „<list>...</list>” subsection (see IV.13).

```
<hdsentinel>
  <item id="1">
    <method>3</method>
    <1>*/10</1>
    <2>*</2>
    <3>*</3>
    <4>*</4>
    <5>*</5>
    <run>/shares/HDS/HDSentinel -r /shares/HDS/hdsreport.html -html &&&</run>
  </item>
</hdsentinel>
</crond>
```

The above entry will cause the „HDSentinel” program located in the „HDS” share to run every 10 minutes. The program will create a report of its work and save it in the „hdsreport.html” file in the same folder. The & (ampersand) character forces the cron job to run in the background.

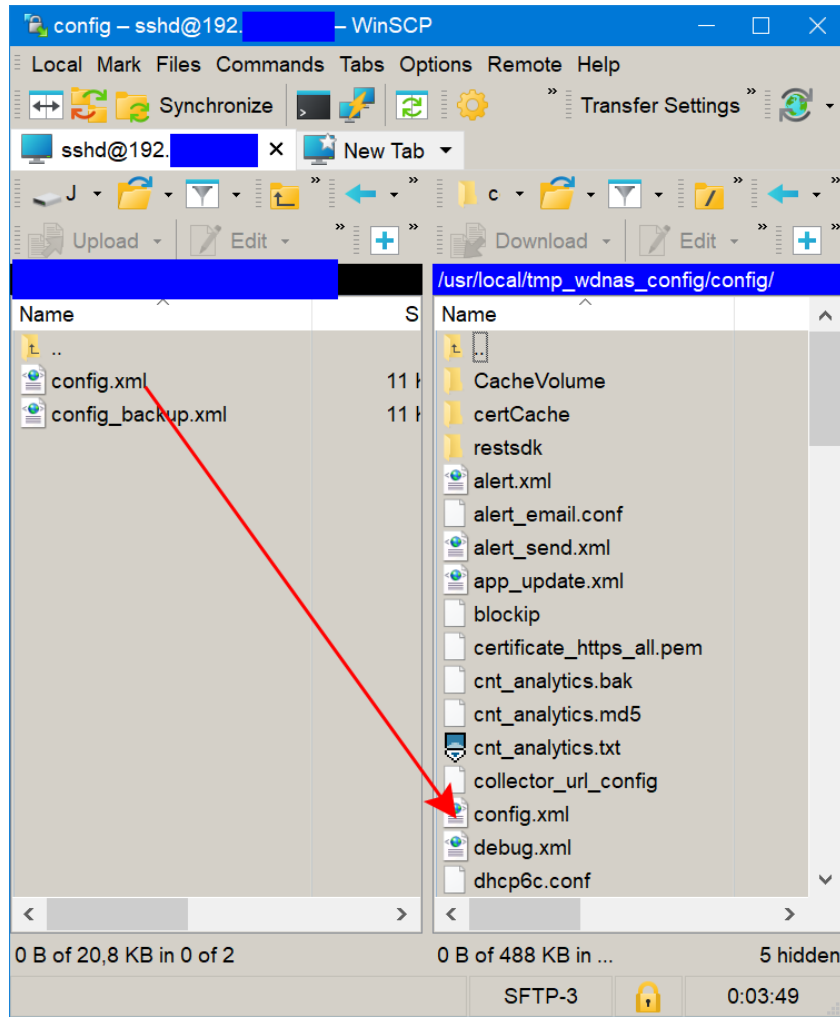
You can read more about this in [3].

After making the above changes to the „config.xml” file, it is ready to be uploaded to the NAS server.

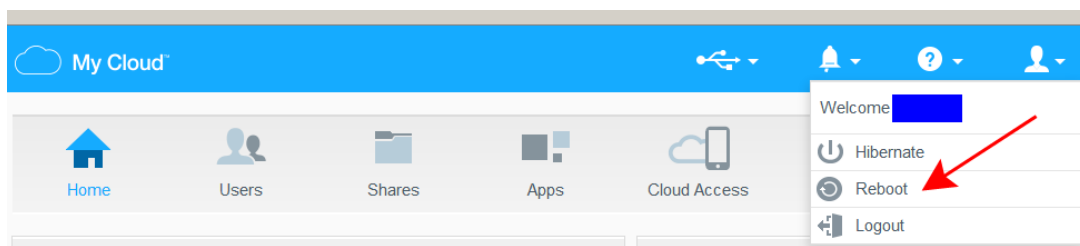
Double-check that you have not made any mistakes!

If you upload a file containing errors to the server, you may permanently damage the server!

15. In WinSCP, copy the modified „config.xml” file to the server folder from section IV.9 (this file will replace the original file).



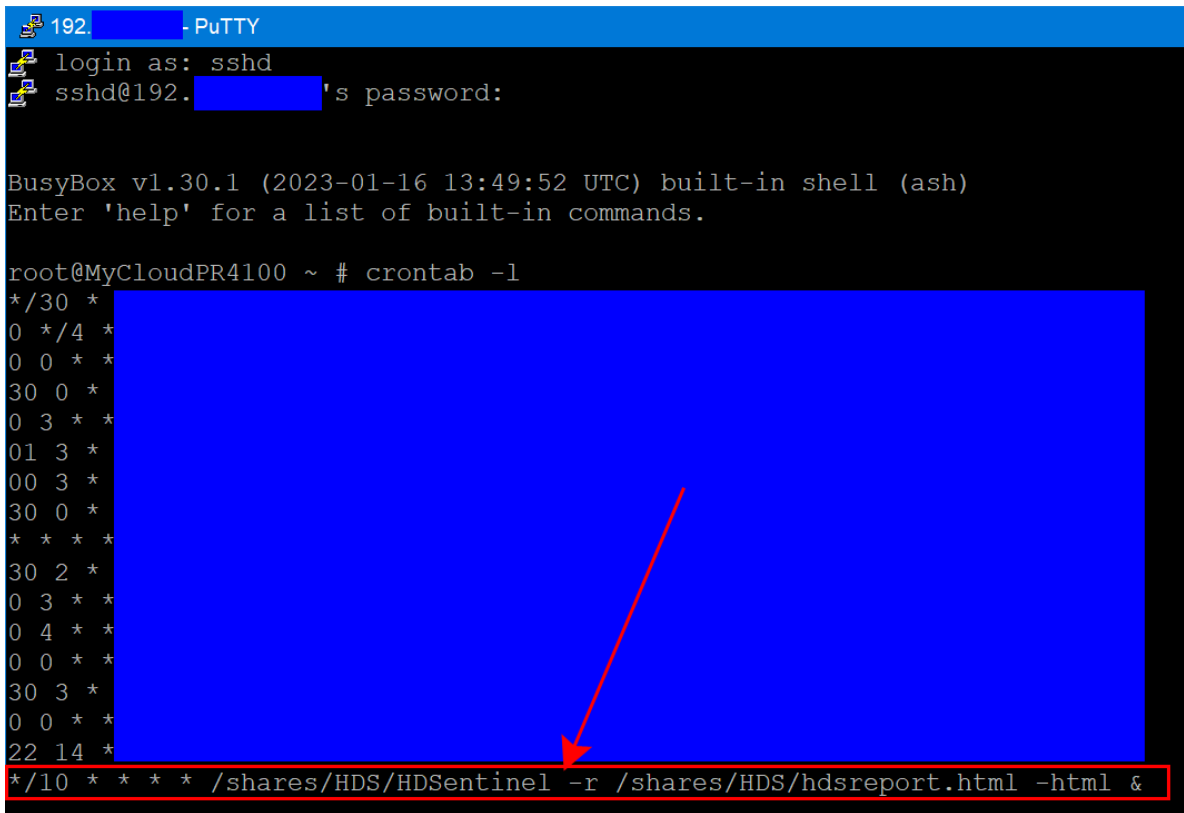
16. Restart the server:



17. Start PuTTY and log in to the NAS server as described in section IV.4.

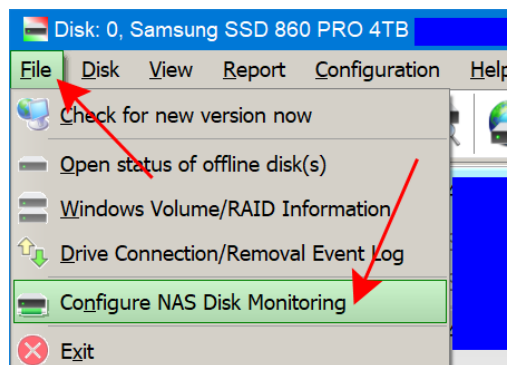
18. Execute the command: `crontab -l`

If there were no errors in the „config.xml” file, the list of tasks displayed should include an entry related to the „HDSentinel” program:

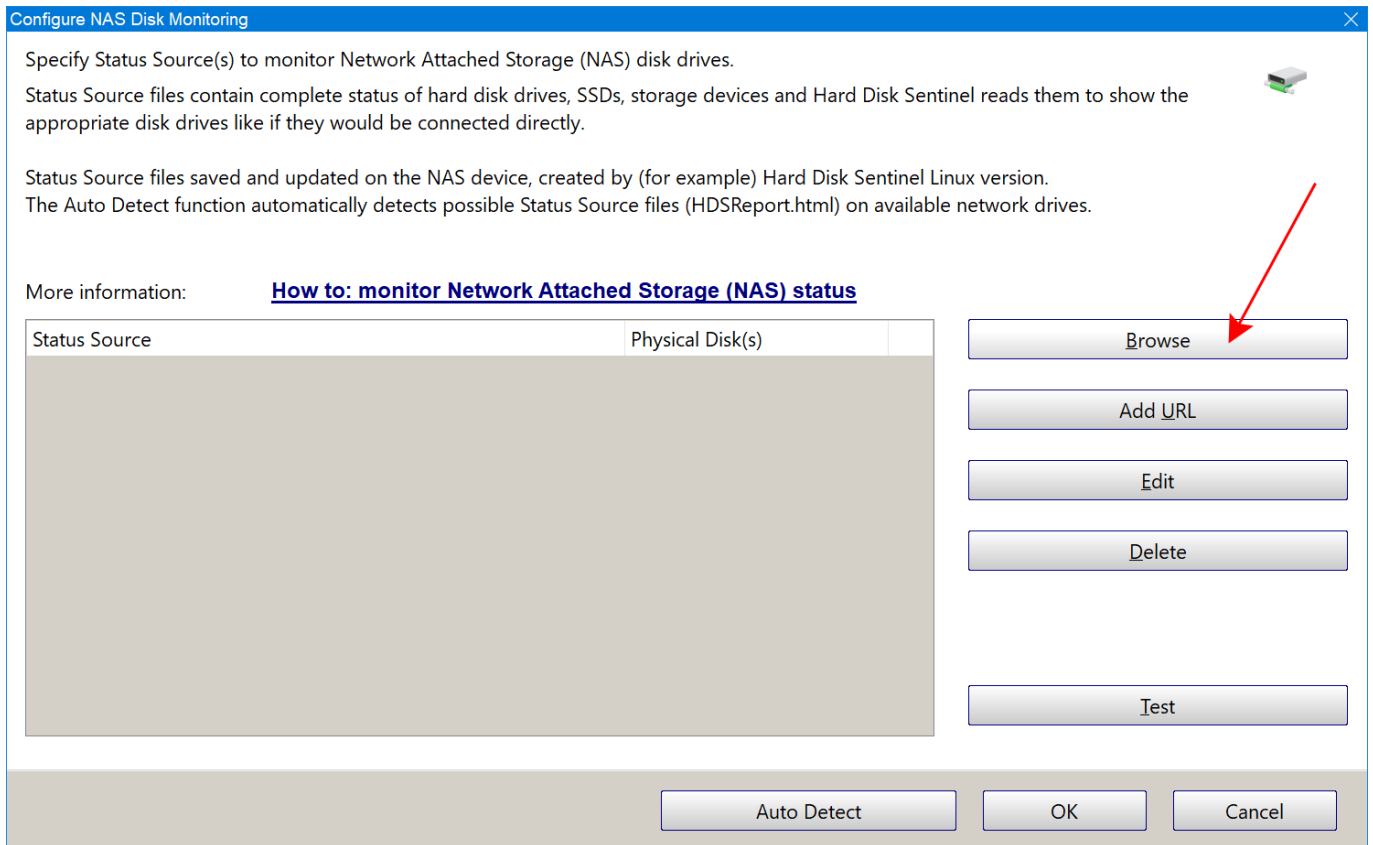


V. Configure the „HDSentinel” program on your PC

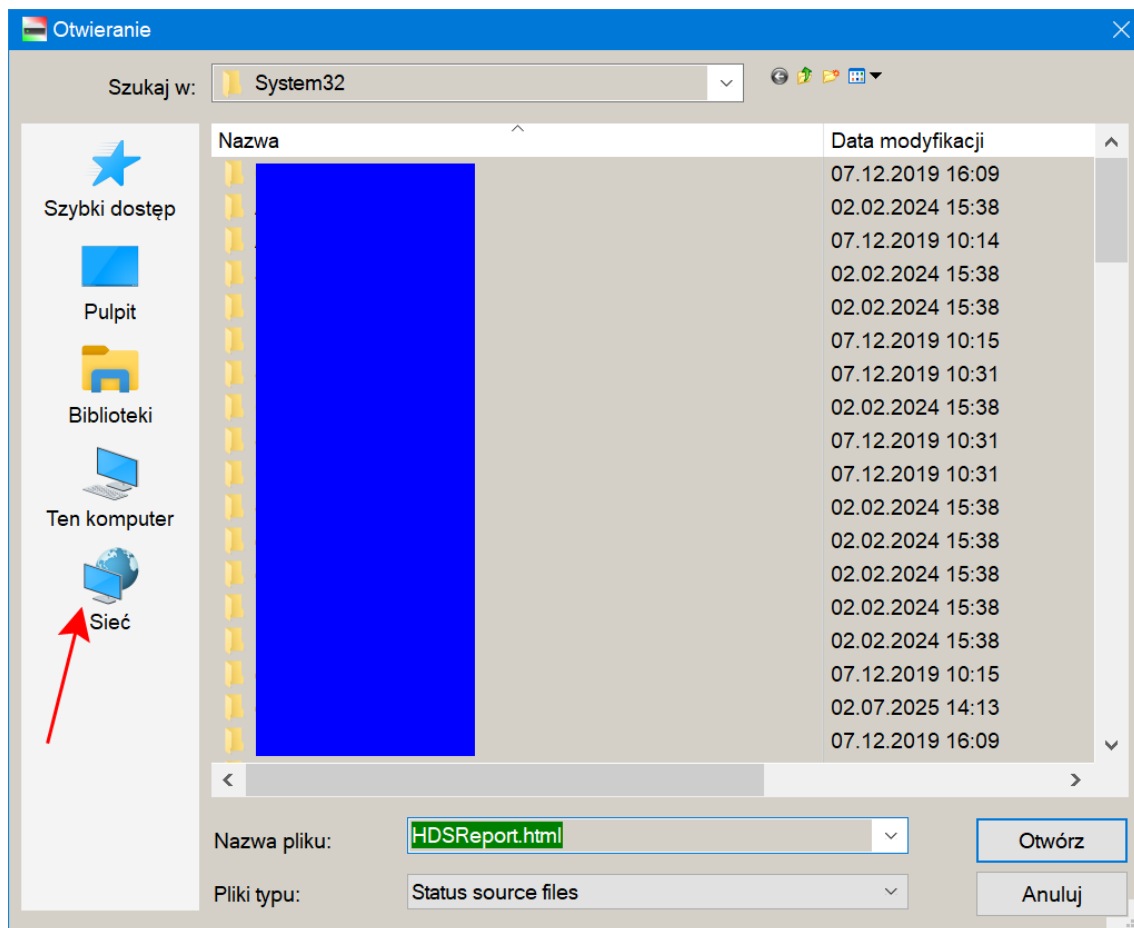
1. Launch the „Hard Disk Sentinel” program on your PC, go to the „File” menu, and select „Configure NAS Disk Monitoring”:



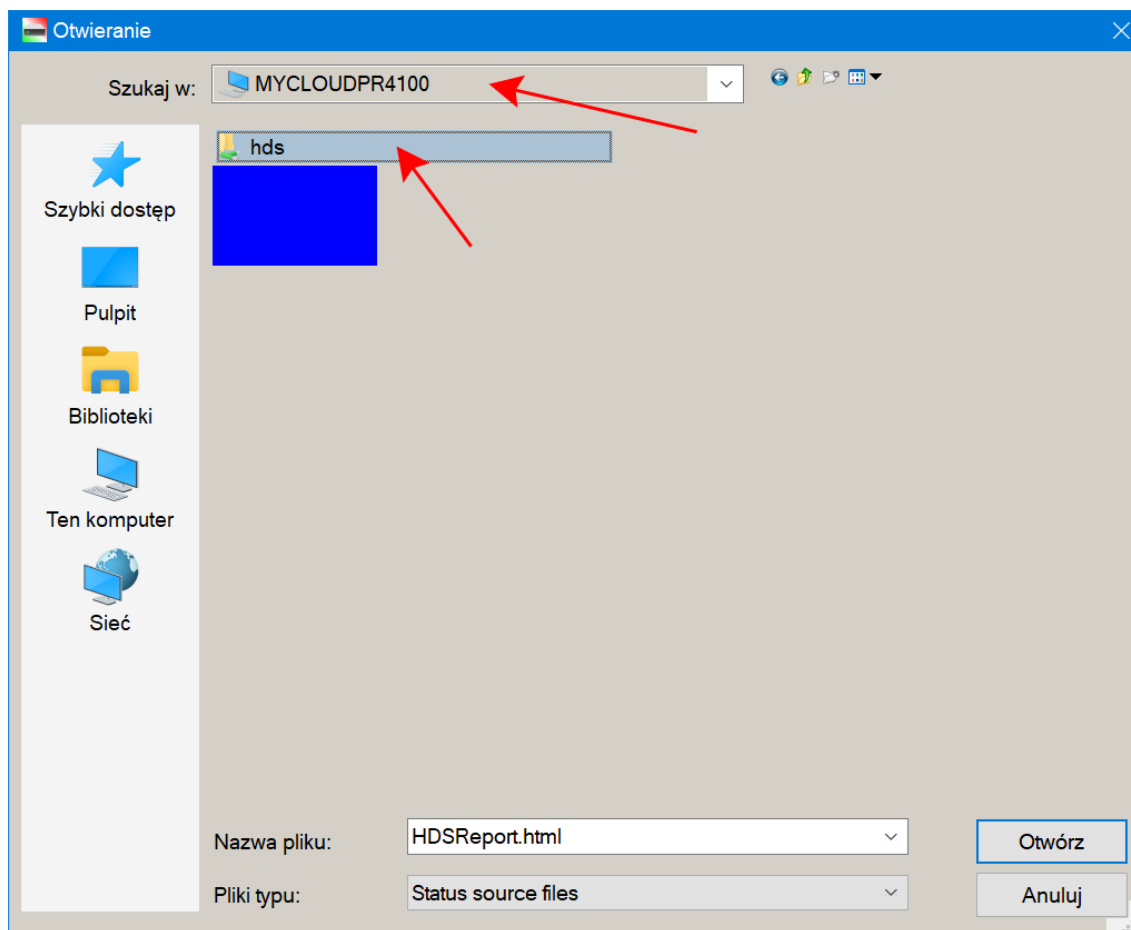
2. Select the „Browse” option:



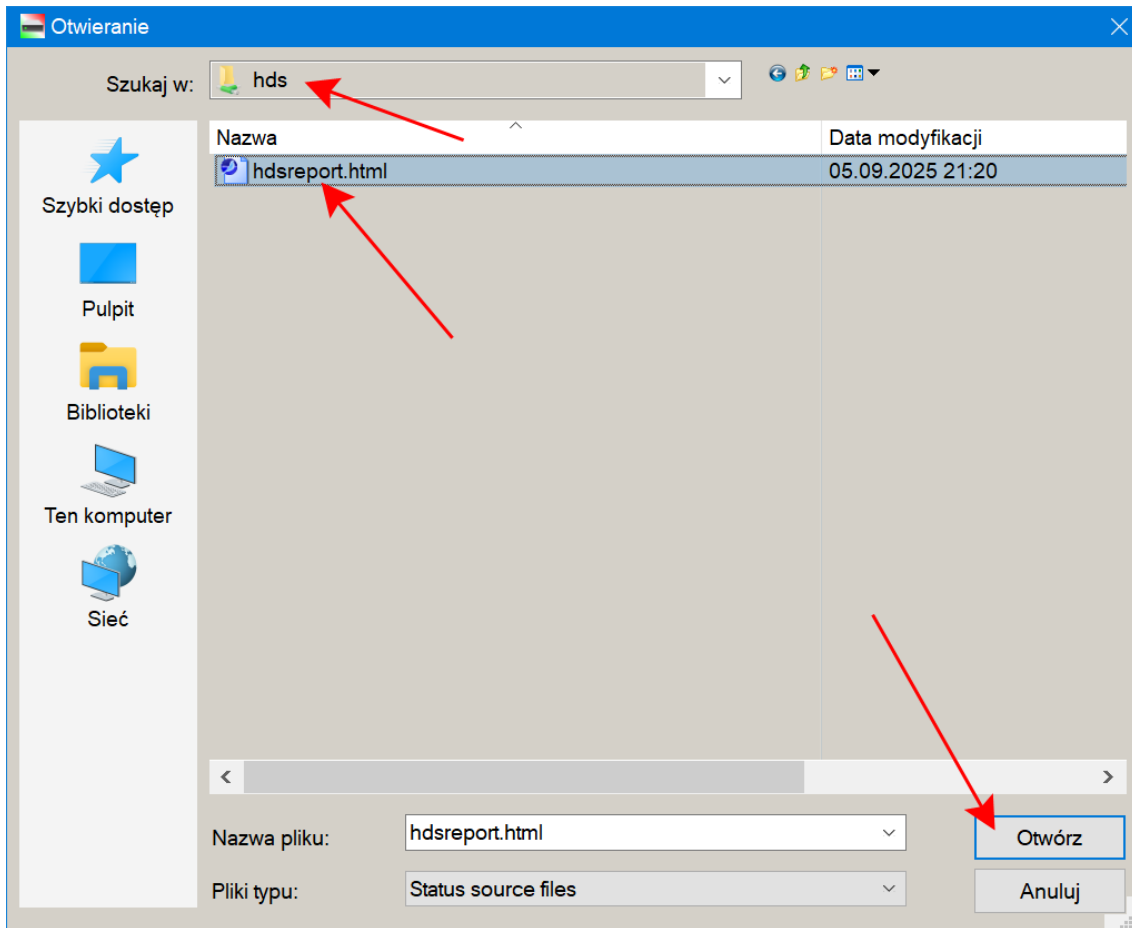
3. Select the „Network” option:



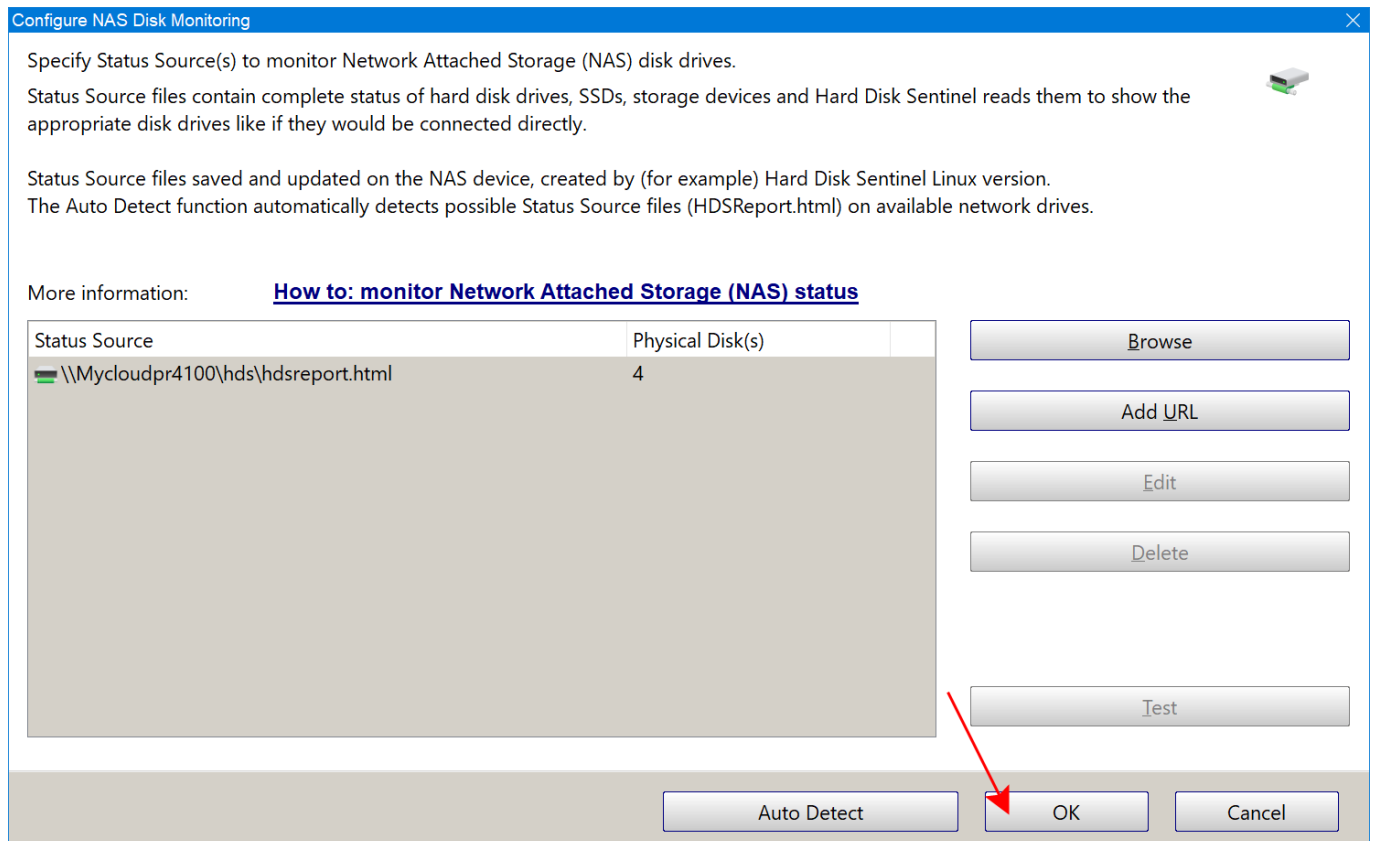
4. Select the NAS server, then select the „HDS” share:



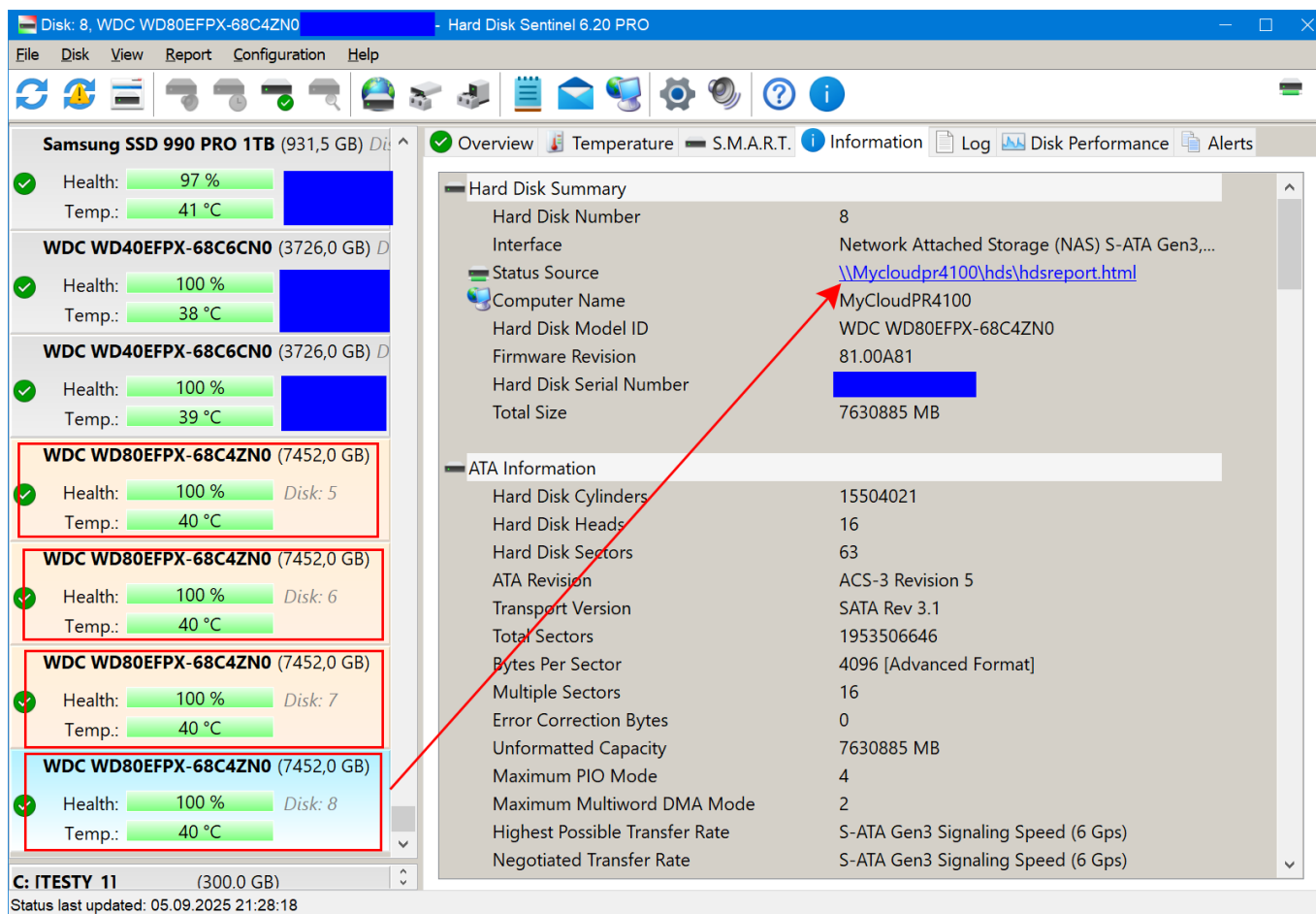
5. Select the „hdsreport .html” file and click „Open”:



6. In the configuration window, click „OK”:



7. The NAS server drives should appear in the main program window:



That's all. You can now disable SSH on the NAS server (see section IV.1).

VI. Bibliography

- [1] Website „How to: monitor Network Attached Storage (NAS) status”
https://www.hdsentinel.com/how_to_monitor_network_attached_storage_nas_status.php
- [2] Guide „Monitor hard disk status of WD MyCloud 1st Gen (FW 04.xx.xx)”
https://www.hdsentinel.com/nas/monitor_hard_disk_status_of_wd_mycloud_gen1.pdf
- [3] Website „How to Make Persistent System Changes (crontab, etc)”
<https://community.wd.com/t/how-to-make-persistent-system-changes-crontab-etc/201268>