Open-E DATA STORAGE SERVER

Manual (Ver. 5.00 up49) November 19, 2008

Copyright

Trademarks

Disclaimer

1 Before you get started

Congratulations on purchasing Open-E Data Storage Server, the ideal solution for network-based storage management. This manual will assist you as you install and configure the hardware.

In order to reach the desired configuration as quickly as possible, please read the following pages thoroughly. The time invested is well spent - after all, you have purchased this solution for your invaluable data.

1.1 Contents of this package

Before you begin installing Open-E Data Storage Server, make sure that the package contains the following items:

- Open-E Data Storage Server flash module,
- Quick Start brochure,
- A CD containing the manual (this document), brochures, images and additional information material,
- Source CD.

If something is missing, please contact your dealer.

1.2 System requirements

- x86-compatible PC
- CPU (2 GHz Pentium IV),
- at least 512 MB main memory,
- USB port,
- One or several suitable hard drives (SATA,SAS, SCSI, ATA),
- Optionally a hardware Raid controller, Fibre Channel and iSCSI Storage.
- Network Interface Card (NIC),

Open-E Data Storage Server contains its own operating system no additional software is required.

note In order to achieve maximum performance, we recommend using a network card with 1 Gb or more (multicards 1Gb/s recommended for bonding), as well as a processor with at least 3 GHz. If several computers are accessing the DSS system, we recommend 1024 MB main memory or more.

1.3 Supported clients

- Microsoft Windows (all versions)
- Linux
- Unix
- Mac OS 8.0, 9.0 and OS X

1.4 Supported network protocols

- TCP/IP
- SNMP

1.5 Supported network file protocols

- SMB / CIFS / Samba
- Apple Talk
- FTP/sFTP

1.6 Required tools

- Grounding strap or mat in order to avoid electrostatic discharge (ESD),
- Tools for opening the computer's chassis (typically, a screwdriver).

1.7 Safety precautions

1.7.1 Personal safety

caution High voltages may occur inside computer equipment. Before removing the chassis, please turn off the power switch and disconnect the power cords.

1.7.2 Safety for your data

If you are not using new hard drives for operating Open-E Data Storage Server, please backup all important data prior to installation. Adding a hard drive to Open-E Data Storage Server goes hand in hand with a complete format of the hard drive, which can possibly delete existing data.

1.7.3 ESD precautions

In order to avoid damage to your computer or to Open-E Data Storage Server, please ensure you are grounded before opening the PC or the ESD package that contains Open-E Data Storage Server. Using grounding straps or mats is the best way to ensure this safety. If you do not have grounding equipment handy, please make sure you are grounded e.g. by touching heater before working with Open-E Data Storage Server, for instance, by touching a heater.

- Avoid touching the components inside the PC unless necessary,
- Please hold Open-E Data Storage Server only on the edges.

2 Features

Open-E Data Storage Server is an all-in-one IP-Storage OS offering NAS and iSCSI (target and initiator) functionality in a single application with excellent enhanced management and superior reliability for organizations of all sizes.

2.1 What is Open-E Data Storage Server

NAS (**Network Attached Storage**) solutions are defined as storage systems that are directly hooked up to a network infrastructure. Also, they operate independently and do not have to be connected to a server via a controller or host adapter. The term “storage” here generally refers to all systems that either provide data storage or actually store or organize data. Currently, data storage is the most common and most widespread type of NAS systems.

NAS solutions are based on a separate operating system (and often also on special hardware), which operates independently from the servers on a network. Typically, this operating system is software that is optimized for providing data (file server).

NAS solutions allow users to add additional storage to existing networks quickly, easily, and cost-efficiently.

iSCSI (**internet SCSI**) is a protocol that encapsulates SCSI (Small Computer System Interface) commands and data in TCP/IP packets for linking storage devices with servers over common IP infrastructures. By using iSCSI, you can supply high performance SANs (Storage Area Networks) using standard IP networks like LAN, MAN, WAN or the Internet.

iSCSI solutions are based on a separate operating system and often also on special hardware. Typically, this operating system allows operating iSCSI technology.

iSCSI solutions allow users to add additional disk devices to existing networks quickly, easily, and cost-efficiently.

iSCSI has a client-server architecture. Clients of an iSCSI interface are called "initiators". Initiators issue iSCSI "commands" to request services from components, logical units, of a server known as a "target" The "device server" on the logical unit accepts iSCSI commands and processes them.

Open-E Data Storage Server provides a fast, reliable, and scalable platform for IP-Storage and combines the power of NAS & iSCSI in a single operating system. No matter if you need file sharing, storage consolidation, backup and recovery, virtualization or replication, Open-E Data Storage Server offers excellent price-to-performance ratio, enhanced manageability, and increased productivity.
The flexible design of Open-E Data Storage Server enables organizations of all sizes to create effective NAS and/or IP-SAN/iSCSI solutions that can adapt to and meet the simplest or most complex storage needs.

Open-E Data Storage Server is built on the proven Open-E NAS-XSR and Open-E iSCSI family with all of its superior security, stability and management advantages, and is Open-E's fourth generation of IP-storage software.
Open-E Data Storage Server adds new back-up capabilities, simplified setup and storage management, extensibility, and is specially tuned to provide optimal data-throughput and data protection for centralized storage. Open-E DSS increases iSCSI target efficiency by supporting multiple iSCSI initiators on different volumes, without sacrificing NAS performance.

2.2 DSS functionality

Open-E NAS Data Storage Server is one of the easiest ways of implementing an NAS server and/or iSCSI technology in your network. Through its simple architecture – in principle, it is a flash memory with a USB 2.0/1.1 port and Open-E Data Storage Server as its operating system – Open-E Data Storage Server can be used with all x86 PCs containing USB ports, an IDE controller and an additional SATA Controller on their mainboard or hardware controller.

To begin working with Open-E Data Storage Server, all you need to do is assign an IP address to the NAS server and/or iSCSI target – either automatically through an existing DHCP server or by assigning it manually. All other settings are handled via a web front-end which can be easily accessed through the IP address of Open-E Data Storage Server using the encrypted https protocol.

Open-E Data Storage Server allows users to create so-called shares (i.e., resources within a network that numerous users or user groups have certain access to). The access rights to the shares are controlled through the user and user group settings.

Open-E Data Storage Server allows users of client stations to delegate disk devices and aggregation and form iSCSI Targets and their local mounting from any site in the network.

2.3 Why Open-E Data Storage Server?

Often, storage in network environments is expanded the following way: file servers have to be shut down in order to install additional drives. Next they need to be reconfigured. This tedious task often includes copying data manually onto larger drives, consuming a lot of time and money.

With Open-E Data Storage Server, you can

- add storage to your existing network quickly, easily, and most important, cost-efficiently.
- consolidated storage and backups for multiple servers.
- improve data availability and efficiency.
- lower costs by centralizing storage management.
- simplify the installation and on-going management of a SAN by using iSCSI versus using Fibre Channel.

Expensive hardware is, therefore, no longer necessary. Take any computer – a new rack server or an old desktop PC with USB ports 2.0/1.1– and exchange the system drive for the Open-E Data Storage Server USB flash module. To store data, Open-E Data Storage Server uses IDE (ATA) and SATA hard drives, connected to ports on your mainboard or hardware RAID controller.
Additionally Data Storage Server supports software RAID, so you can create software RAID over single hard drives or over existing hardware RAIDs.
For example, you can create a software mirror over two hardware RAID5s for very high reliability.

Within a few minutes, you will have up to several hundred gigabytes available on your network – without much effort and any downtime.

2.4 RAID types

This manual is not intended to replace your RAID controller manual. But we want to provide you with an overview of common RAID types so that you can make an informed decision on which type to choose. Depending on whom you ask, RAID means either Redundant Array of Independent Disks or Redundant Array of Inexpensive Disks. Both are correct. In essence, you combine the capacity, speed and security of several disks into one.

RAID 0 forms one large hard disk by concatenating stripes from each member drive. Stripe size is configurable roughly between 64 KB and 1 MB. The result is a lightning-fast RAID, but with no added security. One failing drive may ruin the entire RAID.

RAID 1 mirrors hard drives. By writing identical data onto more than one drive, security is enhanced. A completely defective drive does not cause any loss of data. The drawback is reduced performance and capacity.

RAID 5 combines data striping from RAID 0 with parity checking, therefore combining speed and improved security. The loss of one drive is tolerable.

RAID 6 extends RAID 5 by adding an additional parity block, thus it uses block-level striping with two parity blocks distributed across all member disks. It was not one of the original RAID levels. The user capacity of a RAID 6 array is N-2, where N is the total number of drives in the array. RAID 6 does not have a performance penalty on read operations, but it does have a performance penalty on write operations due to the overhead associated with the additional parity calculations.

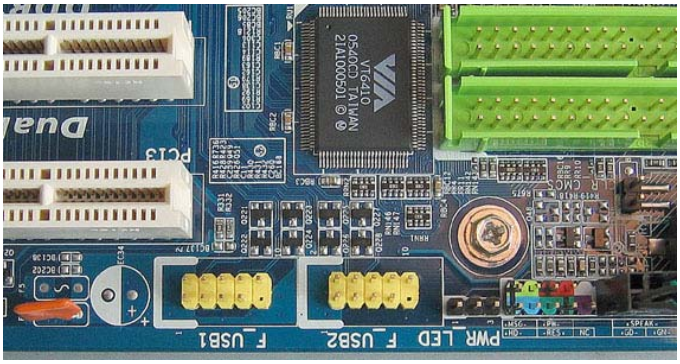
RAID 10 is a combination of RAID 1 and 0, hence the name. Data is written in a striped and mirrored configuration, providing high performance and robust security.

3 Hardware installation

3.1 Getting ready

Switch off the computer, remove the power supply, and open the PC chassis. In tower systems, the side parts often can be removed individually (you just need to remove a few screws on the backside of the chassis . Many machines have U- or O-shaped covers that have to be pulled off (either towards the front or the back). Should you need any assistance, please contact your dealer.

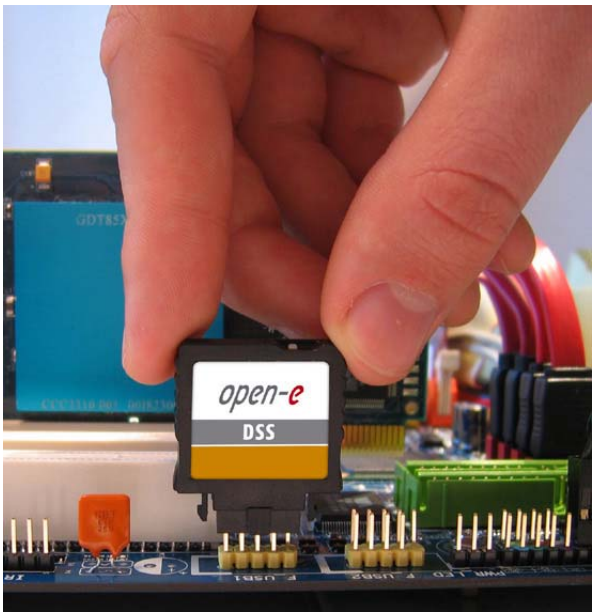
Now locate the USB connectors on your motherboard:



Every motherboard has at least two such ports. To install Open-E Data Storage Server, you have to use an existing one

3.2 Installing Open-E Data Storage Server

If necessary, remove the flat band cable that connects your hard drive with the controller. Open-E Data Storage Server should now be carefully inserted into the USB the connector. As USB ports can have a notch on one side, you can only insert the connector at the preset position (see photo).



That should conclude the installation! Before replacing the chassis do not forget to connect your hard drives to the IDE connector, SATA connector or to the SATA port on the RAID controller. If you have a CD or DVD drive, you can remove it, as Open-E Data Storage Server does not support optical drives, but if you want to make an ISO update it is not necessary to remove the CD drives (see 5.2.3.8).

4 Configuration

4.1 The basic configuration of the Data Storage Server computer

Connect your keyboard and a monitor to the Data Storage Server computer. You will only need those devices for basic configuration or extended maintenance configuration.

note You may have to change the function “Halt On: All Errors” in your PC BIOS, so that the system starts even without the keyboard. The correct configuration is “Halt On: All But Keyboard.”

4.2 First-time operation of Open-E Data Storage Server

Now start your system.

After booting is complete, Open-E Data Storage Server will provide you with information on the current software version and the network settings:

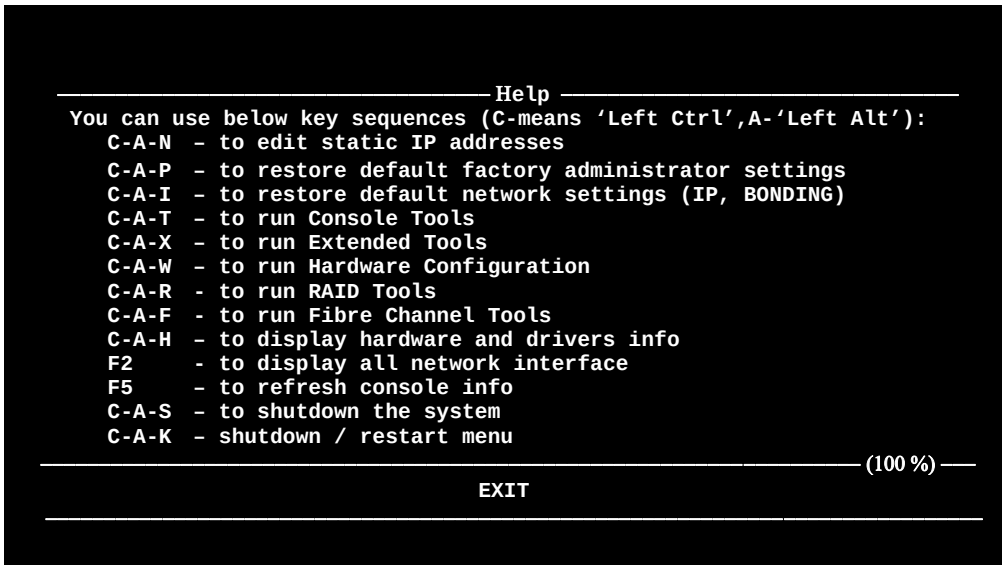
```
Welcome to Open-E Data Storage Server              Press F1 for Help)
-----------------------
Model:                              Open-E Data Storage Server
Version:                            5.00.DB49000000.3278
Release date:                       2008-11-19
S/N:                                00112238
Licensed storage capacity:          16TB

Network settings:
Interface 1:    eth0    IP: 192.168.0.220/255.255.255.0
Interface 2:    eth1    IP: 192.168.1.220/255.255.255.0


TTPS settings:
                port:               443
                allow from:         all

Self test O.K.
```

If your network has a DHCP server, Open-E Data Storage Server should configure the IP settings automatically. If that is the case, you can proceed to 4.3. If your network does not have a DHCP server, Open-E Data Storage Server will start with the default settings: IP address 192.168.0.220 and subnet mask 255.255.255.0.
You can change these values manually by pressing the following key combination: left CTRL, left ALT and N. You can now select a different IP address. Other available console functions will appear after pressing the F1 key (see below).



After a connection has been established, all settings can also be changed remotely via the web browser. If your network requires it, the address of the standard gateway and the broadcast address can be changed.

note For additional information, please read the chapter "Console display functions"

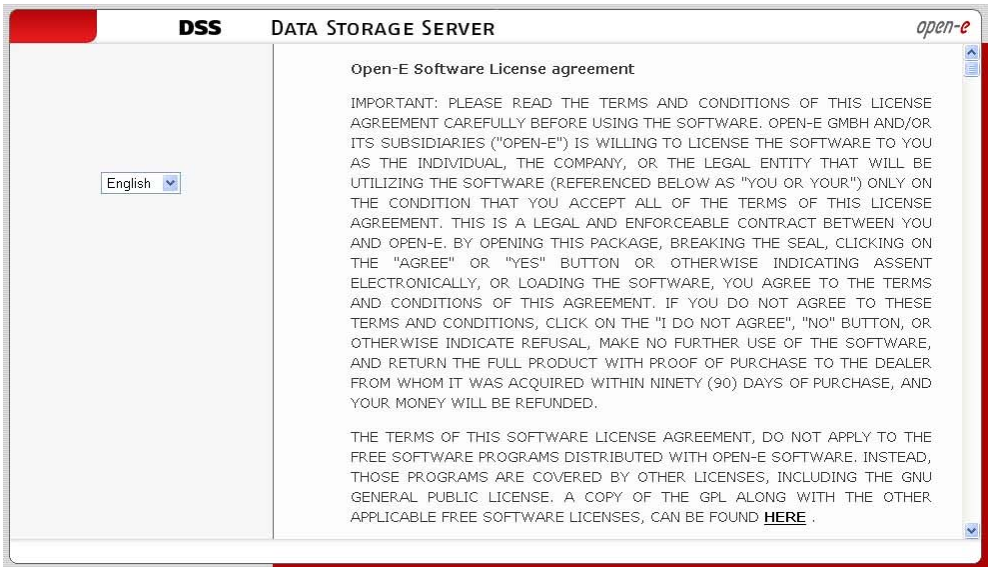
4.3 Logging into Open-E Data Storage Server

You can establish a connection to Open-E Data Storage Server from every network computer. To establish this connection, use a browser (e.g. Microsoft Internet Explorer) and enter the IP address or the name of the computer hosting the Data Storage Server into the URL entry line: https://192.168.0.220 (standard address) or https://dss (this name can be changed in the installation of Open-E Data Storage Server settings).

note For security reasons, Open-E Data Storage Server uses the encrypted SSL protocol (https).

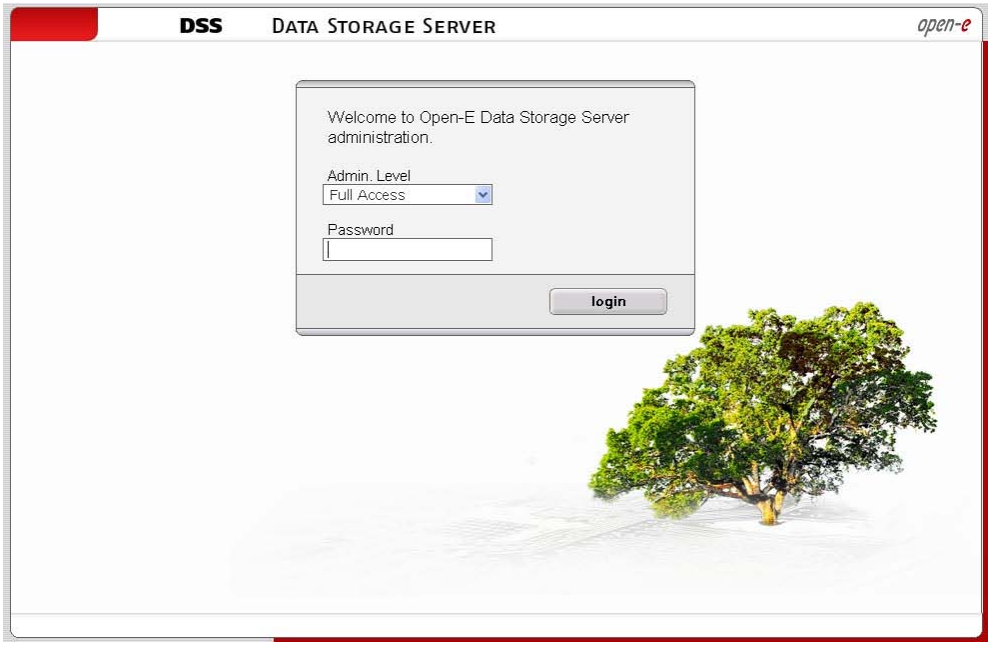
You will now be asked to verify the encryption certification. Since Open-E Data Storage Server only allows to create shares on the Intranet, there is no need for global certification by an authorized body. You can accept the certificate for the session only, but also for all future sessions.

Now you have to accept the license in order to use the Open-E software and you can choose the language you want to use.



note After you first launch Open-E Data Storage Server you will see a page with the software agreement and available language options. Later you can change the language used by modifying language settings, which are located in the Server tree accessible through “Setup”.

After accepting the license agreement you can log into Open-E Data Storage Server using the standard password “*admin*” (this can be changed later). In order to start working, you can now set all the necessary parameters.



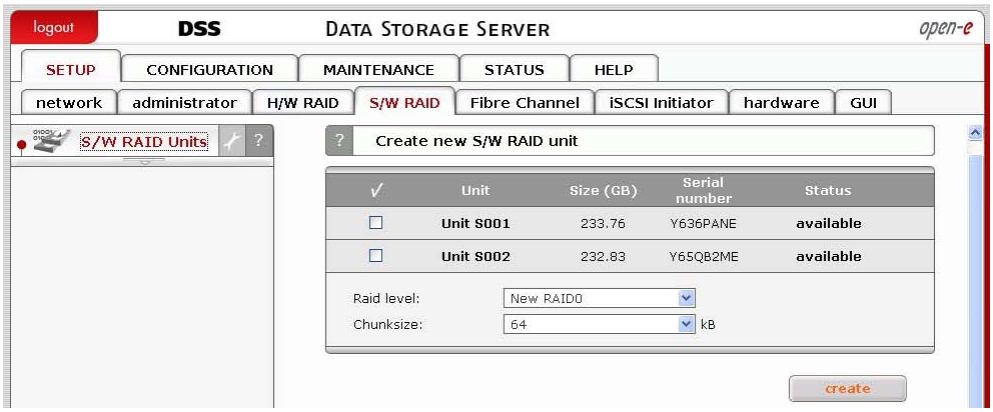
note The password is case-sensitive. If you cannot log into Open-E Data Storage Server, please make sure the Shift and Caps Lock keys are not pressed.

note If your web browser shows something different than expected, please delete the cache and cookies in the settings menu of your web browser.

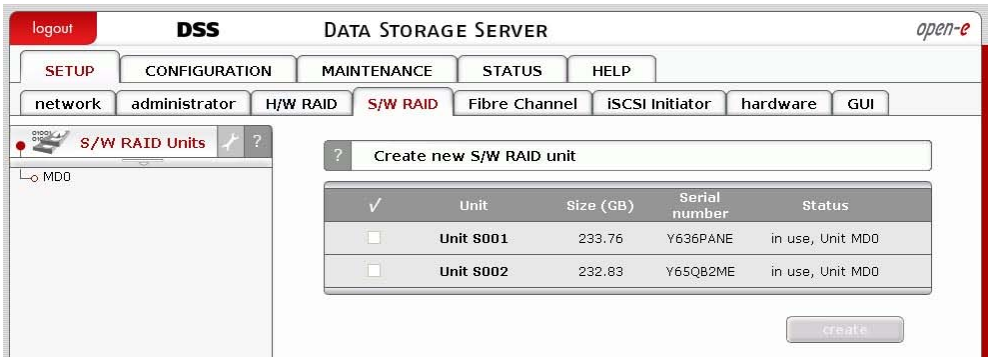
4.4 Create Disk Array

If your system has a hardware RAID, please create a RAID array in the RAID controller setup. Please refer to the RAID controller manual. You do not have to install drivers or RAID array monitoring and maintenance software. If your system has motherboard RAID functionality, please do not use it as it is not supported.

In case you want to use software RAID with single drives or even with installed hardware RAIDs, please go to the “S/W RAID” tree in the “Setup” menu first. You will find a list of available units. A unit can be a single hard disk or disk arrays if you have a hardware RAID in the system. Software RAID can be created for a single hard disk or hardware disk arrays. To create a software RAID, please select relevant units, choose the RAID level and click on the “create” button.

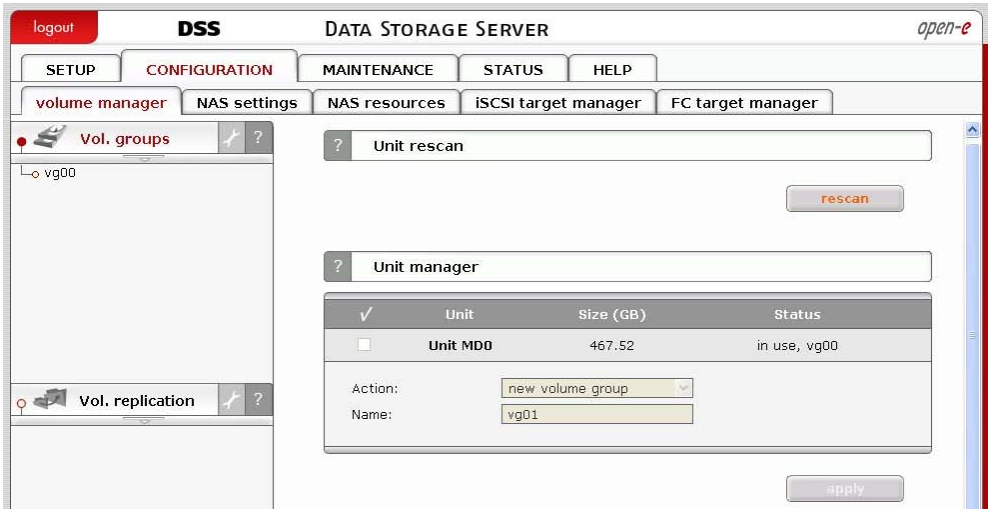


After clicking the “create” button, the status will change to “in use” and additional information describing the kind of disk array (e.g. MD0 is RAID 0) will be displayed.

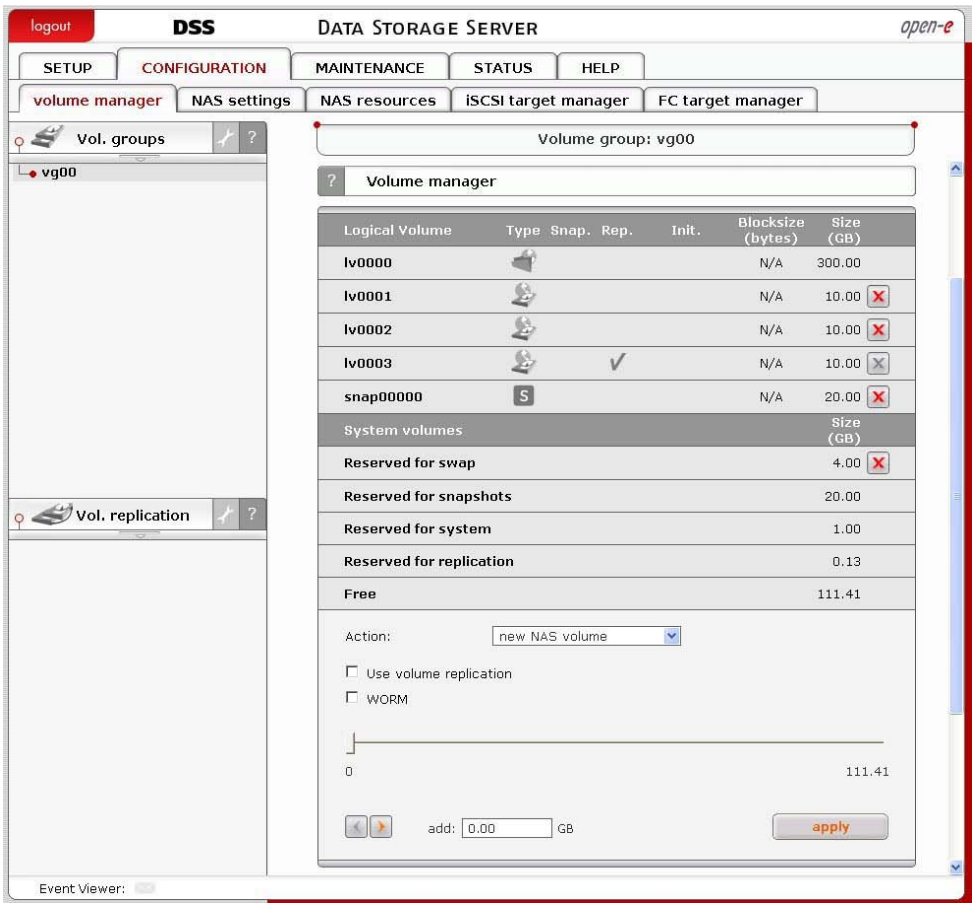


4.5 Adding Disk Array

- In the menu, please select the “CONFIGURATION” →”volume manager” and “Unit manager”.
- You will find a list of available drives/arrays (units) that can be used.
- When creating a new volume group, the system adds selected units only. You can use the default volume group name or change it. After creation is complete, the page is reloaded and the “Status” field shows your drives/arrays as "in use”.



- It is possible to combine two (or more) units into one volume group; by clicking on the right-hand side of the tree diagram on the volume group name, e.g. “vg00,” and using the “Volume Manager” function you can create a new NAS volume and/or a new iSCSI volume
- If you want to use the snapshot feature you should create a snapshot volume.



Next, using the “Volume Manager” function you can add a disk volume to a new LV, or increase the size of existing LVs (you cannot decrease LV size). To set the needed LV size just use the scrollbar. On the right side of it you will find a counter of available space. This function can be also used to reserve disk space for swap, snapshots, system and replication.

4.6 Creating Open-E Data Storage Server shares

In the upper menu, please select “CONFIGURATION” followed by “NAS settings.” Here, you can select the authentication type. In smaller networks, authentication should be done via the used workgroup name, which has to correspond to the workgroup name of the client PC.

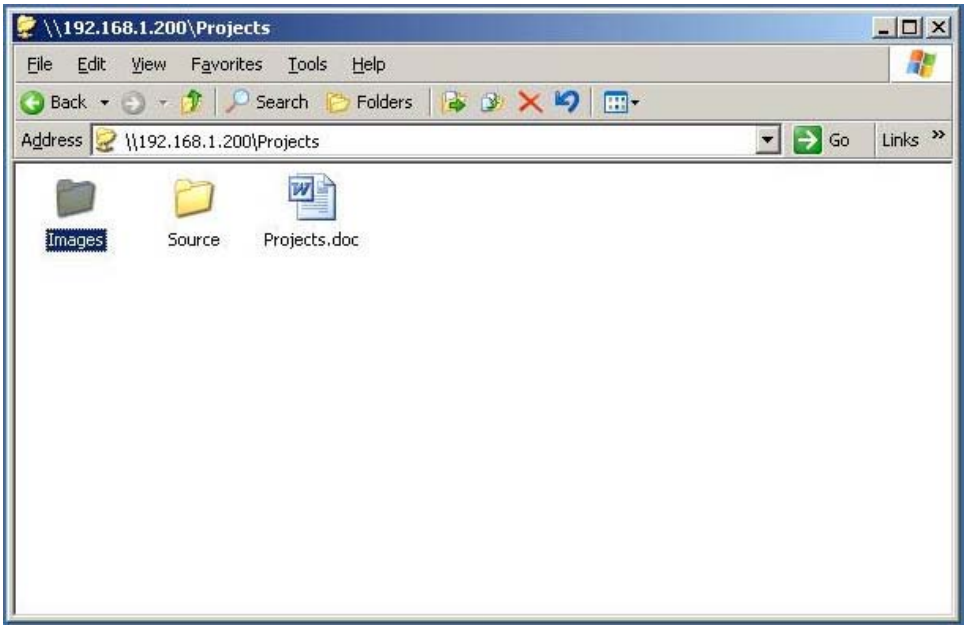
In the menu “CONFIGURATION” → “NAS Resources,” select “Shares” on the right-hand side of the tree diagram. Now create the first share.

note The workgroup/domain name that was configured in Open-E Data Storage Server has to match the network settings. Otherwise, the configured shares will not be visible in the network environment.

note If you made changes to the workgroup and server name in Open-E Data Storage Server configuration, it can take some time until each workstation computer in the Windows network recognizes the new name.

4.6.1 Access to Windows Shares

Access to newly created shares is possible via the Windows Explorer. After entering the IP address of your Open-E Data Storage Server (in this example \\192.168.1.200), all visible shares should be available immediately. Please keep in mind that sometimes it takes a few minutes until new shares or changes to become accessible.
When accessing invisible shares, you need to know the corresponding share name beforehand and attach it to the IP address with a backslash (\\):



Open-E supports Windows ACL (Access Control List) for read, write and execute options, based on the POSIX standard written by SGI.

Some examples on how to use ACL (with ADS or PDC authentication):

1. Deny access to a directory for every user (group):
   a. create a new folder or select one of your existing folders (you must be the owner of the folder or a superuser to set ACL permissions)*
   b. go to the “directory properties” (click the right mouse button on the directory then choose "Properties")
   c. select a the “security” tab
   d. choose the group "Everyone"
   e. click the "Remove" button – only you and your group will have access to the selected directory **
   f. click the "Apply" button

   Now only you have permissions to access this directory.

2. Allow full access to this directory for a group called "WORK":
   a. make sure that the group WORK is created
   b. In the security window click the "Add" button
   c. click the "Remove" button (point 1)
   d. select the group "WORK" (Advanced → Find Now will show you all users and groups) and click OK
   e. enable Full Control in the “Allow” column,
   f. click the "Apply" button.

3. Set “read only” permissions to the file for everyone:
   a. create a new file (you must be its the owner or a superuser to set permissions)*
   b. go to the permissions window,
   c. select the group “Everyone”,
   d. leave only ”read” permissions in the "Allow" column,
   e. click the "Apply" button,
   f. do the same for your group and yourself.

   Now the group “Everyone” has "read only" permissions to this file.

4. Changing the directory owner:
   a. in the Open-E web interface go to Resources → shares
   b. within the "Set Superuser" function select your user and restart the connection (Maintenance → Shutdown → Function Connections reset) or wait about 15 minutes,
   c. go to the file properties for the directory in question (right mouse click on the directory and click the "Security" tab), and click the "Security" tab),
   d. click the "Advanced" button
   e. select the Owner tab
   f. click the "Other Users or Groups" button select the user that will be the new owner (Advanced → Find Now will show all users and groups), click OK***
   g. select the user from the list and click OK and the "Apply" button
   h. click OK and re-open this window to refresh owner information.

5. Allow full access to this directory for the user "BIG BOSS":
   a. make sure that the "BIG BOSS" exists,
   b. in the security window click the "Add" button
   c. select the user "BIG BOSS" (Advanced → Find Now will show you all users and groups) and click OK
   d. enable Full Control in the Allow column
   e. click the "Apply" button

6. Allow “read” access to this directory for a group called "COMPANY":
   a. make sure that the group "COMPANY" exists
   b. in the security window click the "Add" button
   c. select the group "COMPANY" (Advanced → Find Now will show you all users and groups) and click OK
   d. enable "Read & Execute" in the Allow column
   e. click the "Apply" button

7. Create a “read only” directory with full access subdirectories for the group “ALL” (using inheriting permissions):
   a. create a folder called "ROOT",
   b. go to the security window,
   c. remove both “Everyone” and your group,
   d. click the “Advanced” button and then the “Add” button,
   e. select the group “ALL” and click OK,
   f. change “Apply onto” to “This folder only”,
   g. within permissions leave only “Traverse Folder / Execute File” and “List Folder / Read Data” Click OK,
   h. click the “Add” button once again and add “ALL” group,
   i. This time change “Apply onto” to “Subfolders and files only” (this step will put any inherited permissions into effect),
   j. select “Full Control” and click OK
   k. click “Apply” to save the permissions.

   With these settings users from the group “ALL” cannot remove the “ROOT” folder or make any changes to its contents. All new files/folders will be based on the access given by inherited permissions.
   Example:
   - file /ROOT/some_file.txt can be changed but cannot be removed
   - directory /ROOT/directory cannot be removed but a users from the group ALL can create folders and files in this directory,
   - file /ROOT/directory/my_file.txt can be removed or changed by the group ALL (provided the inherited permissions have not been changed)

8. Inherited permissions
   If the file or directory has inherited permissions, all newly created subfolders will inherit the main folder permissions. All permissions can be changed. Please keep in mind that changing permissions in the main folder will trigger the same changes to the inherited permissions of any subfolder within.

9. UNIX Rights in Windows:
   Folder permissions

Permissions	- - x	r - -	- w -	r - x	r w -	- w x	r w x
Traverse Folder / Execute File	√			√		√	√
List Folder / Read Data		√		√	√		√
Read Attributes	√	√		√	√	√	√
Read Extended Attributes		√		√	√		√
Create Files / Write Data			√		√	√	√
Create Folders / Append Data			√		√	√	√
Write Attributes			√		√	√	√
Write Extended Attributes			√		√	√	√
Delete Subfolders and Files							√
Delete							√
Read Permissions	√	√	√	√	√	√	√
Change Permissions							√
Take Ownership							√

Example application of ACL permission in a small company.

The company has 10 users

Name	Group	Position	Rights
Chris	Company	Director	All rights to everything
Robert	Company	Manager	All rights to everything besides the Director's home directory
Jennifer	Company	Secretary	Read access to the "DOCUMENTS" directory
Clint	Company Developers	Main Developer	Read and write to the "DEVELOPERS" directory read and write to the "CHANGES" directory
Brad	Company Developers	Developer	Read to „DEVELOPERS" Read and write to „Changes"
Johnny	Company Developers	Developer	Read to „DEVELOPERS" Read and write to „Changes"
Tom	Company Developers	Developer	Read to „DEVELOPERS" Read and write to „Changes"
John	Company Graphics	Graphic Designer	Read to „GRAPHICS" Read and write to „Changes"
Ben	Company Graphics	Graphic Designer	Read to „GRAPHICS" Read and write to „Changes"
Bill	Company	Cleaner	Only access to his home directory

First create users and groups in your domain:

a. run Start menu → Programs → Administrative Tools → Active Directory Users and Computers,
b. click the right mouse button on your domain name and select New → User
c. fill out all necessary fields to create user Chris,

d. create all remaining users (back to point 2).
e. click the right mouse button on your domain name and select New → Group
f. create the following groups: Developers, Graphics, and Company,
g. add users to groups - right mouse click on the Developers group. On the Members tab click Add. Add users to groups (groups Company, Developers, Graphics).

Connection to a Windows domain:

a. go to the Open-E DSS Web interface and select “Configuration” → “NAS settings”
b. select ADS or PDC (depends on your system - if you have an NT4 Domain or Windows 2003 (with no Kerberos**** fix) then select PDC, else select ADS),
c. enter your domain name - in PDC this will be the IP address and administrator password in ADS enter the full domain name (for example COMPANY.COM.DE),
d. enter your domain/Kerberos server IP address,
e. enter the name and password of an Administrator user account existing on your domain,
f. click the “apply” button to connect the domain.

Creation of shares and set permissions:

a. Create a Company share (go to the Open-E DSS web interface → Configuration → NAS resources → Shares),
b. set permissions for all users or select only company groups,
c. go to the share \\YOUR_NAS_SERVER_NAME\\Company,
d. create folders "WORK", "HOME" and "FORALL",
e. set permissions for the folder WORK - right mouse click → properties → security.
f. deny access for everyone (point 1), change the owner to the user Chris (point 4) with full access and add Robert with full access,
g. create folders DEVELOPER, GRAPHIC, DOCUMENTS and CHANGES in the folder WORK,
h. change the owner of the DEVELOPER directory to Clint (with full rights). Add “read only” access for the group Developers,
i. add full access to the directory GRAPHIC for the group Graphics,.
j. change the owner of the CHANGES directory to Clint (with full rights). Add full rights or the groups Graphics and Developers,
k. give Jennifer “read-only access” to the DOCUMENTS directory,
l. in the HOME directory create a separate private directory for each user, change user (the owner and the directory names should be the same). Remove access for the Company group (point 1).
m. add full access to the directory "FOR ALL" for the group Company.

* If you are a superuser all files and directories will be created as a local ROOT user.

** New directories with no inherited permissions do not have ACL permissions at the beginning - they have only standard UNIX permissions 0777 (Windows 2003 shows every special permission in the normal view in

the security window. Windows 2000 does not show any permissions in the normal view - only in the advanced view). To enable ACL for this directory, first select “Full Access” for everyone and click the “Apply” button. Subsequently do the same for your group and your user. Subdirectories created in this directory should have ACL permissions inherited from their parent. If permissions are inherited then the “ALLOW” column is grey. To disable permission just use the “Deny” column. If you change ACL permissions always check that a new set of permissions for one group does not interfere with permissions for other user/groups or any connections between these accounts. Windows 2003 handles such changes much better than Windows 2000.
.

*** This function is available in Windows 2003 - in other Windows versions only your user can be selected.

**** Kerberos is a server for distributing security keys. Normally it resides only on the domain but it can also be located on an external server. In Windows 2003 this server ignores specified key types, and authorization works only when entering the IP address, not the DSS name.

4.6.2 Accessing Open-E Data Storage Server shares under Linux

Please use the following command to mount an NFS share:

- mount -t nfs 192.168.0.220: /share/share_name /local_mount_point
  where:
  192.168.0.220 is the Open-E Data Storage Server IP address

Please use the following command to mount an SMB share:

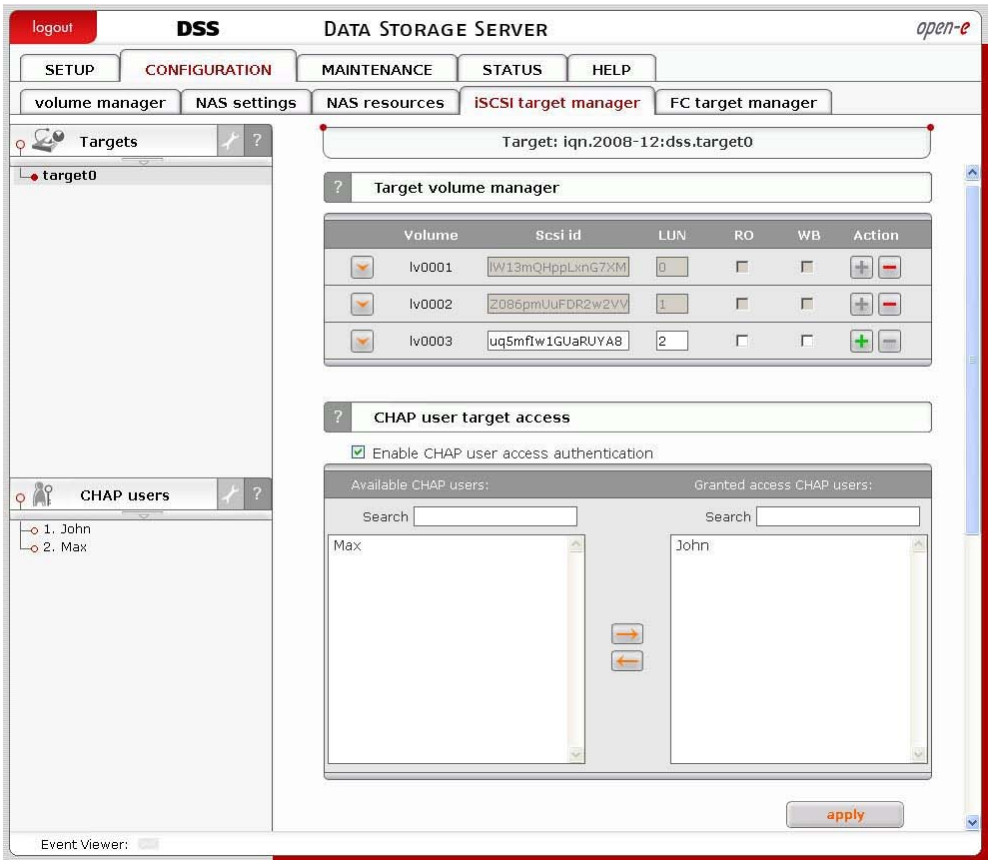
In a shell:
- mount -t smbfs -o username=root,password=12345 //192.168.0.220/test /mnt-smb
  where ‘test’ is the share name

In X-Windows:
- Smb://root@192.168.0.220/

4.7 Creating Open-E Data Storage Server iSCSI targets volume

After creating an iSCSI volume (see 4.5) , please choose “CONFIGURATION” → ” iSCSI target manager”, within the “Create new target” function click the “Apply” button to create a new iSCSI target.

Next in the “Targets” diagram click on the name of a target you have created (e.g. “target0”) and within the “Target volume manager” function click the “add” button located by the logical volume in question,



Using the “Target volume manager” function you can add “target volumes” only within the scope of one volume group.

note You can create as many logical volumes and as many separate iSCSI volumes (LUNs) are required (see step 8).

If you create 5 logical volumes, you may create one target with 5 LUNs or 5 targets with 1 LUN each, or 2 targets where e.g. 3 LUNs belong to the first target and the remaining 2 LUNs belong to the second one.

By clicking on “CHAP users” in the left hand pane you can manage secure access to logical volumes by inputting a CHAP user name and password (password must consist from 12 to 16 characters if you use Microsoft iSCSI Initiator).

4.7.1 Configuring end user workstation

For iSCSI technology to work correctly on end-user computers, you need to install the iSCSI Initiator software (if it is not provided with the operating system). For Microsoft Windows 2000/XP/2003 systems, the Microsoft iSCSI Initiator is available for download from the web.

Correct software configuration consists of installing individual target volumes by adding new disk letters in the system (in Windows XP and 2003) or subfolders as with folders in the UNIX system. All these functions are available via "administrative tools" → disks management.

How to connect iSCSI in Windows 2000/XP/2003:

a. first, you have to install the iSCSI Initiator package. You must be logged in as an administrator to install the Microsoft iSCSI Software Initiator package,
b. next, launch the iSCSI Initiator software,
c. if you have set passwords on iSCSI and Target Access, click on "Secret" within the "General" tab, enter your passwords, and after entering each click "OK" button (your passwordis called a "Target secret"),
d. click the "Add" button on the "Discovery" tab, then enter your Open-E Data Storage Server IP address,
e. next click the "Advanced…" button and check "CHAP logon information," next put in the User name and the Target secret and then two times click the "OK" button,
f. on the "Targets" tab you will see name of available iSCSI targets, e.g. "iqn.2006.10:dss.target0",
g. click "Log On" button, and if you have entered a password, you need to repeat the steps outlined in point "e," then press the "OK" button. The status for the chosen target will now change to "Connected,"
h. next choose Settings → control panel → administrative tools → computer management → disk management,
i. now all available iSCSI target drives will be displayed. In order to use them you have to format them and mount them in the system under a new disk letter.

note Microsoft iSCSI Initiator ver. 2.02 does not support dynamic disks. Target password must consist of minimum 12 and maximum 16 alphanumeric characters. Please read the manual and release notes for the Microsoft iSCSI Initiator for more details, which you can also find on the Microsoft website.

note Please do not ignore the time settings on the Open-E DSS iSCSI target and the client stations. Those settings must be identical. Time can be synchronized using the "Set time function in the Web interface menu Setup.

5 Functions

5.1 Console display functions

While Open-E Data Storage Server can be fully administered remotely through a secure Web interface, some of its functions can be accessed via the console. Open-E Data Storage Server constantly displays the following basic parameters:

- IP address
- Https settings

CTRL+ALT+n

If you press the left CTRL key + the left ALT key + n, you will be asked for a new IP address and a subnet mask. The DHCP server will be shut down.

CTRL+ALT+p

If you press the left CTRL key + the left ALT key + p, all access restrictions will be lifted after entering the administrator password (in addition, there is a reset to the standard https port 443).

CTRL+ALT+i

By pressing a combination of left CTRL key, left ALT key and i, you can reset the original IP address (192.168.0.220) and bonding. During this process, the DHCP server support is turned off

CTRL+ALT+t

By pressing a combination of left CTRL key, left ALT key and t, you can run the Console Tools. A menu with the following functions will appear: Ping, DHCP Ping, Hardware info, Memory info, Time configuration, Language settings, Modify driver options, Console lock/unlock and Boot options.

CTRL+ALT+x

After pressing the left CTRL key, left ALT key and x, the console will display the Extended Tools.

CTRL+ALT+w

After pressing the left CTRL key, left ALT key and w, the console will display the hardware configuration.

CTRL+ALT+r

After pressing the left CTRL key, left ALT key and r, the console will display the RAID Tools

CTRL+ALT+f

After pressing the left CTRL key, left ALT key and f, the console will display the Fibre Channel Tools.

CTRL+ALT+h

After pressing the left CTRL key, left ALT key and h, the console will display hardware and driver information.

F1, F2 and F5

The function key F1 displays help information while F5 resets the console display to default. If you press the F2 key all network interface will be displayed. Shutting down and restarting

Shutting down and restarting

With Ctrl + ALT + K the Open-E Data Storage Server host computer will be restarted, while CTRL + ALT + S will shut it down. Please be careful with this option if any users are connected.

ESC menu

A boot menu is available by pressing ESC after POST (Power-on self-test) during the initial start of the Open-E Data Storage Server system. After pressing ESC, there a menu will appear with which you can launch DSS in different work or memory testing modes:

- **DSS-Single** - system launch with kernel supporting a single CPU,
- **DSS-SMP** - system launch with kernel supporting multiple CPUs,
- **NAS-x86** - system launch with 4GB RAM restrictions(this procedure should work on every unit with a CPU better than 386 and with CPU C3),
- **DSS-Single (Intel I/TA support)** - system launch in a single CPU mode,
- **DSS-SMP (Intel I/TA support)** - system launch in a multiple CPU mode,
- **Memtest** - this mode will perform a memory test on the Open-E Data Storage Server system. It will also display information on memory and its settings,
- **DSS-RESCUE_MODE** - this mode loads only those drivers which enable access to the net (the mode is used if there is a need to connect using remote support) is used if there is a need to connect using remote support).

5.2 Functions of Open-E Data Storage Server via browser access

The following pages will thoroughly describe every function of Open-E Data Storage Server. The functions are divided according to menu options, which are located at the top of the screen

5.2.1 SETUP

Within this tab you can manage network interfaces, administrator settings, hardware RAID controllers, create disk arrays using software RAID, as well as find Fibre Channel, iSCSI initiator, hardware and GUI settings.

5.2.1.1 Network

5.2.1.1.1 Interfaces

Here you can find the tree containing network interfaces. Click on the interface name to see more information about the selected interface.

Function: Server name

Server Name

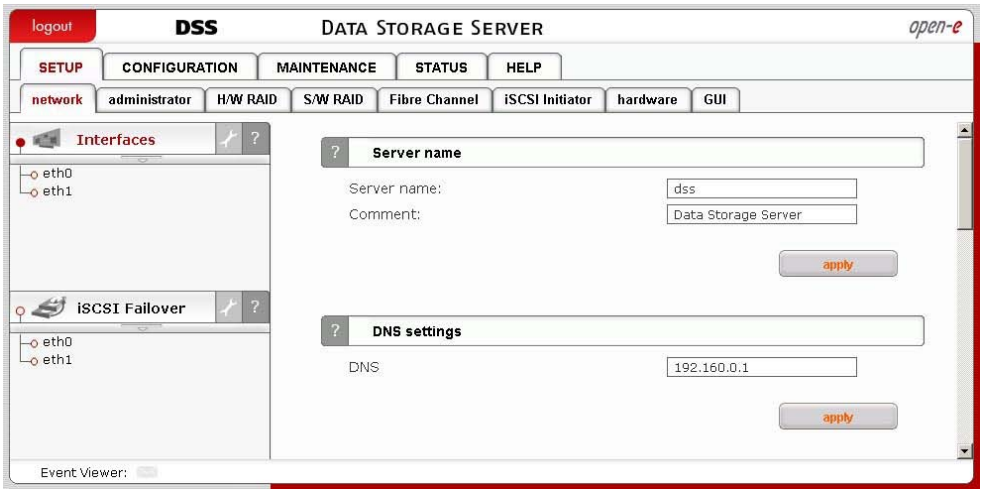
Please enter a server name to clearly identify your server.

Comment

Here you can enter a short description of your server.

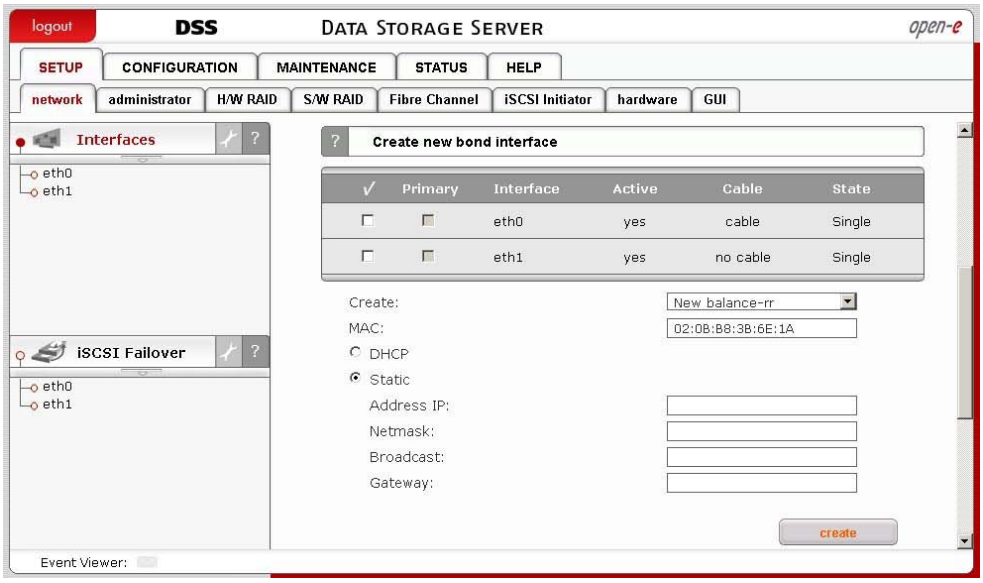
Server name and comment rules:

- please make sure the server name is unique in your network,
- select a server name that clearly identifies your new server,
- please do not use spaces and special characters such as ~!@#$^&()+[]{}*;:'".,%|<>?/\=`_,
- server name cannot consist of digits only,
- comment is not displayed on some systems.



Function: DNS settings

This function enables you to enter DNS addresses. Please use semicolons to separate addresses



Function: Create new bond interface

Bonding allows for load-balancing or fail-over for incoming and outgoing connections. Here you can create or edit bonding network interfaces.

In order to create a bonding interface:

- select the network interfaces you want to create a new bonding interface for,
- select the preferred bonding mode from the Create drop-down menu,
- select dynamic (DHCP) or static configuration for the network interface,
- if you want to get a DNS address dynamically, select get DNS,
- when using static configuration for a network interface, enter the IP address, netmask, broadcast and gateway. Afterwards, click the Create button and a new bonding interface will be created.

note In order to take advantage of bonding more than one ethernet NIC needs to be plugged into the box.

Please note that MAC addresses need to have a 02 prefix, for example: 02:xx:yy:zz:vv:nn

Each network interface is characterized by the following fields:

Primary

A string (eth0, eth2, etc) specifying which slave is the primary device. The specified device will always be the active slave while it is available. Only when the primary is off-line will alternate devices be used. This is useful when one slave is preferred over another, e.g., when one slave has higher throughput than another. The primary option is only valid for the active-backup mode.

Interface

Network interface name.

Cable

Shows if a cable is connected to the NIC.

State

Characterizes the state of the network interface. NIC can be in a bonding or single state.

Bonding modes:

balance-rr

Transmissions are received and sent out sequentially on each bonded slave interface. This mode provides fault tolerance and load balancing.

active-backup

Only one slave in the bond is active. Another bonded slave interface is only used if the active bonded slave interface fails. This mode provides fault tolerance.

balance-xor

Transmission is based on the following equation: [(the source MAC address XOR'd with the destination MAC address) modulo (slave count)]. This selects the same slave for each destination MAC address. This mode provides fault tolerance and load balancing.

broadcast

Transmits everything on all slave interfaces. This mode provides fault tolerance.

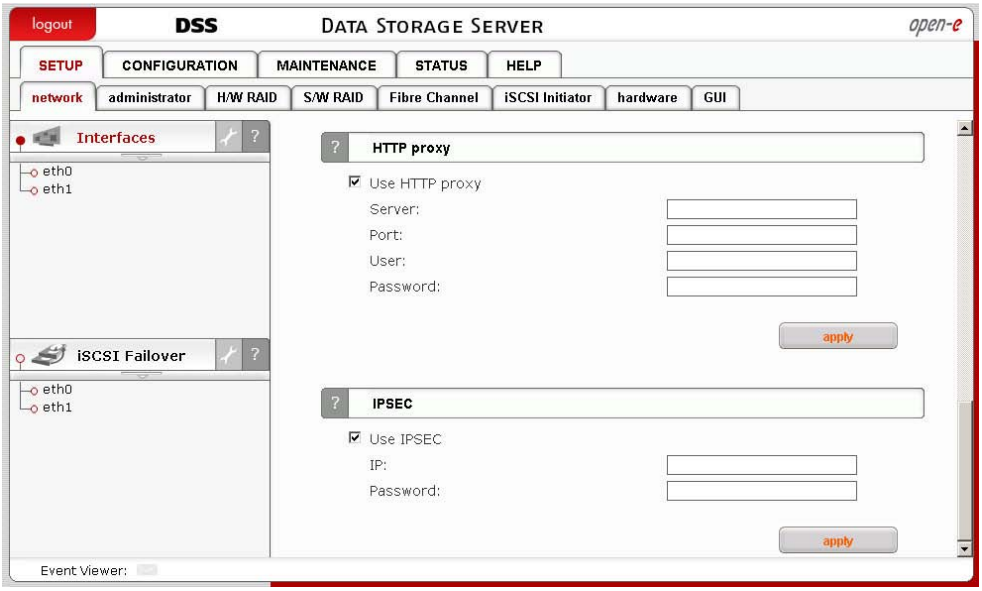
802.3ad

IEEE 802.3ad Dynamic link aggregation. Creates aggregation groups that share the same speed and duplex settings. Utilizes all slaves in the active aggregator according to the 802.3ad specification. Requires a switch that supports IEEE 802.3ad Dynamic link aggregation.

balance-tlb

Channel bonding that does not require any special switch support. The outgoing traffic is distributed according to the current load (computed relative to speed) on each slave. Incoming traffic is received by the current slave. If the receiving slave fails, another slave takes over the MAC address of the failed receiving slave. This mode provides fault tolerance and load balancing.

caution Using cards from different manufacturers or cards based on different chipsets in one bond team may cause low performance or unstable behavior.



Function: HTTP proxy

With this function you can enable or disable an HTTP proxy.

To enable an HTTP proxy:

- select "Use HTTP proxy"
- enter server name, port, username and password
- click "apply" button

note Proxy server name should not contain the http:// prefix, port and the password. An example of a correct proxy server name: *www.server.com.*

Function: IPSEC

IPSEC provides strong authentication and encryption for the connections. It makes nearly impossible to eavesdrop or forge the transmitted data.

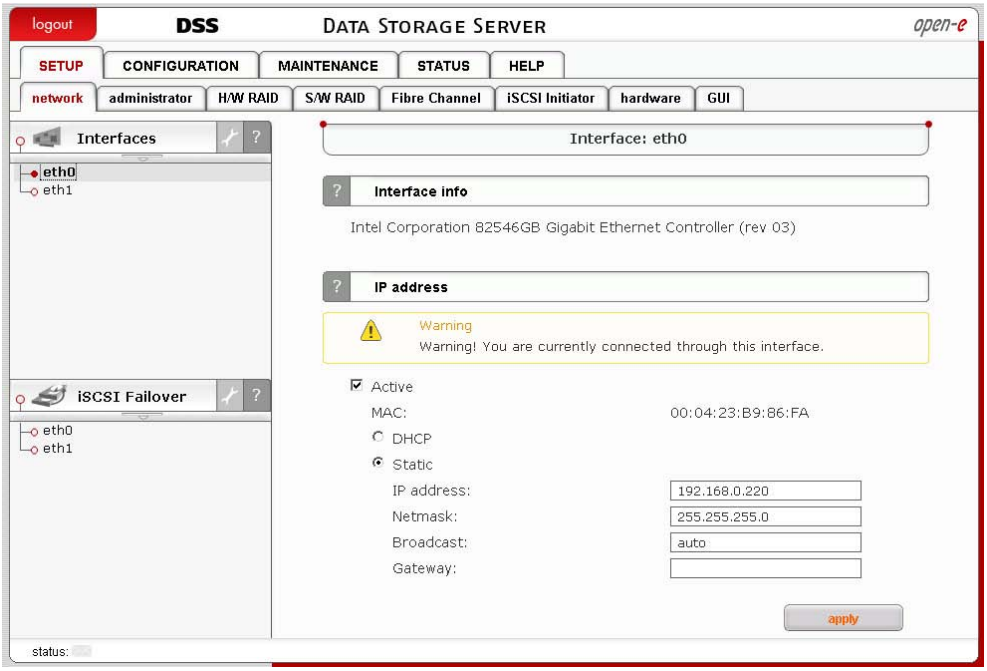
IP

IP address (optionally with a mask) of the clients that will be allowed to connect to the iSCSI target.

Password

The Password cannot contain spaces, special characters like ' " ` or be empty.

note Encrypted data transmission imposes considerable overhead and depending on the amount data transmitted can impact the performance significantly.



Function: Interface Info

Here you can view network interface info.

Function: IP address

Here you can set TCP/IP parameters for selected NIC.

Activate

You can activate or deactivate a network interface by setting this checkbox.

DHCP / Static.

You can use static or dynamic (DHCP) network interface configuration.

Get DNS

If you want to dynamically get a DNS address, select Get DNS.

When using static configuration of network interface, enter:

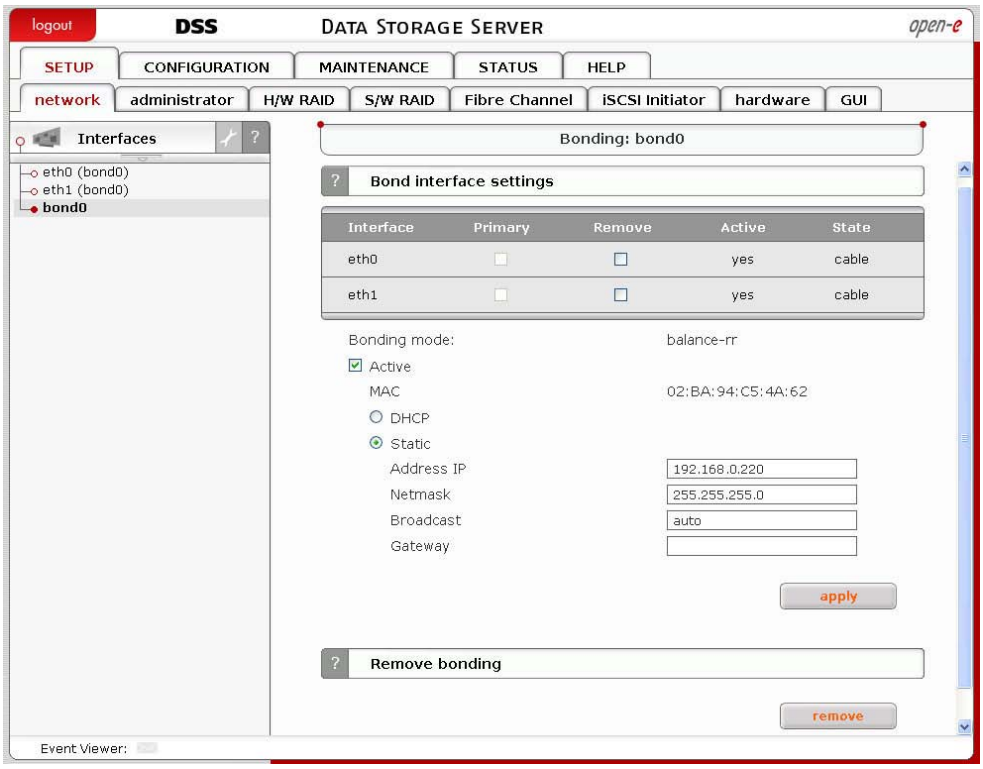
- IP address,
- netmask,
- broadcast,
- gateway.

If you set a new IP address, you will lose your connection with the server during activation and you will have to log in again. In the URL entry line of your browser, please enter the new IP address.

If you do not get access, please use the console to set a new IP address. In order to access servers in another subnet, you need to enter the address of the router as the gateway.

note If you use an NTP server to maintain proper time and date, please make sure you have appropriate gateway and DNS settings.

When creating a bonding interface, a new branch called “bond0” will appear on the left hand side of the screen. By clicking on it you can modify bonding settings (see below).



Function: Bond interface settings

Here you can configure bond interface settings.

To remove a network interface from bonding, tick the Remove field next to it followed by Apply. By unchecking the Active checkbox you can deactivate the bonding. Below, you can change the network configuration (static or dynamic [DHCP]) for the bonding interface.

Each network interface which belongs to a bonding interface is characterized by the following fields:

Primary:
A string (eth0, eth2, etc) specifying which slave is the primary device. The specified device will always be the active slave while it is available. Only when the primary is off-line will alternate devices be used. This is useful when one slave is preferred over another, e.g., when one slave has higher throughput than another. The primary option is only valid for active-backup mode.

Interface:
Network interface name.

State:
Shows if NIC is connected.

note Interfaces which have Virtual IP configured are disabled.

caution Using cards from different manufacturers or cards based on different chipsets in one bond team may cause low performance or unstable behavior.

Function: Remove bonding
Here you can remove a bonding interface.

5.2.1.1.2 iSCSI Failover

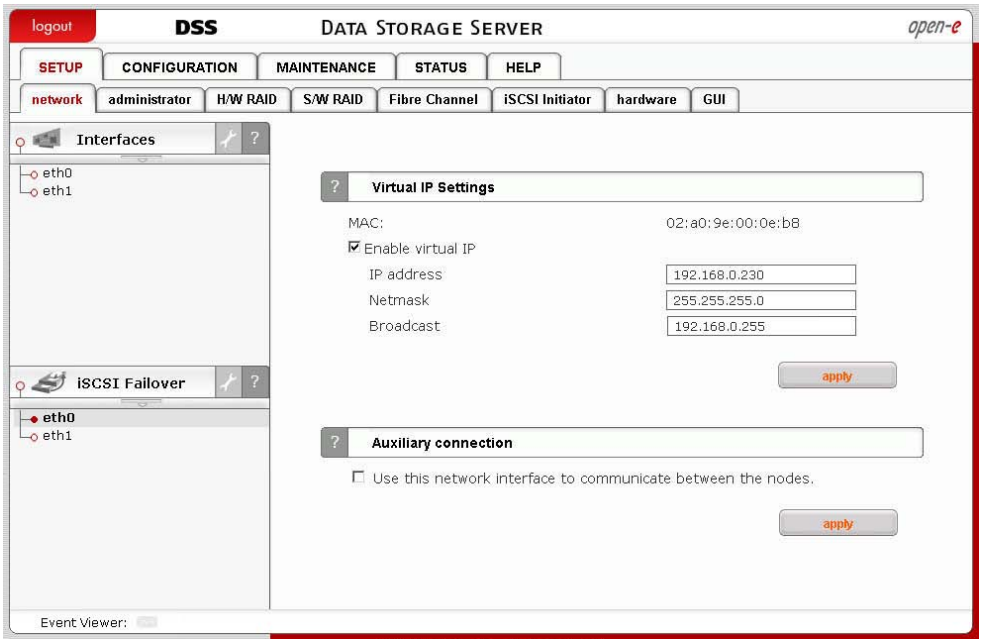
Here you can view list of active interfaces including bonding for which you can configure Virtual IP.
In this section you won't see interfaces which has been already assigned to bond interfaces or are inactive.

Function: Virtual IP Settings
With this function you can view the MAC address and assign virtual IP settings for your chosen interface. The virtual IP is shared between the failover nodes. For example, *primary node* has the IP address *192.168.1.1*, while *secondary node*'s address is *192.168.1.2*. The virtual IP address is *192.168.1.3*. In this situation, the *primary node* (the active node) will be available under *192.168.1.3*. In case of *primary node* failure, the *secondary node* will take over the *192.168.1.3* address to ensure all connections can continue to the same address.

note Virtual IP needs to be unique within its network environment and the same on both nodes (Primary and Secondary).

Changes to virtual IP settings can be done only when failover configuration is not active.

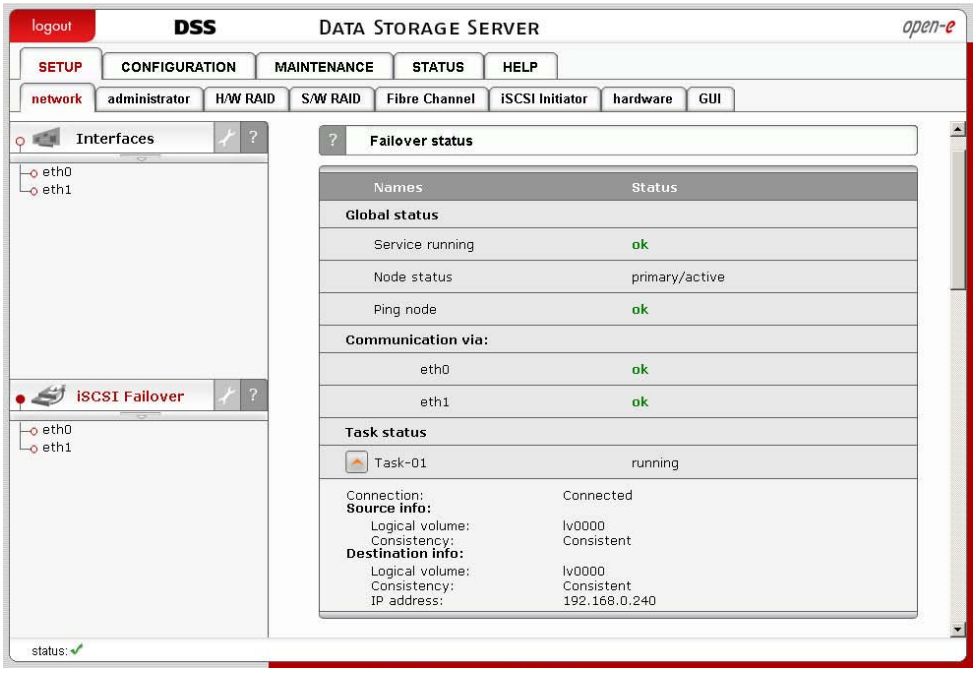
note Virtual IP can be in a different subnetwork than the node IPs, e.g. *192.168.2.1* as opposed to *192.168.1.1* and *192.168.1.2*.



Function: Auxiliary connection

This option is used to configure the interfaces on which the iSCSI Failover sends UDP broadcast traffic. More than one interface can be specified.

note If no interfaces are indicated in this field, the system will trace a signal to the opposite node and attempt to select a successful connection method automatically.



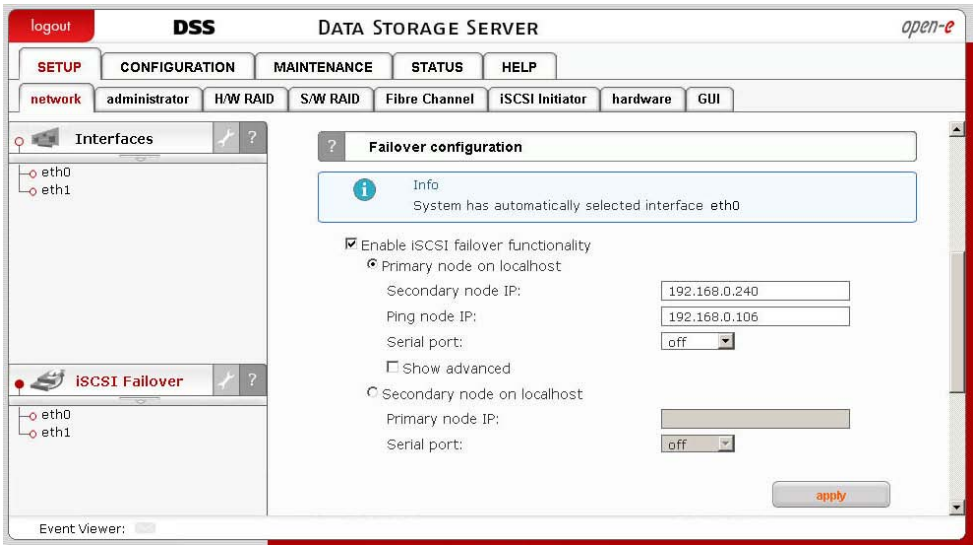
Function: Failover Status

This function displays failover statistics. These include:

- failover initialization status (*service running*),
- node status (*primary/secondary* and *active/passive*),
- ping node accessibility status (*ping node*),
- connection status for the network interfaces configured to communicate within the failover,

Additionally, the function displays the statistics for the tasks taking part in the failover. The tasks are run exclusively on active nodes.

note Switching a node into active state causes the tasks to be executed and the virtual IP addresses to become operational.



Function: Failover Configuration

In this section you can configure your system as either the Primary or the Secondary node.

Primary node on localhost:

1. Secondary node IP - designates the IP of the system which has already been configured as the Secondary node.
2. Warn time - specifies how much time (in seconds) should elapse until the failover functionality issues a warning.
3. Dead time - sets the failure (death) detection time. The dead time directive is used to specify how quickly the system should decide if a node in a failover is dead. **Dead time must be smaller or equal to Init time.**
4. Init time - sets the initial dead time detection interval. The init time parameter is used to set the time which elapses until a failover node is declared dead and the Secondary node becomes the Primary. If the Primary node becomes available before the init time runs out, the state of the failover nodes will not change.
5. Keep alive time - sets the failover keep-alive interval, i.e. the frequency at which failover state packets are sent between nodes.

Secondary node on localhost:
Primary node IP - designates the IP of the system which will be configured as the Primary node.

Ping node IP:
A ping node is a pseudo-member of a failover. It is located outside of the failover and serves to answer ICMP requests from failover members. (this means the ping node **cannot** be either the primary or the secondary node). It is there to make sure the outside connection for the failover members remains online. For instance, if the ICMP request from the active node to the ping node fails, a similar request is performed by the passive node. If this one succeeds, the nodes perform the failover. The ping node needs only to be able to receive and reply to ICMP echo requests.

Serial port:
This options allows you to connect the node via a serial cable. Select the port to which the given cable has been connected.

Keep failover functionality after volume replication failure:
When activated, this option will allow automatic failover to be carried out after the volume replication between the nodes has been broken. Please note that in certain circumstances this may lead to data loss. Details can be found in the pop-up window which appears after ticking the checkbox for this option.

note Warn, dead and init timers are started simultaneously.

note Configuring the cluster with low warn, dead and init timers may result in unstable behavior. Optimal timer settings are dependent on server hardware and network topology. It is recommended to test different timer settings for optimum performance.

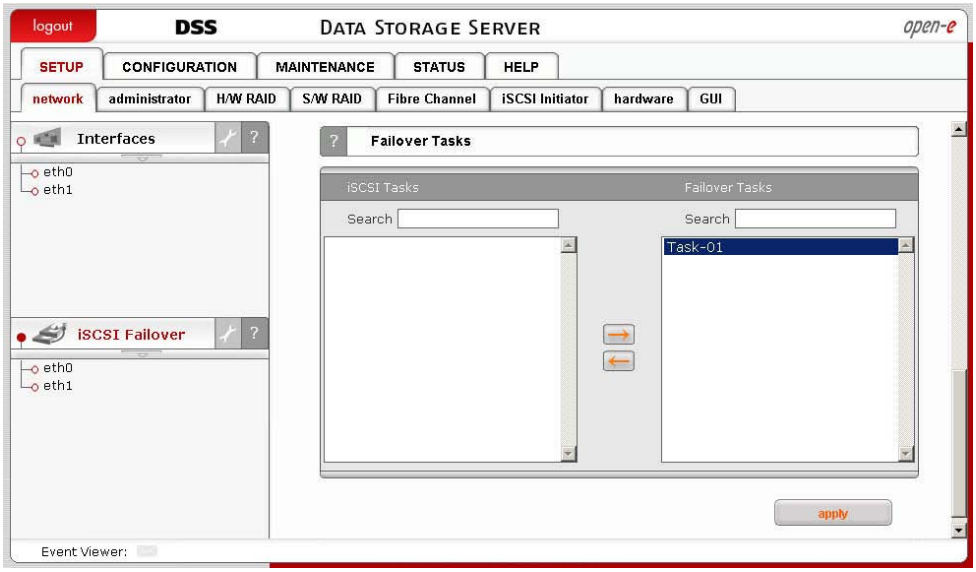
note Before starting failover please make sure the LUN configuration is the same on both nodes, i.e. that the LUNs are of the same size and type (block I/O or file I/O) and that the LUN order is preserved.

WARNING: **Inconsistencies in this area may lead to data loss!**

note If you see the following error message: **Service is under heavy load or the time values you have set are too low**, you need to readjust the time values (they are dependent on your network connectivity and system load). When using low deadtine value, one of your nodes may wrongly assume the other one is dead, which will lead to a situation where both nodes are active (the so-called "split brain").
Please observe the following guidelines for deadtime value tuning:

- set the **keepalive** time to **1000** ms, it should be lower than **warntime**,
- set **deadtime** to **60** s,
- set **warntime** to half the **deadtime** value you wish to use,

- observe the messages in the error box (lower left-hand corner of the Web GUI) or your email, if you have set up email notification for failover. If there are no relevant warnings, your proposed deadtime is fine and you can skip to the next step. Otherwise, set **warntime** to the longest time interval between the hearbeat packets as indicated in the error box. If the errors persist, increase **warntime** further. Please note **deadtime** always needs to be greater than **warntime**,
- set **deadtime** to double the current **warntime** value,
- set **warntime** to slightly less than **deadtime**.



Function: Failover Tasks

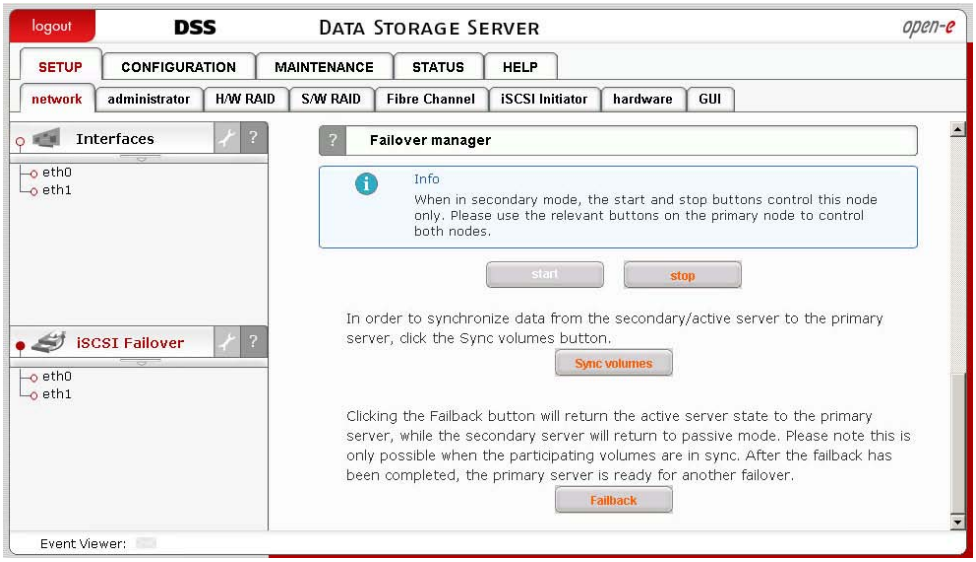
This function displays all available tasks for iSCSI volumes. In order to select a task for a failover, move the selected task to the **Failover Tasks** column. Please note any changes can only be made before the failover is initialized in the **Failover manager** function. To remove a task during failover operation, go to **CONFIGURATION → Volume manager → Replication tasks**.

note The function is available only on the primary node.

note You can only move a task to the **Failover tasks** column when the secondary node has an appropriate reverse task set up.

Function: Failover Manager

This function allows you to stop, run or change the operation mode for the given server.
On the *primary* server the **Start/Stop** action buttons control both servers. On the *secondary* server, they control the secondary server only.
In order to delegate (switch) *active* server state to the *passive* server click the **Manual failover** button. This will initiate a failover event and switch the *primary* server to *suspend* mode, while the *secondary* server will be promoted to *active* mode. **Please note** this will stop the volume replication process.
In order to synchronize data from the *secondary*/*active* server to the *primary* server, click the **Sync volumes** button.



Clicking the **Failback** button will return the *active* server state to the *primary* server, while the *secondary* server will return to *passive* mode. Please note this is only possible when the participating volumes are in sync. After the failback has been completed, the *primary* server is ready for another failover.

note It is only possible to switch the operation mode from *active* to *passive* (by clicking the **Manual failover** or the **Failback** button) when all volumes taking part in the failover tasks (see the **Failover Tasks** function) are consistent and the replication connection has been successfully established. It is not possible to perform the manual failover/failback operations when the replication process is uploading data.

Failover quick start guide

a. Set up volume replication on the primary and the secondary server.
b. On both systems, create a new target with exactly the same:
   - Target Name (Example: iqn.2008-11:mirror01)
   - SCSI-ID (Example: dF5NU3iE8ZAcK2XQ)
   - LUN# (Example: 0) and assign the failover volume clicking on the "+" button.

note Every time you disconnect a LUN from a target (clicking on "-" button) the SCSI-ID and LUN# will be reset to the original default values. So, before clicking the "+" button again, please copy & paste the SCSI-ID and LUN# from the primary to the secondary system. Make sure the primary and secondary system have identical settings. Different settings can cause some initiators to lose connection to the target during failover.

c. From the GUI menu of both systems, enter **SETUP** -> **iSCSI Failover** -> **[interface_designation]** and configure the network interfaces to be used for failover purposes. To enable the Virtual IP select an interface card and click on the Enable Virtual IP box Enter the Virtual IP address, net mask

and the broadcast IP address Click apply The same must be dome on the secondary server.

d. Please note that one of the interfaces in each system needs to have the *virtual IP* (the same for both nodes). In addition, there need to be at least two *auxiliary connections*. The interface with the virtual IP can also serve as one of the auxiliary connections. In Auxiliary connection, click Use this network interface to communicate between the nodes. And click apply.
e. In the **Failover configuration** box click the **Enable failover functionality** for both systems. On the primary node, select **Primary node on localhost** and put the Secondary node IP and Ping node IP, while on the secondary node select **Secondary node on localhost** and put the Primary node IP.
f. In the **iSCSI Failover tasks** box on the primary node select the failover task (i.e. the volume replication task you have set up earlier) and click on the right arrow button, then click on **apply**.
g. Click on **start**, in the **Failover manager** box on the primary system.
h. Check the status in the **Failover status** box; all values must be OK; also, the source and destination volumes should be "Consistent".
i. Connect to the mirror target with iSCSI initiator using the virtual IP previously assigned.
j. Create a partition and format the iSCSI disk.
k. Test the failover function by clicking on **Manual failover** button in the **Failover manager** box on the primary system.
l. Afterwards, the secondary system should show up as *active* in the **Failover status**.
m. In order to test failback, first click on **Sync volumes** button in the **Failover manager** box on the secondary system.
n. Please check the task status in the **Failover status** box. It must be "Consistent".
o. Click on the **Failback** button in the **Failover manager** box on the secondary system.
p. Afterwards, the primary system is back in active mode and ready for failover.

5.2.1.2 Administrator

Function: Administrator access

Use this function to restrict access to server administration.

HTTPS port
You can change the https port here (the default setting is 443).

Allow access IP
Here you can assign IP addresses (separated by a semicolon) that are allowed to access the server administration webpage. When left blank, the field indicates no restrictions.

Lock console without password
Disables access to the console (and LCD keys).

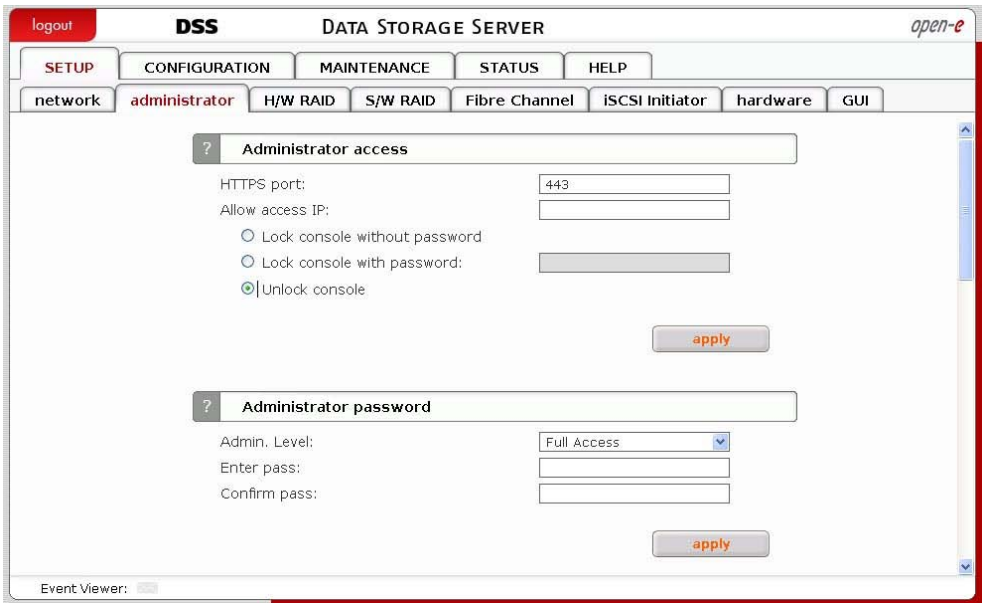
Lock console with password

To get access to the console (and LCD keys) you need to type in the password. Note that this password should be exactly 8 characters long and include only digits from 1 to 4.

Unlock console

Unrestricted access to the console.

note Please exercise caution with this function if all computers in the network receive IP addresses via DHCP: current IP can be replaced by a new one after the lease ends.
Please pay special attention when using the Lock console feature - you will not be able to reset to default administrator access from the console if you make a mistake while setting the IP address.
If you need to restore the default settings, please access the console, press CTRL+ALT+X to enter the Extended Tools view and select Restore default administrator settings.



Function: Administrator password

Using this function you can change the passwords for the server administration accounts.

Enter password

Please enter your new password.

Confirm password

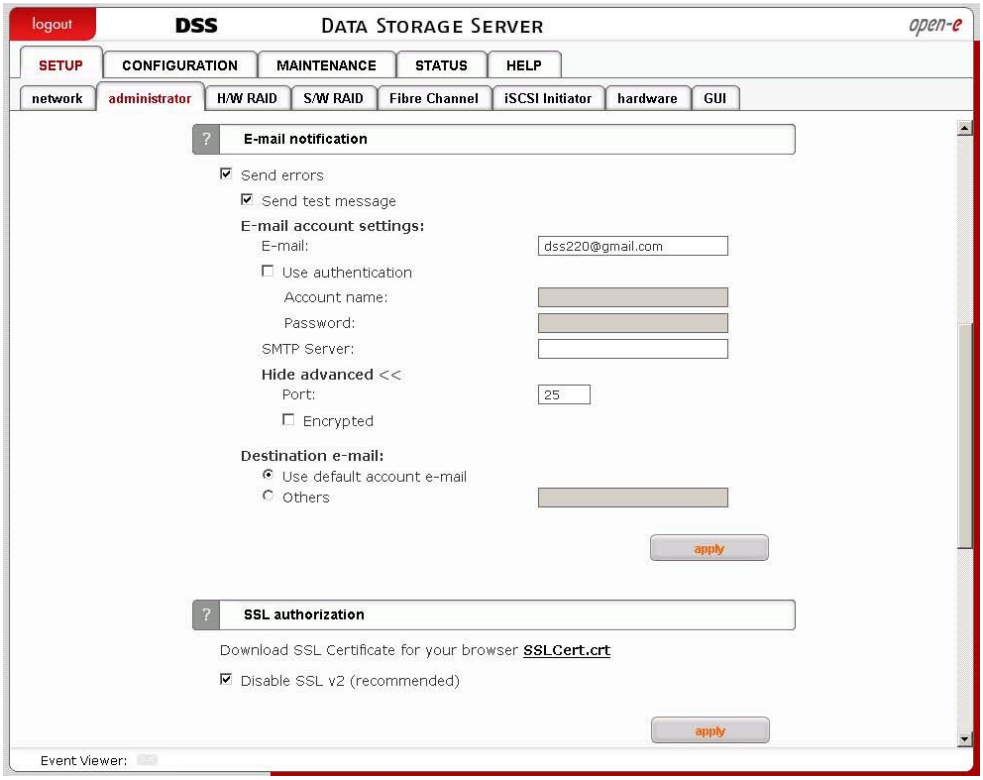
Please retype your new password.

Passwords cannot contain:

- special characters such as ' " `
- spaces.

The default password for each account is *admin*.

note Passwords are case-sensitive. For security reasons, the password you enter will not be displayed. Please make sure the Shift and Caps Lock keys are not pressed.



Function: E-mail notification

The server can send an e-mail notification to the administrator in case of any significant events, critical errors, warnings, etc. To enable this feature check the Send errors box.

E-mail

E-mail address from which notifications will be send.

Account name

Account name for the e-mail address from which notifications will be sent.

Password

Password for the account provided above.

SMTP

SMTP server name.

Destination e-mail

Administrator e-mail address to which notifications will be sent.

Port

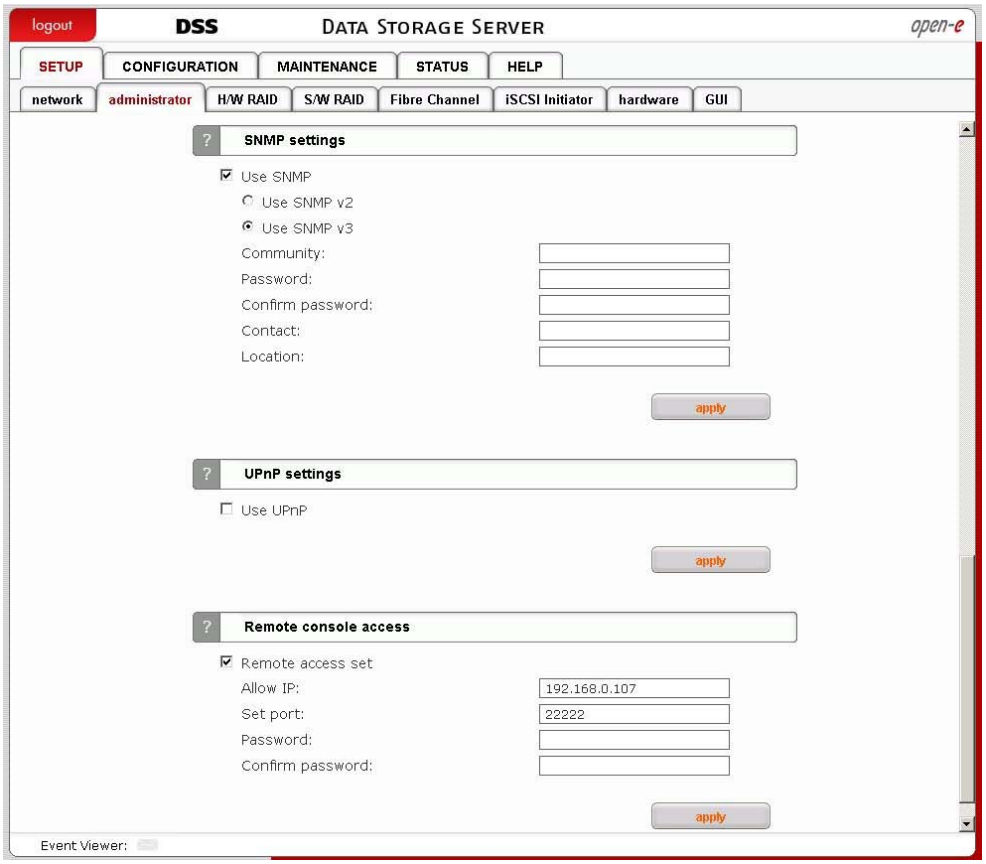
Port number for the SMTP server.

If you want to send a test message, please check the Send test message option. If you want to encrypt e-mail notifications, check the Encrypted option. E-mail notifications are encrypted with the TLS protocol.

Function: SLL certificate authority

To ensure the identity of the web administration tool by letting your web browser automatically check it whenever you connect for administration tasks, click the

SSLCert.crt link to download and install the certificate into the certificate management system of your browser.



Function: SNMP settings

This function enables you to configure access over the SNMP protocol in versions 2 or 3.
With SNMP enabled you receive a wealth of information (CPU usage, system load, memory info, ethernet traffic, running processes).
System location and system contact are only for your information, for example when you connect from an SNMP client, you will see your location and name.
SNMP in version 3 has an encrypted transmission feature as well as authentication by community string and password.
SNMP in version 2 does not have encrypted transmission and authentication is done only via the community string.
The community string you are setting can contain up to 20 characters, while the password needs to have at least 8 characters.

Links to SNMP clients:
http://www.muonics.com
http://www.mg-soft.com
http://www.adventnet.com

note Our storage system supports SNMP protocol in MIB-II standard.

Function: UPnP settings

This function enables UPnP protocol for device notification.

Function: Remote console access

Using this function, you can manage console tools remotely via the SSH protocol (secure shell). The default user is called **cli** and cannot be altered. The password, however, can be changed.

Allow IP
Here you can assign IP addresses (separated by a semicolon) which are granted remote access to the server. When left blank, the field indicates no restrictions.

Set port
The default port is 22222 for security reasons, seeing as high-number ports are invisible to port scanners. You can change the setting only to a port within the 1024-65535 range. You cannot indicate ports already in use.

Password
Password length is 8 characters minimum. Be sure to use strong passwords.

Confirm password
Please retype your new password.

Password cannot contain:

- special characters such as ' " ` ^ & $ # [ ] \/ | *,
- spaces.

To connect to the server from Linux/MacOSX systems use:
ssh -2 -p 22222 -l cli address_ip
where:

- option: -2 indicates the SSH protocol version used for connection,
- option: -p indicates the remote access port,
- option: -l indicates the user (the user needs to be **cli**),
- option: address_ip indicates the address of the server you want to connect to.

You will be asked for the remote access password you have entered on the server.

To connect to the server from Microsoft Windows, download the free SSH client (Putty):

- in the Host Name (or IP address) field please enter the IP address of the server,
- in the Port field please enter the same port as in the server GUI (default 22222),
- in the Protocol field please select SSH,
- in the category: Connection -> Data -> Auto-login-username please enter: cli,
- in Terminal -> Keyboard -> The Function Keys and keypad please select VT100+,
- go back to the Session category, enter the session name in the Saved Sessions field and click on the Save button,
- next click on the newly saved session, click Open and enter the password. (If you have not entered the Auto-login-username, Putty will prompt you for a username, so please enter **cli**).

5.2.1.3 H/W RAID

Please note that your RAID controller must be supported by the Open-E Data Storage Server in order to function properly.

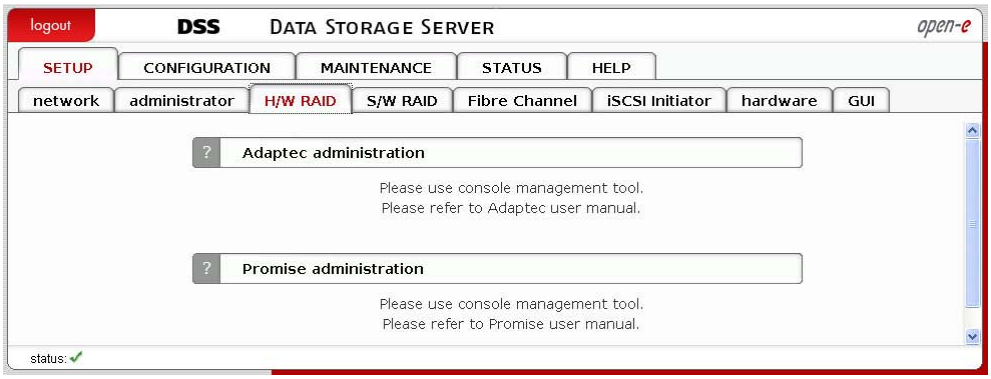
Function: Adaptec administration

If an Adaptec RAID series controller is installed, you can use a command line tool in the console tools (*press F1 in the console to list available keyboard shortcuts*) or the Adaptec Storage Manager tool. When connecting remotely to the Adaptec Storage Manager tool, the default user and password are **raid**.

Reset

Restores factory default settings for the Adaptec Storage Manager.

note It is not recommended to change the Agent system base port number (in the **Agent system port** menu) in Adaptec Storage Manager, because this may cause other services to malfunction.



Function: Promise administration

If you have a Promise RAID controller series installed, you can use the command line tool in the console tools (press F1 in the console to list keyboard shortcuts) and the Promise Array Manager tool. Default username and password for the Promise Array Manager tool are both **admin**.

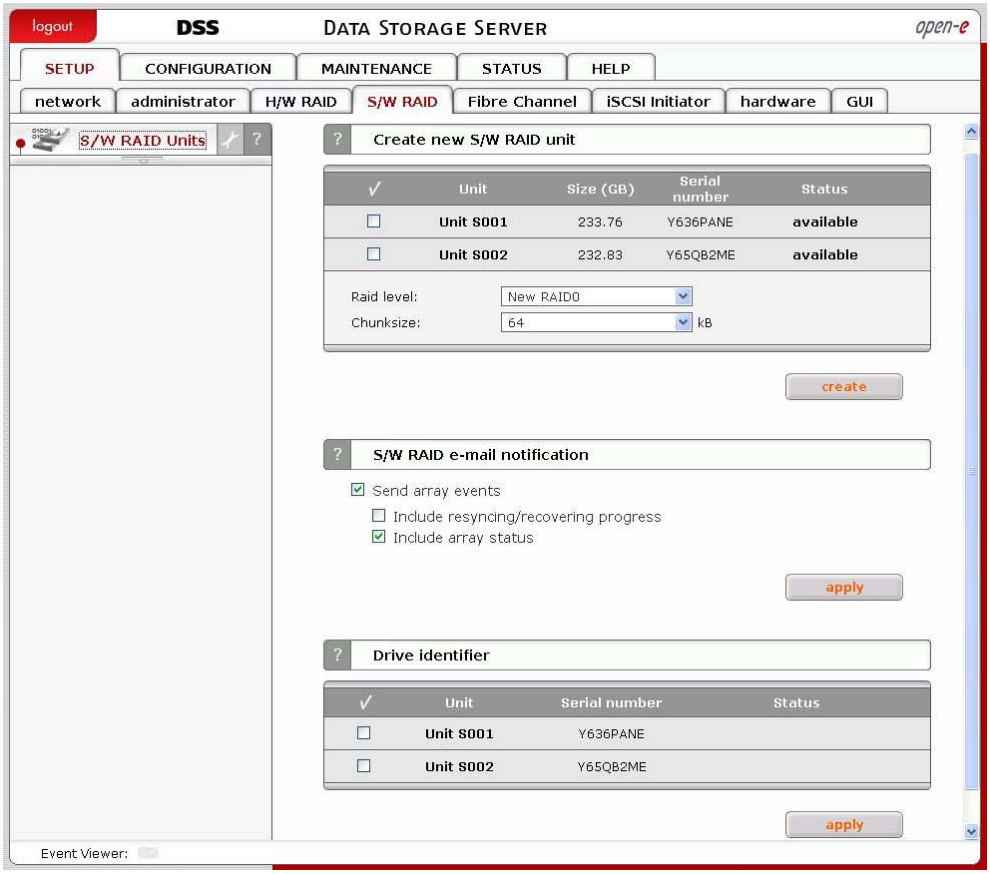
5.2.1.4 S/W RAID

Function: Unit rescan

This function rescans your system for new units.

Function: Create new S/W RAID unit

With this function you can create software RAIDs from out of free (unused) units. If you want to create RAIDs from used units which have already been in use, you need first to delete the contents of these units in the console first, however please be aware this will ERASE all data from the units.



To create a RAID select corresponding units, then use the RAID type and Chunk size menus to configure the new RAID. After setting all required parameters press the Create button.

Allow to create degraded mode

This option allows you to create a RAID1 with one unit, a RAID5 with two units or a RAID6 with three units, even if the minimal number of units is not met.

note Chunk size – the minimal portion of data that is written at a time.

Available RAIDS:

RAID 0: a stripe array; requires [minimum] 2 units. In RAID 0 you can set a chunk size from within 4k ÷ 256k. The destination size of the RAID array will be the sum of the size of each drive in the array

RAID 1: a mirror array; requires 2 units. Destination size will be equal to: (SINGLE) UNIT_SIZE, where (SINGLE) UNIT_SIZE is the size of the smallest unit in the array.

RAID 5: a stripe + parity algorithm array; requires [minimum] 3 units with the same capacity. You can choose the following from the drop-down menus: (layout) parity algorithm [left/right] [symmetric/asymmetric]. DESTINATION SIZE: (NR_OF_UNITS-1)*(SINGLE)UNIT_SIZE, where (SINGLE) UNIT_SIZE is the size of the smallest unit in the array

The (layout) parity-algorithm in RAID 5 is described below.

RAID 5 (layout) parity-algorithm

It is possible to set one of four algorithms for placing data and parity blocks in the matrix. The default option is left-symmetric, which is the best algorithm for large reads. Another recommended value is left-asymmetric.

note Software RAID 5 is not a good choice for writing a lot of very small files!

Left-Asymmetric Algorithm

Unit S0	Unit S1	Unit S2	Unit S3
0	1	2	Parity
3	4	Parity	5
6	Parity	7	8
Parity	9	10	11
12	13	14	Parity

Right-Asymmetric Algorithm

Unit S0	Unit S1	Unit S2	Unit S3
Parity	0	1	2
3	Parity	4	5
6	7	Parity	8
9	10	11	Parity
Parity	12	13	14

Left-Symmetric Algorithm

Unit S0	Unit S1	Unit S2	Unit S3
0	1	2	Parity
4	5	Parity	3
8	Parity	6	7
Parity	9	10	11
12	13	14	Parity

Right-Symmetric Algorithm

Unit S0	Unit S1	Unit S2	Unit S3
Parity	0	1	2
5	Parity	3	4
7	8	Parity	6
9	10	11	Parity
Parity	12	13	14

RAID6: a stripe + parity algorithm array; requires minimum 4 units with the same capacity. You can choose the following from the drop-down menus: (layout)parity algorithm [left/right] [symmetric/asymmetric]. DESTINATION SIZE: (NR_OF_UNITS-2)*(SINGLE)UNIT_SIZE, where (SINGLE) UNIT_SIZE is the size of the smallest unit in the array

The (layout) parity-algorithm in RAID 6 is described below.

RAID 6 (layout) parity-algorithm

It is possible to set one of four algorithms for placing data blocks and parity blocks in the matrix. The default option is left-symmetric, which is the best algorithm for large reads. Another recommended value is left-asymmetric.

Left-Asymmetric Algorithm

Unit S0	Unit S1	Unit S2	Unit S3
0	1	Parity	Parity
2	Parity	Parity	3
Parity	Parity	4	5
Parity	6	7	Parity
8	9	Parity	Parity

Right-Asymmetric Algorithm

Unit S0	Unit S1	Unit S2	Unit S3
Parity	Parity	0	1
2	Parity	Parity	3
4	5	Parity	Parity
Parity	6	7	Parity
8	9	Parity	Parity

Left-Symmetric Algorithm

Unit S0	Unit S1	Unit S2	Unit S3
0	1	Parity	Parity
3	Parity	Parity	2
Parity	Parity	4	5
Parity	6	7	Parity
8	9	Parity	Parity

Right-Symmetric Algorithm

Unit S0	Unit S1	Unit S2	Unit S3
Parity	Parity	0	1
3	Parity	Parity	2
4	5	Parity	Parity
Parity	6	7	Parity
Parity	Parity	8	9

To remove a RAID which has been previously added to a volume group, please enter the Extended Tools in the console (press F1 in the console to list keyboard shortcuts) and first delete the volume group for the RAID in question(the respective function is Delete content of units in the Extended Tools menu). This will enable the Remove button. Otherwise simply press the Remove button.

note You can add spare units to RAID1, RAID5 and RAID6 arrays. Please remember that after creating a RAID, the Info function will show the synchronization progress. Until this process is finished all actions performed on this array will be slower.

tip If units come from the same storage (Fibre Channel or iSCSI), efficiency will drop when using software RAID with them. To achieve optimal performance, you should use units that come from at least two different storages (for Fibre Channel or iSCSI connections).

Function: S/W RAID e-mail notification

It is possible to send notification by e-mail about events on software RAID arrays (e.g. rebuild started, rebuild finished, RAID degraded). In order to do so please check the Send array events box..

note In order to be able to send array events via e-mail you must first enable “E-mail notification” in “setup” → “administrator”.

Include resyncing/recovering progress

This enables information about resync/rebuild progress to be sent via e-mail, provided that any such processes are taking place. E-mail will be sent for every 20% done.

Include array status

Information about the status of event-related array will be added every event.

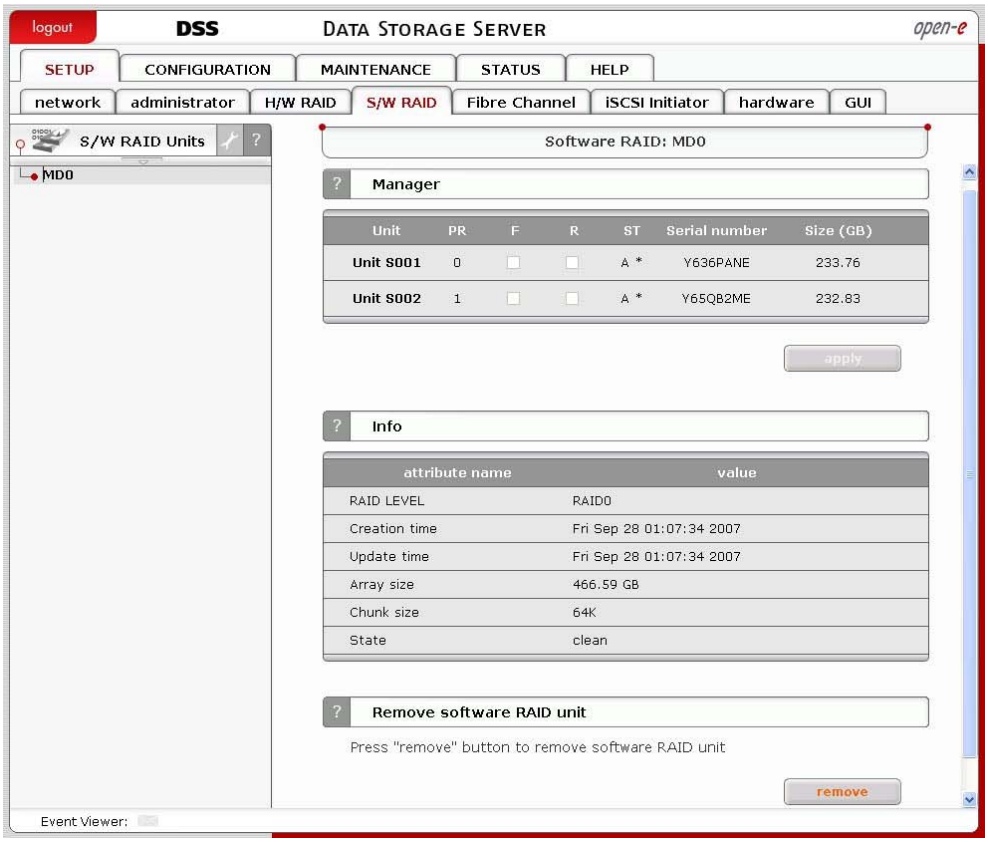
Function: Drive identifier

This function has been designated to assist you in finding disks in your NAS server cage.
If you have a hardware RAID installed, the whole RAID array is shown as a single drive, so you may not be able to determine which drive unit represents which disk when using the S.M.A.R.T. tool or a hardware RAID management tool (depending on the manufacturer of the RAID controller).

When you click on the Apply button, the appropriate disk will start reading and you can determine which disk it is by watching the disk-activity LEDs. For this function to operate properly there should be no other activity in progress on the hard drives in question.

note Identification will stop automatically after one minute if you do not stop it before (by unchecking the appropriate option and clicking Apply). Using this function during normal operation is not recommended and will cause your server to slow down.

After clicking on “MD0” in the left hand pane a tree with the available software RAID units will be displayed.



Function: Manager

In this function you can manage the RAID array.

Available operations:

RAID 0:

- design of this RAID does not allow to manage it in any way. No units can be Failed. If any of them are, the whole array will be disabled.

RAID 1:

- To mark a unit as Faulty check the appropriate option (in the F column) and click Apply.
- To delete any unit from an array check the appropriate option (in the R column) and click on Remove

RAID 5:

- To set unit as a Faulty one mark proper checkbox (in the column F) and click on Apply button.
- To delete any unit from an array mark proper checkbox (in the column R) and click on Remove button.

RAID 6:

- To mark a unit as Faulty check the appropriate option (in the F column) and click Apply,
- To delete any unit from an array check the appropriate option (in the R column) and click Remove,

RAIDs notation:

- PR - priority in array - represents the priority of a spare unit which will be added to the array if another unit is marked as Faulty. The higher the priority, the sooner will this unit be used,
- F - faulty - unit can be removed from the array,
- R - hot remove - unit can be removed from the array without shutting down the system,
- ST - characterizes the state of a unit in the array, which can be:
    - A - this means that unit is active in an array,
    - * - unit number within the array,
    - S - spare or spare rebuilding - this means that the unit is free and can be added to an array or is free and currently rebuilding.

Limitations:

- There is no possibility to set any unit as Faulty if the matrix is degraded or during resync/rebuild.
- When using RAID 1 and RAID 5 there is a possibility to mark only one disk from among active disks as faulty. This regulation is not valid for spare units in an array.

note Only one disk from within the active group in an array can be marked as Faulty or Removed

Function: Info

Using function you can obtain the following information: Creation Time, RAID Level, Array and Device Size, Update Time and State.

note It is recommended to perform as few disk operations as possible during array syncing or rebuilding.
Syncing/rebuilding status will be shown on the fly – there is no need to refresh the page manually.

Function: Software RAID unit remove

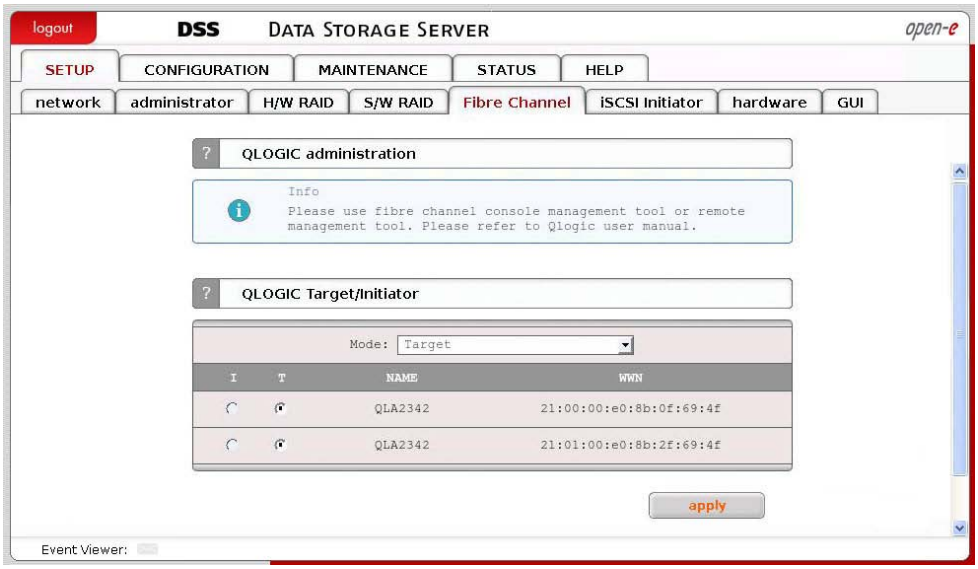
This function allows you to remove a Software RAID unit (MD[nr]).

note This function is available only when no logical volumes are created on the corresponding MD[x] and the unit is not resyncing.
If you want to remove a software RAID unit along with a logical volume

please use the Extended Tools in the console(*press F1 in the console to list keyboard shortcuts*) and remove the logical volume first.

5.2.1.5 Fibre Channel

When a Fibre channel controller is detected you will find here utilities and options specific to the hardware.



Function: QLOGIC administration

If you have a QLA23xx or QLA24xx series controller installed, you can use the command line tool in the console tools (*press F1 in the console to list keyboard shortcuts*).
QLA23xx controller enables remote administration. To access the configuration daemon download the client application SANsurfer from the QLOGIC homepage. Install it on your system and configure it to access the server. Follow the online instructions to configure correctly. If in doubt consult the documentation manual. Make sure you have the essential information handy (IP address of your server, username and password).

note It is not allowed to use controllers from two different families (2Gb and 4Gb family) at the same time.

Function: QLOGIC Target/Initiator

Here you view a list of all connected QLOGIC HBA's.

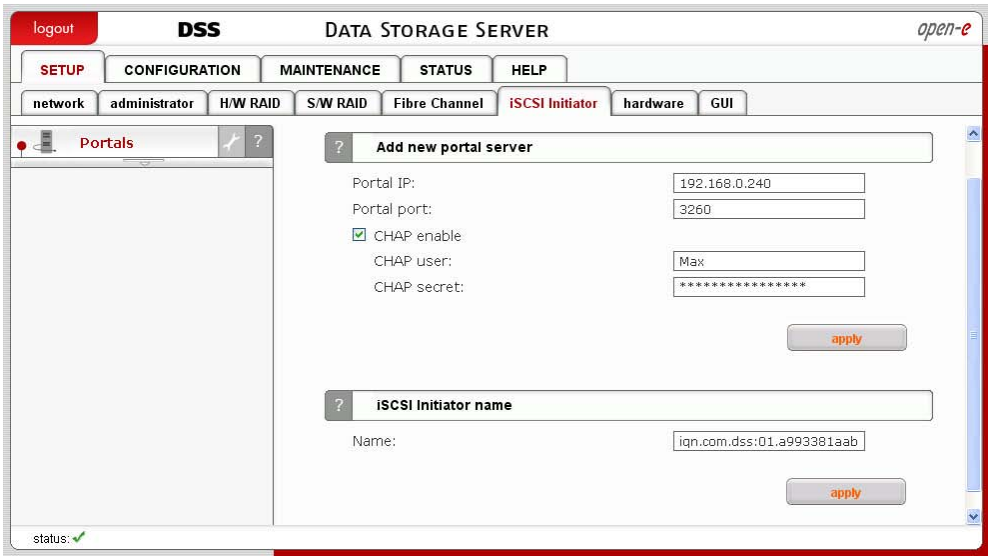
I / T

These options allows you to designate a QLOGIC HBA as either a target or an initiator.

note If your QLOGIC HBA does not belong to the QLA22XX or QLA23XX product family then the target option (I/T) will be unavailable.

5.2.1.6 iSCSI Initiator

Here you can view a list of all connected iSCSI server portals. Click on the portal IP to manage portal targets or remove a portal



Function: Add new portal server

With this function you can connect to a remote iSCSI server and add it as a new portal server. It will be visible in the iSCSI Initiator on the left. Following options are available:

Portal IP:

Please enter the IP address of ithe SCSI server.

Portal Port

Enter the Port on which the iSCSI server runs (the default setting is 3260)

CHAP enable

If you want to enable CHAP user authentication please check the CHAP enable box and enter the CHAP username and its secret.

Function: Initiator iSCSI name

Here you can change the name and the alias for iSCSI initiator name.

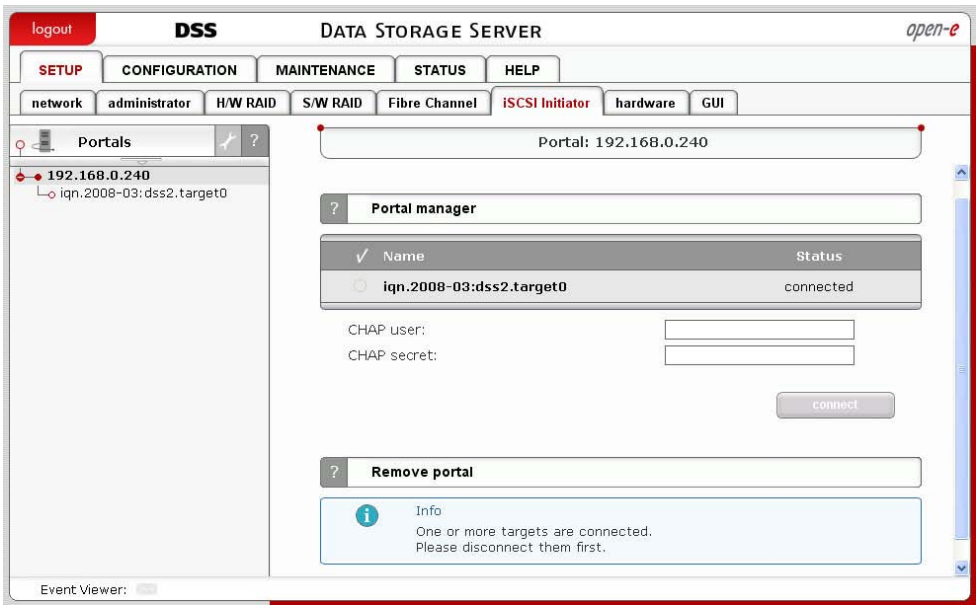
Name

iSCSI initiator name may contain alphanumeric characters: ' . ' ' : ' ' - ' and is considered case-insensitive. Every character entered will be converted to lower case. No spaces and no underscores are permitted.

Function: Portal manager

This function displays available targets for the selected iSCSI portal server. In order to connect to an iSCSI target, select its name and click the “Connect” button. If target authentication is enabled, then also enter the CHAP username and its secret. Connected targets will be available in “CONFIGURATION” → “volume manager” as units. You can manage them as you would local units.

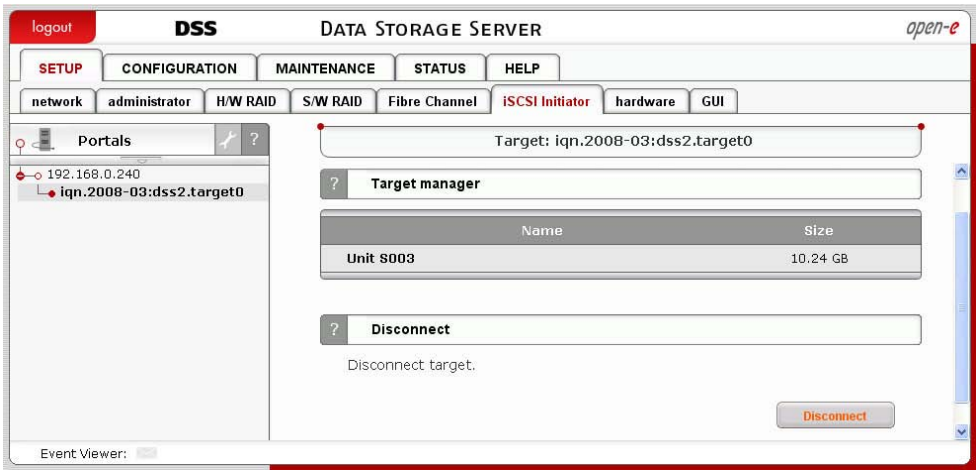
note In order to disconnect from a target, select its name in the iSCSI Initiator tree and click the Disconnect button. To remove an iSCSI portal server, first you need to disconnect all targets from it.



Function: Remove portal

Here you can remove the selected portal server.

note You can only remove a portal server if all its targets are disconnected from it. In order to disconnect a target from a portal server, please select it from the iSCSI initiator tree and click on the “Disconnect” button.



Function: Target manager

Here you can view the connected target's name as well as its size. You can also disconnect the target from the portal server using the “Disconnect” function.

Function: Disconnect

Here you can disconnect the selected target from the portal server..

note You can only disconnect a target from a portal server if the target in question does not belong to any volume group or software RAID unit.

Otherwise please first remove the volume group or software RAID unit in the console tools(*press F1 in the console to list keyboard shortcuts*).

5.2.1.7 Hardware

Function: UPS settings

Here you can configure your UPS device (Uninterrupted Power Supply). In order to use UPS device, please select the option **Use UPS.**

Set UPS vendor

Select the UPS vendor for your UPS device. Vendors APC and MGE are available.

UPS Mode:

Single

This option determines that the server is the only system attached to this UPS and that there is no action necessary to do a remote shutdown for other systems in the network.

Master

This option determines that the server is connected to the UPS and sends a signal through the network to shut down other systems in the network.

Slave

This option determines that the server reacts to a power down-signal from the UPS master.

When using an APC-originated device with the Master UPS mode enabled the following fields are available:

Net port

TCP port on which the master UPS is connecting to the slave UPS.

Slave

IP address of the slave APC UPS.

When using an APC-originated device with the Slave UPS mode enabled the following fields are available:

Net port

TCP port on which the slave UPS is connecting to the master UPS.

Slave

IP address of the master APC UPS.

When using an MGE-originated device with the Master UPS mode enabled the following fields are available:

User name

User name allowed to connect from the slave UPS.

Password

Password for the user name above.

Slave IP

IP address of the slave MGE UPS.

When using an MGE-originated device with the Slave UPS mode the following fields are available:

User name

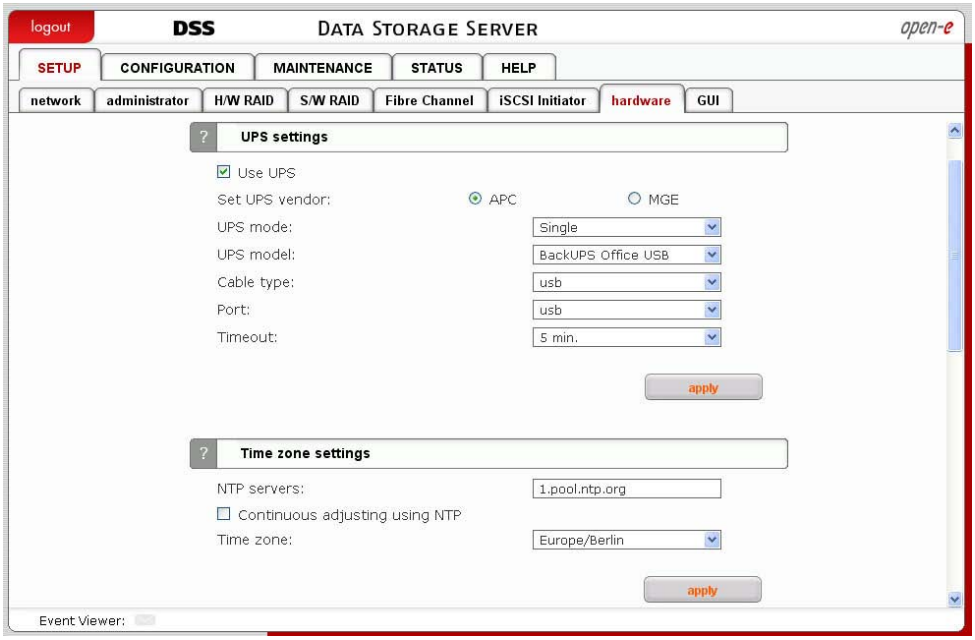
User name which will connect to the master UPS. It needs to be the same as the one on the master UPS.

Password

Password for the user name above.

Master IP

IP address of the master MGE UPS.



UPS model

The model of your UPS device.

Port

Port to which the UPS is connected.

Cable type

Cable type for your APC UPS.

Timeout

The timeout defines the time between a power failure and the moment the system shuts down.

Timeout - Battery Limit

This option enables you to sustain the system as long as the battery holds (the system will shut down when the battery charge drops to 5% or when there are 3 minutes left to total battery discharge).

Turn off UPS after system shutdown

This will turn off the UPS device after the time period set in the Shutdown grace delay (SLEEP) parameter in the UPS EEPROM expires.

note When using slave and master UPS modes, all UPS devices need to come from the same vendor.

Function: Time zone settings

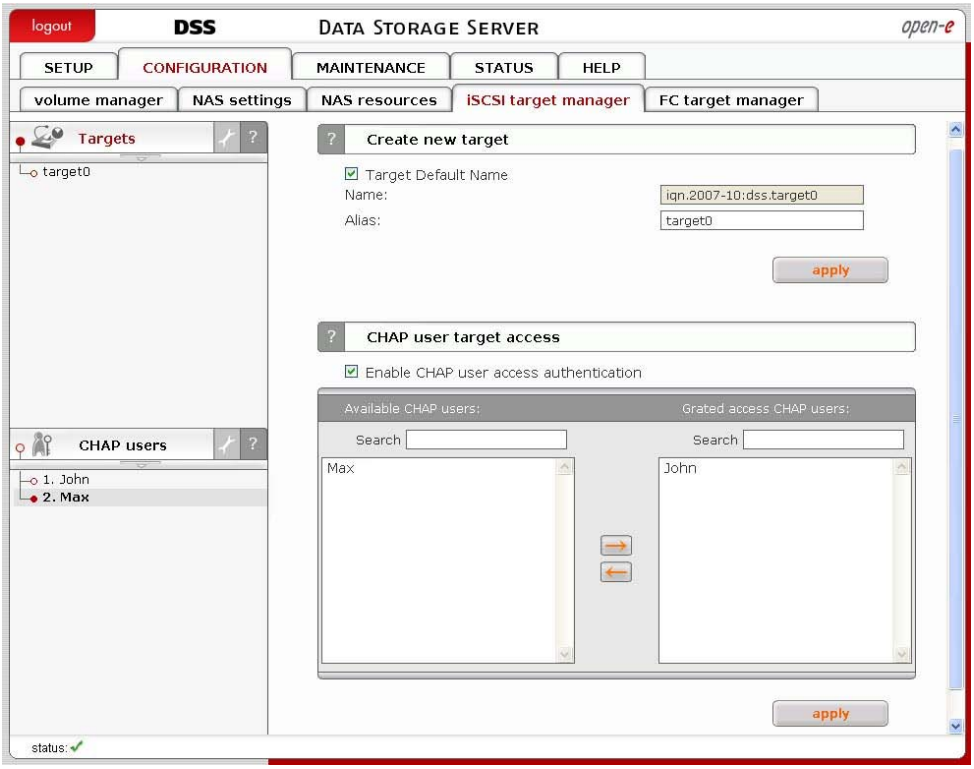
This function allows you to adjust NTP server settings.

Please select an NTP server (Network Time Protocol: for more info please see: *www.ntp.org*)

You may provide a fully qualified host name or an IP address. Select time zone suitable for your location.

With the Continuous adjusting using NTP option enabled your system time will be monitored and corrected if the difference between the local time and the server time changes. Enabling this option is especially recommended when using domains.

note Time setting is very important for proper functioning of the server. The gateway and (with host names) DNS network settings must be configured beforehand.



Function: Set time

With this function you can set the time and date:

Manual

Type in the time and date using the following format: *hh:mm:ss yyyy-mm-dd*..

Use this PC time

The time and date on the PC you run the web browser on will be used.

NTP server

This will pick up the time and date from an NTP server. In this case please make sure you have Internet access and proper network setup, specially gateway and DNS. You can check proper Internet access by using ping from the NAS console (*press F1 in the console to list keyboard shortcuts*). To use this option you must set the correct NTP server in the “Clock” function settings.

note Time setting is very important for proper functioning of the server.

Function: Power button settings

In this section you specify what action will be performed when the power button is Pressed

Options:

Reboot
Restart computer.

Halt
Power off computer.

None
No action.

Multifunction
After selecting this option, the following power button behavior will become active:

- I - shutdown (1)
- I_I - restart (2)
- I_I_I_I - network settings reset (5)
- I_I_I_I_I_I_I_I_I_I - administrator settings reset (10)

Key:
I - single power button press
_ - maximum time period in which a press will increase the press counter

note After the _ period expires, each subsequent press will reset the press counter (unless the previous count meets one of the schemes outlined above).

Function: S.M.A.R.T. e-mail notification

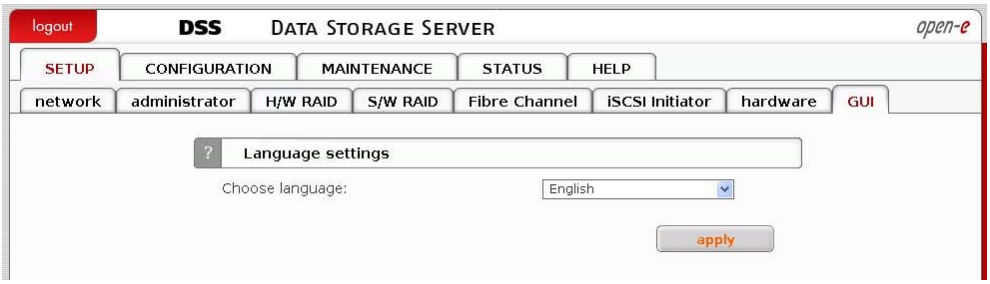
This function allows you to check hard disk status via S.M.A.R.T. and send the results to an e-mail address.
S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) is a monitoring system for computer hard disks whose function is to detect and report various reliability indicators in the hope of anticipating failures.
In order to enable S.M.A.R.T. e-mail notification, you need to:

- first enable the E-mail notification function in the “Setup” → “Administrator” menu,
- enable S.M.A.R.T. in the Hardware configuration tool in the console (*press F1 in the console to list keyboard shortcuts*),
- when S.M.A.R.T. is enabled you will see all the detected hard drives with information on unit number, size and serial number,
- check the box next to the unit for which you want to receive S.M.A.R.T. status and press “Apply” button,
- if everything is OK, the unit status will report as PASSED, otherwise it will show up as FAILED.

5.2.1.8 GUI

Function: Language settings

Select preferred language and click "apply" button.



5.2.2 CONFIGURATION

5.2.2.1 Volume manager

Function: Unit rescan

This function rescans your system for new units.

Function: Unit manager

This function allows you to manage physical storage devices - units (hard drives or RAID arrays).
Units that report as *Available* can be used to create a new volume group, a new dynamic volume, or to expand existing volume groups.

It is possible to combine two (or more) units into one volume group:

- when creating a new volume group the system adds selected units only. You can use the default volume group name or change it,
- by selecting "**New dynamic volume**",
- if you want to expand an existing volume group select the "**Add to ...**" action with the name of the volume group in question.

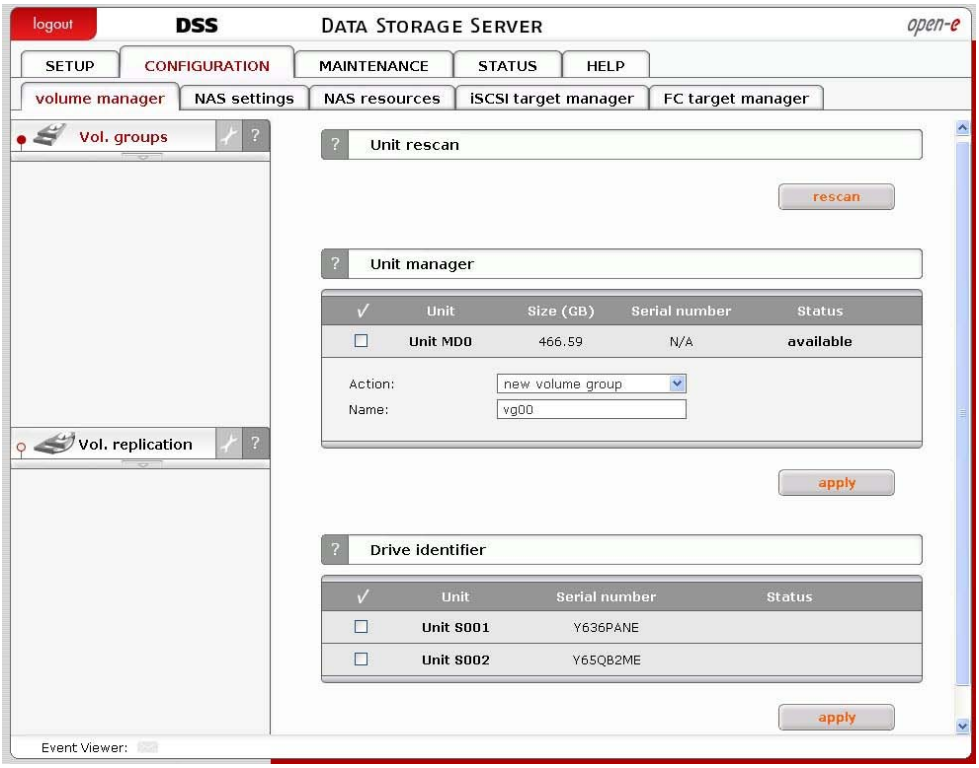
After the creation process the page is reloaded and the **Status** field should show your drives/arrays as being *In use*.
For further volume group management, e.g. logical volume setup, please click on the volume group name in the tree diagram in the left-hand pane. With the **Volume Manager** function you can create a new NAS volume (N) and/or a new iSCSI volume (I).

Disk notations:

- S0,S1, ..., S[x] - every disk with the S notation is part of a SATA / JBOD / RAID unit,
- H0,H1, ..., H[x] - units with the H letter are IDE units,
- MD0,MD1, ..., MD[x] - this denotes software RAIDs.

note

- Units already being used in a volume group can be made available again by using the **Delete content of units** function in the console. Please be aware that this will remove all data from the unit!!!,
- You can only use units with capacities greater than 5 GB, smaller units are not supported.



Function: Unit identifier

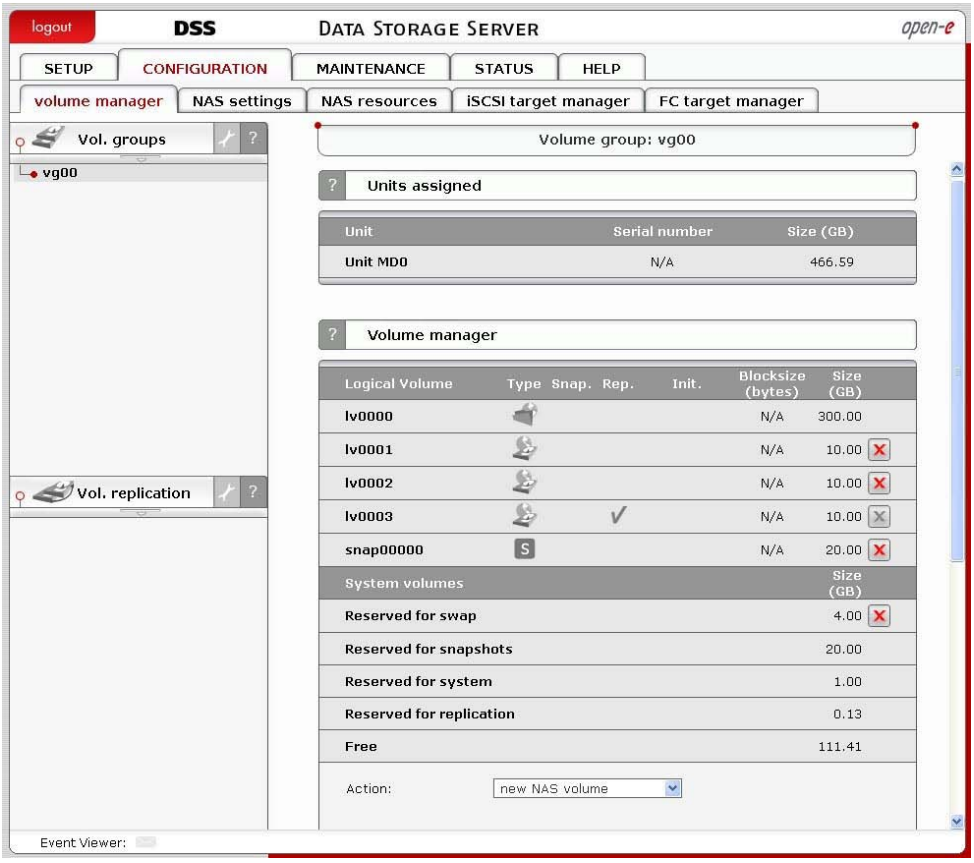
This function has been designated to assist you in finding disks in your NAS server cage.
If you have a hardware RAID installed, the whole RAID array is shown as a single drive, so you may not be able to determine which drive unit represents which disk when using the S.M.A.R.T. tool or a hardware RAID management tool (depending on the manufacturer of the RAID controller)..

When you click on the “Apply” button, the appropriate disk will start reading and you can determine which disk it is by watching the disk-activity LEDs. For this function to operate properly there should be no other activity in progress on the hard drives in question.

note Identification will stop automatically after one minute if you do not stop it before (by unchecking the appropriate option and clicking “Apply”). Using this function during normal operation is not recommended and will cause your server to slow down.

Function: Units assigned

With this function you can view physical units attached to this volume group



Function: Volume manager

This function allows you to:

- expand existing and create new NAS (N), iSCSI (I) or Fibre Channel (FC) volumes,
- reserve disk space for swap,
- create, expand and delete snapshots.

In order to add storage space to an existing NAS, iSCSI or FC volume, select expand [volume_name] from the drop-down menu. Use the scroll bar to indicate the size.

Use volume replication

Selecting this option when creating a new volume or expanding an existing one (NAS (N), iSCSI (I) or Fibre Channel (FC)) will enable volume replication for that volume.

In order to remove replication functionality from a volume:

- select the expand option from the Action combo box, e.g. expand lv0001,
- uncheck the option Use replication,
- leave the volume size unchanged,
- click the Apply button.

WORM

Write Once Read Many - this option is available for NAS volumes only; WORM-enabled volumes can be read multiple times, but written to only once. Enabling WORM for a NAS volume is only possible after selecting new NAS volume from the drop-down menu. Once WORM is enabled it cannot be undone; It is not possible to remove WORM from an existing volume.

note WORM volumes are subject to the following limitations:

- they cannot be used for volume replication,
- a share created on a WORM volume cannot be used as a destination share in a data replication process,
- a share created on a WORM volume cannot be published via NFS and cannot be accessed via HTTP (**HTTP share access** function),
- a share created on a WORM volume cannot be used as an antivirus quarantine share,
- a share created on a WORM volume cannot host a local backup database.

note Maximal NAS (N), iSCSI (I) and Fibre Channel (FC) volume size (with replication) is limited to 4193120MB (megabytes).

If your volume (including volume replication) fails to be created, increase the Vmalloc size. This can be done via the Hardware Console Tools (ALT+CTRL+W) → Tuning options → Vmalloc size.

Initialize

This option is available when creating an iSCSI (I) or Fibre Channel (FC) volume. It is here for security reasons. The volume will be initialized after the creation process. There can be only one volume being initialized at any one time. If there are more volumes to be initialized, a *Waiting* indicator will appear near the one(s) enqueued. Using the button next to the indicator you can send the initializing volume to the back of the initialization queue. Every volume that is waiting for initialization in queue can also be sent to the back of queue.

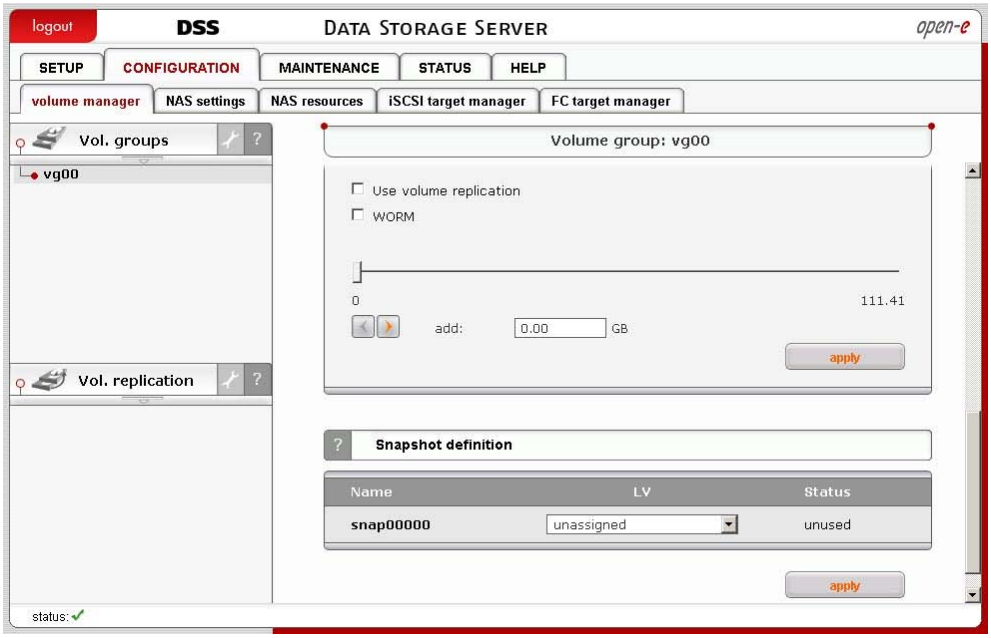
Blocksize

This option is available when creating a Fibre Channel volume (FC). Blocksize indicates the nominal size, expressed in bytes, of a block of data. Possible values:

- 512 bytes
- 1024 bytes
- 2048 bytes
- 4098 bytes (default)

Blocksize has an influence on performance and space management. The greater value the better performance, but data might take up more space. This option is unavailable when expanding an FC volume and for FC snapshots.

note When adding each new unit there will be 4 GB space reserved for swap (if a swap has not been already created). Additionally, 1 GB of space is reserved for internal system use.



Function: Snapshot definition

Here you can set the logical volume to which the snapshot will be assigned.

Name

Snapshot name.

LV

Select Logical volume to which snapshot will be assigned. If Logical volume has no snapshot assigned yet, then in LV field will be "unassigned".

Status

Snapshot status. Can be one of the following:

Active

Snapshot is active.

Inactive

Snapshot is inactive, probable reason: overflow.

Unused

Snapshot is currently unused.

The snapshot function enables the system administrator to freeze the data content of the volume at a certain time. From this moment on, the users work on a virtual data volume, all changes to the volume are stored in a different partition. The storage of all changes is independent of the filesystem - it takes place on the block level. Snapshots can be created (active state) /removed (unused state) manually or automatically.

note Please be reasonable when you are calculating the space reserved for snapshots. Please set as much space for a snapshot as you expect to change during snapshot activity, e.g. when you are performing a backup from a snapshot which takes one hour please set the size of this snapshot to as much space as will be changed during one hour. The snapshot will become inactive if the contents (data changed on logical volume) exceed the snapshot capacity. You do not lose data in that case. However, the old dataset, which has been frozen with the snapshot, is not available any longer.

When you define a schedule, use only as many snapshots at the same time as actually needed. A large count of active snapshots can slow down the system considerably.

Manual creation and removal of snapshots can be done via the following path: **CONFIGURATION → Volume manager → vg[nr] → Function: Volume Manager.**

How to access NAS snapshot

After a snapshot has been created and activated, you can access it by following these steps::

- Go to menu **CONFIGURATION → NAS settings** menu and select the network protocol on which the snapshots will be accessible, exactly like all other shares. This needs to be done only once. When establishing access to a snapshot the second time, this action is not necessary. You can activate access to snapshots on the following protocols:
    - NFS,
    - SMB (Network neighborhood),
    - FTP,
    - AFP.
- create a new share that will be assigned to the activated snapshot,
- go to the **CONFIGURATION → NAS resources** menu,
- within the Create new share function:
    - enter share name,
    - use the Specified path option and select the snapshot that you want to have access to,
    - click Apply to create a share,
- now you can start to explore your share(snapshot) using the specified network protocol.

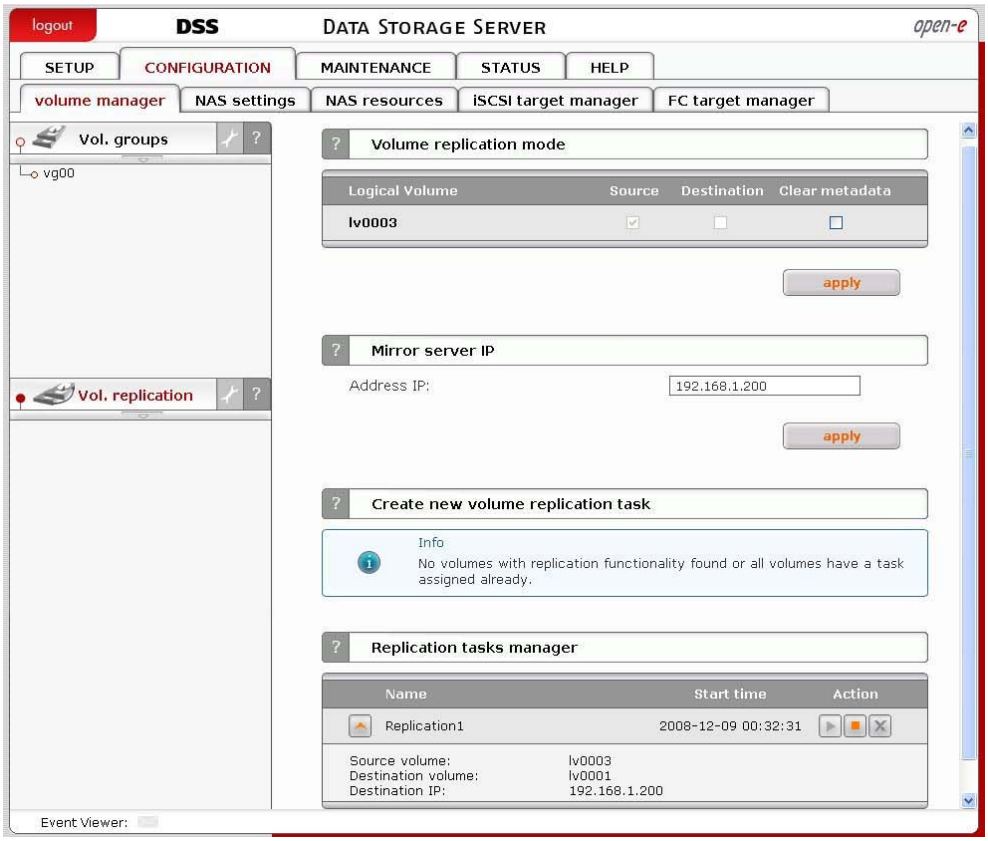
How to access iSCSI target snapshot

After a snapshot for an iSCSI target has been created and activated, you can access it by following these steps:

- Go to menu **CONFIGURATION → iSCSI target manager → Targets →** [target_name] menu,
- enter the Target volume manger function and click the Add button on the right side of the snapshot you would like to have access to. A new LUN will be added to the target,
- now you can connect with your iSCSI initiator and use your snapshot target,
- here is an example (Microsoft Windows environment): please download Microsoft iSCSI Initiator and follow its instructions,
- start the software and add targets,
- access the Target Portals menu and enter the IP address of the iSCSI server and the socket (default 3260),
- in the Available targets menu please log into a previously added target,
- now your snapshot target will show up in your system and you can use it.

Function: Volume replication mode

Here you can set the replication mode for every logical volume (with replication functionality available). A volume can be in a **source (S)** or a **destination (D)** replication mode.
You can also clear the **metadata (CM)** of a volume. Metadata describes the replication data.
Clearing metadata is required when you want to start the replication process from the beginning. Another usage example is when the data on the source volume is inconsistent and you want to restore it from the destination volume. In this situation you need to switch replication modes between the volumes (i.e. the destination volume should now be in source mode, while the previous source should be switched to destination mode). Before starting a replication for a new source and destination please clear the metadata from the previous destination volume. When replication is complete the data on the previous source volume will be consistent. If a volume is set to the destination replication mode then it will not be visible in the iSCSI initiator.



Function: Mirror server IP

Here you can set the IP address for a mirror server. It needs to be entered in order to define the volume replication task.
Setting the source IP address on the destination server is for security reasons. This will allow only the source IP address to send data to the destination target.

Function: Create new volume replication task

Using this function you can create a volume replication task. This creates a mirror copy of data from the source volume to the destination volume in real time, meaning that if you, for example, create a file on the source volume the same file

will be created on the destination volume. Destination and source volumes need to be the same size in order to successfully perform the replication. Replication can be performed only between two mirror replication servers.

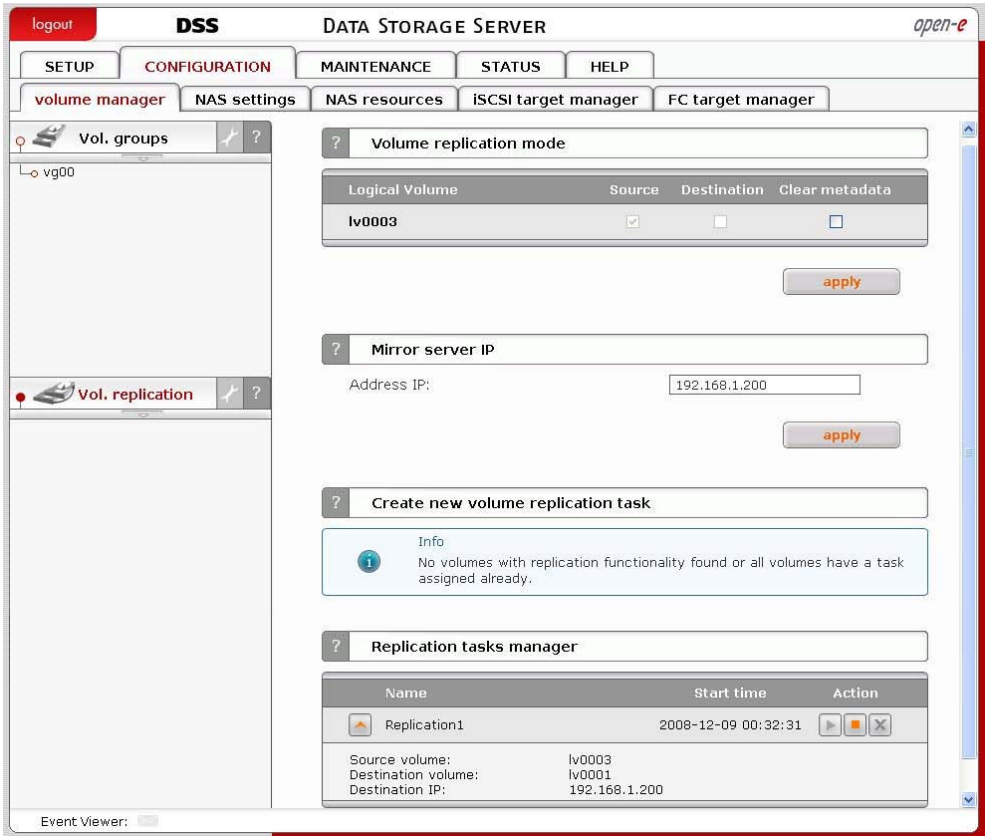
Please note this function allows you only to create replication tasks. In order to enable them, use the **Replication Task Manager** function.

Please enter the task name, select the source volume and the destination volume. Click **Create** in order to create a replication task.

note Volume replication process runs on randomly selected ports from 12000- 13999.These ports have to be open in firewalls for both incoming and outgoing traffic.

Function: Replication tasks manager

Here you can run, stop and delete existing replication volume tasks. When a replication task is running you cannot change the replication mode for the logical volume, delete the metadata or change the mirror server IP address. You need to stop the replication process first.



5.2.2.2 NAS settings

Function: Authentication method

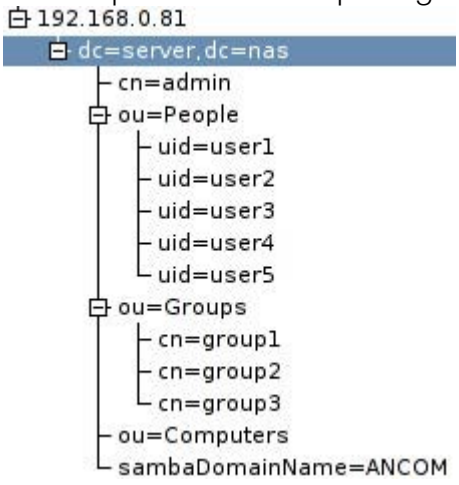
The server administrator can choose one of the following authentication methods for the users:

Workgroup (internal LDAP)

With this method you need to create all user/group accounts in the **NAS Resources** menu. In the **Workgroup** field please enter your network workgroup name. New users are assigned to the default group called **Users**.

Workgroup (external LDAP)

In the case of external LDAP (Lightweight Directory Access Protocol) the NAS server imports users/groups from an external LDAP server. Please fill in all fields accordingly. In the **Show advanced** list you can set the Base DN, and the LDAP administrator DN (Distinguished Name) and password. **Base DN** should look like this: "dc=server,dc=nas" (DC - Domain Component), where "server" and "nas" can be set exactly as they are set on the remote LDAP server. In the **LDAP administrator DN field** you should enter the base DN (as above) with an additional prefix such as "cn=admin," (CN - Common Name). Users should be stored in the Organization Unit (ou) "People," groups in "Groups" and computers in "Computers."See sample organization tree below:



Windows (PDC)

In this case the NAS server will use the Windows Primary Domain Controller user database for user authentication. This method can be used with NT4/2000/2003 servers. If a Windows 2000/2003 server runs the ADS native mode, please use the Widows (ADS) method.

note If you encounter problems getting connected to a PDC server running under NT4, please get connection follow the instructions below:

1. run the Server Manager program from the **Start** menu→ **Programs**→ **Administrative Tools** (Common) → **Server Manager**.
2. in the **Server Manager** menu select **Computer**->**Add to Domain**. WARNING: If a NAS resource has already been added, you must remove it,
3. in the **Computer Name** field enter the NAS server name (NetBIOS name),
4. click **Add**,
5. next, access the NAS server web administration and go to **CONFIGURATION** → **NAS settings**,
6. choose **Windows (PDC)** as the authentication method,
7. in the **Server IP** field enter the NT server IP address,
8. in the **Name** and **Password** fields enter the NT4 administrator account name and password,
9. click **Apply**. WARNING: If the connection fails, you will need to restart the process (go back to point 1).

Windows (ADS)

This option can be used for Windows 2000/2003 ADS servers:

- Please enter the realm name of your Windows 2000/2003 server. It can be found in the Windows system by clicking the right mouse button on **My Computer** and selecting **Properties**, then clicking the **Computer name** tab. Realm name is the same as the domain name.
- The KDC IP address must be taken from the same system as the realm name.
- Enter the administrator login and password,
- Click **Apply** to connect to the Windows (ADS) domain.

note In order to connect to an NAS share via AFP (AppleTalk Filing Protocol) while user authentication is set to ADS (Active Directory Services) and the Mac workstation prompts for username and password, please enter the username as follows:

User Name: **DOMAIN_NAME+USER_NAME** (the "+" character belongs to the syntax!)

DNS server IP should be the same as the domain controller IP!

Workgroup (NIS server)

Please choose this option if you want to use a user/group database from a Network Information Service server.

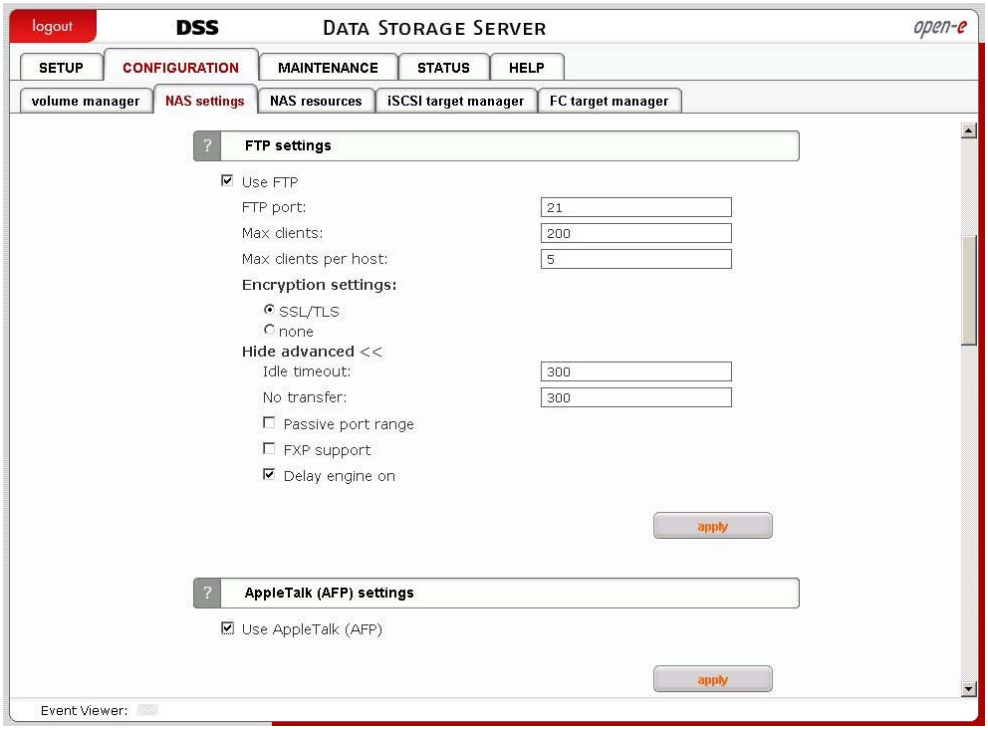
note

1. Workgroup name cannot begin/end with space and cannot contain special characters such as: ~!@#$^&()+[]{}*;:'".,%|<>?/\=`
2. When changing the authentication method you run the risk of losing ACLs (Access Control Lists). In this case please set user/group access rights for every share and reset ACLs.
3. If SMB authentication is enabled, please edit the Windows registry: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanworkstation\parameters\ and change the value of the DWORD 'enableplaintextpassword' key to '1' hexadecimally.

Function: NFS settings

Click **Use NFS** to enable access to shares and/or snapshots via NFS. Network File System (NFS) is a protocol for distributed file system which allows a computer to access files over a network as easily as if they were on its local disks.

note If the hosts file has an entry in the DNS field but does not have the reverse DNS entry then the connection to NFS will not work.



Function: FTP settings

To enable FTP services check Use FTP.

FTP port

Determines the port the FTP service is listening to.

Max clients

Limits the total number of concurrent FTP connections.

Max clients per host

Limits the total number of connections originating from a single host.

Min. port
Minimal port number for the FTP passive mode. Needs to be smaller than the maximum port number.

Max. port
Maximal port number for the FTP passive mode. Needs to be greater then 1024.

Encryption settings

SSL
Data transfer will be encrypted with the SSL protocol.

None
Data will be send without any encryption.

Advanced settings

Idle timeout
This option allows you to set a timeout (in seconds) for an idle connected client. An idle client does not receive any data on either the control or the data connection. Inputting 0 equals no timeout.

No transfer
This option allows you to set a timeout (in seconds) for a connected client whose data connection is idle (e.g. it is not sending or receiving data). Control connection is not subject to this timeout. Inputting 0 equals no timeout.

Passive port range
Range of port addresses when FTP service is connected in passive mode.

FXP support
Enables support for the File eXchange Protocol.

Delay engine on
Enables runtime delay. It is recommended to keep this option on for security purposes.

note The possibility to access the server via FTP (File Transfer Protocol) offers additional flexibility, as users can access storage either from the Intranet or Internet. An FTP client (e.g. SmartFTP) is ideal, but the Internet Explorer or a similar browser is also suitable.

To establish a connection, the FTP client needs several pieces of data:

- IPaddress: 192.168.0.220 (this is the standard address)
- Port: 21
- User: anonymous
- Password: 123

Access rights allocation is done via the IP address of the PC currently in the process of accessing. Read access is therefore granted on the basis of these usually typical and anonymous login data. As a standard, the FTP server uses port 21, but that can be changed via the FTP port setting. If you use the Internet Explorer when accessing, you need to enter the following data into the address line: *ftp://192.168.0.220*. You will not be prompted to enter the username and password, as the Internet Explorer first establishes an anonymous connection. If you have changed the FTP port, add this information to the address line the following way: *ftp://192.168.0.220:4711* (in this example, 4711 represents the new port number).

How to enter IP address

In order to allow specific computers access enter the privileged IP addresses separated by semicolons.

For example: 192.168.0.1; 192.168.0.2; 192.168.0.222; etc.

In order to assign writing privileges to the entire address area between 192.168.0.1 and 192.168.0.254 enter:

192.168.0.0/24

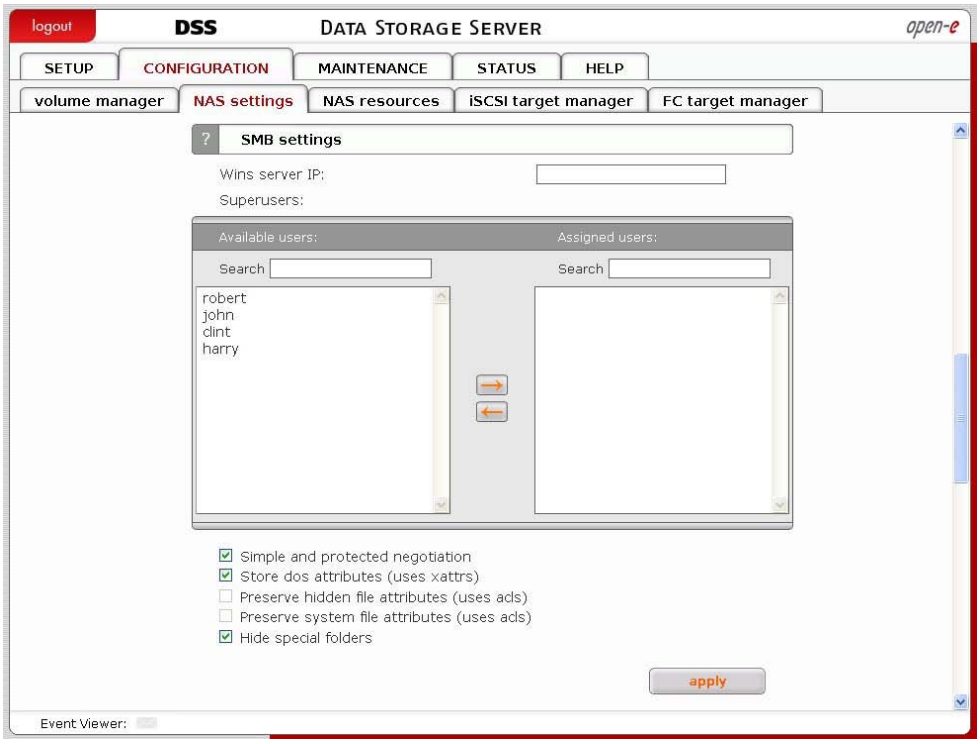
In order to assign writing privileges to the entire address area between 192.168.0.1 and 192.168.255.254 enter:

192.168.0.0/16

There are many more combinations possible. You can find additional information about IP calculation on the Internet.
Just search for **ipcalc.** For example, *192.168.0.1/28* will set the range from 192.168.0.1 to 192.168.0.14; *192.168.0.100/29* will set the range from 192.168.0.97 to 192.168.0.102 etc.
You can easily calculate the network IP range using an IP address calculator like the one available here: http://www.subnet-calculator.com/

Function: AppleTalk (AFP) Settings

Here you can activate the AppleTalk protocol in the network to access shares on the NAS Server.



Function: SMB settings

This function allows you to edit SMB protocol specific parameters. There are several options you can change:

Wins server IP

If you have a WINS server on your network you should indicate the WINS server IP here..

Superuser

Superuser is a user who has the permission to take ownership of folders and files which belong to other users. These rights can be useful when an administrator wants to change access rights (ACL) for folders or files created by other users. To give superuser privileges to a user select them in the menu. Superuser privileges allow to modify, remove and add new files to the share. This includes all files and directories, even those the superuser does not have ownership of.

Simple and protected negotiation

Simple and Protected Negotiation (SPNEGO) is a negotiation protocol. If you use a PDA device to access shares on NAS please uncheck it.

note To connect to your PDA device use netbiosname, not IP address.

Store DOS attributes (uses xattrs)

This option enables you to preserve all MS-DOS attributes using Linux xattrs attributes. It cannot be set when you are using the options **Preserve hidden file attributes** or **Preserve system file attributes**.

Preserve hidden file attributes and Preserve system file attributes (uses ACLs)

These options enable you to preserve the following MS-DOS attributes: hidden and system. These attributes are mapped to x (EXECUTE) attributes for group and others in the Linux POSIX ACL. Windows ACL permissions are also mapped to Linux attributes. In order to avoid attribute mismatch, it is strongly recommended to disable these options. These cannot be set when you are using the **Store DOS attributes** option.

Hide special folders

This option hides special folders that are created by MAC OS/OSX systems. With that option enabled, users cannot see MAC OS/OSX system files via the SMB protocol

MAC OS/OSX system files:

6. .DS_Store,
7. .AppleDouble,
8. Temporary Items Network,
9. Trash Folder,
10. TheFindByContentFolder,
11. TheVolumeSettingsFolder,
12. .AppleDesktop,
13. .AppleDB,

14. Icon?,
15. .VolumeIcon.icns,
16. .FBIndex,
17. .FBClockFolder.

note Changes to the ACLs and/or xattrs settings need to be confirmed seeing as these changes can make files invisible to users. It is not recommended to change these settings on severs that already have some data stored. If after changing the **Preserve hidden file attributes (uses ACLs)** and/or **Preserve system file attributes (uses ACLs)** settings any files are not visible, users can use the following command which will remove the hidden attribute from the files: *attrib -S -H x:|*.* /s /d* ,where: *x* - network drive.

Any change to SMB settings will disconnect users that are currently connected. These also need to be accepted by users; the acceptance prompt will only appear if any users are connected to SMB. If the user clicks the **Cancel** button the settings will be saved but the connection to SMB will not be reset

Function: UID & GID synchronization

Synchronize UID and GID database with NIS server

Enable this option if you want to synchronize user id and group id database with NIS server.

NIS server domainname

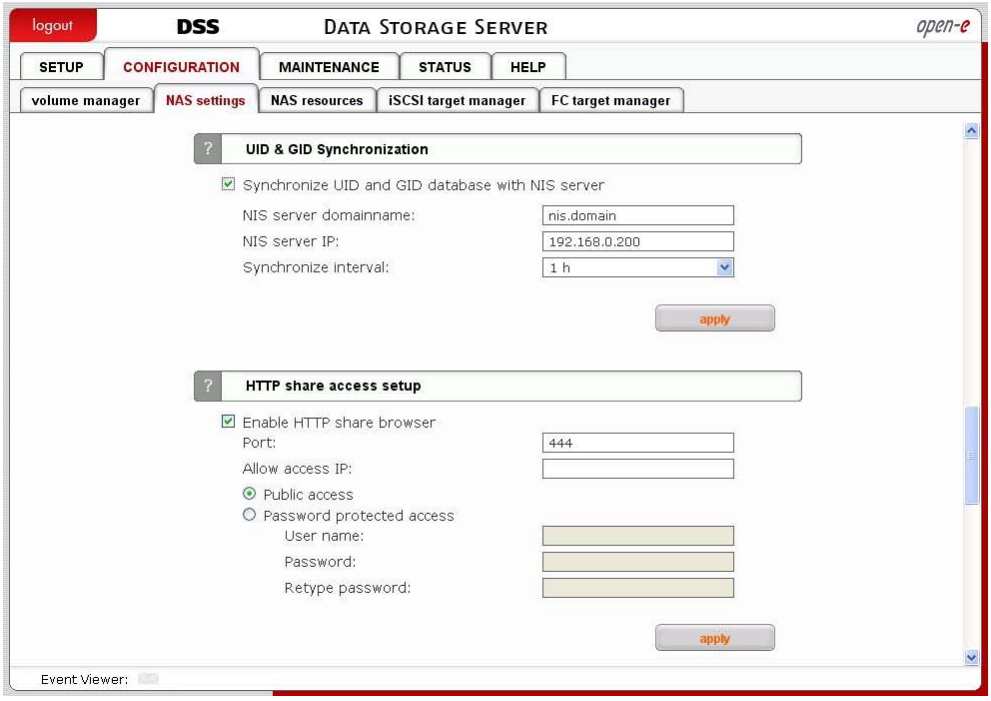
NIS server domainname without **http** prefix.

NIS server IP

IP address of your NIS server.

Synchronize interval

Time period when synchronization will be run.



Function: Http share access setup

Here you can set up a http access to shares.

Turning this option on will enable the http share browser. Access to shares will be available via a Web browser. You can browse and download your files when you enter the following in the address line:

https://SERVER_IP_ADDR:PORT
https://SERVER_NAME:PORT

For example:

https://192.168.0.220:444

Port

Port on which the http share browser will be available, the default port is 444..

Allow access IP

List of IP addresses which will have access to the http share browser

You can set up one of the following access modes for the shares:

Public access

When this option is set, everybody will have access to the shares over http.

Password protected access

When this option is set, access to the shares will be password protected.

User name

Please enter a username that will have access to the shares over http.

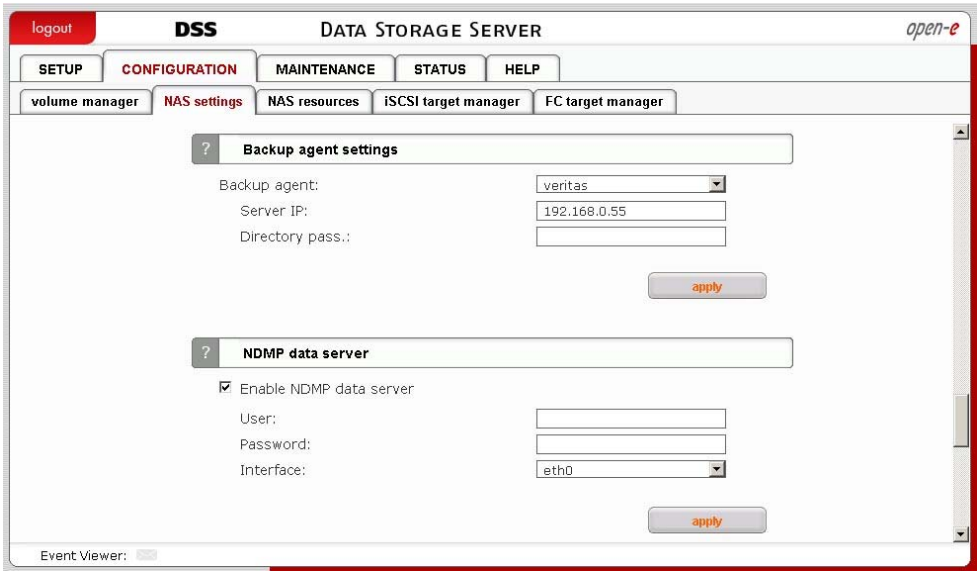
Password

User password.

Retype password

User password confirmation.

note In order to access your share via a Web browser, you need to enable the **Use http share access** option for the share in question. You can do this via the **Http share access** function in the CONFIGURATION → NAS resources → [share_name] menu



Function: Backup agent settings

Here you can enable one of pre-installed backup agent (client). Currently, agents are supported:

- Veritas - Backup Exec,
- Dantz - Retroclient,
- CA - BrightStor.

If you enable the backup agent, your backup server will find the agent running on the NAS server and will use it for backup. Alternatively, you can find and backup the NAS shares over the network neighborhood. But using a backup agent will be significantly faster.

Veritas:

Here you need to provide an IP address of a server running the Backup Exec. The Backup Exec may prompt for the **Directory Pass** password.

Backup:

1. in the Veritas Backup Exec set up a user in the menu Network → Logon Account Management,
2. next enter the password provided earlier in the NAS Server function Backup client setting,
3. after clicking Backup a Backup Job Properties window will appear, in which a list of network shares will be displayed,
4. after clicking the Remote Selections branch followed by Unix Agents, a NAS server name will appear,
5. after clicking the server displayed as "NAS_server/logical volume," a window called Logon Account Selection will appear in which you need to select the same username as in step 1,
6. after user selection, the logical volume and NAS server shares will appear. Selecting the correct share and clicking Run Now will cause this share to be backed up.

note Under some settings, the Logon Account Selection window will not appear automatically. In this case you need to right-click the servername ("NAS_Server/share_volume") and select Connect As... in the context menu. Only then will the Logon Account Selection window appear.

Restore:

1. after selecting Restore, a Restore Job Properties window will appear,
2. in Properties → Source on the left side of the window click Selection, and the name of the NAS server whose shares have been backed up earlier will be displayed,
3. choose the folder you want to be restored from the correct backup file,
4. from the Source → Resource Credentials menu choose a user account for the NAS (NAS_server/share_volume) server and click Run Now.

hint In order to use a incremental method, select it from the Setting → General → Backup Method menu. Please use the following method: "Incremental - Using modified time" (Reset Archive bit - does not work on XFS partition types).

BrightStor:

Allow IP or Network IP:

Please enter the appropriate backup server's IP address in order to grant it access to the NAS server. If you leave this field empty, all BrightStor backup servers in the network will have access to the NAS server.

User:

After providing a username only this BrightStor user will have access to the NAS server. If left empty, all users will be able to access the NAS server.

Before you start to back your data up you need to configure the device the backup will be stored on and add your NAS server as the source. Please follow these steps in order to perform this:

1. from the menu bar select Configuration, followed by Device configuration. The Device configuration wizard will appear. It will assist you in configuring backup devices on your server,
2. select Windows Server and click Next,
3. within the options select File System Device and click Next,
4. click Add, which will cause a file system device to be added to the list,
5. click on the Location field in the newly created entry and select the path that will be mapped to the file system device,
6. click the Finish button to complete the Device configuration wizard,
7. click Exit to quit device configuration,
8. the last thing to do is to format your newly created file system device. In order to do this, choose Device from the Quick start menu and select your newly created filesystem device,.
9. click on the Format button and the format form will appear,
10. enter the media name and click OK to format the media.

NAS server configuration:

1. select Backup from the Quick start menu,
2. right-click on Unix/Linux Systems in the Source branch,
3. select Add Machine/Object and the Add client form will appear,
4. enter the host name and the IP address of your NAS server,
5. click Add in order to add your NAS to the list,
6. click Close to quit the Add Machine/Object form.

Backup:

1. select Backup from the Quick start menu,
2. in the Source branch, select the NAS server volumes you want to back up,
3. click the Start button and the Security and agent information form will appear,
4. click the Agent button if you want to modify NAS server information,
5. click OK and the Submit job form will appear,
6. if you want to start the backup process later make sure that the job execution time is properly set,
7. enter the job description and click OK to start the backup process.

Restore:

1. select Restore from the Quick start menu,
2. from the Source branch, select the NAS server volumes you want to restore,
3. click Start followed by OK, and the Submit job form will appear,
4. if you want to start the backup process later make sure that the job execution time is properly set,
5. enter the job description and click OK to start the restore process.

Retroclient:

NAS server configuration:

1. select Configure from the menu, then click on Clients and the Backup Clients form will appear,
2. click Add and the Add backup client form will appear,
3. enter the IP address of your NAS server and click on Add. The Connection form will appear,
4. enter the password to connect to the NAS server and click OK. The password for Dantz Retroclient is set to admin. The NAS server is now properly configured to work with Dantz Retroclient..

Backup set creation:

5. from the menu, select Configure followed by Backup sets and the Backup sets form will appear,
6. click on the Create New button and the Backup sets creation wizard will appear. Click on Next,
7. from the backup media options, select File and click on Next,
8. enter the name and the location where the backup will be stored. Click on Next,
9. select backup set security and click Next,
10. click on Finish, which will conclude the backup set creation process.

Backup:

1. select Backup from the menu, then click on the Backup button and the source selection form will appear,

2. select the NAS server volumes which you would like to back up. Click OK,
3. the Backup process form will appear, click on Backup to start the backup process.

Restore

1. select Restore from the menu, then click on the Entire volume button,
2. select the source backup set from which you want to perform the restore process,
3. select the destination NAS server volume,
4. click OK followed by Replace to begin the restore process..

The password for Dantz Retroclient is set to "*admin*".

note Full computer name in Windows can be found in preferences of "My computer" → Computer Name → Full Computer Name.

Function: NDMP data server

NDMP (Network Data Management Protocol) is a protocol for direct communication between NAS and backup devices. It bypasses the backup server, thus providing better speeds.

In order to use NDMP, click the **Enable NDMP data server** checkbox.

User

Enter here the user authorized to access the NDMP server. The same user name and password should be configured at the NDMP client software.

Password

Enter here the password for the authorized user.

Interface

Select the network interface to be used for the NDMP server.

note The NDMP Data server can be used with the following software:

NDMPCopy

NDMPcopy transfers data between filers using the Network Data Management Protocol (NDMP). When you use rsh to perform this transfer, the data flows from the source machine to the rsh host and then again from the rsh host to the destination machine. This can put a double load on the network and unnecessary load on the rsh host. With NDMPcopy, data is transferred directly from the source machine to the destination machine, and the NDMP host and network are not burdened with the extra load. The program can be downloaded from the official NDMP web site (http://www.ndmp.org).

NetBackup

NetBackup should be configured with following parameters:

- at least one NDMP host should be configured,
- at least one client of the /"NDMP, NDMP/" type should be added.

Steps for backup process in 3-way mode:

- it is necessary to run **Device Configuration Wizard** and add at least two NDMP hosts (the first is a source and the second is a destination with the tape drive). It is also possible to add NDMP hosts from **Media and Device Management/Devices/NDMP Hosts,**
- next, create policy rules and set policy storage unit which is identical to the destination NDMP host,
- finally, set the ndmp client which is the origin for the backup process.

After the steps above have been completed the backup in 3-way mode can be established from the NDMP host to the storage unit through NetBackup management.

note The Data Storage Server with the enabled NDMP Data server functionality can be used in the following data backup scenarios:

Server to server copy with NDMPCopy

The data can be moved between two Data Storage Severs using the NDMPCopy utility.
To copy data user must define source and destination and authentication credentials for data servers. The command line for copying data is the following: ndmpcopy source destination [options].

Source has the following format: src_filer:src_dir, where src_filer is the name of the filer being copied from, and src_dir is the absolute pathname of the directory being copied. The destination has the format dest_filer:dest_dir, where dest_filer is the name of the filer being copied to, and dest_dir is the absolute pathname of the directory to which the source directory is being copied. The destination directory is created if it does not already exist.

Options:

- *-sa none | user:password source authentication*. If this flag is followed by the word *none*, then no authentication is used. If it is followed by a user specification then text authentication is used. The default is text authentication with user root and no password.
- *-da none | user:password destination authentication*. If this flag is followed by the word *none*, then no authentication is used. If it is followed by a user specification then text authentication is used. The default is text authentication with user root and no password.
- *-sport port*. NDMP port to use for the source filer. This should normally be left unchanged. The default is 10000.
- *-dport port*. NDMP port to use for the source (DESTINATION?) filer. This should normally be left unchanged. The default is 10000.
- *-dhost hostname*. The destination host for data transfer (if it is not the same as the destination NDMP host). This is useful if your destination host has multiple network interfaces and the bulk data should go over a different link than the NDMP connection. One example of this would be if the filers are connected to the host running ndmpcopy via a 10 Mb/s ethernet, but the filers are linked together by a 100 Mb/s ethernet as well. The hostname should be specified by:

- *-dhost*. The name or IP address of the interface on the destination machine.
- *-level 0 – 9*. Without the *-level* option ndmpcopy always performs a level 0 dump. When the *-level* option is provided the restore process is requested to "incrementally restore" the dumped files and uses the *restore_symboltable* file in the process so that incremental dumps can be carried out. Each restore will leave behind a *restore_symboltable* file regardless of this option.
- *-v*. Increase the verbosity. The default (level 1) will display the dump log messages received from the dumping filer. One *-v* (level 2) displays NDMP status information as well.
- *-q*. Increase the quietness (decrease the verbosity). This flag will counteract any *-v* flags present. If there are more *-q* flags than *-v* flags, no status information will be displayed. Usually it does not make sense to specify both *-q* and *-v*, but it is a possibility.

Backup/restore with regular backup software

You can use the **NetBackup** application to backup the data through the NDMP DATA interface. It is necessary to install the NetBackup server and client software as explained in the original NetBackup Install Guide.

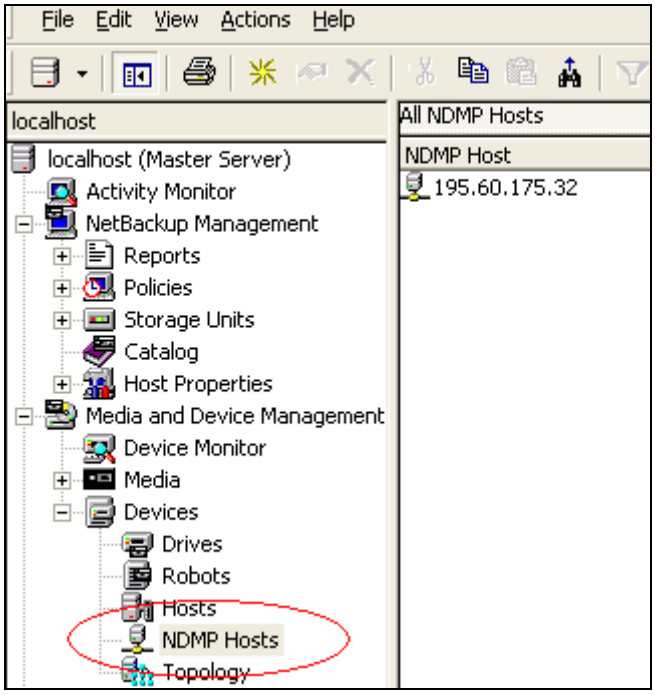
Next, configure the NetBackup application to use the remote/local NDMP server as follows:

- add and configure devices (robots for the tape managing, disk arrays, tapes),
- add the storage unit which defines the media on the NDMP host and the media server,
- create the NDMP policy and define:
  - attributes,
  - NDMP client to backup,
  - path on this client to the backup,
  - storage unit to be use,
  - schedules.

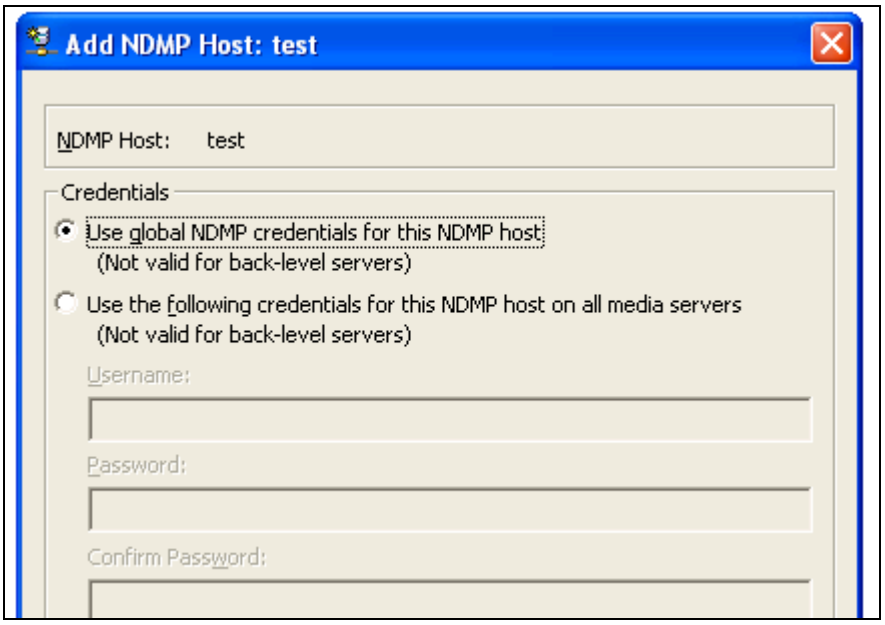
How to configure NDMP in NetBackup

Configuration of storage devices.

1. To start configuring storage devices in the NetBackup Administration Console, select Device Management → Devices → NDMP Hosts to view detailed information about the NDMP servers that are referenced in your Media Manager configuration.



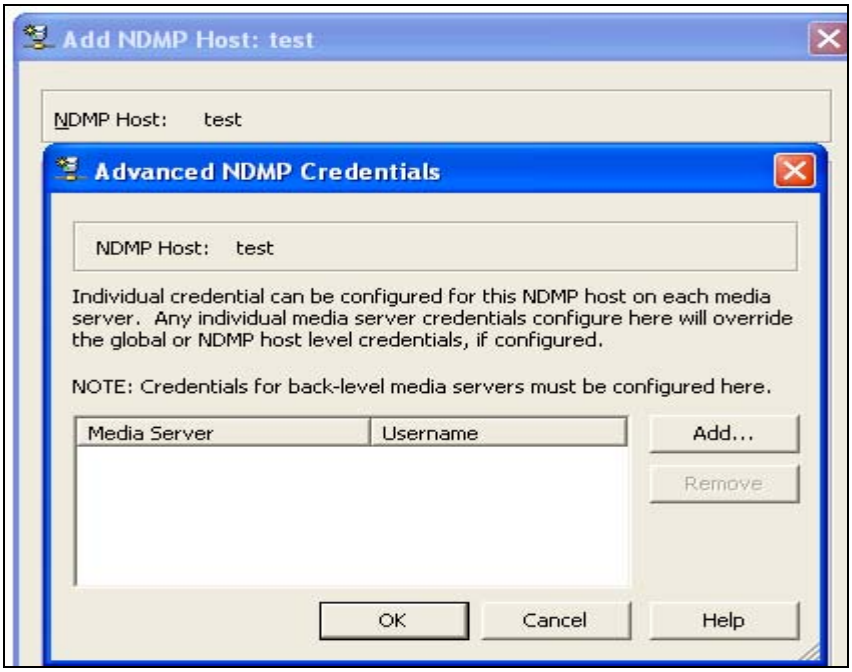
2. To add an NDMP host, select Actions → New → New NDMP Host. Specify the NDMP host name. After that, the new NDMP Host dialog appears.



Specify the following:

- Use global NDMP credentials for this NDMP host.
  Select this option to enable all NetBackup media servers under the master server to access this NDMP host using a pre-defined global NDMP login. This login is created under Properties → Master Server → Properties → NDMP, on the NDMP Global Credentials dialog.
- Use the following credentials for this NDMP host on all media servers.
  Select this option to enable all NetBackup media servers connected to the NDMP host to access the NDMP host using the login and password you specify on this dialog.

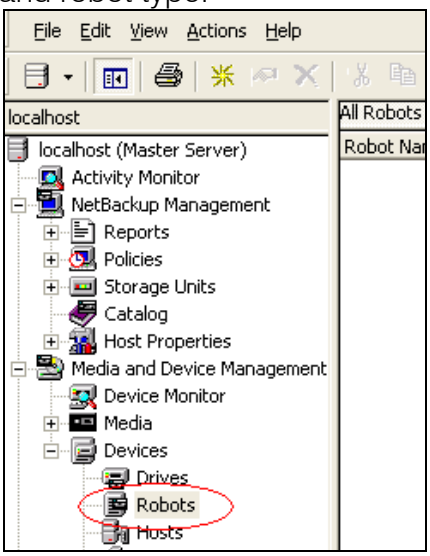
- Use different credentials for this NDMP host on each media server.
  Select this option to specify NDMP logins for particular NetBackup servers, then click Configuration. The Advanced NDMP Credentials dialog appears.

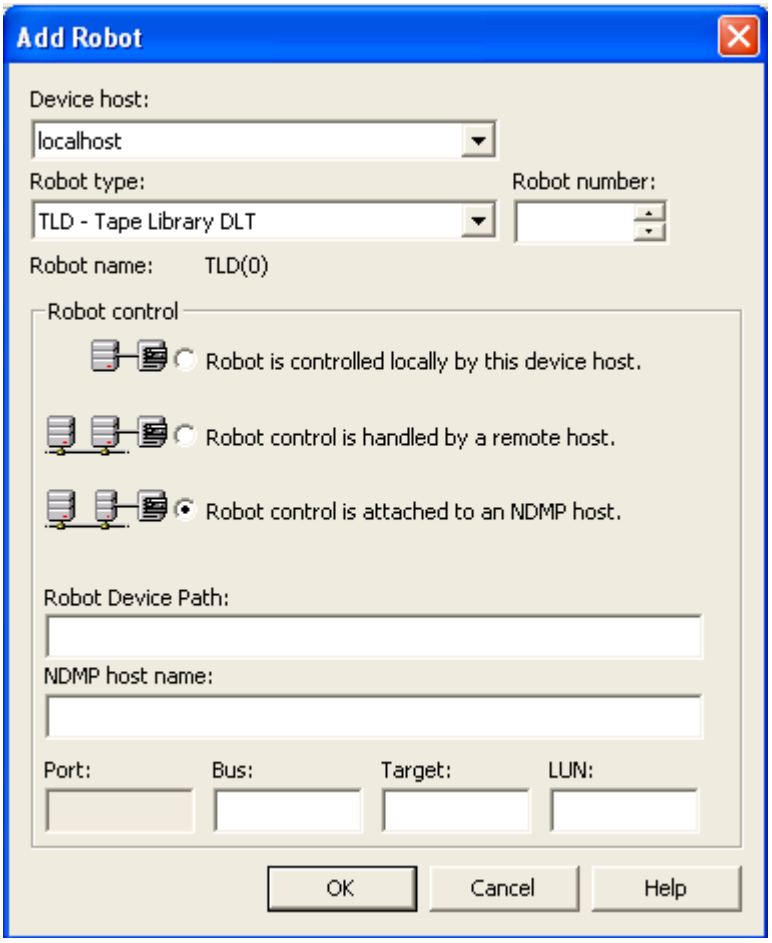


  Press Add to add one or more servers and specify each server credential as in the previous case. To perform three-way backups, you must authorize access to the desired NDMP host as described in the previous section.

- Three-way backups: for the hostname, specify the NDMP host that has no attached tape drive.
- NDMP to Media Manager backups: for the NDMP host name, specify the NDMP host that will be backed up to the media manager storage unit defined on the NetBackup server.

3. To start configuring robots in the NetBackup Administration Console, select Media and Device Management → Devices → Robots. To add a robot, select Actions → New → New robot. After that, the new Robot dialog appears. The properties that appear in this dialog vary, depends on the server platform type and robot type.





Specify the properties for the robotic library.

Media Manager Robot Types

Robot Type	Description
ACS	Automated Cartridge System
ODL	Optical Disk Library
TL4	Tape Library 4MM
TL8	Tape Library 8MM
TLD	Tape Library DLT
TLH	Tape Library Half-inch
TLM	Tape Library Multimedia
TSH	Tape Stacker Half-inch

Robot Control Configuration Overview

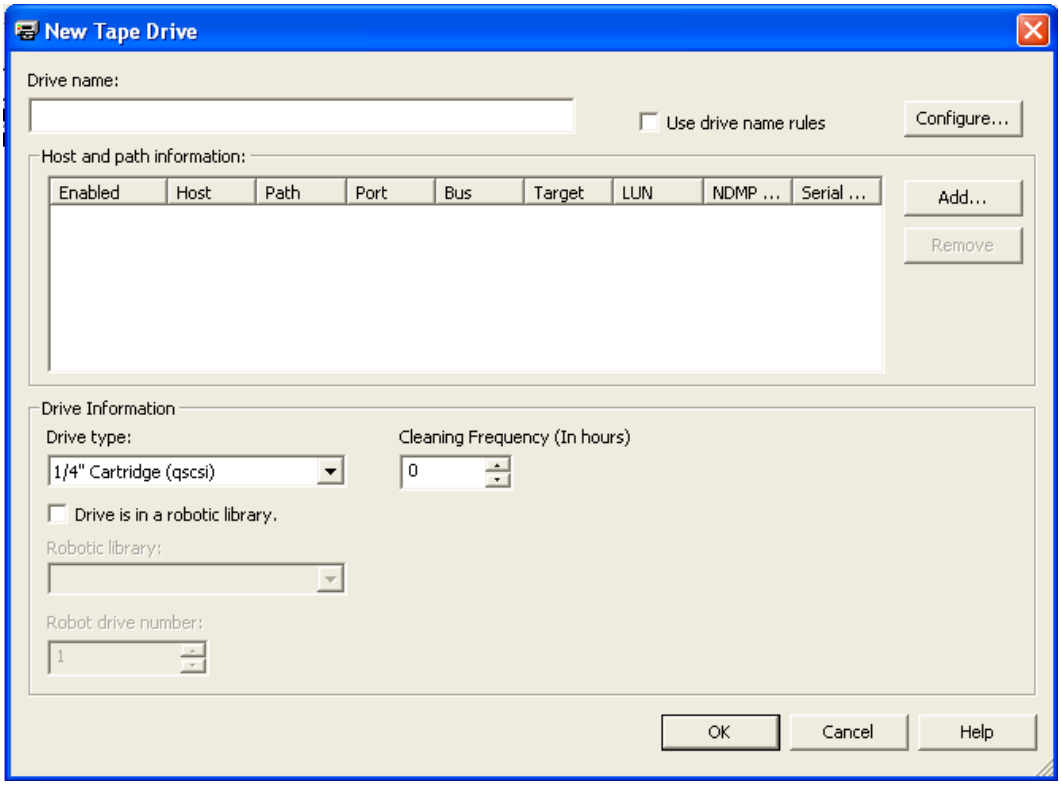
Type of Robot Control	Media Manager Robot Type	Supported Media Server	Platform Information Required for Configuration
Local	ODL	AIX, Solaris, and HP-UX (except HPIA64)	Robotic device file
Local	TL4	UNIX	Robotic device file
Local	TL4, TL8, and TLD	Windows	Robot device or Port, Bus, Target and LUN

Type of Robot Control	Media Manager Robot Type	Supported Media Server	Platform Information Required for Configuration
Local	TL8	UNIX	Robotic device file
Local	TLD	UNIX	Robotic device file
Type of Robot Control	Media Manager Robot Type	Supported Media Server	Platform Information Required for Configuration
Local	TLH	Local UNIX (except HPIA64, AIX, Linux and Linux64) and Windows	Library name
Local	TLH	AIX	LMCP device file
Local	TSH	AIX, Solaris, Linux, and Linux64	Robotic device file
Remote	ACS	All except HPIA64 and Linux64	ACSLS host
Remote	TL8	All	Robot control host
Remote	TLD	All	Robot control host
Remote	TLH	All (except Linux64)	Robot control host
Remote	TLM	All (except Linux64)	DAS/SDLC server
NDMP	ACS, TL8, TLD, and TLH	Windows, AIX, Solaris, HP-UX, and Linux (except Linux64)	NDMP host name and Robot device

For robot control attached to an NDMP host, you must specify Robot Device path, NDMP Host name and SCSI coordinates (only for windows hosts).

After pressing OK, a prompt appears asking whether you want to stop and restart the NetBackup Device Manager Service; (this also stops and restarts any robotic processes). If your changes are complete, answer yes to this prompt.

4. To add a drive in the NetBackup Administration Console, select Media and Device Management → Devices. Select Actions → New → New Tape Drive. The properties that appear in this dialog vary slightly, depending on the type of host platform and the robot type.



Drive Name

This name is used to identify the drive. It is important to note that each drive name must be unique. Descriptive names are recommended. Drive names are limited to 48 characters.

Drive Name Rule

Select the Use Drive Name Rules checkbox to automatically create drive names based on
the rules you specify. You can use drive name rules when a drive is first added to your configuration. The default drive name rule creates names in the format VendorID.ProductID.INDEX. For example, the default name for a Quantum DLT8000 drive is QUANTUM.DLT8000.000. You can update the global drive name rule or create a local drive name rule. A global rule is stored in the EMM database and used on all connected device hosts. The global rule is used for the drive name unless a host-specific rule, or local rule, is specified.

Use any of the following drive attributes as part of a drive name rule.

- Host name
- Robot number
- Robot type
- Drive position
- Drive position information varies depending on the robot type. Drive position information can be ACS coordinates, TLM/TLH vendor drive name, or simply the robot drive number.
- Drive type
- Serial number
- Vendor ID
- Product ID
- Index

A Custom Text field is also available which accepts any of the allowable Media Manager characters.
Press Configure to use the name configuration wizard.

Host and Path Information

Specify the device host and path for the drive by pressing Add. You can specify multiple paths to the same physical device. Adding multiple paths may cause the drive to become shared.

Drive Type

Specifies the type of drive that you are adding

Media Manager media types

Media Type	Description
QCART	1/4 inch cartridge tape
HCART	1/2 inch cartridge tape
HCART2	1/2 inch cartridge tape 2
HCART3	1/2 inch cartridge tape 3
4MM	4MM cartridge tape
8MM	8MM cartridge tape
8MM2	8MM cartridge tape 2
8MM3	8MM cartridge tape 3
DLT	DLT cartridge tape
DLT2	DLT cartridge tape 2
DLT3	DLT cartridge tape 3
DTF	DTF cartridge tape

Tape drive specification examples

Manufacturer	Media type	NetBackup default drive type
Certance		
	LTO	HCART
Exabyte		
	VXA-2	8MM2
HP		
	Ultrium 230 (LTO)	HCART
	Ultrium 460 (LTO2)	HCART2
	Ultrium 960 (LTO3)	HCART3

Manufacturer	Media type	NetBackup default drive type
IBM		
	3580 Ultrium (LTO)	HCART
	3580 Ultrium 2 (LTO2)	HCART2
	3580 Ultrium 3 (LTO3)	HCART3
	3590B	HCART
	3590E	HCART
	3590H	HCART
	3592J	HCART2
Quantum		
	DLT 4000	DLT2
	DLT 7000	DLT
	DLT 8000	DLT2
	SDLT 220	DLT3
	SDLT 320	DLT2
	SDLT 600	DLT
	SLT1	DLT
	DLT VS80	DLT
	DLT VS160	DLT
	DLT-V4	DLT
	LTO-2	HCART2
	LTO-3	HCART3
Sony		
	AIT-1	8MM
	AIT-2	8MM
	AIT-3	8MM2
	AIT-4	8MM3
	S-AIT	HCART
	DTF-1	DTF
	DTF-2	DTF
STK (Sun StorageTek)		
	T9840A	HCART
	T9840B	HCART
	T9840C	HCART3
	T9940A	HCART2
	T9940B	HCART2
Tandberg		
	LTO	HCART
	LTO2	HCART2
	LTO3	HCART3
	VXA-172	8MM3

Manufacturer	Media type	NetBackup default drive type
	VXA-320	8MM3
	SLR7	QSCSI
	SLR75	QSCSI
	SLR100	QSCSI
	SLR140	QSCSI

Cleaning Frequency.

NetBackup does not support cleaning drives in some robot types. If you want to set up a frequency-based cleaning schedule for the drive, set the number of mount hours between each drive cleaning. When you add a drive or reset the mount time to zero, Media Manager starts recording the amount of time that volumes have been mounted in that drive. If the drive is in a robotic library that supports drive cleaning and a cleaning cartridge is defined in that robotic library, cleaning occurs when the accumulated mount time exceeds the time you specify for cleaning frequency. The mount time is reset when the drive is cleaned. If you do not specify a cleaning frequency (the default frequency is zero), you can still use automated drive cleaning with the TapeAlert feature, provided the following conditions have been met:

- The drive supports TapeAlert.
- A cleaning volume has been defined in Media Manager.
- The host platform, robot type, and drive support drive cleaning.

If drive is robotic library specify option Drive is in robotic library and specify library parameters.

Robotic Library

This dialog box allows you to select any currently configured robotic library that can control the drive.

Robot Drive Number

Robot drive number specifies the physical location in the robot of the drive that you are adding. When adding more than one drive to a robot, you can add the physical drives in any order. For example, in a TL8 robot you can add drive 2 before drive 1. If you assign the wrong number Media Manager does not detect it initially, but an error will occur when the robotic control attempts to mount media on the wrong drive. Configuration of drives using the correct Robot Drive Number is important to the proper mounting and utilization of media. The Robot Drive Number, commonly set based on correlation of the drive serial number with drive serial number information from the robotic library, should be determined and validated before the device configuration is considered complete.

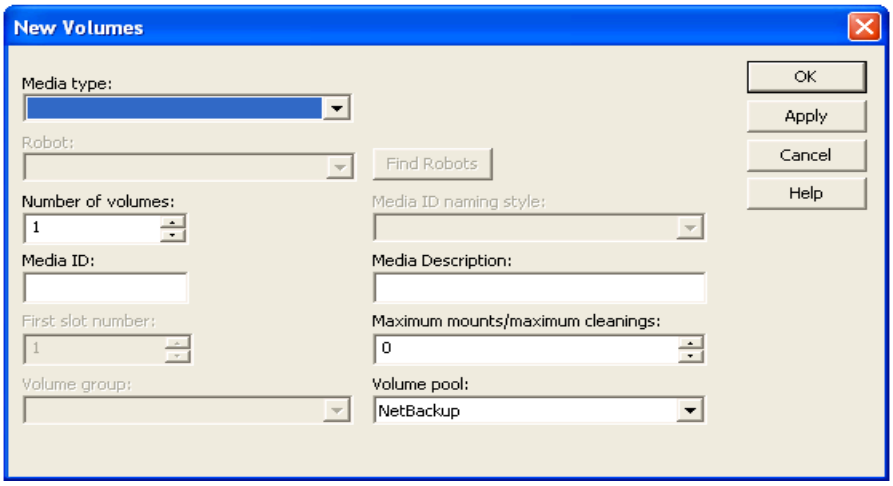
Configuration of media used.

Media Manager volumes are logical units of data storage or cleaning capability on media that have been assigned media IDs and other attributes, which are recorded in the EMM database. The attributes in the database include information to show the robotic location. This residence information for a volume includes the robot host, robot type, robot number, and slot location.

In the NetBackup Administration Console, select Media and Device Management → Media. A media management window similar to the following appears.

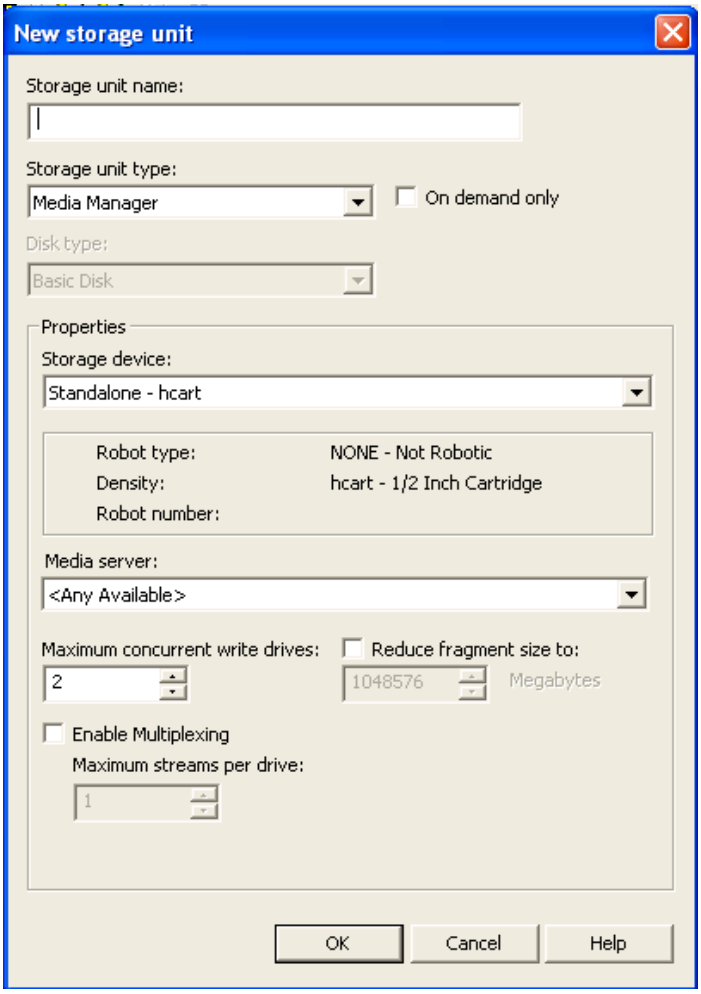
To add a volume, the Volume Configuration wizard can be used.
To use robot inventory to add robotic volumes, perform the Update Volume Configuration procedure. During the update, Media Manager assigns the media IDs and other attributes. You can also configure volumes automatically by inserting the media into a standalone drive. For an unused volume, NetBackup assigns a media ID, labels the volume, and uses it (if it needs a volume of that type for a backup). Media Manager adds the media ID (designated by NetBackup) and other attributes for the volume.

To add volume manually use Action → New → New Volumes.



Configuration of NDMP storage units

1. On the NetBackup master server, add an NDMP-type storage unit for the devices that will contain the backup data. In the NetBackup Administration Console, select NetBackup Management → Storage Units.
2. To create a new Storage Unit use Actions → New → Storage Unit . The New Storage Unit dialog appears.



For Storage unit name, enter a unique name for the storage unit.
For Storage unit type, select NDMP.
For On demand only: This specifies whether the storage unit is available only when a policy or schedule specifically requests it. If this option is not used, the storage unit is available to any NDMP policy or schedule.
For Storage device, select the type of device for this storage unit.
For NDMP host, specify the NDMP host where the tape drive is physically attached.

Configuration of NDMP polices.

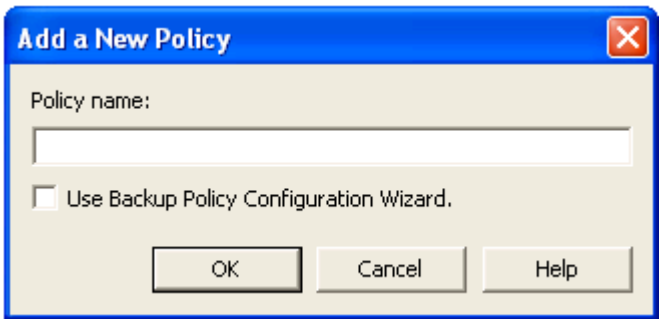
Backup policies define the rules that NetBackup follows when backing up clients. A backup policy can apply to one or more clients. Every client must be covered by at least one backup policy. The best approach to configuring backup policies is to divide clients into groups according to any backup and archiving requirements, then create a policy for each group.

To display information about all policies on the current master server, click Summary of All Policies. A summary of all polices appears in the Details pane, subdivided into panes displaying Polices, Schedules, Clients, and Selections. To display the general attributes for a specific policy, select that policy in the left pane. The Details pane shows the general attributes for that policy only. Double-click on a policy to display the attributes in tabs, available for editing.

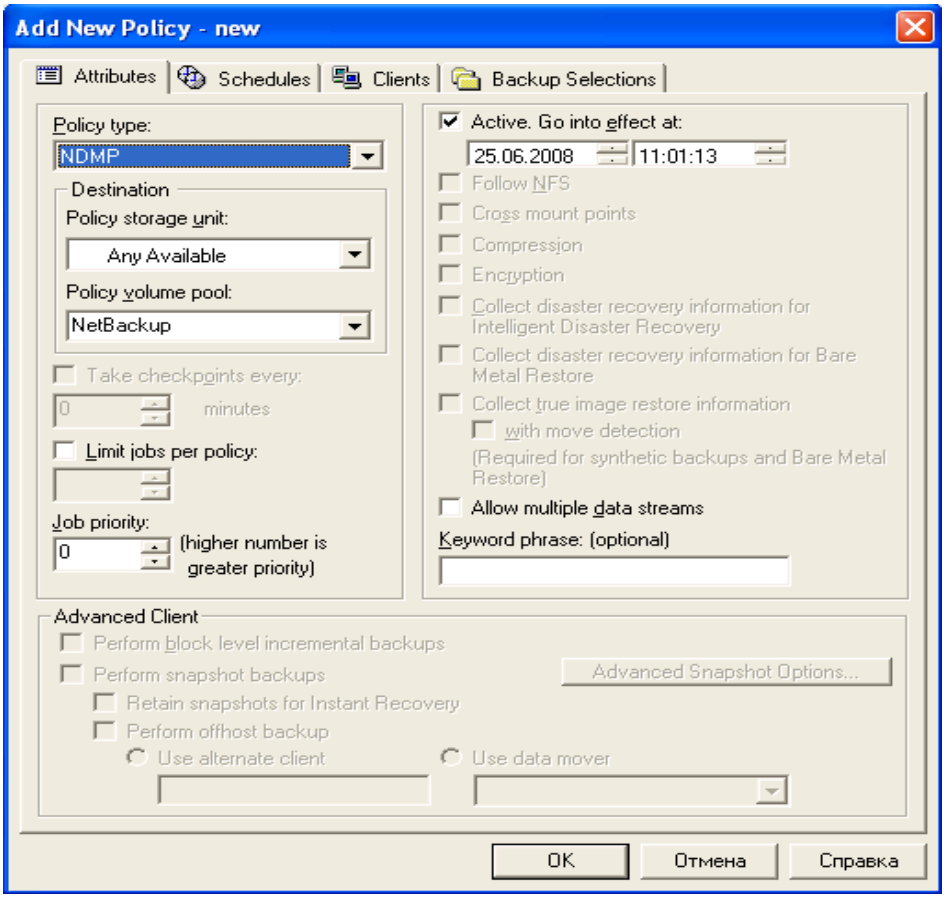
The easiest way to set up a backup policy is to use the Backup Policy Configuration Wizard. This wizard guides you through the setup process, simplifying the process by automatically choosing default values that are good for most configurations.
In the NetBackup Administration Console, select Master Server or NetBackup Management.
From the list of wizards in the Details pane, click Create a Backup Policy.

To create a policy rules without wizard.

1. In the NetBackup Administration Console, expand NetBackup Management → Policies. Select Actions → New → New Policy.



2. Type a unique name for the new policy in the dialog. Than a new dialog “Add New Policy – policy name” appears:



It is necessary to specify the following policy attributes in it:

a. Policy Type: NDMP
b. Policy Storage Unit:
   - If the NDMP host has more than one storage unit and you want to direct backups for this policy to a specific storage unit, specify the name of that storage unit.
   - For a three-way backup, specify a storage unit that was defined for the target NDMP host with attached tape.
   - For NDMP backup to Media Manager devices, specify a Media Manager storage unit defined for a device connected to a NetBackup media server.

Specify the following parameters for every client in NDMP policy:
Hostname: Name of the NDMP host
Hardware and operating system: NDMP NDMP

Files:
The Backup Selections list must specify directories from the perspective of the NDMP
host. Two examples:
/home/dir1/
/vol1

The following Backup Selections capabilities are NOT supported for an NDMP policy:

- Wildcards in pathnames. For example, /home/* is an invalid entry.
- Individual file names. Only directory or volume names are allowed.
- Exclude list (because client software is not installed on the NDMP host).

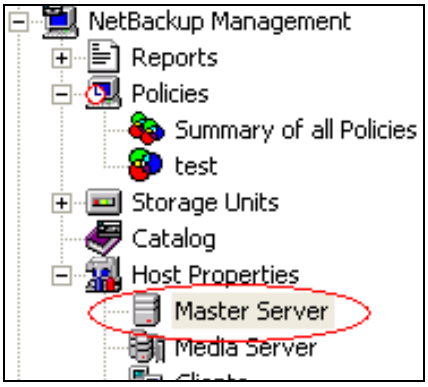
You can specify any of the following backup types in a schedule for an NDMP policy:

- Full
- Cumulative Incremental
- Differential Incremental

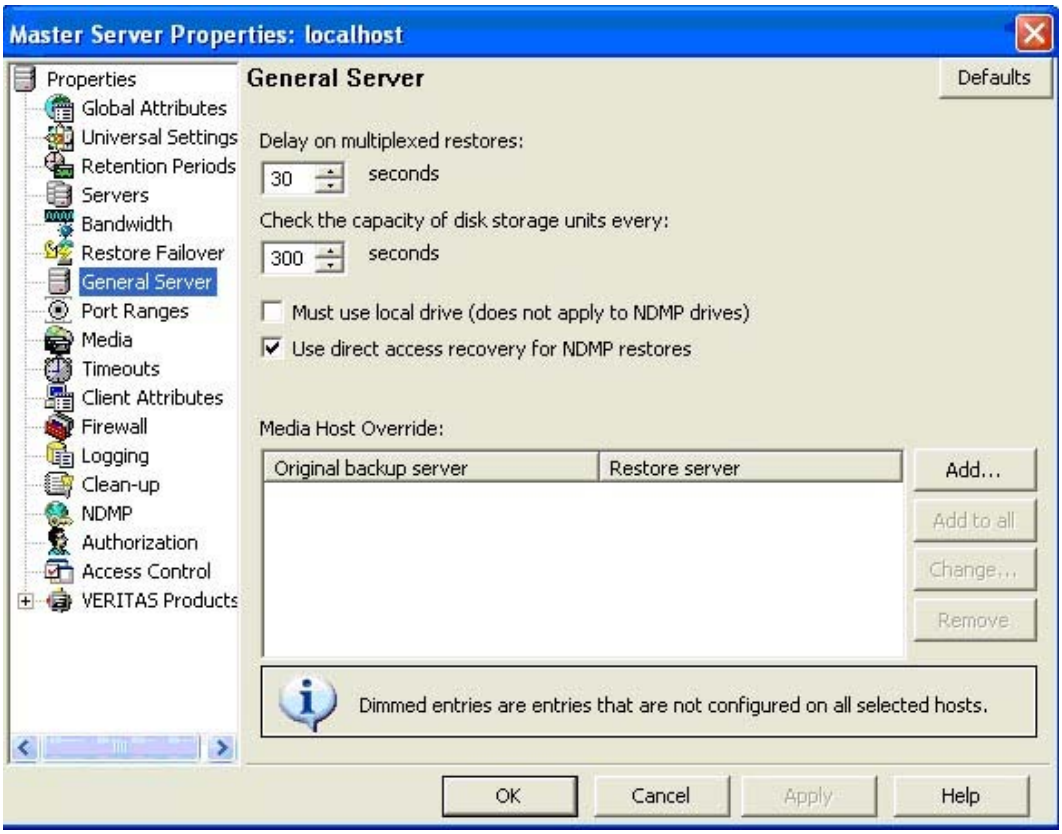
Specify Override policy storage unit only if this client of NetBackup (the NDMP host) has more than one storage unit and you want to use a specific storage unit for this schedule. In this case, the client must be the only client in this NDMP policy.

Customize server preferences.

By default NetBackup for NDMP is configured to use Direct Access Recovery (DAR). For each restore, NetBackup automatically determines if the use of DAR will speed up the restore. NetBackup uses DAR only when it will result in a faster restore. DAR can be turned off if desired. This may be necessary if you are having problems with DAR and your NDMP host is an older machine or is not running the latest NAS OS version. NetBackup restricts maximum files with DAR to 1024.



To change DAR setting in the NetBackup Administration Console, expand Host Properties and click on Master Servers or Media Servers. Right-click on the name of the server and select Properties.



Click on “General Server”. Uncheck the Use direct access recovery for NDMP restores box, and click Apply. This disables DAR on all NDMP restores.

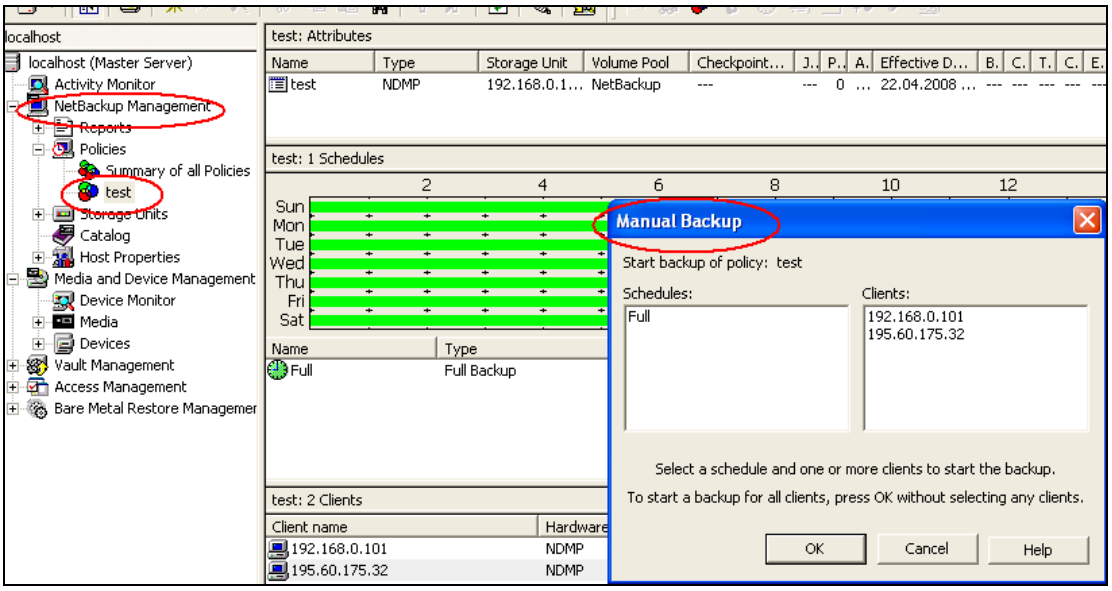
Backup process

Automatic Backup of an NDMP Policy

Use this item with properly configured NDMP policy scheduling.

Manual Backup of an NDMP Policy

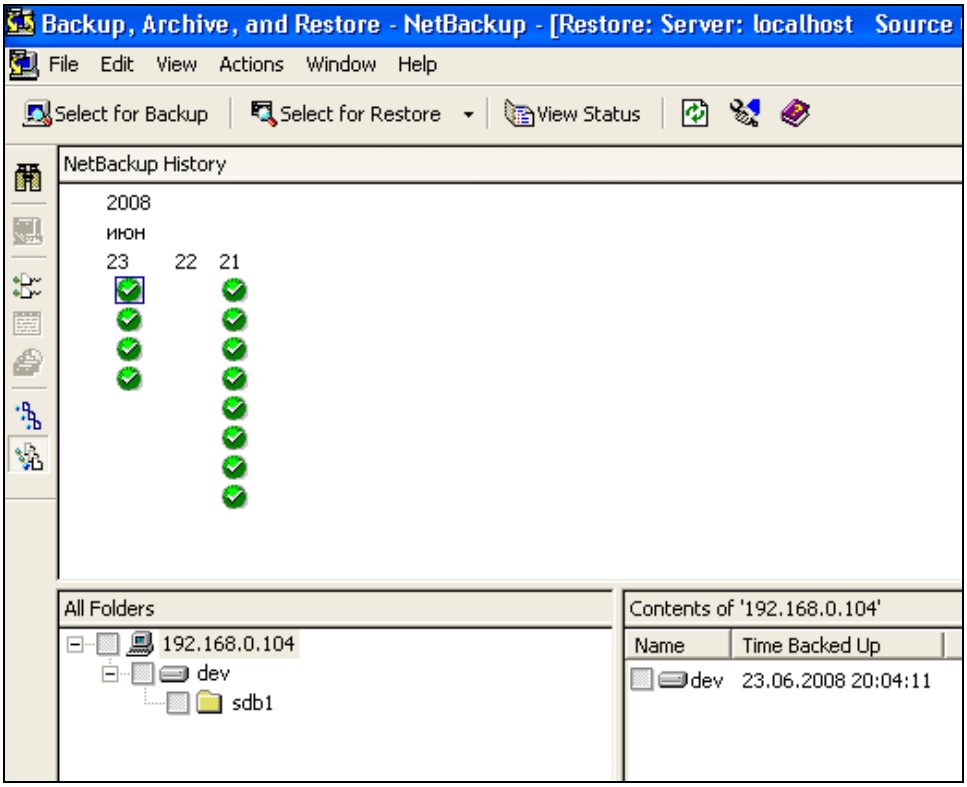
Click on Policies. Right click on the NDMP policy name and select Manual Backup from the pop-up menu. This opens the Manual Backup dialog.



In the Manual Backup dialog, select a schedule, then select the clients (NDMP hosts) that you want to back up. If you do not select any schedules, NetBackup uses the schedule with the highest retention level. If you do not select any clients, NetBackup backs up all configured
NDMP hosts. Click OK to start the backup.

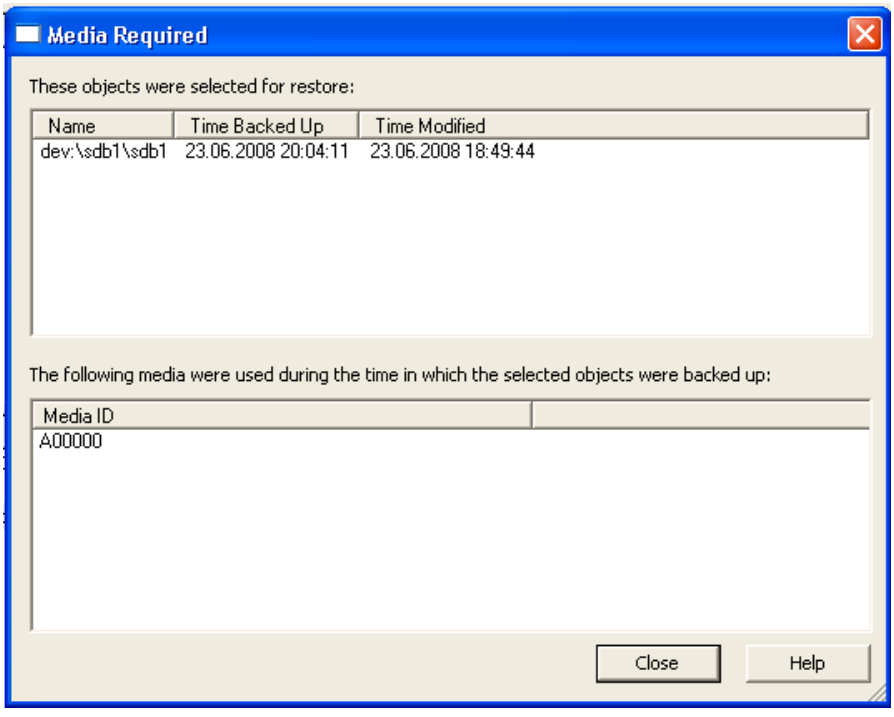
Restoration process

The administrator can use the Backup, Archive, and Restore interface on a NetBackup server (master or media server) to restore files to the NDMP host from which they were backed up, or to a different NDMP host. On the File menu, click Select Files and Folders to Restore, then click either from Normal Backup or from Archived Backup (depending on whether you are restoring from a normal backup or an archive).
There may be a delay while NetBackup reads information about the backups and builds the list of files you can restore. The title bar of the window displays the names of the server and client used for the operation.

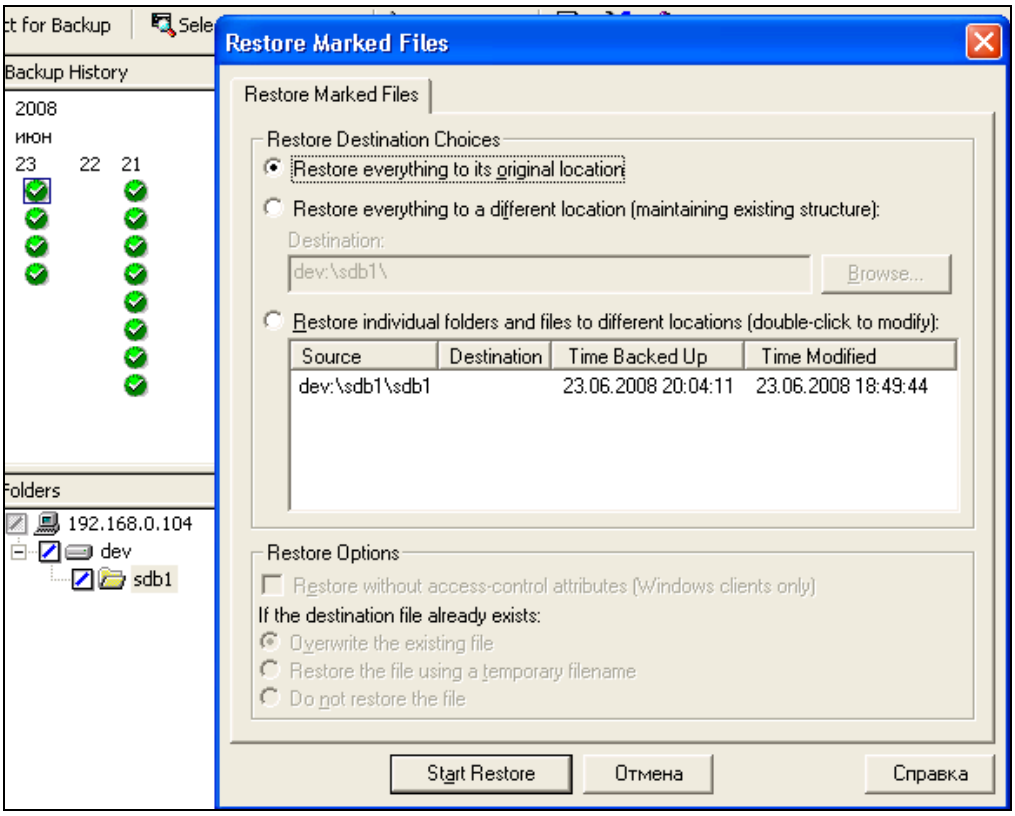


To select an item, click in the check box to the left of the item. A check mark indicates an item is selected; a diagonal slash mark indicates that only some items within a folder are selected. You can select items in the All Folders pane or the Contents pane.

To preview a list of the media required for restore, select Actions → Preview Media. If the backup images required to restore the data are on disk storage units rather than removable media such as tape, no media will be listed if you try to preview media.



On the Actions menu, click Start Restore of Marked Files. The Restore Marked Files dialog appears. The items marked for restore are listed in the dialog window.

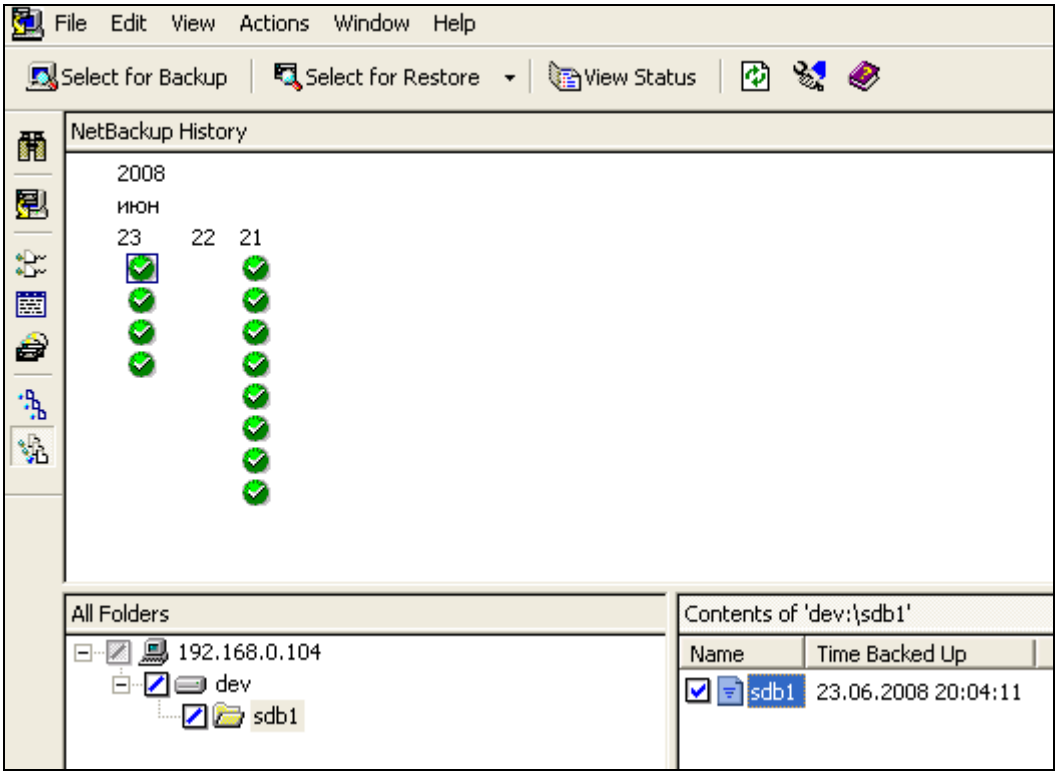


Specify restore parameters and press Start Restore. A dialog appears, indicating that the restore began successfully and asking if you want to view the progress of the operation.

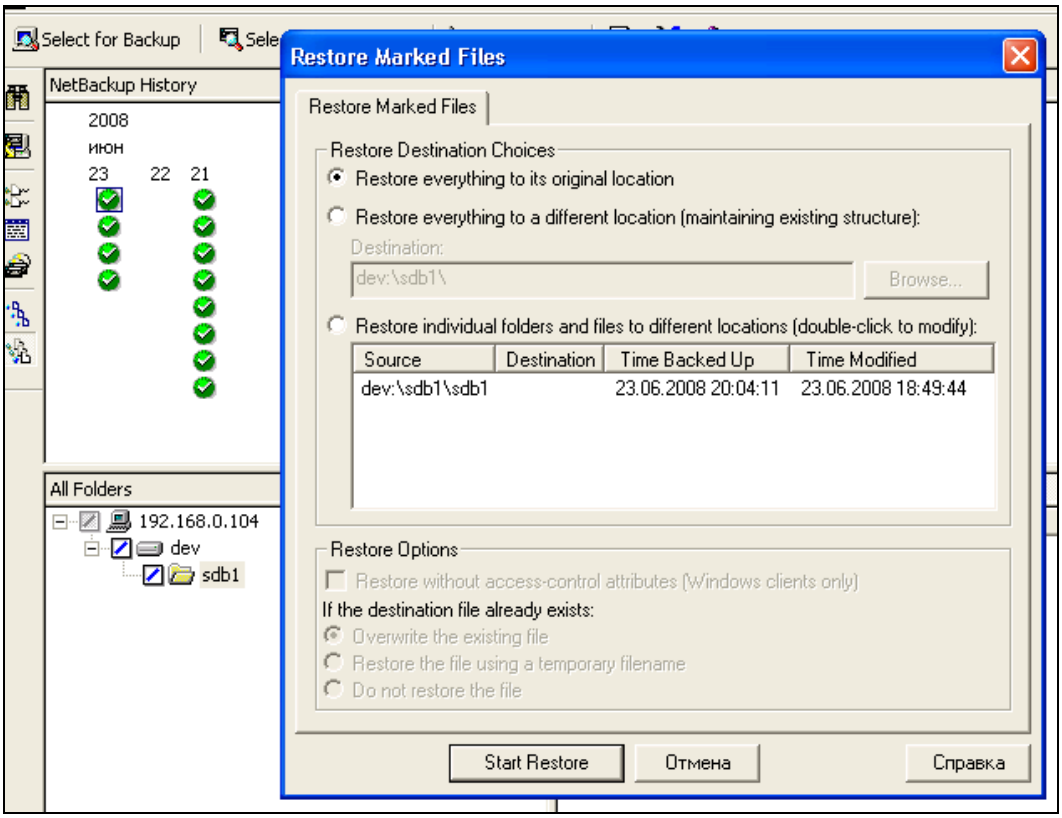
To view the status of the restore, click Yes in the dialog. The View Status dialog appears, from which you can view the progress of the restore. The restore may take a few minutes to complete. After starting a restore operation, you can close Backup, Archive, and Restore and perform other tasks on your computer. NetBackup will continue the restore operation in the background.

Using NetBackup to backup and restore special device files through NDMPD

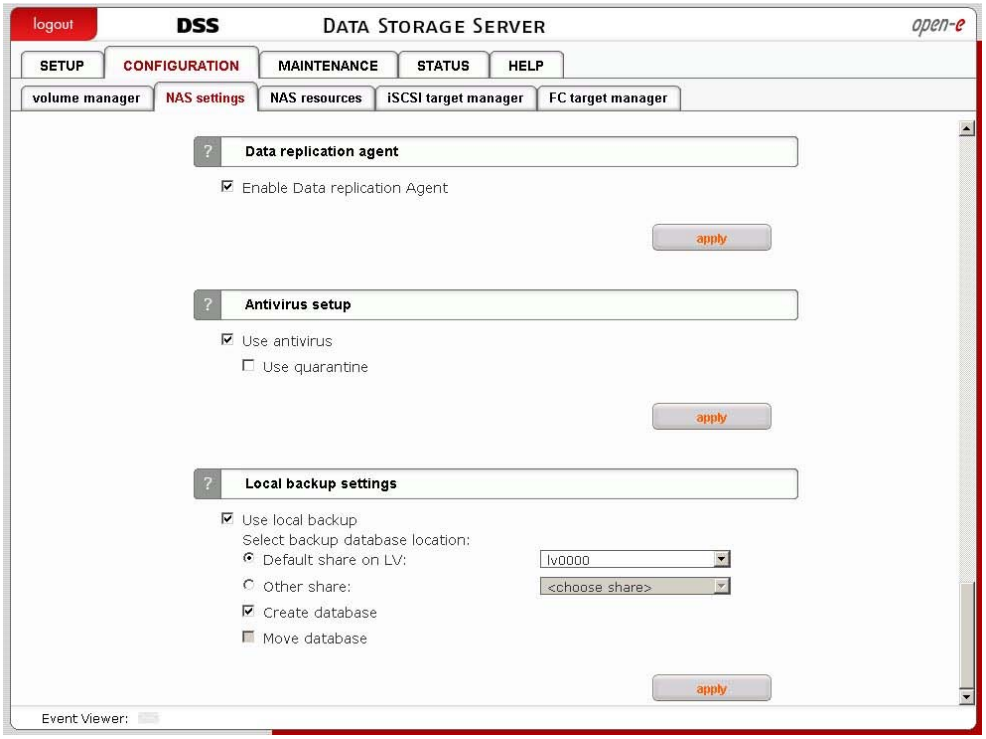
As described before in this guide, NetBackup does not allow you to add files in the Policies backup selection path. But to perform a backup of a single file (or group of files), you can add the path with a file name. Backup id: Treat it as a directory, but NDMPD handles this case properly and creates a correct backup image. Then to restore these files in the Backup, Archive, and Restore application, you need to select the image and check the desired file. Because NetBackup treats all as directories, you have a folder which consists of a path and the name of a file. All parts of this path must be checked with a slash, not a check, as described in the picture.



On this picture, we can see the backup of a special file /dev/sdb1. This image looks like we're doing a backup of the directory /dev/sdb1/. After selecting Start Restore, the Restore Marked Files dialog appears.



You can see that NetBackup tries to restore to the /dev/sdb1 file sdb1 – but this is ok. NDMPD handles this case and restores the file /dev/sdb1.



Function: Data replication agent

This function enables the data replication agent.

note It is mandatory to enable this function in order to replicate to the destination share.

note Data replication is performed by the rsync application.

Function: Antivirus setup

This function provides antivirus protection for your data.
Antivirus scans the following file types:

- Archives and compressed files:,
  - Zip,
  - RAR (2.0),
  - Tar,
  - Gzip,
  - Bzip2,
  - MS OLE2,
  - MS Cabinet Files,
  - MS CHM (Compiled HTML),
  - MS SZDD compression format,
  - UPX (all versions),
  - FSG (1.3, 1.31, 1.33, 2.0),
  - Petite (2.x).
- mail files,
- MS Office document files,
- executables files.

The Use quarantine feature allows you to choose whether you want to move infected files to the default folder (quarantine_dir), which is automatically created on shares, or manually choose the quarantine directory on a previously created share.
To get to know more about the infected files examine the logs (you can download them in **MAINTENANCE** -> **Hardware**). The relevant logs are the following:

- scan_shares_ANTIVIRUS_[antivirus_task_name].log for regular antivirus scanning,
- clamd.log for SMB online scanning.

note If the **Use quarantine** option is disabled you will only be informed about the infected file.

Please note that antivirus scanning may decrease the overall system performance

Function: Local backup settings

This function enables local backup functionality.

Use default share on LV
With this option you can store a database of all backups on the default share within the selected logical volume.
Use other share
With this option you can store database of all backups on selected share.
Create database
Use this option to create a backup database on the selected share.
Move database
If this option is checked then existing backup database will be moved to selected share.

note It will not be possible to create a backup database on a share if it contains any files other than backup database files. If you want to create a backup database on such a share, you have to first delete all files from it..

5.2.2.3 NAS resources

Here you can configure NAS resource operations. All you need to do is the use the tree diagrams on the left hand pane, which will allow you to manage all shares, users and user groups in a structured manner.

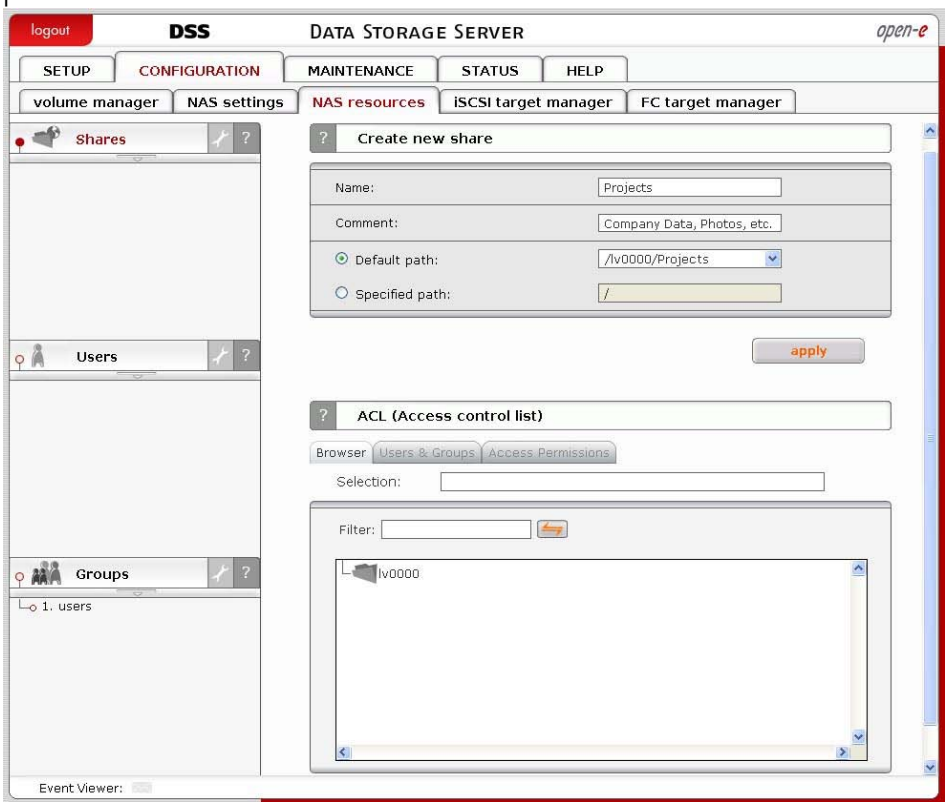
5.2.2.3.1 Shares

Here you can find a list of all your Open-E Data Storage Server shares. After clicking on “Shares,” the “Create new share” function allows you to define a new share, set up a comment for it (optional) or set its path. You will find all existing shares organized below. You can edit them with a simple click. All parameters except the name are modifiable. If you need change the name, delete it and assign a new name.

Windows users will see the name of the share in their network environment folders when they click on the icon for the Open-E DSS server. Comments are only visible if the users take a look at the share properties, or if shares are listed in detail.
The path represents the physical location of the data on the Open-E Data Storage Server share volume. The user does not have access to this information. In order to simplify the navigation through the directories, you can use the browser function.

Function: Create new share

To create a share, enter the share name, a comment (optional) and set its path. To use the default share path, leave the Default path box checked. If you want to use a specific path, please check the Specified path box and select path to the share.



note Please do not use spaces and special such as:
~!@#$^&()+[]{}*;:'".,%|<>?/\=`,

note The workgroup/domain name configured in the **NAS settings** tab has to match the network settings. Otherwise, the configured shares will not be visible in the network environment. If you have made changes to the workgroup and server name in the NAS configuration, it can take some time before each workstation computer in the Windows network detects the new name.

Function: ACL (Access control list)

With this function you can assign ACL permissions to your folders or files.

Browser

Filter

Allows to show only folders or files from given name.

Selection

Shows where you are in directory's browser.

Users & Groups

Available Users & Groups

List of available users and groups which can have access permissions assigned to them.

Selected Users & Groups

List of selected users and groups which will have access permissions assigned to them.

Access Permissions

Recursive

If this option is checked the ACL permissions will be assigned to all folders and files within the selected folder.

Set owner

If this option is selected the designated user(s) or group(s) will be owner(s) of the selected folders or files.

Access Permissions:

- read,
- write,
- execute (for folders this means the permission to open, while for files, the permission to execute).

In order to assign ACL permissions:

- select folder or file,
- click tab Users & Groups,
- select which users or groups will be available to assigned access permissions,
- click the access permissions,
- select user ([U]) or group ([G]) or User(owner) or Group(owner),
- check the appropriate boxes under Access Permissions,
- click Apply.

Examples:

Example 1.

This example presents a situation in which User1 has read access permissions for directory A only and does not have access permissions for subdirectory B at all.

A User1 r-x
B User1 ---

Example 2.

User1 has access permission only for reading for directory A. Can enter sub directory B, but no files are visible.

A User1 r-x
B User1 --x

Example 3.

User1 can enter the subdirectory C and can read and write files within that subdirectory.

A User1 r-x
B User1 --x
C User1 rwx

note Designating the user as a superuser within the **SMB settings** function will automatically assign all access permissions to that user.

Assigned access permissions will be available under sFTP, FTP and SMB network protocols.

User(owner) or Group(owner) can also have access permissions assigned. These permissions may be different from the ones assigned to the same user in the Users/Groups list.

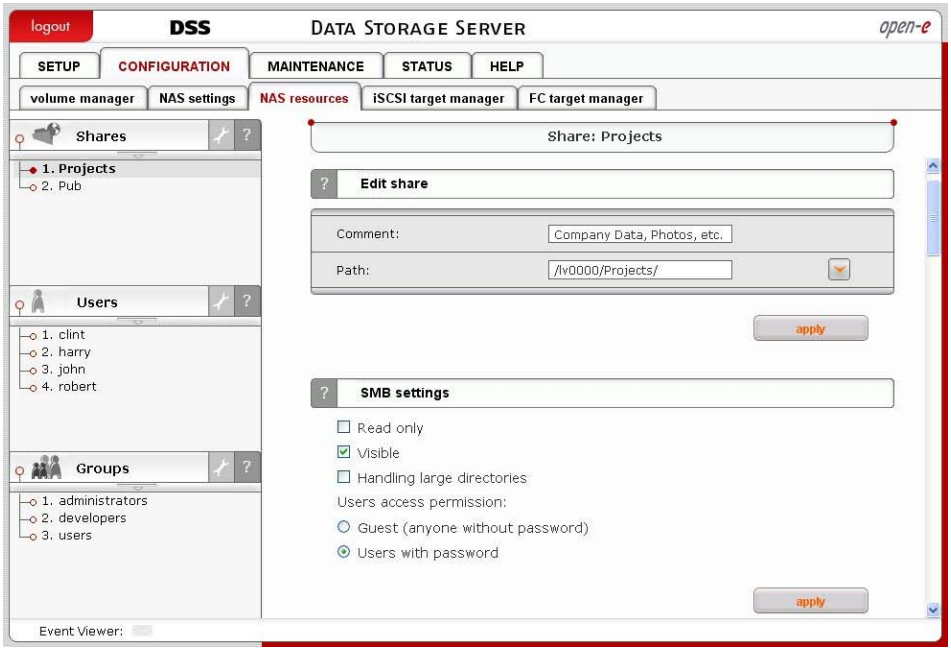
After clicking the “Create” button on the left pane, the name of an earlier established share will appear, in this case “Projects”. By clicking on that name, you will see all available options for setting up the share:

Function: Edit share

Here you can edit the share path and add or delete directories by click on  button.

Function “SMB Settings”

This function allows you to change the SMB protocol settings for this share. To restrict access to read-only, make sure the **Read-only** box is checked. Uncheck the **Visible** box to hide the share from the browse list. Select **Guest** to allow anonymous access to the share. Select **Users with password** to enforce user authentication.



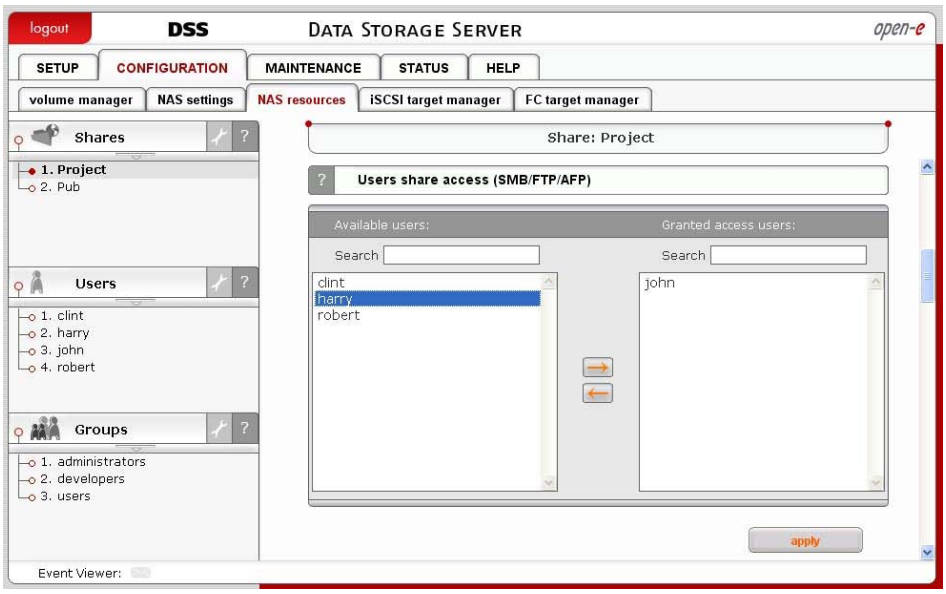
Handling large directories

This option allows you to significantly speed up file listing. The prerequisite is to convert all file and directory names to lower or upper case exclusively. Please select your preferred choice below.

note You will need to convert your existing file and directory names to lower or upper case before selecting this option, as otherwise they will become inaccessible.

note Please note that due to case sensitivity issues the operations above may have negative impact on Unix-like systems. Please prepare accordingly beforehand. Windows is not affected.

In functions “Users share access (SMB/FTP/AFP)” and “Groups share access (SMB/FTP/ASP)” you can grant access to the shares to available users and/or groups.

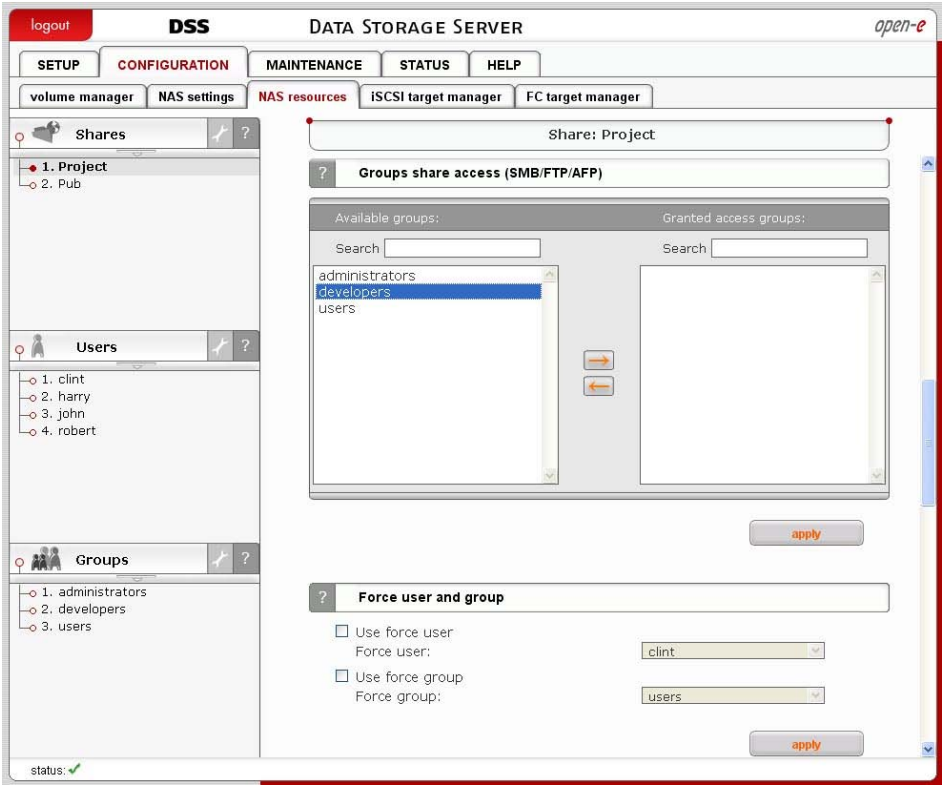


Function: Users share access (SMB/FTP/AFP)

Add the users access to the shares by selecting the users and clicking the button  . To remove access for users to the specified shares, select the users and click the appropriate arrow button  to remove them from the Granted access users list.

note You can use the following keyboard keys in the lists (you need to first set the focus on the preferred list):

- Home: jump to the first,
- End: jump to the last,
- Shift + arrow key: multi-select,
- letter key: jump to the first entry starting with the pressed key.



Function: Groups share access (SMB/FTP/AFP)

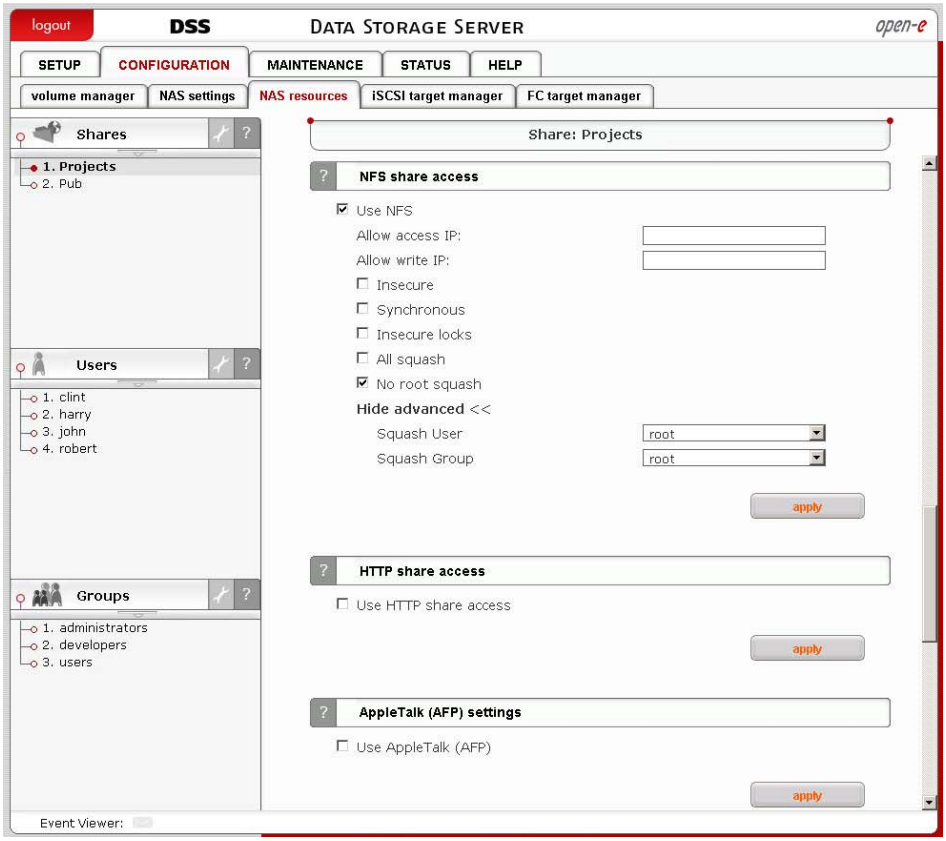
Here you can add groups which are granted access to this share.

note You can use the following keyboard keys in the lists (you need to first set the focus on the preferred list):

- Home: jump to the first,
- End: jump to the last,
- Shift + arrow key: multi-select,
- letter key: jump to the first entry starting with the pressed key.

Function: Force user and group

This function allows you to force the selected user and group to be the owners of all objects created from this point on.



Function: "NFS share access"

Please click **Use NFS** to activate access to this share via NFS.

note In order to mount this share via NFS, please use the following syntax:
mount -t nfs IP_addr:/share/share_name /local_mount_point
or
mount -t nfs IP_addr:/share/share_name /local_mount_point

Share is a keyword and must always be added to the syntax.

In order to mount a share in synchronous mode please use:

mount -t nfs IP_addr:/share_name /local_mount_point -o sync
or
mount -t nfs IP_addr:/share/share_name /local_mount_point -o sync

In order to mount a share in asynchronous mode please use:

mount -t nfs IP_addr:/share/share_name /local_mount_point -o async
or
mount -t nfs IP_addr:/share/share_name /local_mount_point -o async

When using synchronous mode, data is not stored in a buffer, but transferred at once. In asynchronous mode the data is first stored in a buffer and then transferred.
The name of the share is case sensitive in the mount syntax. It is important to exercise due caution in this respect, as otherwise you might not be able to access the share

You can use following NFS option fields:

Allow access IP
Please enter an IP address or an address range which should be allowed to access NFS. You can enter a single IP, multiple IPs separated by a semicolon, or an IP address range. IP addresses not be added to the Allow write IP list will have read only access.

Allow write IP
Please enter an IP address or an address range which should be allowed to write to NFS. You can enter a single IP, multiple IPs separated by a semicolon, or an IP address range.

Insecure
Allows incoming connections to originate from ports greater than 1024.

Synchronous
When this option is enabled, the local file system will wait for the data to be written to the NAS server. NFS performance will be lowered, however this will ensure that the data will be written directly to the NAS server and will not be stored in the system cache.

Insecure locks
Disables authorization of locking requests. Some NFS clients do not send credentials with lock requests, hence working incorrectly with secure locks, in which case you can only lock world-readable files. If you have such clients you can use the Insecure locks option.

All squash
Maps all user IDs to the user **nobody** and all group IDs to the group **nogroup**.

No root squash
Select this option to grant the client machine's root user the root access level to the files on the NAS server. Otherwise the client root will be mapped to the user **nobody** on the NAS server.

note When you leave the Allow access IP and Allow write IP fields blank, all computers in the subnet will have write access to NFS. When you set the Allow access IP field and leave the Allow write IP field blank, the specified computers will have read only access and none will have write access. When you set the Allow write IP field without setting the Allow access IP field, the specified IPs will have write access and all computers in the subnet will have read only access.

- xxx.xxx.xxx.xxx
- xxx.xxx.xxx.xxx;xxx.xxx.xxx.xxx; ....
- xxx.xxx.xxx.xxx/network_prefix_length.

note Some Linux distributions have UDP as the default protocol for NFS. In case of problems, it is recommended to switch to TCP by using the

following syntax: *mount -t nfs -o tcp ip_address:/share /mnt/point*.

If the host has an entry in the DNS field but does not have a reverse DNS entry the connection to NFS will not work

Function: Http share access

With this option you can enable http access for selected share.

In order to access https-enabled shares via Web browser, please enter the following in the address line of your browser:

https://SERVER_IP_ADDR:PORT
https://SERVER_NAME:PORT

For example:

https://192.168.0.220:444

note In order to access your share via a Web browser, you need to turn on the **Enable http share browser** option in the **CONFIGURATION → NAS settings → Http share access setup** function.

Function: AppleTalk (AFP) Settings

With this function you can activate the AppleTalk protocol in the network to access shares on the NAS Server.

How to use AppleTalk with the NAS server:

- enable AppleTalk in the **CONFIGURATION → NAS settings** menu,
- select the share to be made accessible via AppleTalk in the **CONFIGURATION → NAS resources** menu,
- enable AppleTalk for this share.

How to connect to the NAS AppleTalk server:"

In MAC OS 9:

- open the Chooser (**APPLE MENU → Chooser**),
- click on **AppleShare**,
- if the NAS server does not appear on the fileserver list, click on **Server IP address** and enter the NAS server IP,
- click **OK** and choose the login type. Enter a username and password if you want to log in as a specified user,
- from the available options select the shares you would like to mount,
- the icons of the mounted shares will appear on the desktop,
- to open the share click on its icon,
- to unmount the share drop its icon into the trash bin.

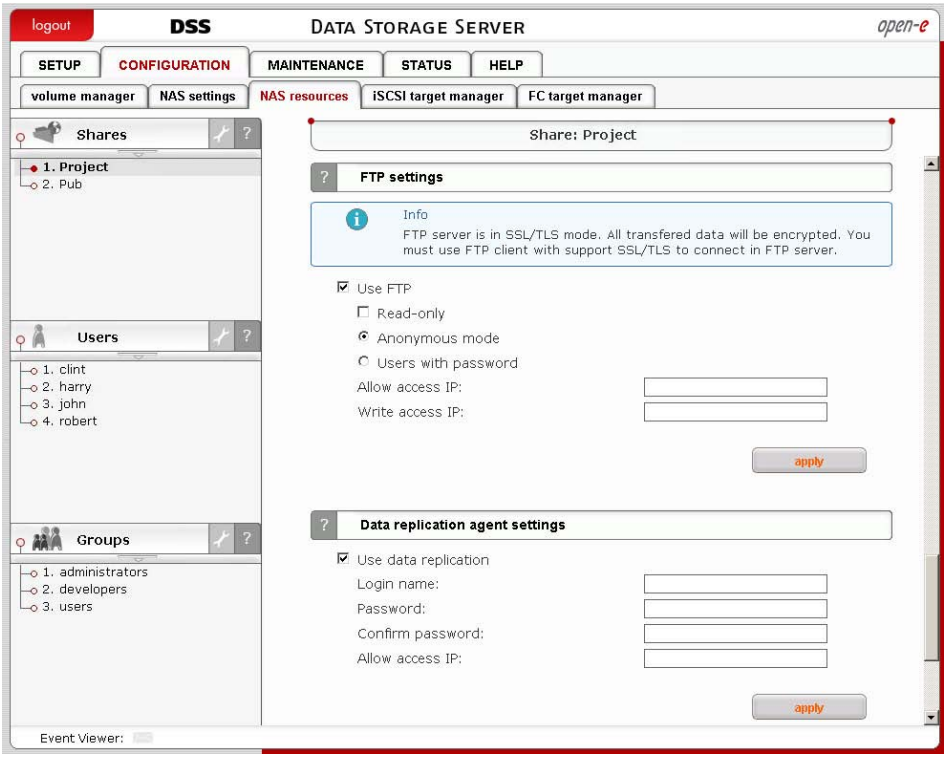
In MAC OSX 10.3:

- click on the MAC HD, then **Applications** followed by **Utilities**,
- check if AppleTalk is active from the Directory Access; if not, activate it,

- if the NAS server does not appear on the Network list, open a Web browser and enter the IP address of the AppleTalk server. afp://192.168.1.3 ("afp://" is crucial here),
- choose the login type. Enter a username and password if you want to log in as a specific user,
- if you cannot log in, click on **Directory Access/Authentication** and change the searching path for authentication information,
- from the list of available shares select all those you want to mount,
- the icons of the mounted shares will appear on the desktop.

Alternative method:

- click on **Connect to server** from the Finder (GO submenu),
- enter: afp://ip_address,
- you can add a link to the AFP server by clicking on the + sign. This adds a link in the Favorite Servers field,
- choose the login type and enter a password if you want to log in as a specific user,
- from the list of available shares select all you want to mount,
- the icons of the mounted shares will appear on the desktop.



Function: "FTP Settings"

You can enable FTP services for each share separately. Your choices here include:

- Anonymous mode,
- Users with password.

Selecting Anonymous mode will enable FTP sharing with anonymous users. The access is set to READ+WRITE by default for all IPs. To change that, activate the **Allow access IP** and **Write access IP** options. Clicking **Apply** will make the share available over FTP.

To connect to this share FTP client software is required – e.g. Internet Explorer has FTP support. To connect with IE when using the Anonymous mode, please enter the following in the address line: *ftp://<Server IP>/pub/* (e.g. *ftp://192.168.0.220/pub/*). When using an SFTP client, please type in the following: *ftp://<Server IP>/share/* (e.g. *ftp://192.168.0.220/share/*). *Share* is a keyword. Many FTP client programs need a username and a password to establish connection. In the Anonymous mode the username is **anonymous** and there is no password (i.e. the password field should remain empty). All anonymous shares are in the folder called *share*. Any user connecting from an IP which has not been granted full access will see all the shares but will be unable to see any restricted directories.
It is good practice to use email address for anonymous login password. Only few FTP clients support SFTP(SSL/TLS).

note An anonymous user will see only files and directories owned by them.

Selecting the **Users with password** mode will enable secure FTP sharing with username and password authorization. There are few FTP clients which support SFTP(SSL/TLS).

Here is a list of the software which has been tested:

- CoreFTP (Windows),
- FileZilla (Windows),
- IgloFTP (Windows and Linux),
- SSLFTP (Linux console client).

When the **Users with password** option is enabled, users have access to the share after inputting the authorized username and password.

note If the NAS server uses Windows domain authorization the short domain name along with a plus sign must precede the username, e.g. *DOMAIN+Administrator*.

To connect to a share via the Users with password mode, switch the encryption type in your SFTP client to SSL or TLS. All Users with password shares are in the *shares* folder. Users see only the authorized shares.

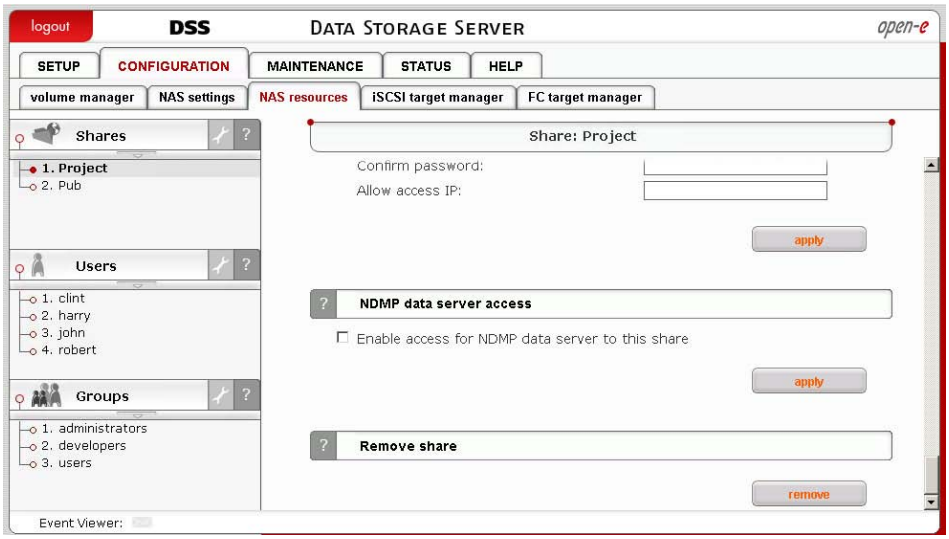
note If you are unable to see any directories when connected to the FTP server please make sure that you have the rights to access any shares over FTP. If you still cannot see any directories please switch your FTP client to passive mode.

note Most FTP clients have bookmarks which allow for setting up IP, a port home folder, etc. Suggested home folder for the Anonymous mode users is *pub* while for the Password mode users it is *shares*.

Function: Data replication agent settings

This function allows you to configure data replication for a share.
In order to enable it, check the **Use data replication** box.

note It is recommended to set a login name, a password and an Allow access IPs list, as otherwise everyone will have access to the share.



Function: NDMP data server access

This option enables NDMP for this share. Please make sure you have checked the Enable NDMP data server in CONFIGURATION → NAS Settings → NDMP data server beforehand.

Function: Remove share

Click **Remove** to remove the share.

note No data (directories or files) will be deleted on the logical volume. You can recreate a deleted share at any time. Just go to the **NAS resources** menu, click on **Shares** (as if you were creating a new share), browse the directory structure to find the folder you want to assign to the share. Finally, in the **Name** field please enter your share name and click **Apply**. Now you can find the deleted share again in your network neighborhood.

5.2.2.3.2 Users

In the mode “Workgroup internal LDAP” the category “Users” serves as data entry mask for user accounts. In principal, the process is the same as when you create shares.

Function: Create new user

To create a user, enter their username and password, retype the password and press **Create**.

note User name cannot:

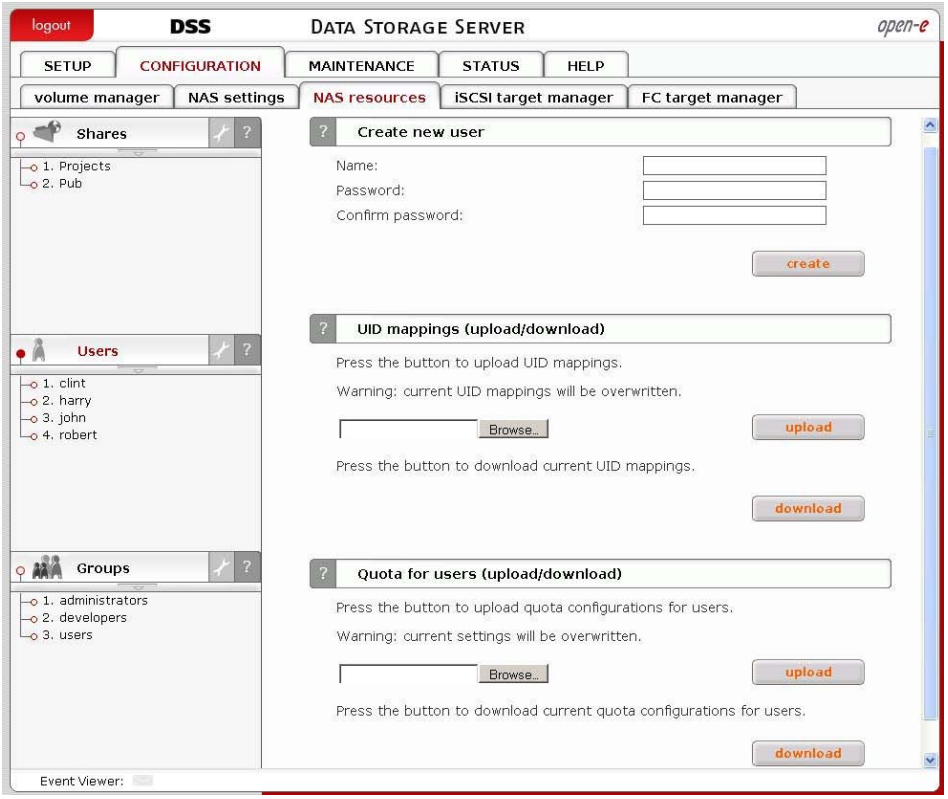
- contain characters: ~ ! @ # $ ^ & ( ) + [ ] { } * ; : ' " ., ; % | < > ? / \ = `,

- begin or end with a space.

Password cannot:

- contain the following special characters: ' " `,
- contain spaces.

If users forget their password, there is no way to retrieve it. You can only set a new password.



Function: UID mappings (upload/download)

This function allows you to upload and download UIDs (user IDs). With it you will be able to modify multiple user IDs at the same time.

To upload UID:

- locate the configuration file *uid_mappings.csv* (format: *user_name;uid*) by clicking the **Browse** button. This file should be encoded in UTF-8,
- press the **Upload** button to import UID mappings,
- If there are any errors while importing UIDs please examine the *uid_mappings_import.log* file in the log package.

note Warning: current UID mappings will be overwritten. Press **Download** button to download uid_mappings.csv.

Function: Quota for users (upload/download)

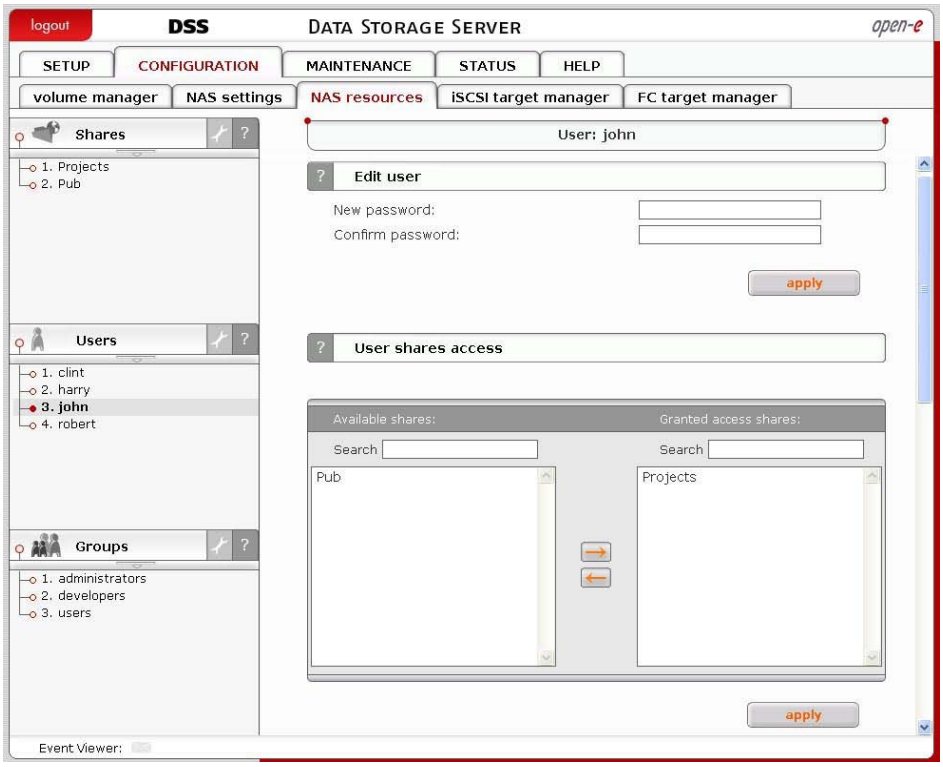
This function allows you to import and export user quota mappings.

To upload quota:

- locate the configuration file *quota_users.csv* (enconding: UTF-8; format:user_name; hard_quota-in kbytes) by pressing **Browse**,
- press the button to upload quota configurations for users,
- if you encounter errors while uploading the quota please examine the *quota_users_import.log* file in the log package (available via **STATUS → Hardware → Function: Logs**).

note Warning: current settings will be overwritten. Press **Export** to download quota_users.csv

Then by clicking on name e.g. “john”, you will see all available functions helpful for setting the user:



Function: Edit user

To change the password for a user enter and confirm the new password and click **Apply**.

note Password cannot contain:

- special characters such as: ' " `,
- spaces.

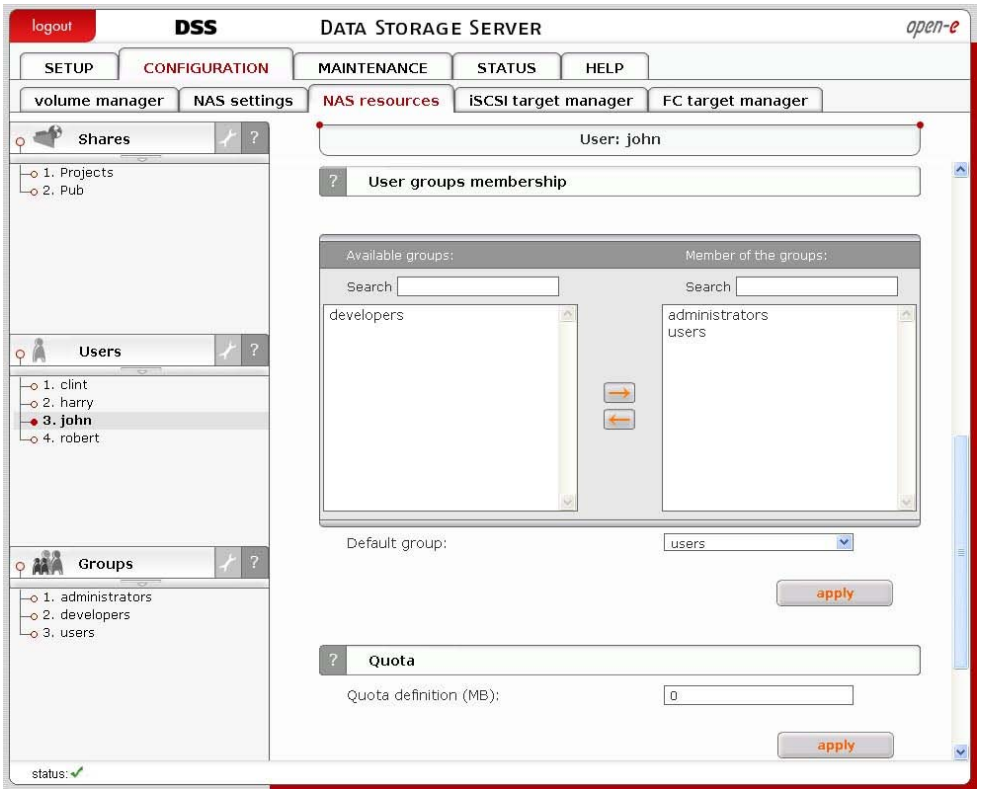
Function: Users share access

Add user access to shares by selecting shares and clicking the button. To remove user access to specified shares, select the users and click the appropriate arrow button ← to remove them from the **Granted access** users list.

note You can use following keyboard keys in the lists (first set focus to desired list):

- **Home**: jump to the first,

- **End**: jump to the last,
- **Shift + arrow key:** multi-select,
- **letter key:** jump to the first position starting with pressed key.



Function: Users group membership

This function allows you to view and change user group membership when connected to the local LDAP users and groups database.
To assign this user to a group, select its name from the **Available groups** list and click on → button. To remove group membership, select the group from the **Member of the groups** list and click on ← button.

note You can use following keyboard keys in the lists (first set focus to desired list):

- Home: jump to the first,
- End: jump to the last,
- Shift + arrow key: for multi-select,
- letter key: jump to the first position starting with pressed key.

Function: Quota

You can assign a quota (a limit) on the amount of space a user is allowed to allocate on the shares to which they have access.
To remove any limitations for a user, you need to set their quota to 0.

note Max quota value per user/group is 2TB. All greater values will be limited to 2TB

Function: Rename user

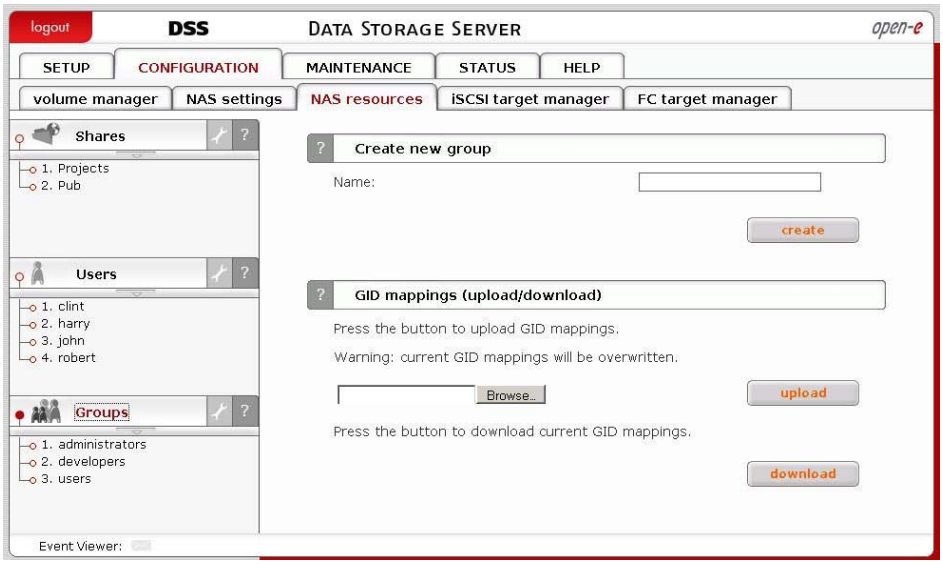
This option allows you to rename an existing user.

Function: Remove user

Click **Remove** to remove the user from the system. All the files the user has ownership of will be preserved.

5.2.2.3.3 Groups

In the mode “Workgroup internal LDAP,” you can define entire groups consisting of different users. In addition, you can assign these groups certain access rights. By clicking on “Groups,” a data entry mask opens up, allowing you to create a new group. Assigning the access rights is done the same way as for users (see 5.2.2.3.2).
In the modes “Workgroup (external LDAP)” and “Windows (PDC)” and “Windows (ADS)” the groups are automatically synchronized with the external server.



Function: Create new group

To create a group, enter its name and press **Create**.

note Group name cannot:

- contain special characters such as: ~ ! @ # $ ^ & ( ) + [ ] { } * ; : ' " . , % | < > ? / \ = `,
- begin or end with a space.

Function: GID mappings (upload/download)

This function allows you to upload and download GIDs (group IDs).
Using this function you will be able to modify multiple group IDs at the same time.
To upload GIDs:
:

1. find the configuration file *gid_mappings.csv* (format:group_name;gid) by pressing the **Browse** button. This file should be encoded in UTF-8,,
2. press the **Upload** button to upload GID mappings,,

if you encounter errors while importing GIDs please examine the gid_mappings_import.log file in the log package (available via STATUS → Hardware → Function: Logs).

note Warning: current GID mappings will be overwritten. Press "download" button to download gid_mappings.csv.

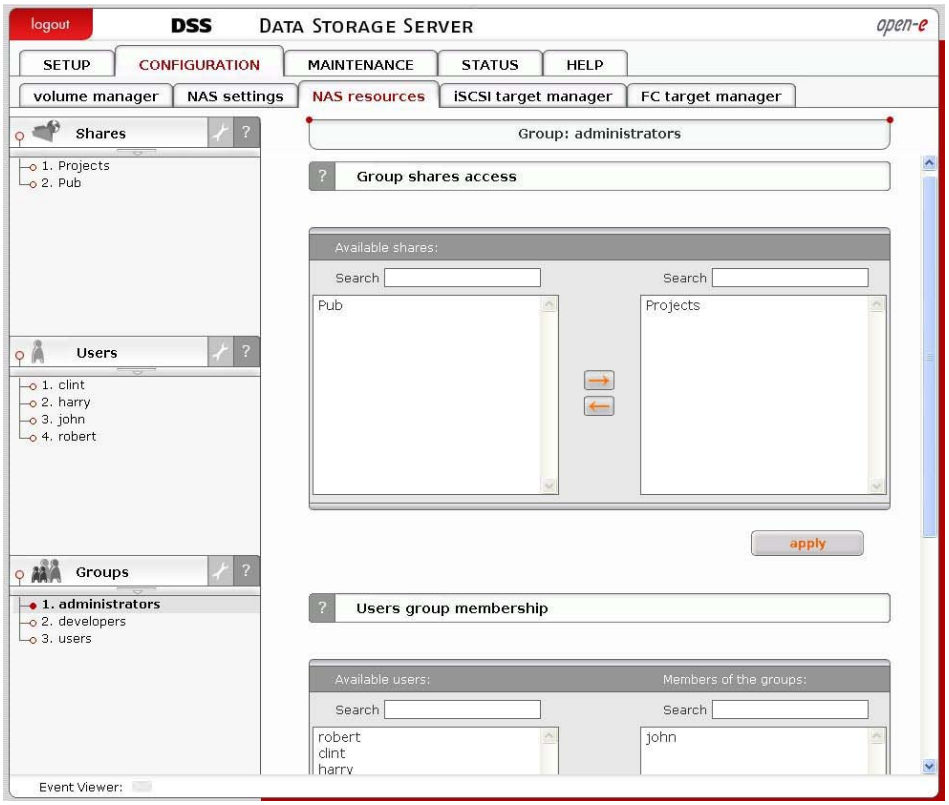
Then by clicking on group name e.g. “administrators”, you will see all available functions helpful for setting the groups:

Function: Group shares access

Here you can add the shares for this group, that has access to, by selecting the shares and clicking the button →. To remove the access from this group, that has the specified shares, select the shares and click the button ←.

note You can use following keyboard keys in the lists (first set focus to desired list):

- “Home”: jump to the first,
- “End”: jump to the last,
- “Shift” + arrow key: for multi-select,
- “letter key”: jump to the first position starting with pressed key.



Function: Users group membership

While connected to local LDAP users and groups database this function allows you to view and change user groups membership.

To assign users to this group, select users from “Available users” list and click on button. To remove membership from a user select users from the Members list and click on button.

While connected to external users and groups database you are able to check which users are members of this group.

Function: Remove group

Click "remove" button to remove the group.

5.2.2.4 iSCSI target manager

Function: Create new target

To create a target assign a name or leave the "Target Default Name" option checked.

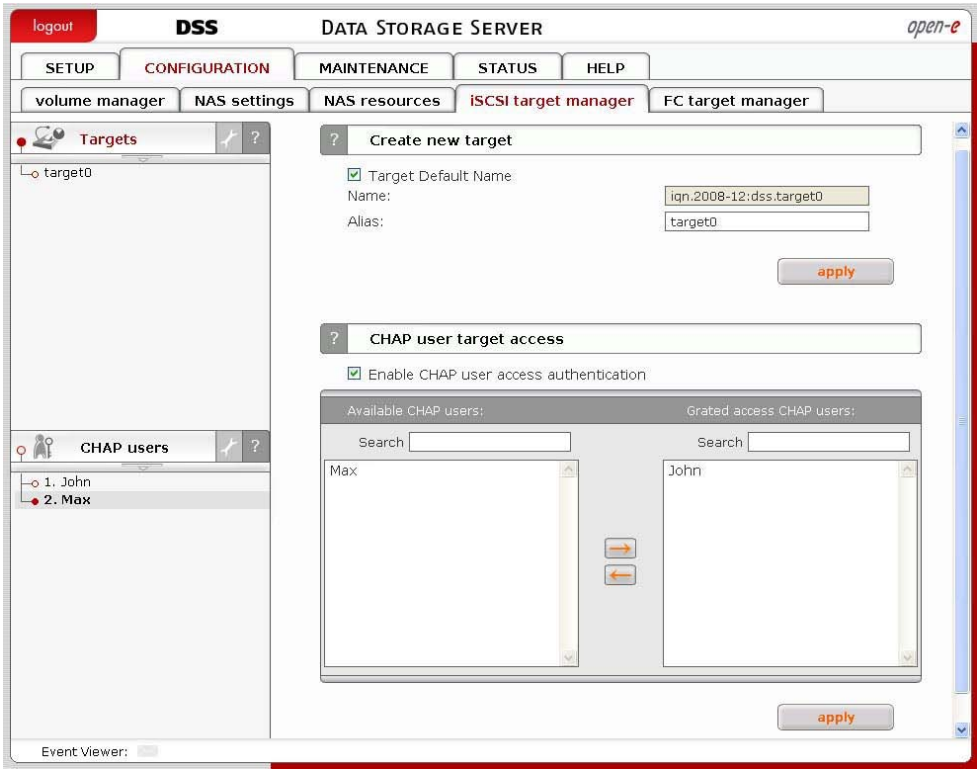
Name

Target name can contain alphanumeric characters: ' . ' ' : ' ' - '. A target name is considered case-insensitive. Every character entered will be converted to low-case. No spaces and no underscores are permitted.

Alias

Alias is a name, under which target will be visible in Targets tree. The same naming rules apply for alias as for name.

note The server name will be used as a part of the default target name.



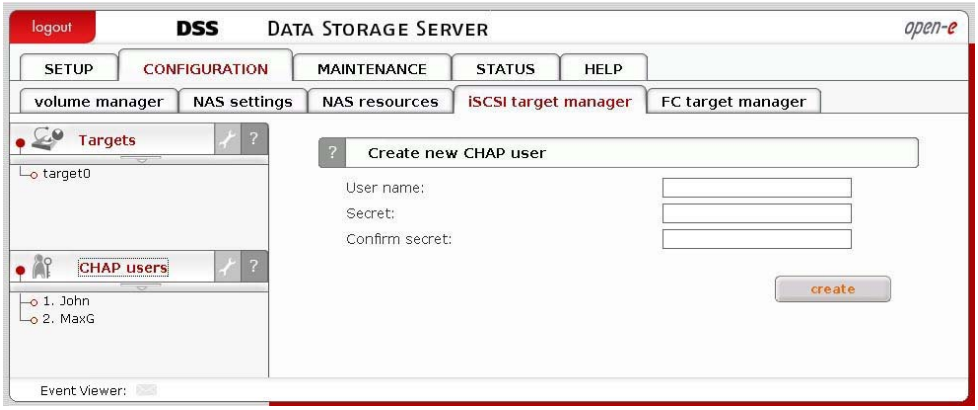
Function: CHAP user target access

Add CHAP users that are granted to access to this target.

note You can use following keyboard keys in the lists (first set focus to desired list):

- "Home": jump to the first,
- "End": jump to the last,
- "Shift" + arrow key: for multi-select,
- "letter key": jump to the first position starting with pressed key.

If you enable CHAP user access authentication but will not select any users to have access, then nobody will have access to the Target.



Function: Create new CHAP user

To create CHAP user enter name, password, retype password and press create button.

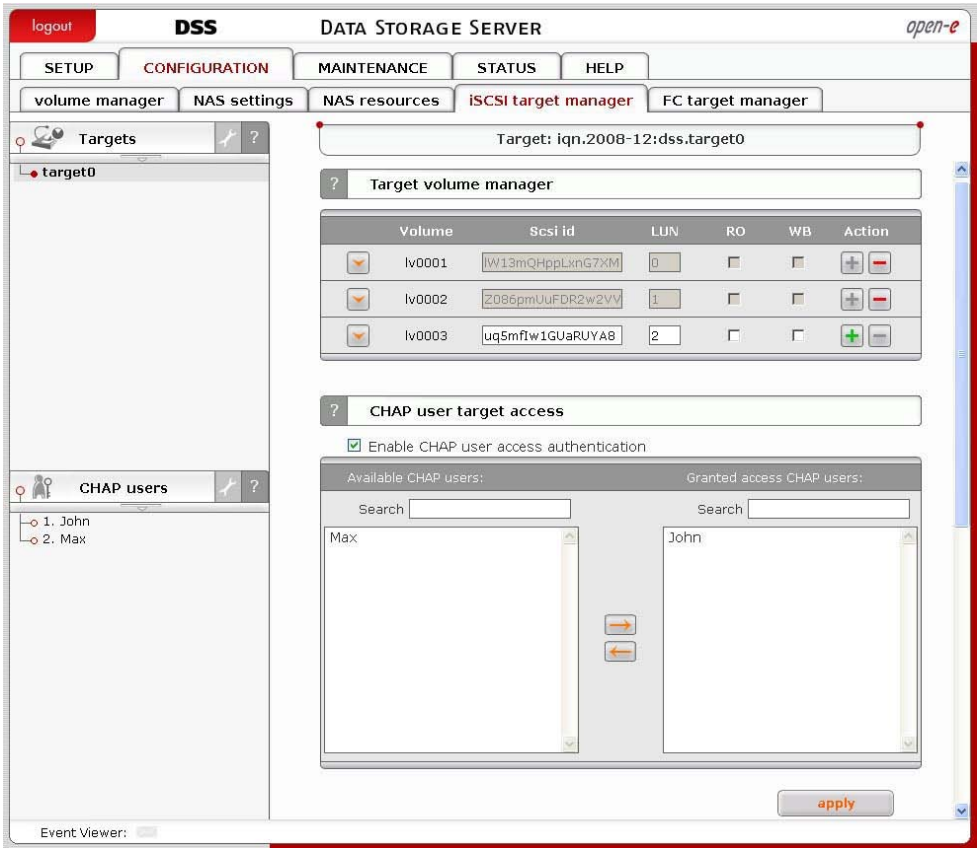
note CHAP user name cannot:

- contain characters: ~ ! @ # $ ^ & ( ) + [ ] { } * ; : ' " ., % | < > ? / \ = `,
- begin or end with a space.

Password cannot:

- contain characters: ' " `,
- spaces,
- the length of the password must be within 12 - 16 characters.

If CHAP users forget their password, there is no way to retrieve it. You can only set a new password.



Function: Target volume manager

This function lets manage free and already assigned target volumes and snapshot volumes. To assign a volume to the target click the “Add” button associated with that volume. Similarly to remove already assigned volume from the target click "Remove". In certain circumstances you may need to adjust the LUN of the volume you are about to add. Normally, however, the LUN assignment is taken care of for you automatically. You should leave the default values.

In SCSI ID field you can edit SCSI identifier for logical volume (logical unit). Every logical unit must have unique SCSI ID. In case of logical units are configured for failover their SCSI ID must be identical on the primary and secondary nodes.

RO

Read Only, if it is turned on the LUN will be visible as a write protected disk. To switch the RO option when it's disabled, you must first remove the volume from the target and then add it again setting the flag as desired. Target volumes and snapshots are not read only (RO -unchecked) by default.

WB

Write-back cache. This functionality improves performance of data write. Write is acknowledged as completed as soon as the data is stored in the disk cache. In later time the disk cache commits the write to disk.

If RO and WB are disabled (RO and WB - unchecked) then Write-through cache is used by default. This means that writes are not stored in cache. Instead, all writes are acknowledged after they are committed to disk.

Function: CHAP user target access

Add CHAP users that are granted to access to the Target Server.

note You can use following keyboard keys in the lists (first set focus to desired list):

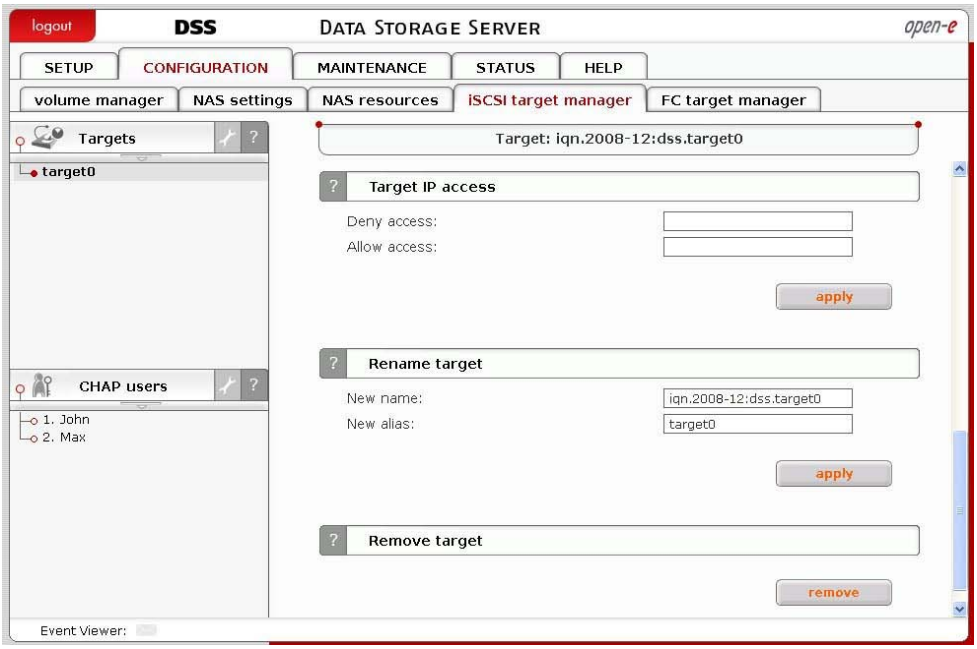
- Home: jump to the first,
- End: jump to the last,
- Shift + arrow key: for multi-select,
- letter key: jump to the first position starting with pressed key.

If you enable CHAP user access authentication but will not select any users to have access, then nobody will have access to the Target Server.

Function: Target IP access

You can assign network classes or specify individual IP addresses that are permitted or denied to access the target. Entries should be delimited by semicolons. When no entries are present in Denied access or Allowed access fields everyone is permitted to access the target. Specifying at least one entry in Allowed access field excludes all the clients that do not match it from accessing the target. When you specify at least one entry in Denied access field, every CHAP user or CHAP users from network class address are denied from accessing the target. When you specify any IP address in Allowed access field, CHAP users from that address are allowed to access the target even if the same address has been specified in Denied access field. If you enter only Allowed access field then Denied access field will be automatically entered with 0.0.0.0/0 entry.

note Please note that already active sessions to the target will persist regardless of the newly applied settings. You can ensure that the settings are forced immediately after you apply them by going to **MAINTENANCE → shutdown → iSCSI connection reset** and resetting the connections manually. Keep in mind that all the unsaved client data might be lost.



When you enter network class address in normal form, it will be automatically converted to short form.

Examples:

Deny access: 0.0.0.0/0
Allow access: 192.168.2.30/0;192.168.3.45

These settings deny access from every IP address or network class address, only addresses in the Allow access field are granted access to the target.

Deny access: 192.168.0.0/16
Allow access: 192.168.2.30;192.168.10.230;192.168.30.0/24

These settings deny access to any IP addresses from the network 192.168.0.0/16, grant access for IP addresses 192.168.2.30, 192.168.10.230, all IP addresses from network 192.168.30.0/24 and all IP addresses that have not been denied in the Deny access field.

Function: Rename target

Provide a new target name. A target name is considered case-insensitive. Every character entered will be converted to low-case.

Function: Remove target

This function removes all volumes from the target.

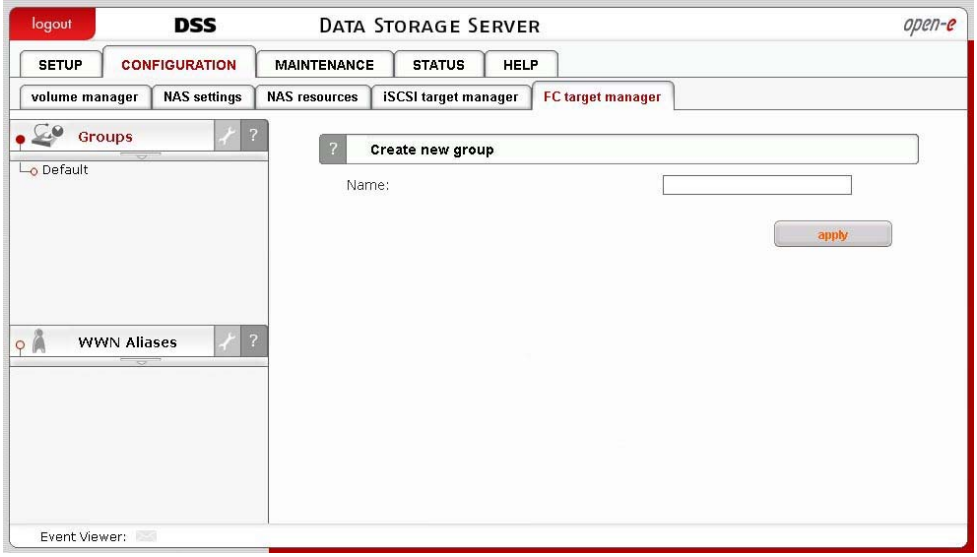
note Please note that the data stored on the volumes are not automatically removed. You can assign the volumes to different targets and still see the data. Please remove the data prior to removing target in order to prevent leakage of sensitive or classified information.

5.2.2.5 FC target manager

5.2.2.5.1 Groups

Here you can view list of all Fibre Channel Groups.

note Group **Default** is a public group. If some WWN belongs to another group than public, then this WWN will not have access to this public group and only will have access to the group where it's assigned to.

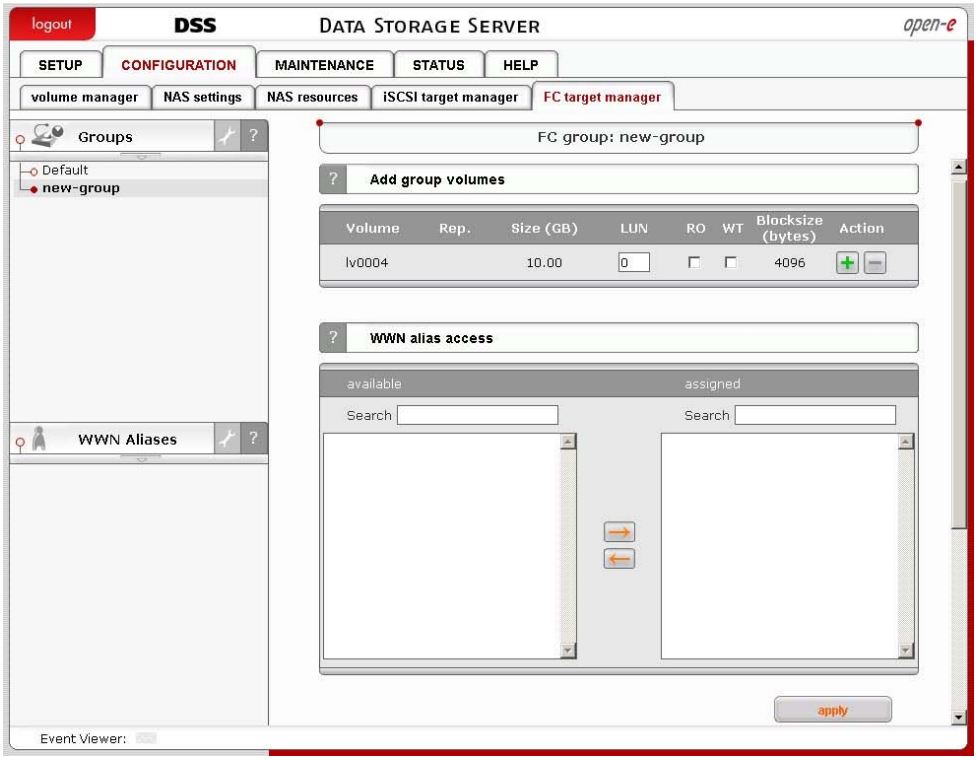


Function: Create new group

To create a group enter its name and click button apply.

Name

A group name is considered case-insensitive. Every character entered will be converted to low-case. Only a-z 0-9 . - and : chars are allowed.



Function: Add group volumes

This function lets manage free and already assigned FC logical volumes. To assign a volume to the group click the “Add” button associated with that volume. Similarly to remove already assigned volume from the group click "Remove". In certain circumstances you may need to adjust the LUN of the volume you are about to add. Normally, however, the LUN assignment is taken care of for you automatically. You should leave the default values.

RO

Read Only, if it is turned on the LUN will be visible as a write protected disk. To switch the RO option when it's disabled, you must first remove the volume from the group and then add it again setting the flag as desired. FC logical volumes are not read only (RO -unchecked) by default.

WT

Write-through cache. Data is written to logical volume at the same time as it is cached. This type of caching provides the advantage of internal consistency, because the cache is never out of sync with the logical volume.

If RO and WT are disabled (RO and WT - unchecked) then Write-back cache is used by default. This means that write is acknowledged as completed as soon as the data is stored in the disk cache. In later time the disk cache commits the write to disk.

Blocksize

It shows current blocksize of FC volume.

Function: WWN HBA access

Here you can add WWN aliases which are granted access to this group.

WWN

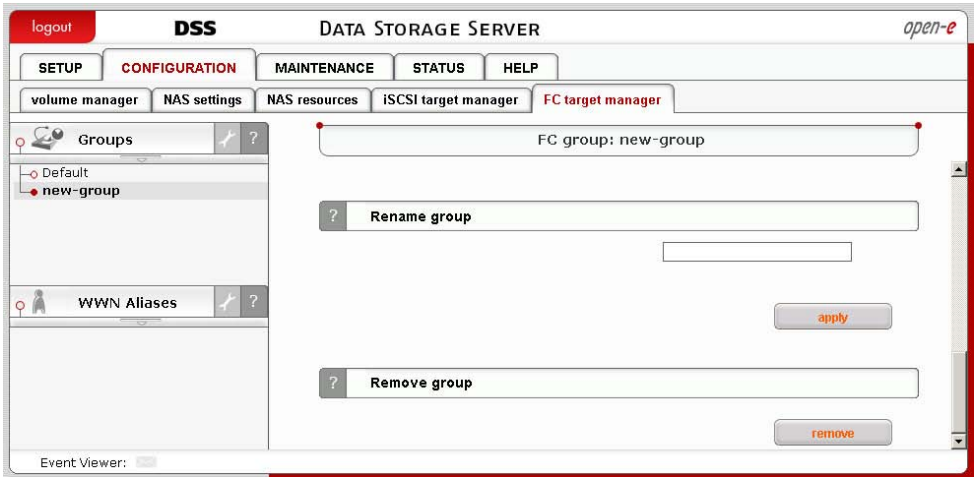
Worldwide name, it's a unique identifier in a Fibre Channel storage network. Each WWN is has a fixed 64-bit name assigned by the manufacturer and registered with the IEEE to ensure it is globally unique. It can include only chars from A to F, a to f, digits from 0 to 9 and a : char. You can find it in manual of your HBA card, bios or directly on label of your HBA card. Example of WWN: *1A:FF:AC:4D:00:1F:99:F3*.

HBA

Host Bus Adapter. HBA connects a host system to other network and storage devices. In this case it's referring to devices for connecting Fibre Channel.

note You can use the following keyboard keys in the lists (you need to set the focus on the preferred list first):

- **Home**: jump to the first entry,
- **End**: jump to the last entry,
- **Shift + arrow key**: multi-select,
- **letter key**: jump to the first entry starting with the pressed key.



Function: Rename group

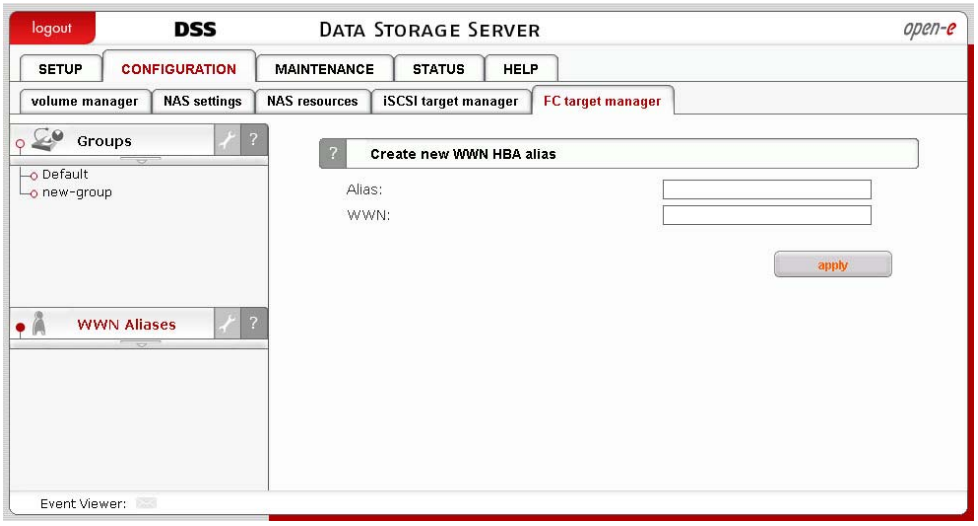
Provide a new group name. A group name is considered case-insensitive. Every character entered will be converted to low-case. Only a-z 0-9 . - and : chars are allowed.

Function: Group remove

Here you can remove selected group. All LUN and WWN alias associations will be also removed.

5.2.2.5.2 WWN Aliases

Here you can view list of all Fibre Channel WWN Aliases.



Function: Create new WWN HBA alias

To create new WWN (Worldwide name) alias for HBA (Host Bus Adapter):

- enter the alias and WWN to which its referring,
- press create.

WWN

Worldwide name, this is a unique identifier in a Fibre Channel storage network. Each WWN has a fixed 64-bit name assigned by the manufacturer and registered with the IEEE to ensure that it is globally unique. It may include characters from A to F, a to f, digits from 0 to 9 and an : character only. You can find the WWN in your HBA card manual, BIOS or directly on the HBA card label. Example of WWN: *1A:FF:AC:4D:00:1F:99:F3*

Alias

Short text name for a WWN. May only include characters from A to Z, a to z and digits from 0 to 9.

HBA

Host Bus Adapter. HBA connects a host system to other network and storage devices. In this case HBA refers to devices for connecting Fibre Channel.

Function: WWN Alias info

Here you can view the WWN and the alias of the FC HBA.

Function: Remove WWN HBA alias

Here you can remove the selected WWN HBA alias.

WWN

Worldwide name: This is a unique identifier in a Fibre Channel storage network. Each WWN is a fixed 64-bit name assigned by the manufacturer and registered with the IEEE to ensure it is globally unique. It can include only characters from A to F, a to f, digits from 0 to 9 and a : character. You can find it in the manual of your HBA card, Bios, or directly on the label of your HBA card. An example of a WWN: *1A:FF:AC:4D:00:1F:99:F3*.

HBA

Host Bus Adapter. HBA connects a host system to other network and storage devices. In this case it's referring to devices for connecting Fibre Channel.

5.2.3 MAINTENANCE

This page accessed with the Maintenance tab contains settings and functions pertaining to general management operations.

5.2.3.1 Shutdown

Function: System restart

This function allows you to restart your system.

Function: Create schedule for restart

Here you can create new schedule task for system restart.

Comment

You can enter comment for system restart.

Time select

Select time when restart task will be started.

Function: Schedules for restart

Here you can see all schedules created for a restart task.

Function „System shutdown“

Using this function, you can shut down the server.

Function: Create schedule for shutdown

Here you can create new schedule task for system shutdown.

Comment

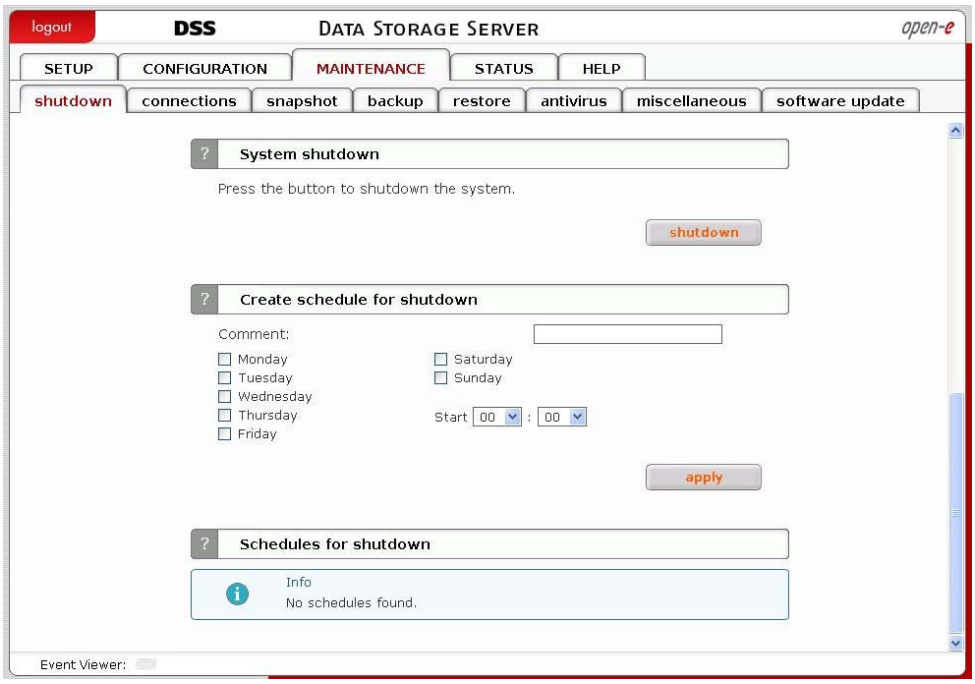
You can enter comment for system shutdown.

Time select

Select time when shutdown task will be started.

Function: Schedule for shutdown

Here you can see all schedules created for a shutdown task.



5.2.3.2 Connections

Function: NAS connections reset

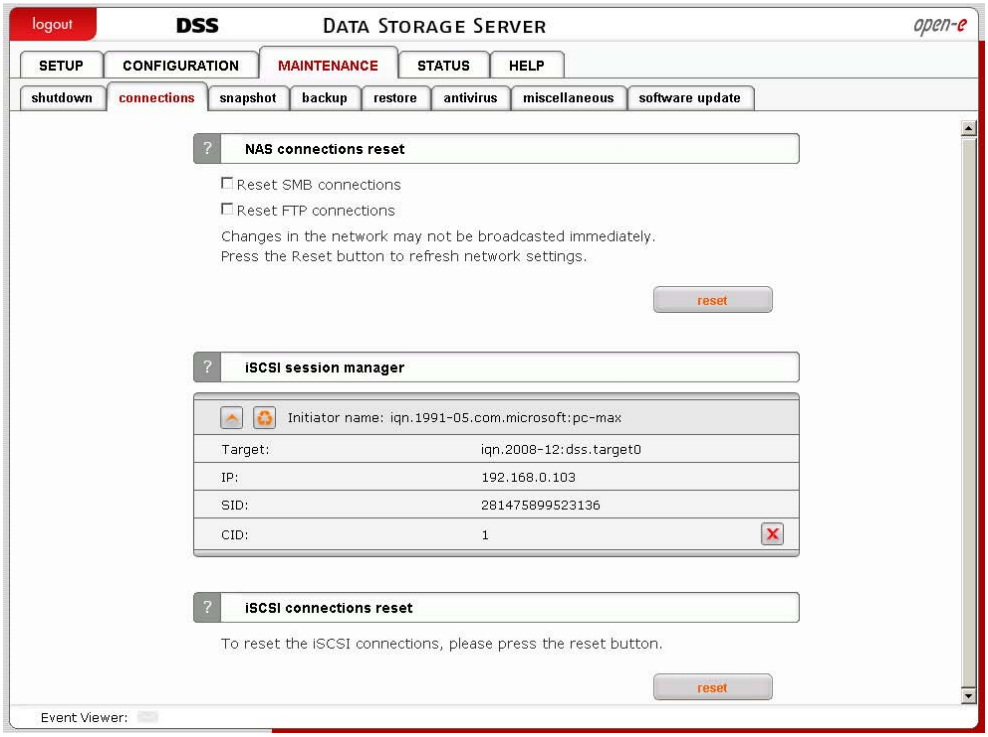
This function forces an immediate broadcast of changes to shares or access rights you have made over your network. It is dedicate for SMB and FTP connections. You can check or uncheck corresponding check boxes.

caution This function disconnects all users connected to the shares on specified protocol, which may lead to data loss if any files are open.

Function: iSCSI session manager

This function presents current connections to iSCSI targets. You can find here information like: target name, IP address, CID (ID of connection) and SID (ID of the session).

note You can cancel connection to iSCSI targets, but the initiator may automatically reestablish connection if it's enabled on initiator side. In order to block initiator form reconnecting to target you have to deny IP address in “SETUP” → iSCSI target manager → Targets → target[nr] → Function Target IP access.



Function: iSCSI Connection reset

This function presents current connections to iSCSI targets.
You can find here information like: target name, IP address, CID (ID of connection) and SID (ID of the session).

note You can cancel connection to iSCSI targets, but the initiator may automatically reestablish connection if it's enabled on initiator side. In order to block initiator form reconnecting to target you have to deny IP address in SETUP → iSCSI target manager → Targets → target[nr] → Function Target IP access.

5.2.3.3 Snapshot

Function: Snapshot tasks

With this function you can manually activate (start) or deactivate (stop) snapshots. Click on the snapshot alias in the left-side panel where you can define the time schedule to activate the snapshot.

To view snapshot details click on the down arrow button:

LV
Name of logical volume the snapshot is assigned to.

Size
Size of the space reserved for the snapshot (point-in-time) data in GB.

Status
Status of snapshot contains the following combinations:

In use
Snapshot is currently used by:

- active backup or replication task,
- created by time schedule or created manually.

Unused

Snapshot is available for backup or replication tasks also for time schedule or manual start.

Active

Snapshot is activated by backup or replication task also time schedule or created manually. In case the snapshot was created by backup or replication task: the point-in-time data is available for that task. In case the snapshot was created by time schedule or manually: the point-in-time data can be accessed via:

- NAS share (if the snapshot was assigned to NAS volume),
- iSCSI target (if the snapshot was assigned to iSCSI volume),
- FC group (if the snapshot was assigned to FC volume).

Inactive

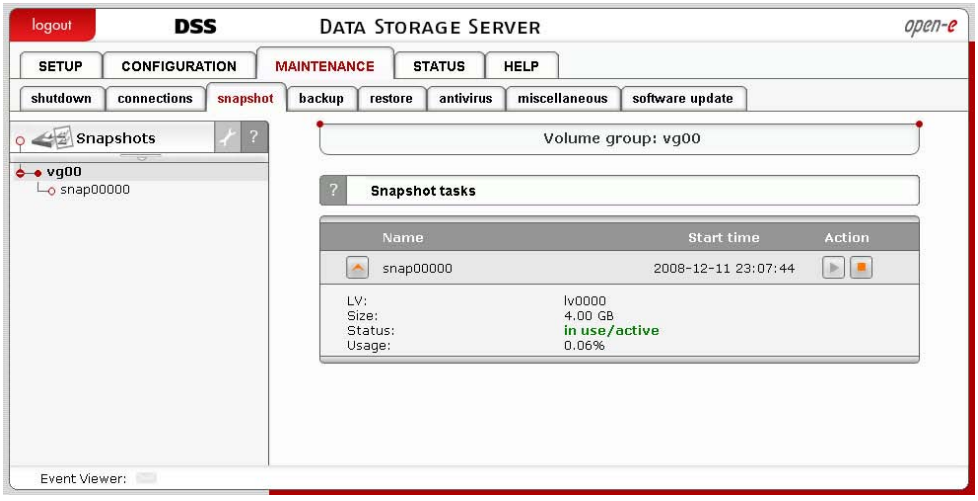
Snapshot becomes inactive when the reserved space reaches 100%. Be aware that this will prevent access to the point-in-time data! Please click on the "stop" button in order to set back to "unused".

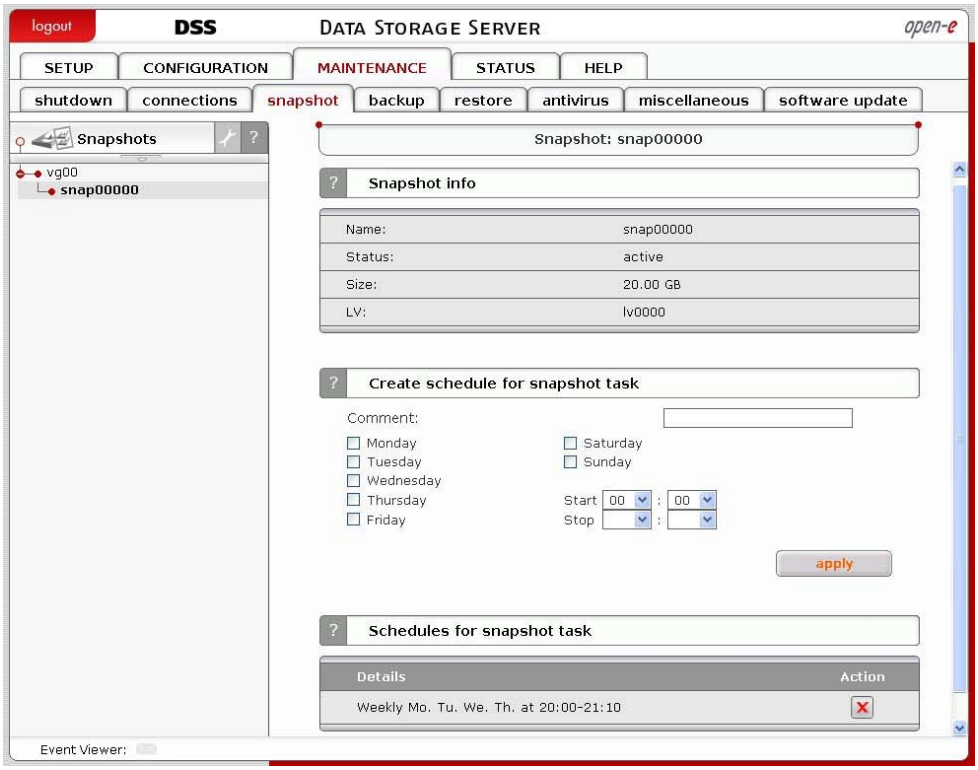
Usage

Shows the usage percent of the reserved space. The usage percent is equal to the amount of user data changes on the volume. Once this reaches 100%, the snapshot status states "in use/inactive" and the point-in-time data can not be accessed any more. In this case, click on the "stop" button in order to remove the inactive snapshot.

note

- Please do not manually start or create a time schedule for a snapshot that is already assigned for backups or replication tasks. This will block the backup or replication tasks as they are specifically assigned to activate the snapshot during the process.
- The snapshot utilizes copy-on-write technology. The more active snapshots you have, the lower write performance of the volume will be. It is recommended to have no more than 2-3 active snapshots per volume.
- Snapshots cannot be activated on an inconsistent volume. Inconsistent volumes exists on the destination system, while volume replication is initializing. Once initialization is completed, the inconsistent volume will be consistent and the snapshot can be activated.





Function: Snapshot info

Here you can see information for selected snapshot.

Name

Name of snapshot.

LV

Logical volume for which snapshot is assigned.

Status

Status of snapshot. Can be one of following:

Active

Snapshot is in active state.

Inactive

Snapshot is inactive, probable reason: overflow.

Unused

Snapshot is currently unused.

Size

Size of snapshot.

Function: Create schedule for snapshot task

Here you can create schedule for selected snapshot task.

Comment

You can enter comment for snapshot schedule.

Time select

You can start creating of the snapshot immediately by selecting "Now" from Time select drop down list or add to schedule.

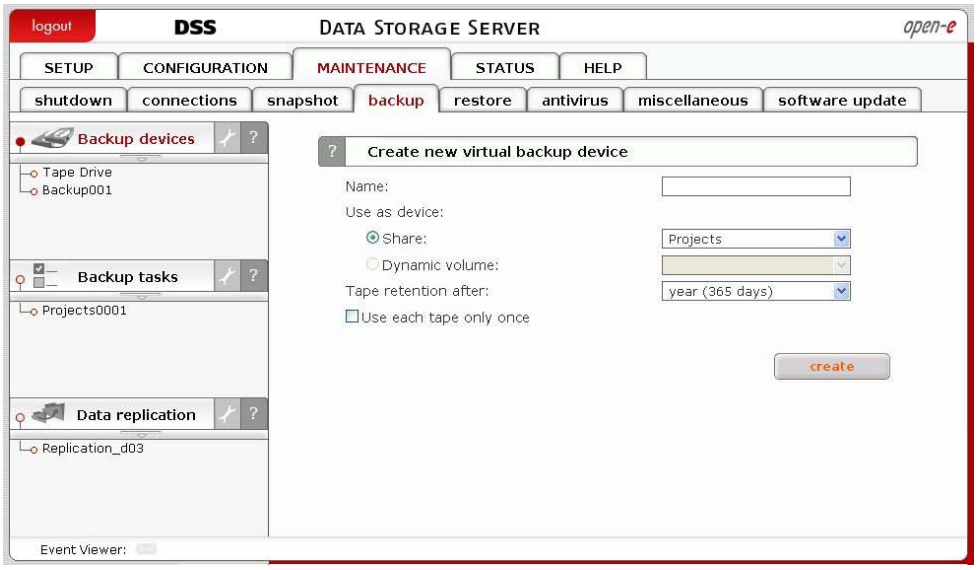
Function: Schedules for snapshot task

Here you can see all schedules created for a snapshot task.

5.2.3.4 Backup

5.2.3.4.1 Backup devices

Here you can view list of all backup devices. Click on device name to edit device settings, create new tape for the device, manage tapes or remove the device. In case when tape backup device (physical device) is connected, "Tape Drive" entry will appear on backup devices tree.



Function: Create new virtual backup device

In order to store backup of the data on virtual tapes please create virtual backup device.
This device will be used as backup destination in backup task setup.
Please provide:

- Name for device,
- Select share where the virtual backup device will be stored.

note It is recommended to create dedicated share for every virtual backup device.

- Time retention of tape,
- If you want to make one backup on one tape only, select option use each tape only once.

Click "Create" button to create new backup device.
Next step:

- Once new virtual backup device is created, click on its alias in left panel and create virtual tapes in Function: Create new tape.
- Then create new backup task.

Function: Backup device settings

Here you can set settings for selected backup device.

Time retention of tape

Time after the tape will be rewritten from the beginning.

Use each tape only once

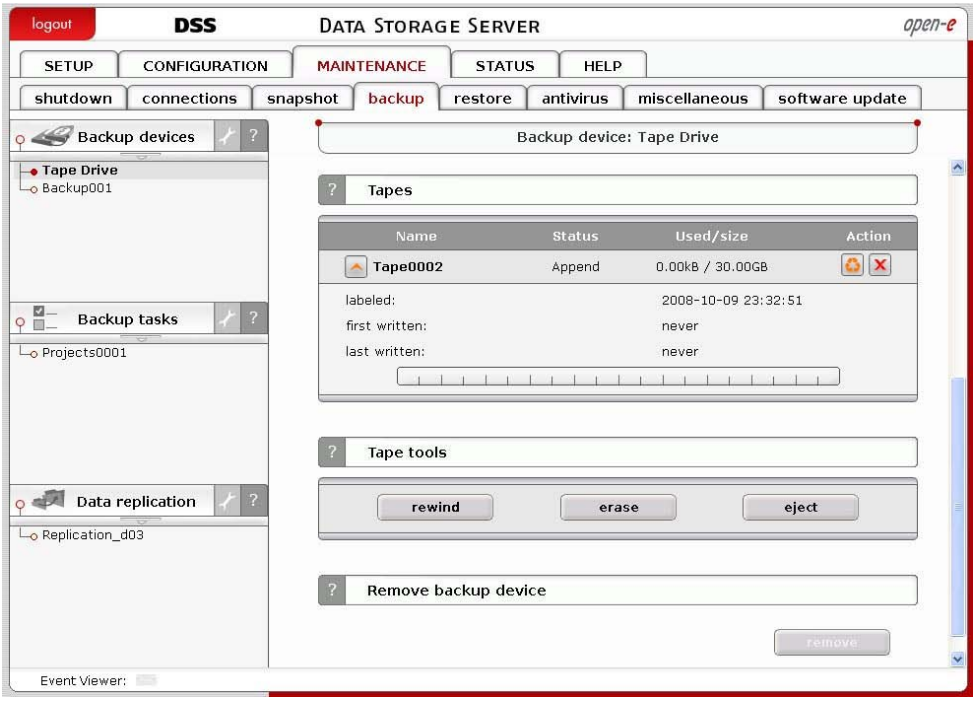
Means that each backup will be made on one tape only.

Function: Label new tape

With this function you can label new tape that will be used to make backup.
In order to label a new tape:

- enter tape name,
- select slot,
- optionally you can limit tape size,
- click "Apply".

note Make sure to insert tapes in to streamer device in proper order, otherwise tapes may have wrong slot number assigned after making backup.



Function: Tapes

Here you can view information on all tapes used with selected backup device and manage them.
Function provides following information:

Name

Name of the tape.

Status

Status of the tape. Status can be one of following:

- Full - tape is full and will not be used for backup until retention time is over,
- Append - new backups will be written at the end of the tape,
- Recycle - the tape will be set to this state when tape status has been set to purged and there is no other appendable tapes available. Tape will be set for new write from the beginning of the tape(old data will be deleted),
- Purged - this status will show up when tape retention time is over(old data is still on tape),
- Error - tape will not be used because of errors on tape,
- Used - tape has been set as used once only and cannot be append any more,
- Busy - tape is actually used for backup write.

Used/size

Shows how many MB of data has been written to tape and how many MB of data can be written to that tape.

Action

Action that can be performed on tape:

- Show more info on tape,
- Manually set tape to purged status,
- Remove the tape.

Function: Tape tools

This function provides tools to manage your tape device. Tape tools:

- tape rewind,
- tape erase,
- tape unload / eject,
- tape load.

Select tape from

Here you can select from which drive or slot tape will be used. If tape is in drive then it will be described as following: Drive drive_nr:slot_nr:bar_code_name, ex. Drive 0:1:Tape 1. If tape is in slot then it will be described as following: Slot slot_nr:bar_code_name, ex. Slot 1:Tape 1.

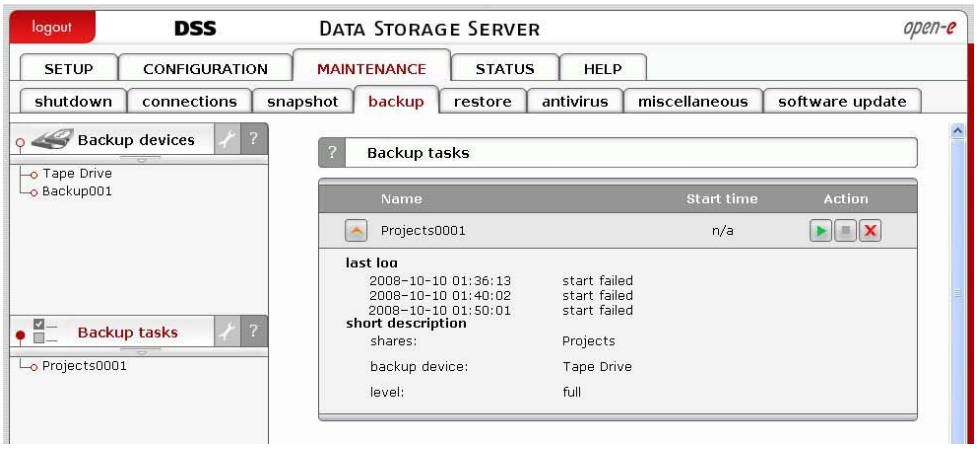
note When tape library device is connected then tape **unload** tool will appear. If streamer device is connected then tape eject tool will appear.

Function: Remove backup device

This function removes selected backup device.

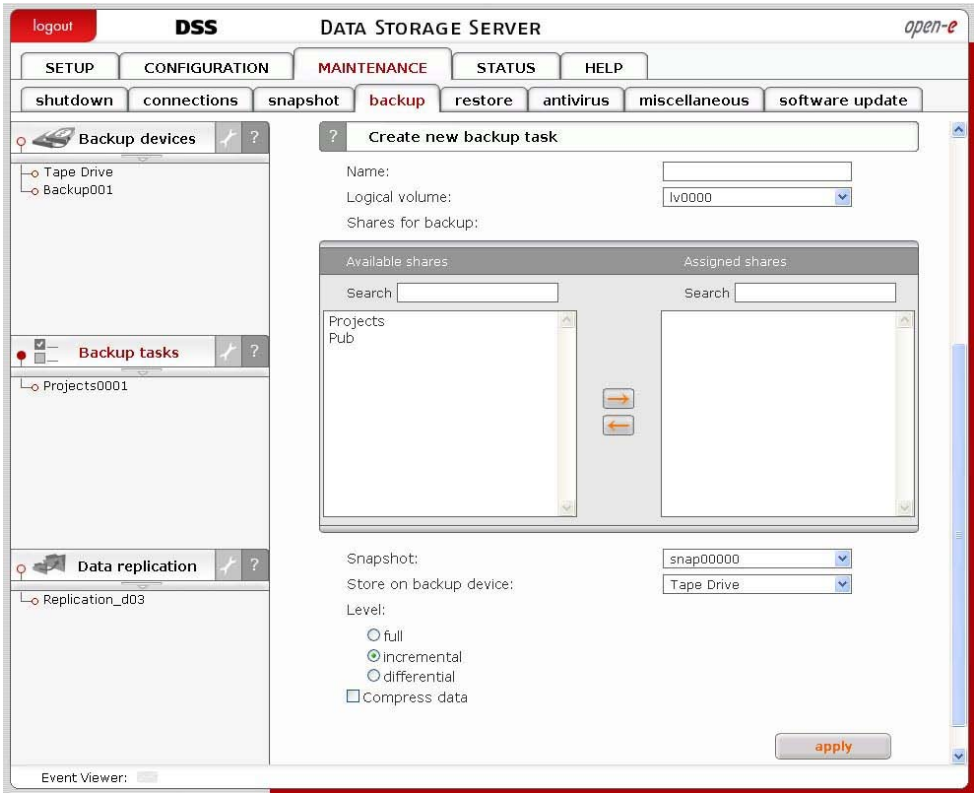
5.2.3.4.2 Backup tasks

Here you can view list of all created backup tasks. Click on backup task name to see more information about it.



Function: Backup task

Here you can run, stop or delete desired backup task. All previously created tasks will be visible



Function: Create new backup task

Here you can create new backup task.

In order to create backup task:

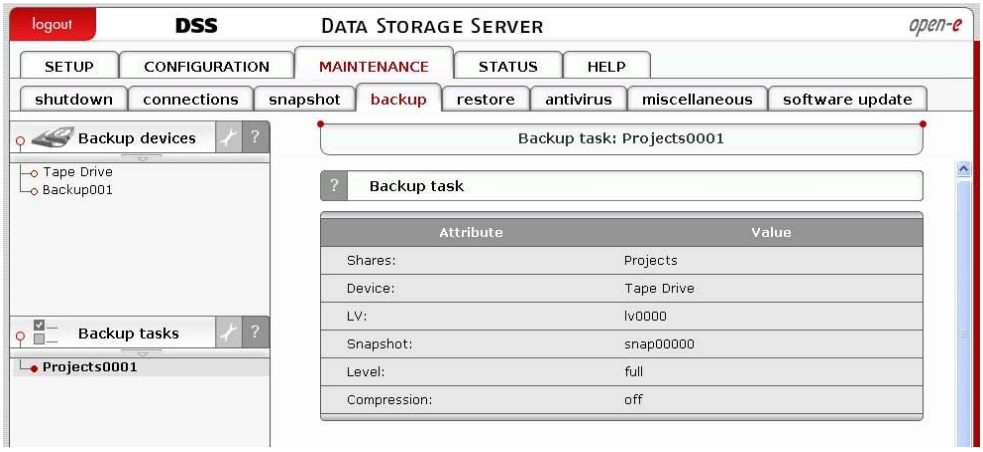
- Enter task name,
- Select Logical Volume,
- Select Shares for backup,
- Select Snapshot from which backup will be made,
- Select backup device on which backup will be made,
- Select backup level,
- If you want to compress data on backup, select option compress data, select option compress data.

Backup levels:

Full
This will backup all your data.

Incremental
This will backup only new data.

Differential
This will backup all new data from last full backup.



Function: Create new schedule for backup task

Here you can create new schedule for selected backup task.

Comment

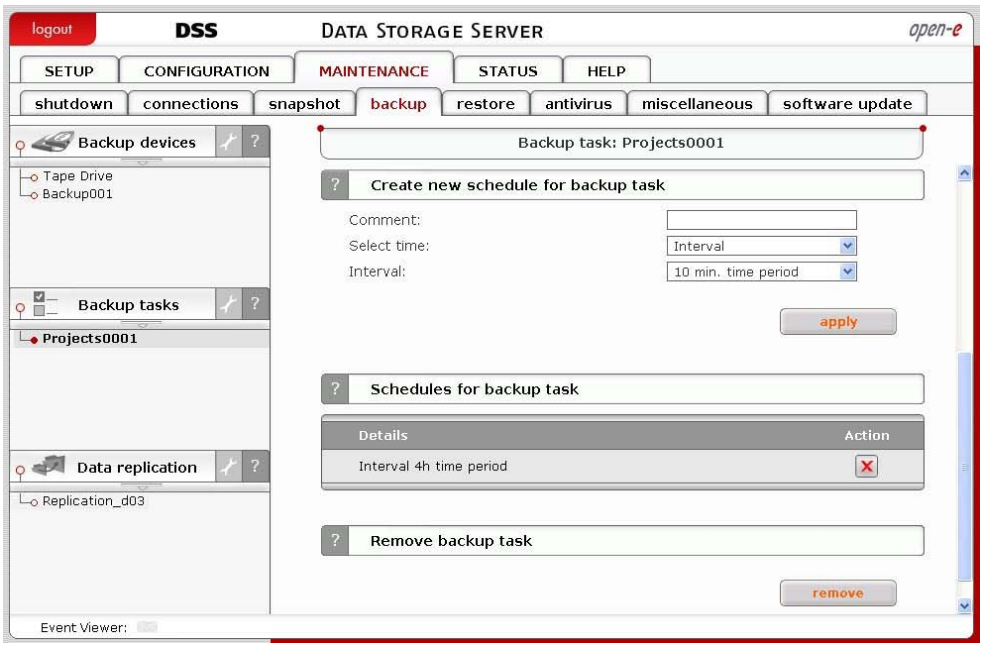
You can enter comment for backup schedule.

Time select

You can start backup task immediately by selecting "Now" from Time select drop down list or add to schedule.

Interval

Select time period that backup will be run.



Function: Schedules for backup task

Here you can see information on all schedules created for selected backup task. You can also delete any schedule by clicking "delete schedule" action button.

Function: Backup task remove

Here you can remove selected backup task.

5.2.3.4.3 Data replication

Here you can view list of all data replication tasks.

Function: Create new data replication task

This function allows you to create new data replication task. Data can be replicated as source or destination in the same time.

Task name
Please enter task name.

Source share
In order to set share as source, select it from the drop down list and enter Destination IP, where share will be replicated.

Snapshot
Snapshot assigned for data replication.

Destination share
Select destination share from the drop down list and enter destination agent login and password.

Dest. agent login
Enter destination agent login.

Dest. agent password
Destination agent password.

Log replication errors
Turn it on, if you want to log replication errors.

Replicate whole files
If this option is turn on, then all parts of a file will be replicated, if not only changed part of a file will be replicated. It's recommended to turn it on, if speed of network is faster than local partition write speed.

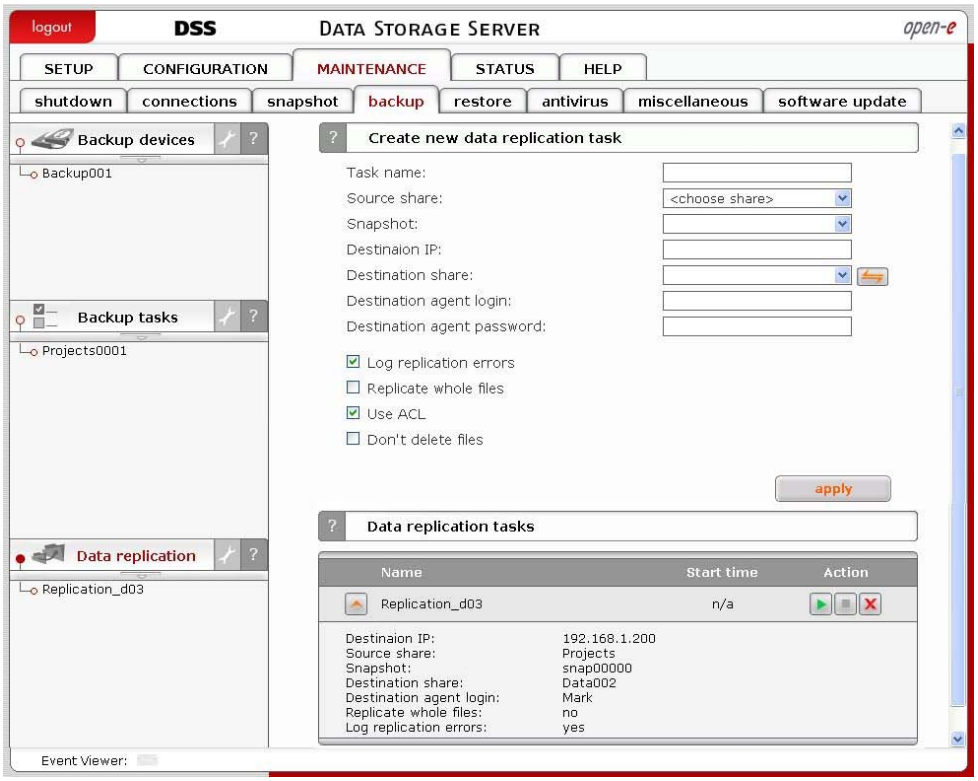
Use ACL
Turn it on if you want to have files replicated with Access Control List permissions.

Don't delete files
If this option is disabled, on destination every different files than on source will be deleted. If you want to keep these files you have to disable this option.

note In order to set share as a destination, one should enable Data replication agent in setup → NAS settings menu, then enable replication option for each share. There is no need to enable Data replication agent, if replication would be only set as source.

It's not possible to make data replication and backup in the same time. Backup has higher priority than data replication. Data replication will be stopped, if it has been setup in the same time with Backup, when using snapshots from the same Logical Volume. You will see snapshot error in Data replication status, because snapshots cannot be used twice in the same time, if they are set to the same Logical Volume.

In order to make data replication over the internet you have to configure the firewall port to: 873.

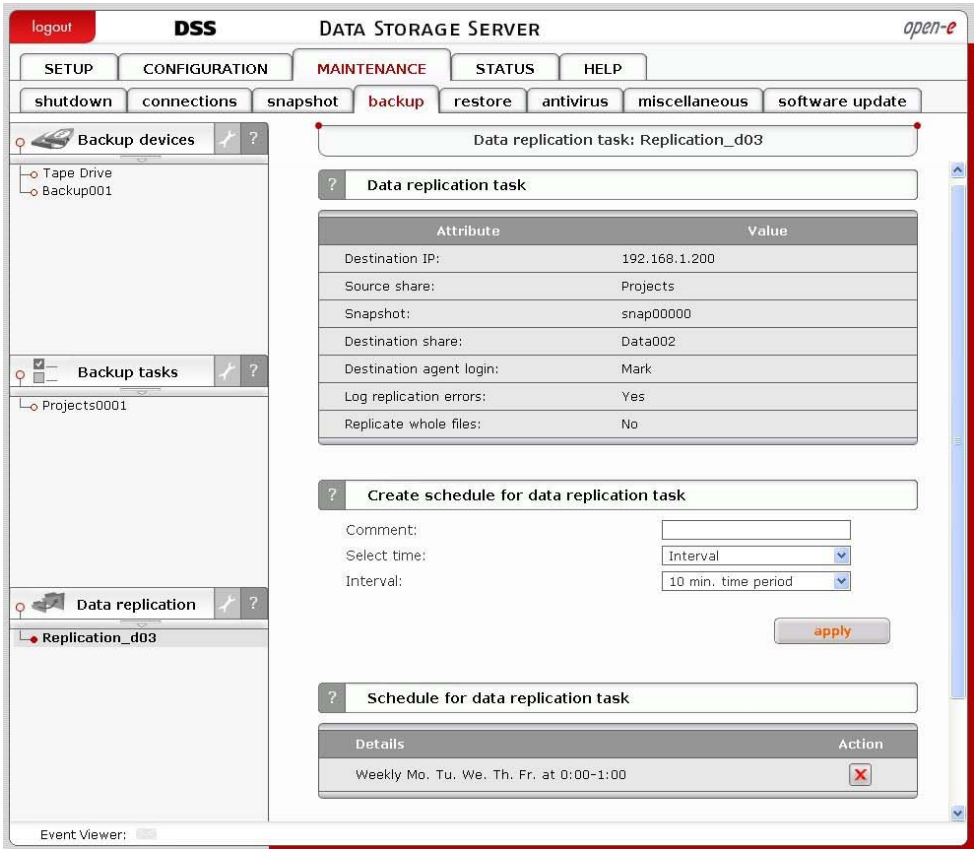


Function: Data replication task

Function shows information on selected data replication task.

You can view:

- Destination IP,
- Source share,
- Snapshot,
- Destination share,
- Log replication errors info,
- Replicate whole files info.



Function: Create schedule for data replication task

Here you can create schedule for selected data replication task.

Comment

You can enter comment for replication schedule.

Time select

You can start replication immediately by selecting "Now" from Time select drop down list or add to schedule.

Interval

Select time period that replication will be run.

Function: Schedule for data replication task

Here you can manage all schedules created for selected data replication task.

5.2.3.5 Restore

Here you can view a list of all restore tasks

Function: Backup restore tasks

With this function you can run, stop or delete backup restore tasks.
Every task is characterized by the following fields:

Name

Name of restore task.

Start time

Time when the restore task has been started.

Action

Action that can be performed on restore task.

Additional task info:

Last log

Shows action logs.

Short description

Device

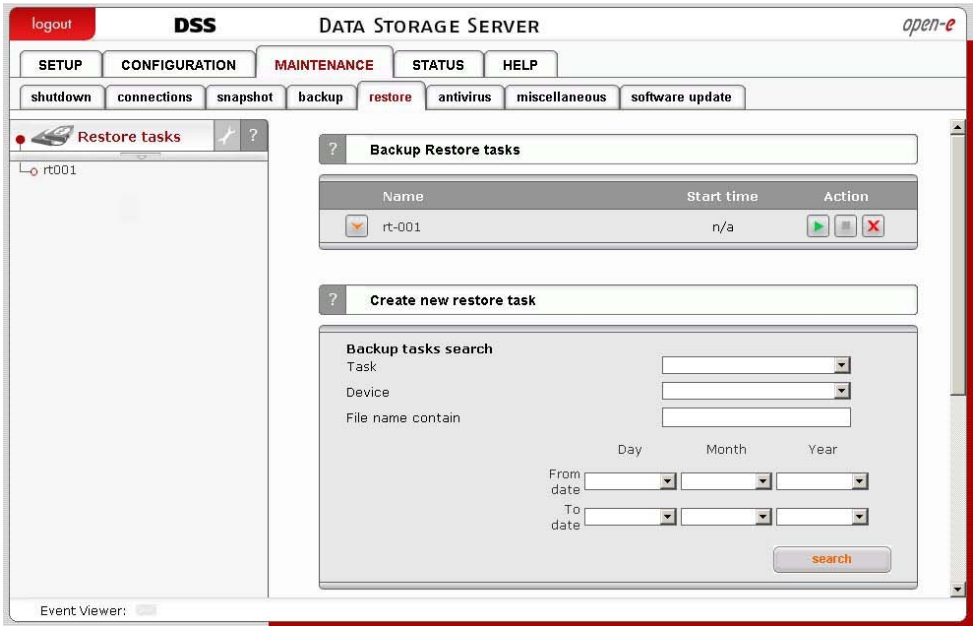
Shows if the task is running on a virtual drive or a tape drive device.

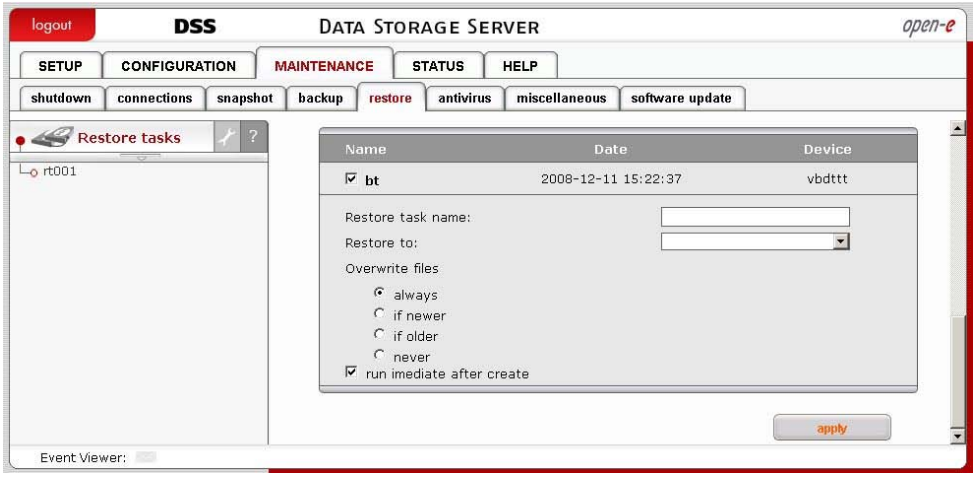
Destination share

Name of the share where the data will be restored.

Jobs

Number of running jobs for this task.





Function: Create new restore task

With this function you can search for backup tasks and create new restore tasks for the selected backup tasks. You can search according to the following criteria:

Task
Task name.

Device
Backup device name.

File name contain
This will show only those backup tasks which contain files whose names follow the search criteria. Wildcards are permitted with filenames. For example, if you put in 'M???', all backup tasks will be shown containing filenames which start with the letter M and are 4 characters long. If you put in 'M*' all backup tasks containing filenames which start with the letter M will be shown /- length is not a factor. The filename cannot start or end with space or contain special characters such as ` / ; " $ % ! ~ @ > < = + ^ # & \ ' : ,

From date, To date
Date range for the backup task. The date in the **From date** field should be earlier or the same as the one in the **To date** field. Both dates need to be in full format.

If you do not select any search options all backup tasks will be shown.

Every backup task found is described by the following fields:

Name
Backup task name.

Date
Date of backup task creation.

Device
Backup device name.

Details
Additional details:

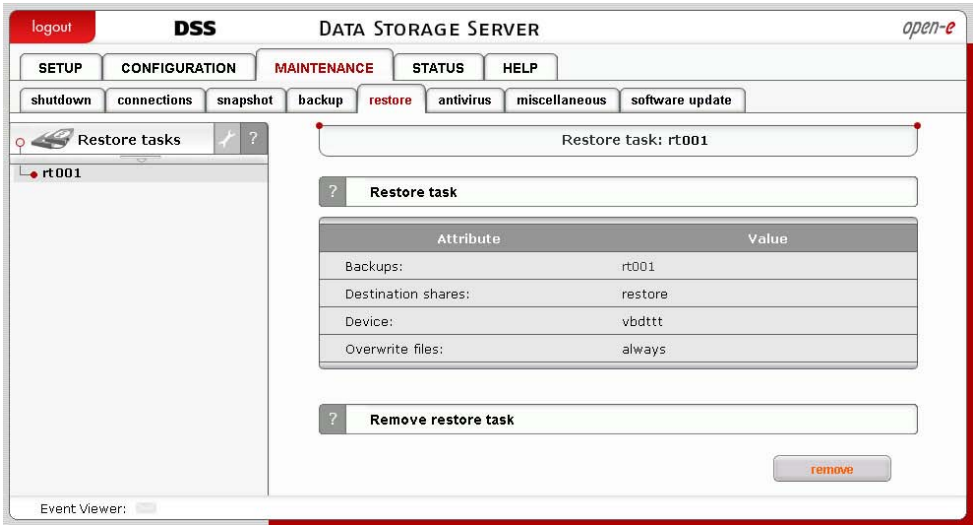
Files
Number of backed up files.

Size
Size of backup.

Required tape(s)
Tapes on which the backup is stored.

In order to create a new restore task:

- select backup task(s),
- enter a **name** for the restore task,
- select the share to which the backup will be restored (**restore to**),
- choose the overwrite options,
- select the option **Run immediately after creation** if you want to run the restore task immediately after the task has been created task creation.
- click **Apply**.



Function: Restore task

Here you can view the details for the selected restore task.

Backups

Names of backup tasks that are assigned to this restore task

Destination shares

Shares to which the restore will be made

Device

Backup device type

Overwrite files

Overwrite options

Function: Remove restore task

Here you can remove the selected restore task.

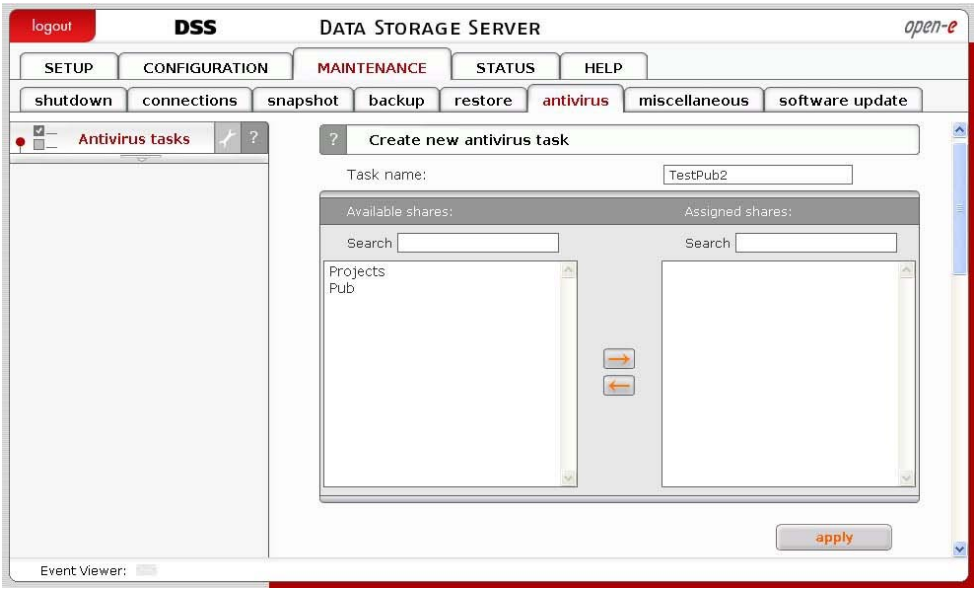
5.2.3.6 Antivirus

Function: Create new antivirus task

Here you can create a new antivirus scan task.

- Enter task name,
- Select shares for scan,
- Click "apply" to create a task.

note Antivirus doesn't scan archives protected with password.



Function: Antivirus tasks

Here you can run, stop or delete desired antivirus task. All previously created tasks will be visible here.

Function: Update virus definitions

With this function you can update virus definitions. Select mirror from which definitions will be downloaded. Select when update should be made. If you

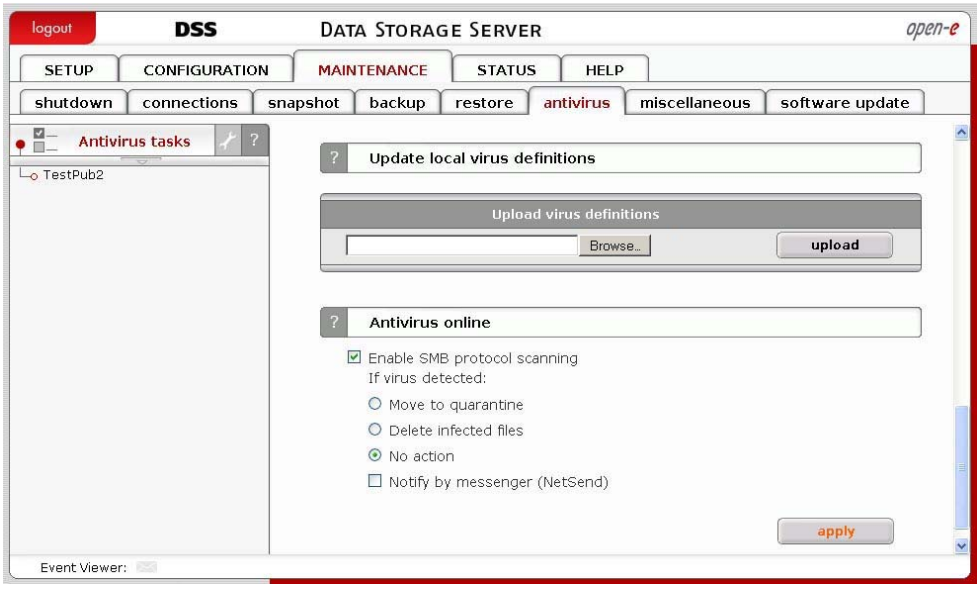
select "now", update will be made instantly. In another case update will be made now and every selected time.

Function: Update local virus definitions

With this function you can upload virus database. In order to do this:

- Click on button "browse" and select database file, downloaded from http://clamav.net/,
- Click button "upload"

Two types of database file is supported: "daily" and "main". Database file should have "cvd" extension.



Function: Antivirus online

This function gives Antivirus online protection for your network protocols. Any files transferred on the server will be scanned.
The feature Enable SMB protocol scanning allows scanning online files via SMB.

Options:

Move to quarantine

Allows moving infected files to quarantine share previously chose. Name of infected files will change with prefix vir- and randomly signs without extension.

Delete infected files

Allows automatically deleting infected files without warning!

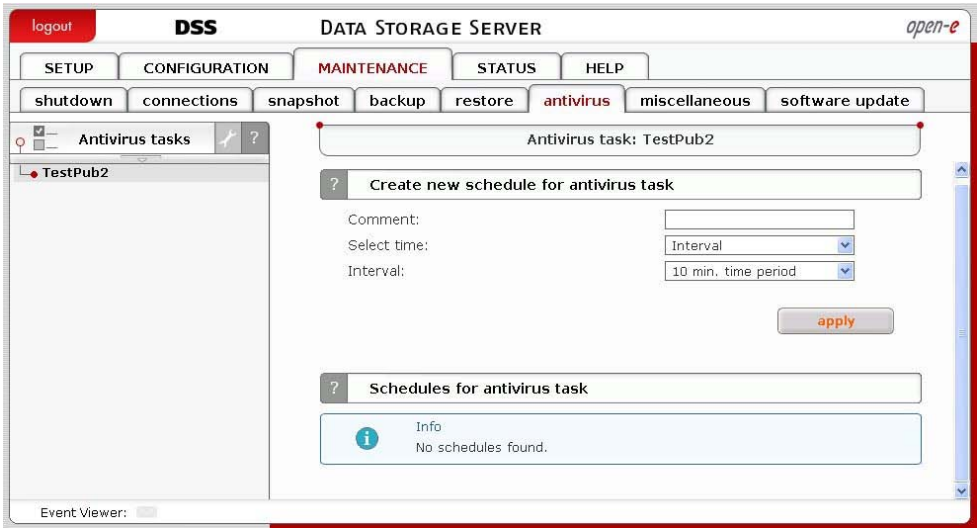
No action

Allows to choose no action on founded infected files.

Notify by messenger

Allows to get fast information about infected files by Windows Messenger (net send).

note To verify the information about the infected files look in logs. You will get the info which files are infected and with what viruses.



Function: Create new schedule for antivirus task

Here you can create new schedule for selected antivirus task.

Comment

You can enter comment for antivirus schedule.

Time select

You can start antivirus task immediately by selecting "Now" from Time select drop down list or add to schedule.

Interval

Scan will be made every "selected time". E.g. if you choose interval 1 h. - each one hour share will be scanned.

Weekly

Scan will be made in selected days at specified time.

Function: Schedules for antivirus task

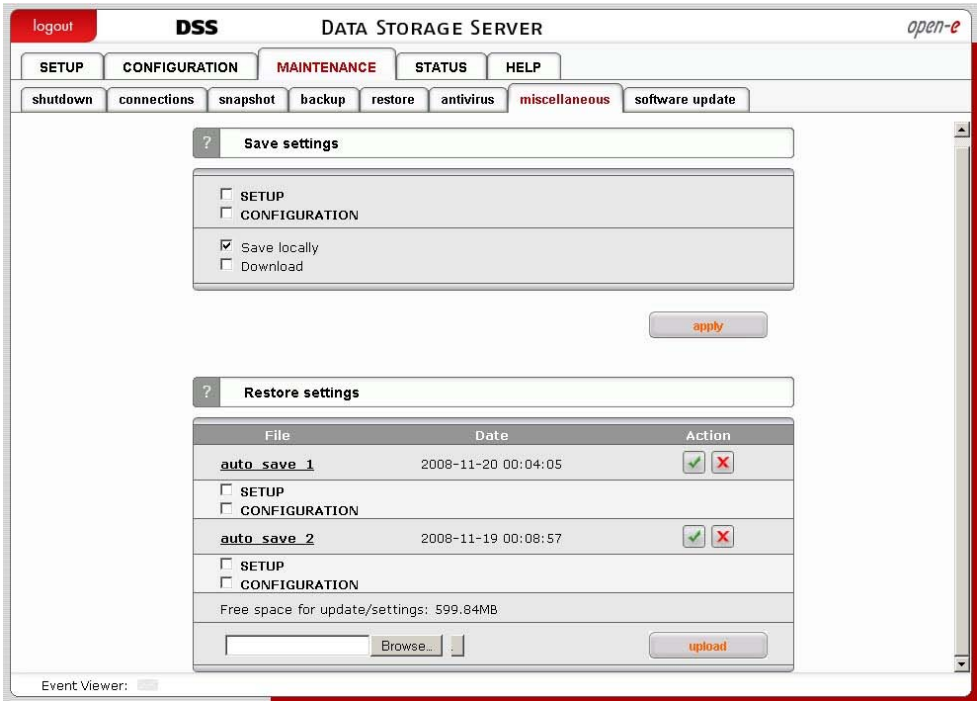
Here you can manage all schedules created for selected antivirus task.

5.2.3.7 Miscellaneous

Function: Save settings

With this function you can store the configuration settings.
Select settings you want to store and click Apply. Settings can be saved locally on the server (it will be visible in function **Restore setting**) and/or downloadable file. Each time you save settings locally a new entry will be created and during restoring you can select which settings to restore.
You can restore the settings using function **Restore settings.**

note Settings will be saved automatically every time server is restarted or shutdown. You will see new settings files, named auto_save_X / auto_save_last.



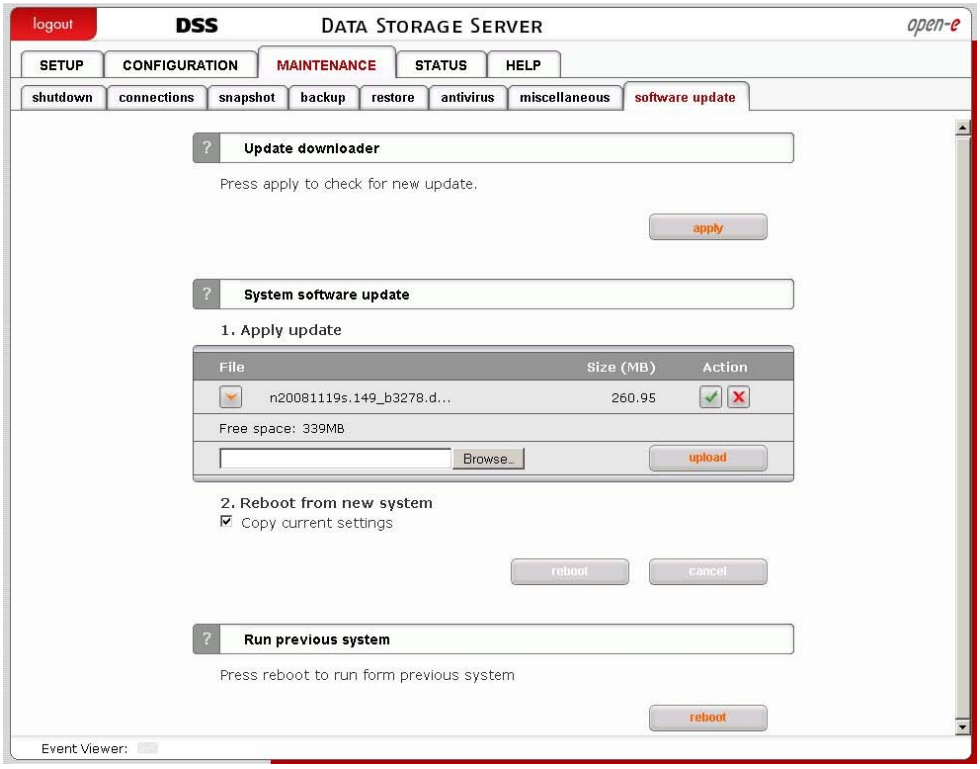
Function: Restore settings

With this function you can restore the configuration settings (previously saved). You can restore settings from files saved locally or upload configuration settings file (previously downloaded). For each entry you can see the configuration file name, date of creation and actions that can be applied. By clicking Details action button you can select witch settings to restore. To restore settings click on Restore action button.
You can delete configuration settings file by clicking Delete action button. You can download configuration settings file by clicking its name. In order to upload configuration settings file (previously saved) browse a file name and click on Upload button.
You can save the settings using function **Save settings**.

note Settings will be saved automatically every time server is restarted or shutdown. You will see new settings files in function Restore settings, named auto_save_X / auto_save_last.

5.2.3.8 Software update

This function allows you to update the system software. There are two ways of updating Open-E DSS software.



Function: Update downloader

With this function you can check if there is new update available and download it. In order to download a new update you need to be registered at www.open-e.com. You also have to remember to setup correct DNS and Gateway address in “SETUP” → “network” menu.

Function: System software update

This function allows you to update the system software.
When you upload the update file you will see its name and size. With each update file you do following action:

- See release notes,
- Make update (Update button),
- Delete update file (Delete button).

After making update you can reboot system from new system with option **Reboot from new system**. If you want to copy current settings check option **Copy current settings**. Click button **reboot** to reboot from new system.

Information about serial number:

- First three digits are related to system version. If after update this value has been changed then it means that it was full update and many of system components was updated.
- After dot 8 digits string is related to small updates. For example if small update with newer drivers is installed then one of zeros will be changed to 1.
- Last four digits are related to build number. Some critical and small updates can change its value when i. e. system sources are updated.

note Some updates need a system restart. In this case you will be informed about needed restart in confirmation message.

Function: Run previous system

With this function you can run previous system.

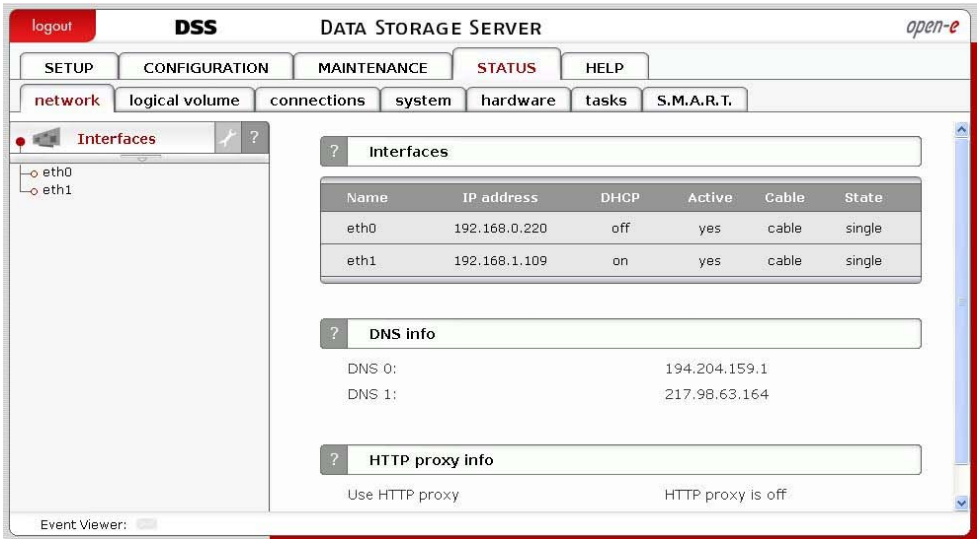
5.2.4 STATUS

This function provides a quick overview of the most important system parameters of your Open-E Data Storage Server. The corresponding sub-functions are network, logical volume, connections, hardware, tasks and S.M.A.R.T.

5.2.4.1 Network

Function: Interfaces

Here you can view network interfaces info. In table you can see network interface name and IP address, DHCP information, cable status.

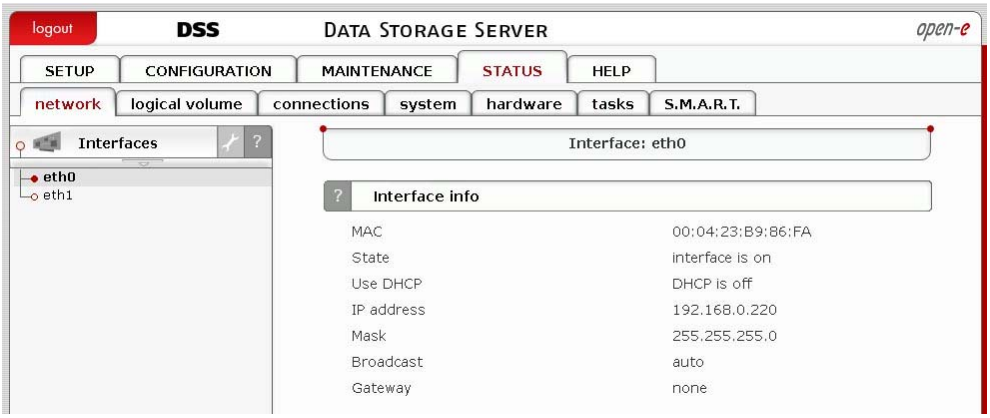


Function: DNS info

Here you can view network interfaces DNS information.

Function: HTTP proxy info

With this function you can view HTTP proxy information. You can see if proxy is enabled and which HTTP proxy IP address is assigned to it.



Function: Interfaces info

This function shows information about selected network interface. You can view here:

- MAC address,
- State,
- DHCP status,
- IP address,
- Mask,
- Broadcast address,
- Gateway address.

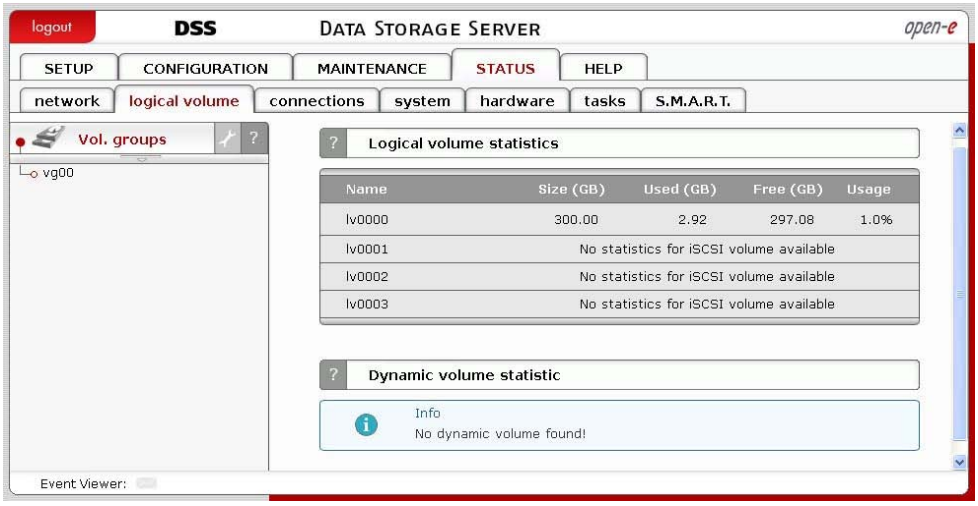
5.2.4.2 Logical volume

Function: Share volume statistics

This function contains statistical data on the share volume.

Function: Dynamic volume statistics

This function contains statistical data on the dynamic volume.



Function: Logical volume statistic

Here you can see information on selected share volume.
Function provides following information:

Usage

Percentage usage of space by share volume.

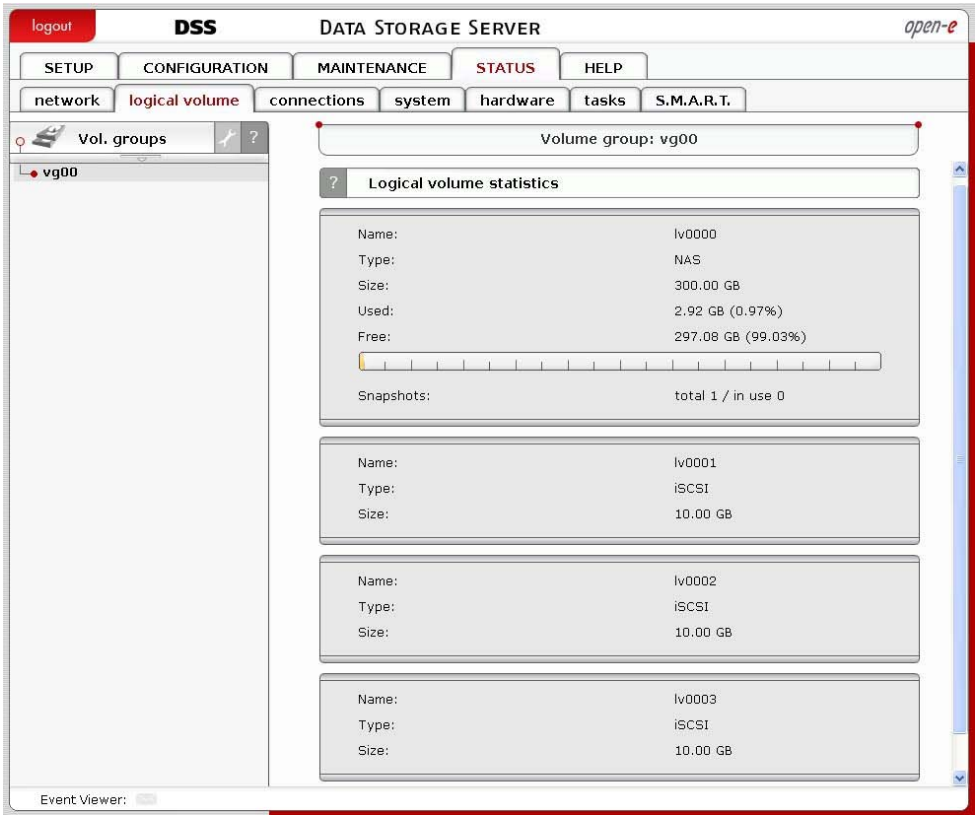
Size
Size of share volume.

Used
Current date usage of space on share volume.

Available
Available space on share volume.

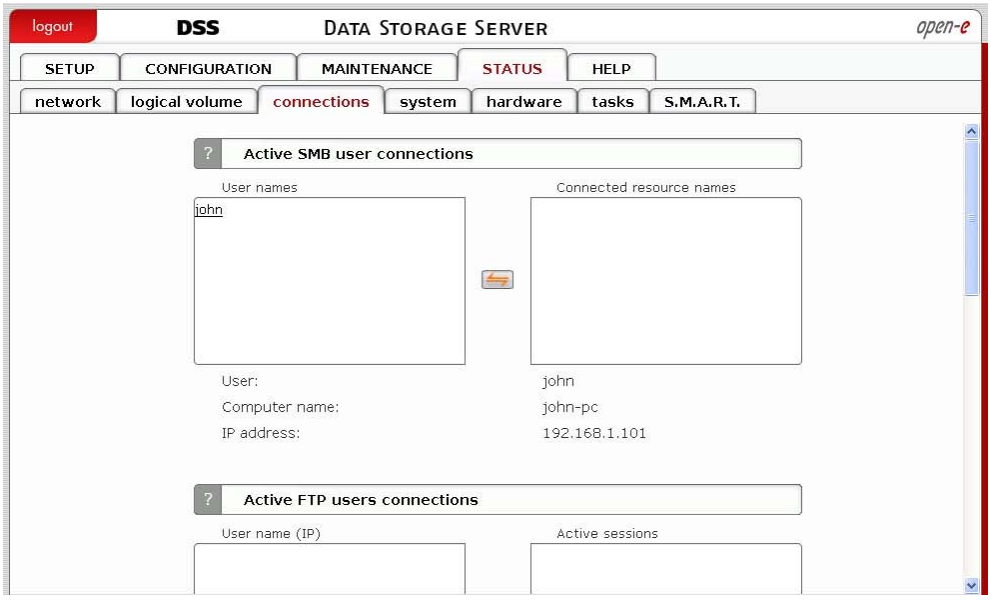
Total snapshots
Number of all snapshots assigned to share volume.

Snapshots active
Number of active snapshots.



5.2.4.3 Connections

This function displays what user connections are currently active.



5.2.4.4 System

Function: Services

Here you can view statistics for services.

Service

Service name.

State

Describes state of service, can **On** or **Off.**

Status

Describes if service is currently running (Active) or not running (Inactive).

After clicking details button close to service name, following info on selected service is available:

Name

Name of process that belongs to service.

Description

Information about process.

Count

Count of processes.

Function: Added license keys

Here you can view all added license keys.

Key

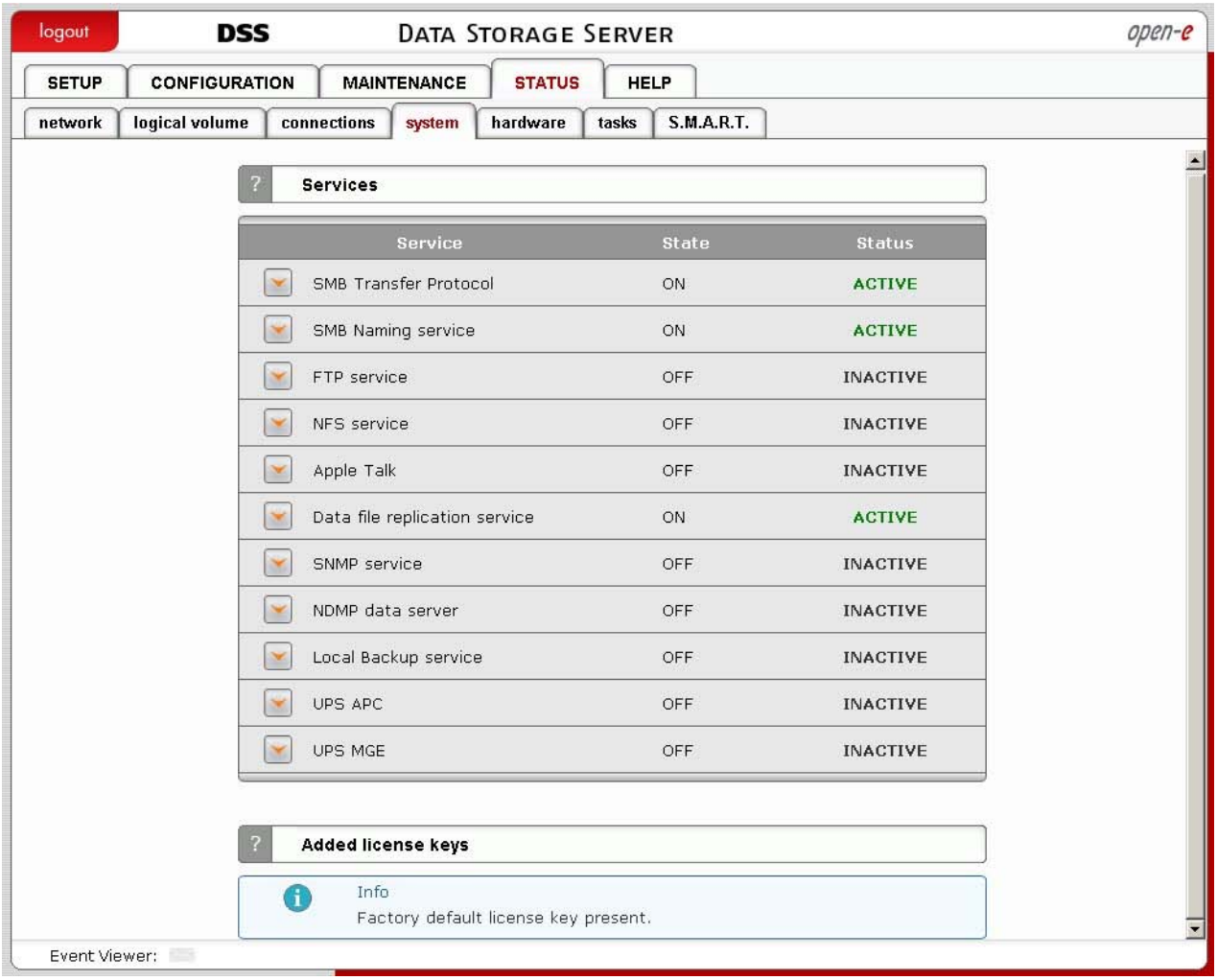
License key.

Type

Type of license key, can be: storage limit or MRCP.

Amount

Detailed amount for license key type.



5.2.4.5 Hardware

The “Hardware” option provides you with information on UPS and network controllers and the drivers (e.g. network driver and RAID driver).

In addition, you may also download the latest Open-E Data Storage Server log files or view specified or all log files without downloading in compressed form. You can also check usage of memory (RAM) and (SWAP) and also hardware monitoring.

Function: UPS status

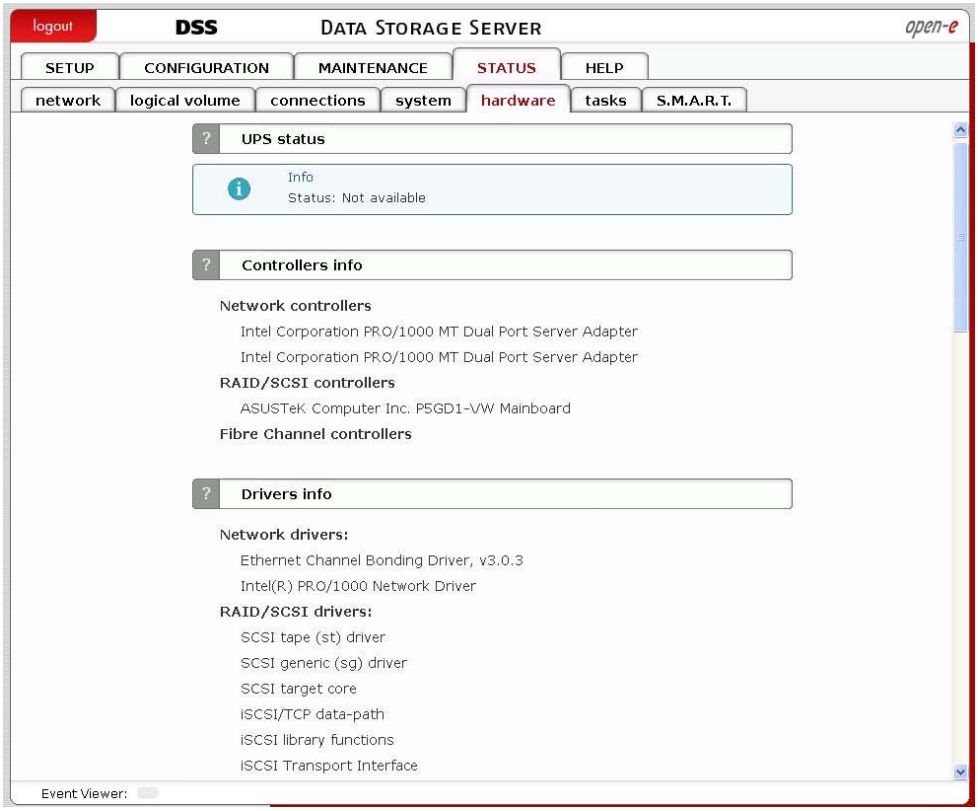
The UPS status presents the current status of ups device.

Function: Controllers info

This table lists the components installed in your server.

Function: Drivers info

This table presents active drivers loaded for hardware detected during boot-up process.



Function: Logs

This function lets downloading or removing the logs gathered during operation of the Server. In the logs all system information, which are needed for troubleshooting in case of problems can be found.

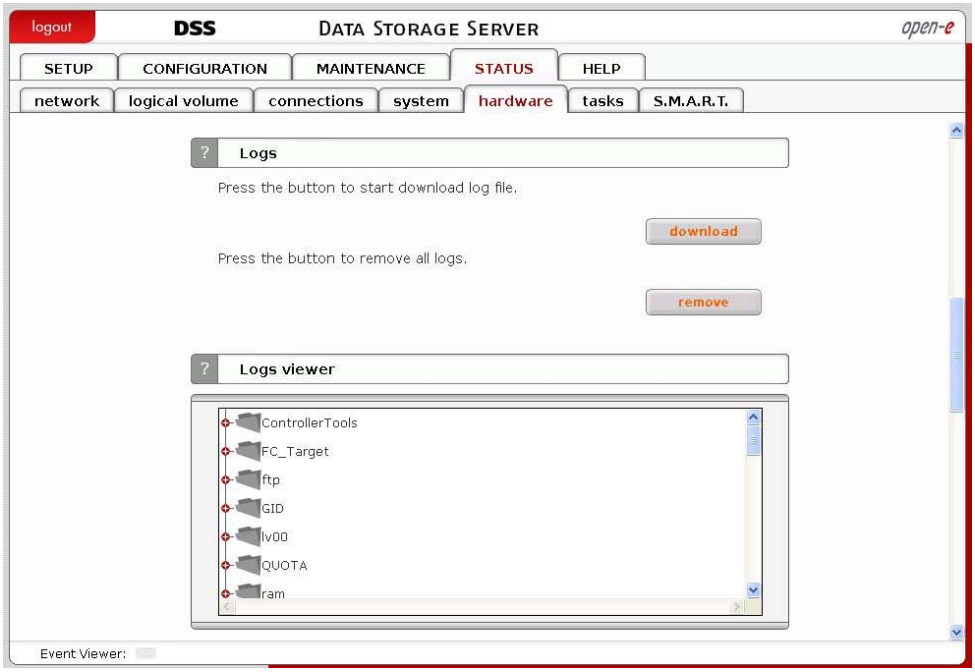
note Recovery Information of the logical volume manager are also stored in the logs. It is recommended to download logs after creating the logical volumes and store them in a save place as source for logical volume and volume groups recovery in case of a critical hardware failure.

note While generating the logs a simple speed test of the disks is done. When software Raid is used with a lot of single disks, this may take up to few minutes.

Function: Logs viewer

This function allows you to view specified log file without downloading all log files in compressed form.

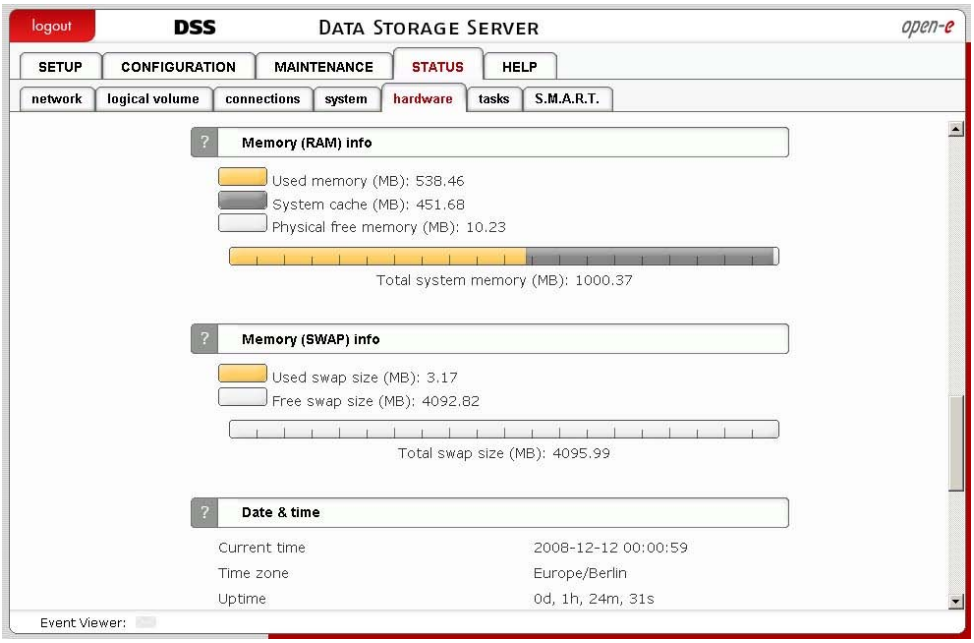
To view a log file just click on name of that file. Depending of Web browser you use you may be asked to choose appropriate program to view specified log file. To change folder just click on the name.



Function: Memory (RAM) info

This function presents the current memory usage.

note Memory allocated by system cache will be released when some application will require additional memory. If there is almost no free memory you can enable swap or install more memory modules.



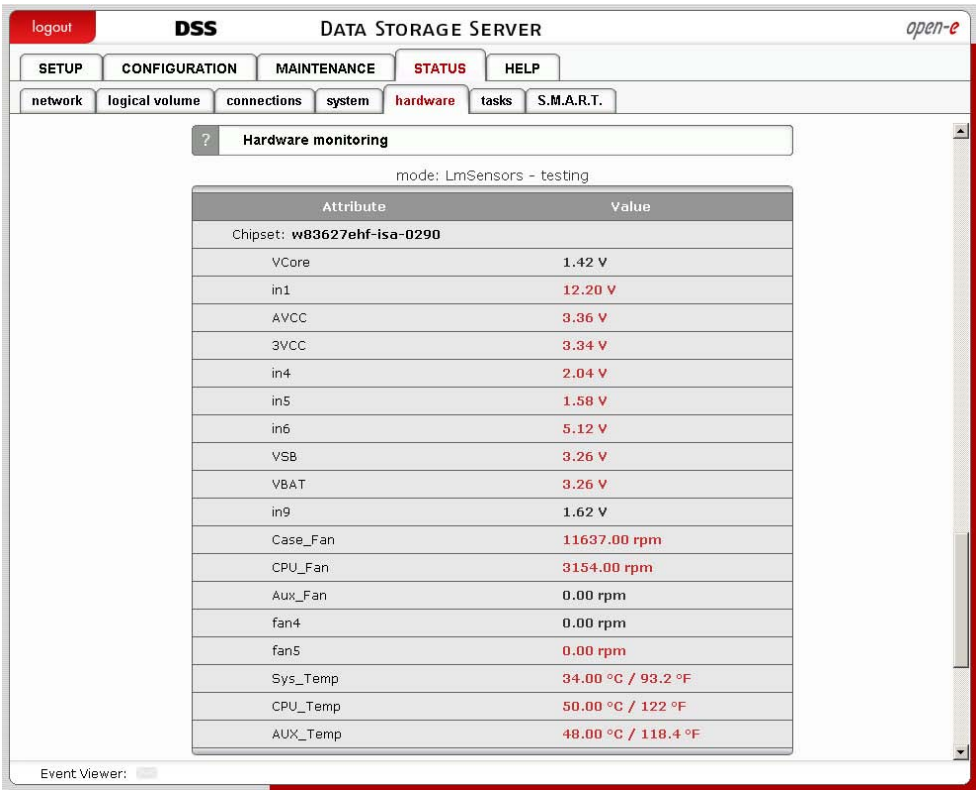
Function: Memory (SWAP) info

The memory (SWAP) info presents the current status of swap usage.

note Swap is used to store memory areas on hard drives instead of RAM (Random access memory). Operating systems dumps memory area to swap when this area was not in use since a long time and there is a need to allocate some additional memory.

Function: Date & time

This function presents current date and time of your server.



Function: Hardware monitoring

This function monitors hardware. To enable it, you need to access the **Hardware Configuration tool** in the console followed by **Hardware options** (*press F1 in the console to list keyboard shortcuts*).

When using the **LmSensors** hardware mode you can find information on the following parameters here:

- Motherboard temperature,
- CPU temperature,
- Chipset temperature,
- Vcore,
- Fan rotation speed.

After initializing, a chipset selection window appears, followed by sensor selection.
The sensor selection screen comprises of three columns. The first column displays the sensor name as indicated by lmsensors; the second displays the sensor name as indicated by the user; the third displays the ideal value for the given sensor.
After a sensor has been selected you will be presented with its configuration window. The state of the sensor is indicated at the top. Configurable values are divided between two columns.

- **Label** - the user-modifiable sensor name.
  Ideal value.

- **Minimal value** - if the current value is smaller than the minimal value it will be marked in red in the server GUI.
- **Maximum value** - if the current value is larger than the maximum value it will be marked in red in the server GUI.
- **Multiplex** - the actual current value will be multiplied by the multiplex value, the result being shown as the current value.
- **Addition** - the addition value will be added to the actual current value, the result being shown as the current value.
- **Ignore -** when this option is enabled, the sensor in question will not be displayed in the server GUI.

When using the **mbmon** (motherboard monitor) hardware mode you can find information on the following parameters here:

- motherboard temperature,
- CPU temperature,
- chipset temperature,
- Vcore.

Supported chipset family	
winbond	LM78/LM79, W83781D, W83782D, W83783S, W83627HF, W83697HF, AS99127F, ASB100
wl784	W83L784R, W83L785R, W83L785TS-S
via686	VT82C686A/B
it87	IT8705F, IT8712F
gl52	GL518SM, GL520SM
lm85	LM85, ADM1024, ADM1025, ADM1027, ADT7463, EMC6D10X
lm80	LM80
lm90	LM90, ADM1020, ADM1021, ADM1023
lm75	LM75

When using **xyratex** hardware mode you can find here information on following parameters:

- Disks status,
- Fans speed,
- Fan PWM,
- Power status,
- Fan status,
- Temperature.

When using **IPMI (sensors)** mode you information which you can see depends on motherboard. To be able to enable this mode you need to have motherboard with sensors management component that support access via IPMI.

When using **Intel SSR212 2U** mode you can find here information on following parameters:

- Power status,
- Memory Voltage,
- Voltage levels,
- Box Temperature,

- CPU Temperature,
- FAN speed.

When using **Intel SR2500ALLX** mode you can find here information on following parameters:

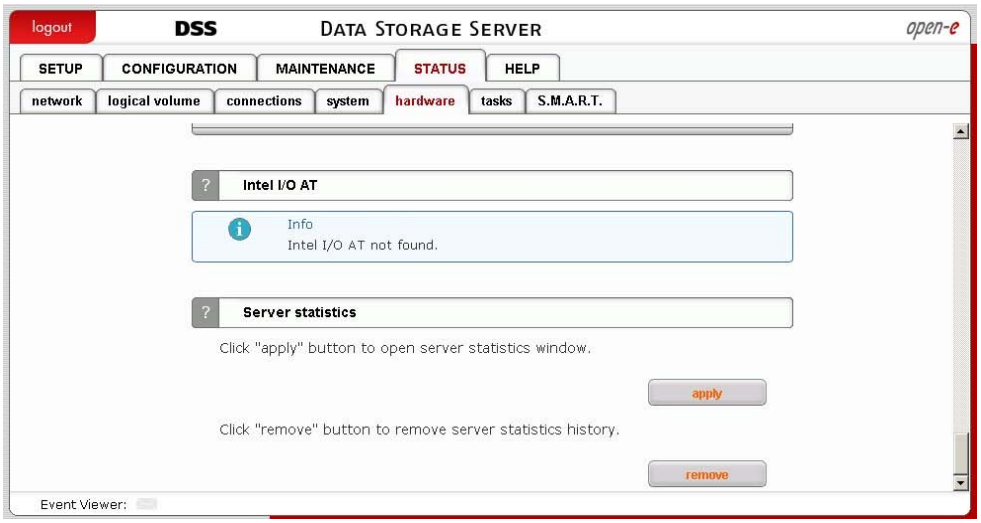
- Power status,
- Memory Voltage,
- Voltage levels,
- Box Temperature,
- CPU Temperature,
- FAN speed,
- Disks status.

When using **AOC-SAT2-MV8** mode you can find here information on following parameters:

- Unit - Displays unit name,
- Bay - Number of bay in which unit is inserted,
- Serial Number - Serial number of unit.

When using the **Intel SSR212MC2** mode you can find information on the following parameters here:

- Disc status - displays disk status,
- BBU status - displays backup battery unit status,
- BBU Capacity Info - displays backup battery unit capacity stats,
- BBU Properties - displays backup battery unit properties,
- BBU Design Info - displays backup battery unit design parameters,
- IPMI Sensors - IPMI Sensors stats.



Function: Intel I/O AT

Here you can view the status of Intel I/O AT. The primary benefit of Intel I/O AT is its ability to significantly reduce CPU overhead, freeing resources for more critical tasks. Intel I/O AT uses the server's processors more efficiently by leveraging architectural improvements within the CPU, chipset, network controller, and firmware to minimize performance-limiting bottlenecks. Intel I/O AT accelerates TCP/IP processing, delivers data-movement efficiencies across the entire server

platform, and minimizes system overhead. Intel I/O AT provides network acceleration that scales seamlessly across multiple Gigabit Ethernet (GbE) ports.

DMA status
In this section you can view which of the four DMA channels are used.

Bytes transferred
Shows a count of bytes transferred through each DMA channel

Function: Server statistics

Here you can open window with server statistics. Following statistics are available:

- System load,
- Memory,
- Uptime,
- Network.

5.2.4.6 Tasks

Here you can view statistical information on tasks from backup, data replication, volume replication, antivirus and snapshots.

Function: Running tasks

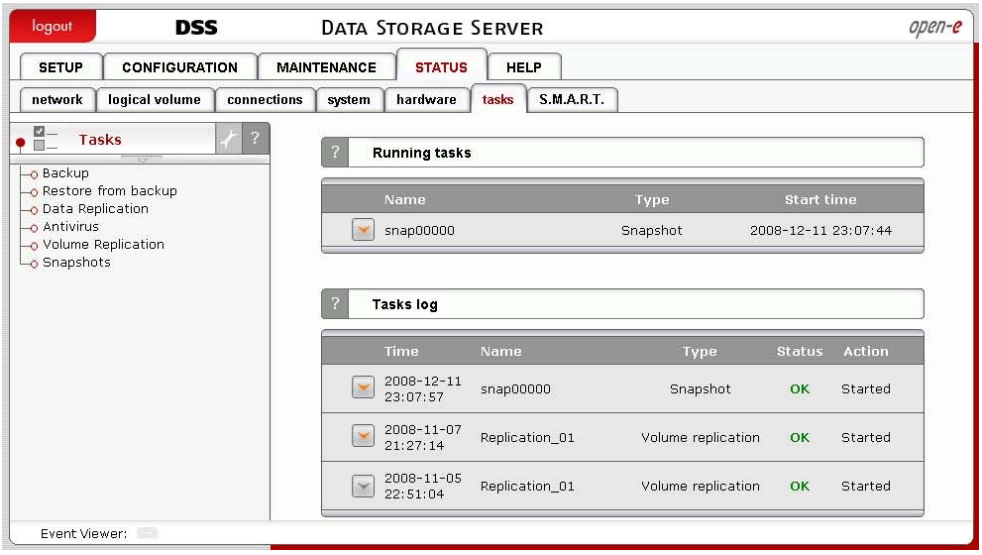
This function displays information about all currently running tasks.
You can see here all tasks from:

- Backup,
- Data replication,
- Volume replication,
- Antivirus,
- Snapshots.

Every running task is described by:

- Name,
- Type,
- Start time,
- Details.

In order to see details of running task click on "Show details" button.
More info about details, can be found by clicking task type in Tasks tree and clicking help from function **Running tasks**.



Function: Tasks log

This function displays information logs from all task types.
Every task log is described by:

Time

Time of task start.

Name

Name of the task.

Type

Type of task. Type can be one of following:

- Backup,
- Data replication,
- Volume replication,
- Antivirus,
- Snapshots.

Status

If action was successful, status will be **OK**, in another case status will be **FAILED.**

Action

Describes following states:

- Started,
- Stopped,
- Finishes.

Details

Task log details.

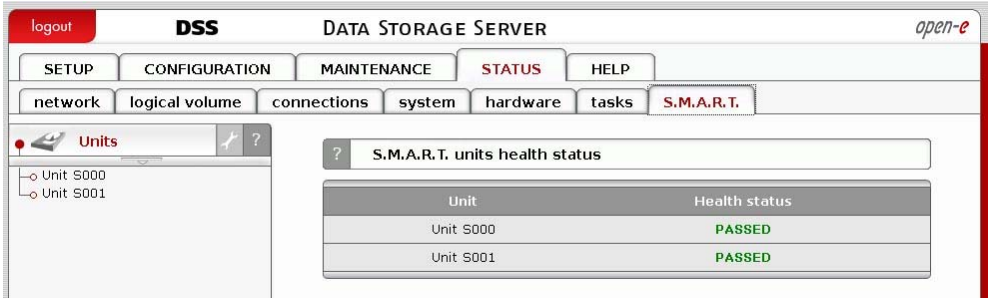
In order to see details of task log click on "Show details" button.

More info about Task log details, can be found by clicking task type in Tasks tree and clicking help from function **Tasks log.**

5.2.4.7 S.M.A.R.T.

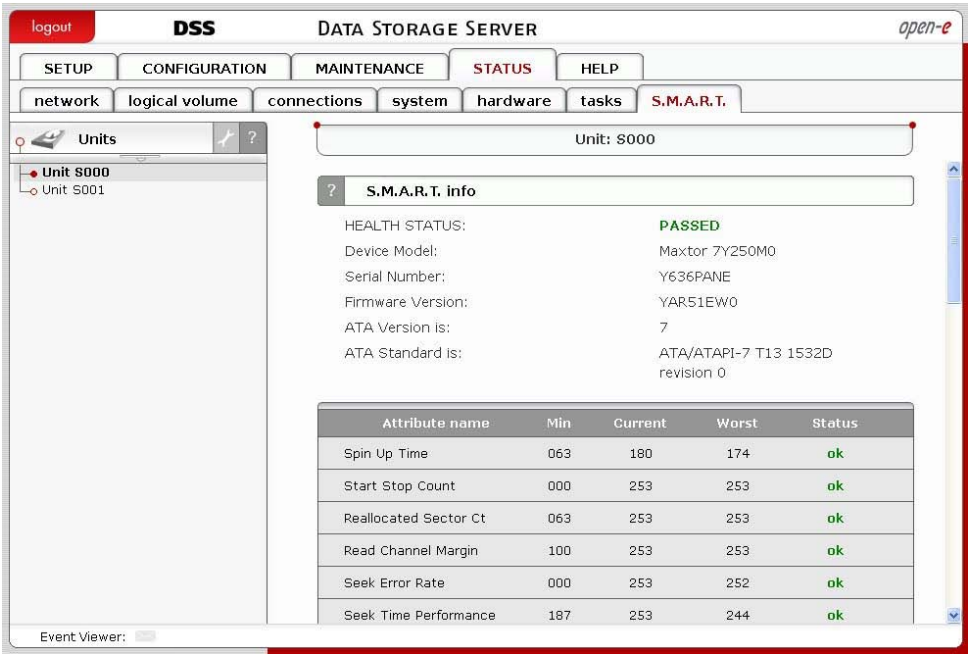
Through the S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) system, modern hard disk drives incorporate a suite of advanced diagnostics that monitor the internal operations of a drive and provide an early warning for many types of potential problems. When a potential problem is detected, the drive can be repaired or replaced before any data is lost or damaged.

Here you can find tree with hard drives for which you can view S.M.A.R.T. information.
It is possible to view information about separate hard drive or summary for all drives in the system.
To view S.M.A.R.T. information for a hard drive - please click on appropriate drive name.
To view summary please click on "all units"



Function: S.M.A.R.T. units health status

This function allows you to check S.M.A.R.T. status of hard disks.
S.M.A.R.T. is a monitoring system for computer hard disks to detect and report on various indicators of reliability, in the hope of anticipating failures.
To enable S.M.A.R.T. checks you need to use Hardware Configuration tool on console and enable it in Functionality options (press F1 on console to *find out keyboard shortcuts*).

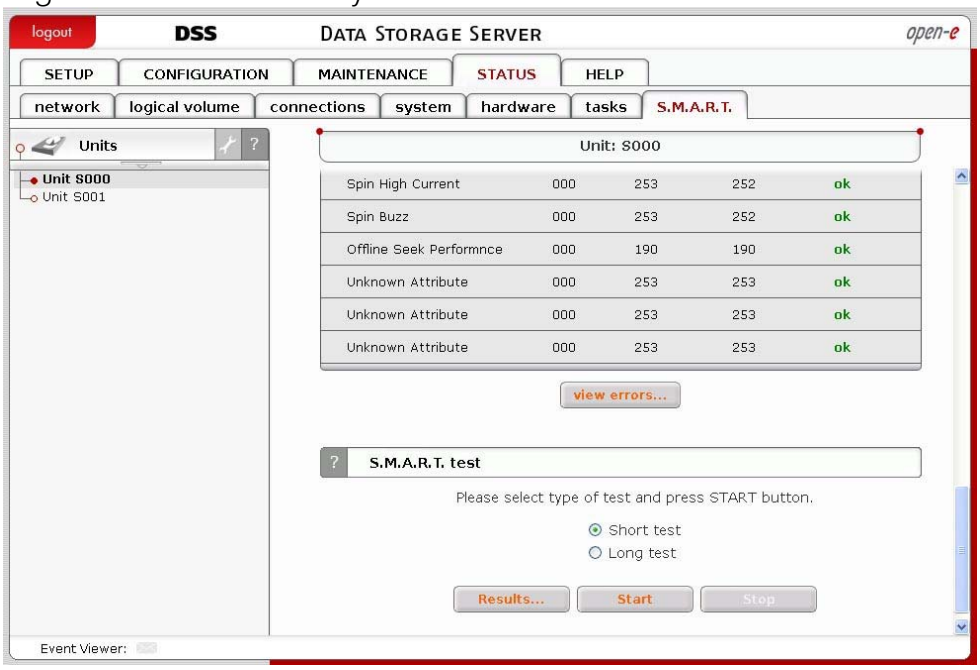


Function: S.M.A.R.T. info

This function allows you to view S.M.A.R.T. parameters which this disk is able to return.
In the upper part of this function you can see elementary parameters of hard drive such as device model or serial number. Below there is a table with S.M.A.R.T. attributes. In first column you will find an attribute name, in second - minimum threshold value of this parameter, then current value, next worst value and after the status.

note If value of attribute have ever exceeded worst of this value then the status will be "failed".
If value of attribute is on the edge of worst value then the status can be "pre-failed".
On some hard drives part of attributes can be displayed as "Unknown_Attribute" - this can happen when producer of that hard drive have done some modifications in S.M.A.R.T. and this changes are not yet supported by our software.

Button "view errors" provide you ability to view S.M.A.R.T. log of that drive which is generated automatically.



Function: S.M.A.R.T. test

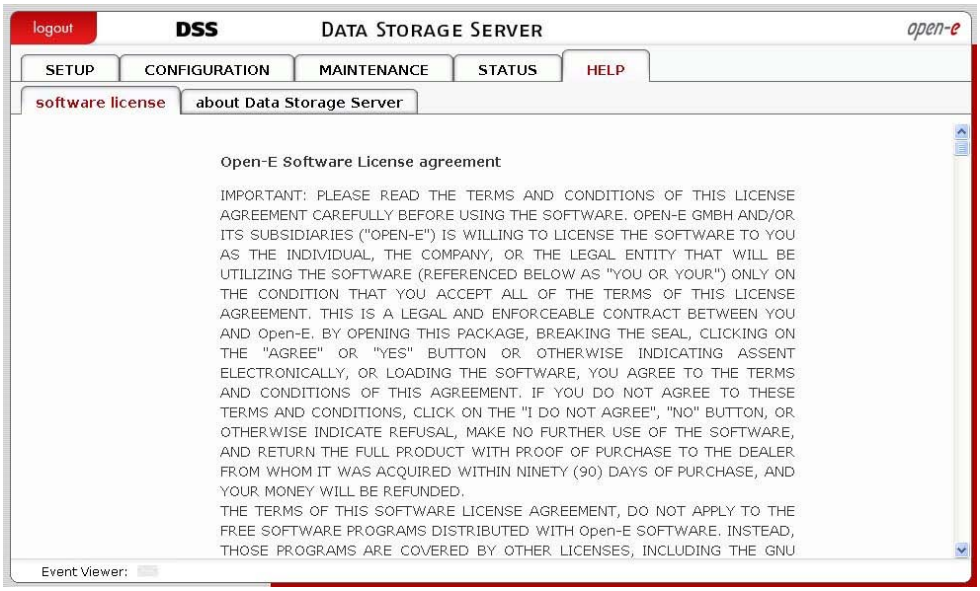
This function allows you to perform short and long test of hard drive.
You will be informed about progress of test.
After finish of test please click on "results" button to view test log.
Performing a test is not recommended during normal (daily) usage of that hard drive.

note It can happen that on some motherboards and controllers S.M.A.R.T. tests will not work.

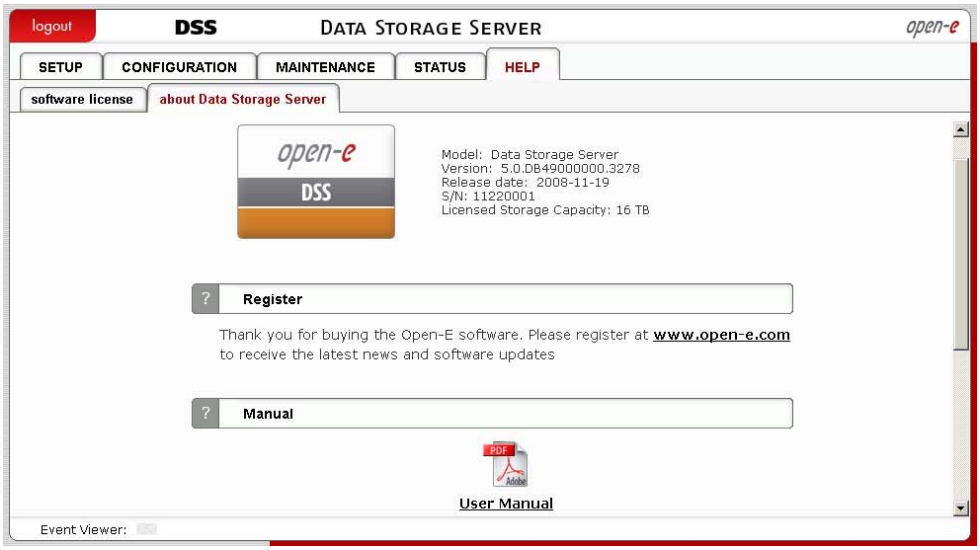
5.2.5 HELP

5.2.5.1 Software License

When accessing Help - “software License” you can read the license for software included in Open-E Data Storage Server.



5.2.5.2 About Data Storage Server



Function: Register

Here you can find a link to our registration form. Note that registration is required to receive updates and new versions. Registration also gives you an opportunity to receive e-mail notifications on software news.

Function: Manual

You can download the manual here and print it for quick reference.

note In order to read the manual, you need a PDF viewer such as the Acrobat Reader (http://www.adobe.com).

Function: Service:

Please have the following information available before contacting the technical support team:

- logs, which you can download via: Status → Hardware → Logs.
- your software version, which you can find in: Help → About.

Function: Add license key

Here you can enter a license key to expand the functionality of your server. For example, you can add a license key for a greater storage capacity.

You log out by closing the browser window.

6 Troubleshooting Guide

Here is a list of common error messages and their significance as well as corresponding tips on how to resolve the underlying problems. If your error message is not listed here please contact the Open-E support and service team (see the “help” section above). Our staff will help you find a solution.

Error: user already exists

There cannot be more than one user with the same name. You cannot create a user twice. Check your spelling. Remember, usernames are not case-sensitive. You can check existing usernames by collapsing the tree diagram on the left.

Error: values are not valid

You have entered an invalid parameter. IP addresses have the following format: aaa.bbb.ccc.ddd. All four parameters range between 0 and 255 and are always separated by periods.

Error: resource already exists

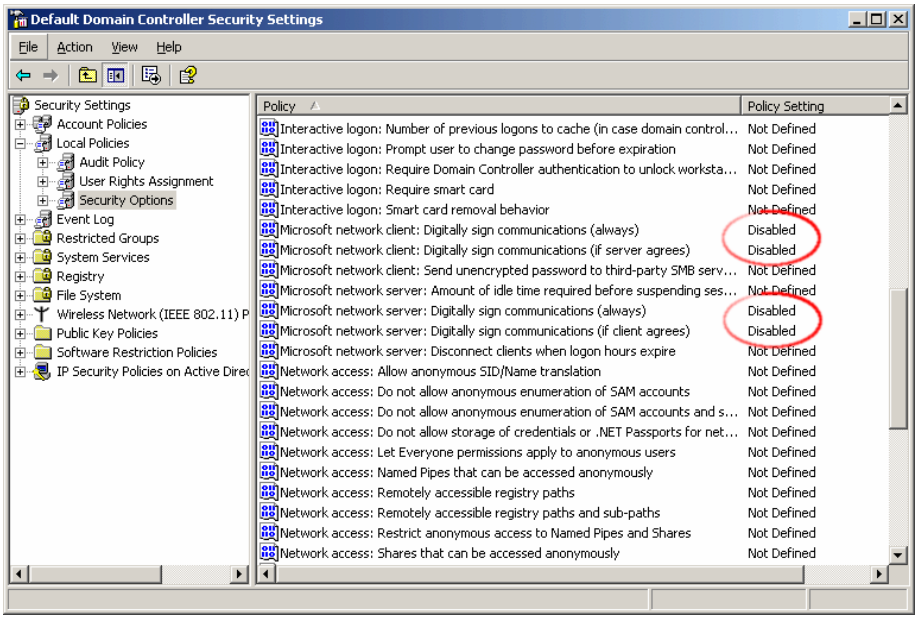
You cannot create more than one resource with the same name. You cannot create a resource twice. Check your spelling. Remember that resource names are not case-sensitive. You can check existing resource names by collapsing the tree diagram on the left.

Error: passwords do not match

Make sure that you type the same password in each entry field. For safety reasons, the passwords are not displayed. Type slowly. Check that the Shift, Caps Lock, Control, and Alt keys are not pressed.

Error: Open-E Data Storage Server cannot import the user database from a Windows Server 2003 domain.

In this case the following setting within the local security guideline may solve this problem:



Error: Update file not found

You instructed Open-E DSS to perform a systems update, but did not supply a valid Open-E DSS update file. Download the latest Open-E DSS update file from the www.open-e.com Web site. Next, copy the upgrade file into your "update" folder (please spell upgrade in lower case). Finally, select "update" from the menu.

Error: No share volume

You must create a volume for file sharing before you can create any resource shares or search for shares. Consult this manual's “Getting Started” section for instructions on creating a share volume.

Error: No share volume to browse

You must create a volume for file sharing before you can create any resource shares or search for shares. Consult this manual's “Getting Started” section for instructions on creating a share volume

Error: Invalid user name

Usernames cannot:
(1) Contain characters such as ~ ! @ # $ ^ & ( ) + [ ] { } * ; : ' " . , % | < > ? / \ = `
(2) Begin or end with a space
The use of the Windows SMB (Server Message Block) protocol, also known as CIFS or Samba, places some restrictions on the use of special characters. These restrictions have historical reasons, but are still binding today. Usernames must not contain any of the above mentioned characters.

Error: invalid user password

A user password cannot begin or end with a space. Spaces are not legitimate characters at the beginning and end of a password. Maybe you inadvertently hit the space bar during password entry. Please reenter your password.

Error: invalid administrator password

Administrator password cannot begin or end with a space. Spaces are not legitimate characters at the beginning and end of a password. Maybe you inadvertently hit the space bar during password entry. Reenter your password.

Error: invalid resource name

Resource name cannot:
(1) contain characters such as * : " | < > ? / \ ` # $ & ( ) + ; ' .
(2) begin or end with a space.
The use of the Windows SMB (Server Message Block) protocol, also known as CIFS or Samba, places some restrictions on the use of special characters. These restrictions have historical reasons, but are still binding today. Resource names cannot contain any of the above mentioned characters. Note that the list of invalid characters is slightly different than the ones for other name fields.

Error: invalid workgroup name

(1) contain characters such as ~ ! @ # $ ^ & ( ) + [ ] { } * ; : ' " . , % | < > ? / \ = `
(2) Begin or end with a space

The use of the Windows SMB (Server Message Block) protocol, also known as CIFS or Samba, places some restrictions on the use of special characters. These restrictions have historical reasons, but are still binding today. Workgroup names cannot contain any of the characters listed above. Note that the list of invalid characters is slightly different than the ones for other name fields.

note Invalid characters for workgroup names are different than the ones for other fields.

.

Error: invalid server name

Server name cannot contain:
(1) Characters: ~ ! @ # $ ^ & ( ) + [ ] { } * ; : ' " . , % | < > ? / \ = `
(2) Spaces
(3) Digits only

The use of the Windows SMB (Server Message Block) protocol, also known as CIFS or Samba, places some restrictions on the use of special characters. These restrictions have historical reasons, but are still binding today. Server names cannot contain any of the above mentioned characters. Note that the list of invalid characters is slightly different than the ones for other name fields. In addition, server names cannot be constructed from numbers only, they must contain alpha characters.

Error: invalid resource comment

Resource comment cannot be longer than 256 characters,
Resource comments have a limit of 256 characters which cannot be exceeded,
Use a shorter comment.

Error: invalid directory name

Directory name cannot:
(1) contain characters such as: * : " | < > ? / \ ` # $ & ( ) + ; ' .
(2) Begin or end with a space

The Open-E DSS internal operating system does not allow certain characters to be used for directories. The above mentioned characters are invalid, just as trailing or leading spaces. Choose a different name.

7 Appendix A

Open-E Software License agreement

IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. OPEN-E GMBH AND/OR ITS SUBSIDIARIES ("OPEN-E") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND OPEN-E. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE", "NO" BUTTON, OR OTHERWISE INDICATE REFUSAL, MAKE NO FURTHER USE OF THE SOFTWARE, AND RETURN THE FULL PRODUCT WITH PROOF OF PURCHASE TO THE DEALER FROM WHOM IT WAS ACQUIRED WITHIN NINETY (90) DAYS OF PURCHASE, AND YOUR MONEY WILL BE REFUNDED.

The terms of this software license agreement, do not apply to the Free Software Programs distributed with Open-E software. Instead, those programs are covered by other licenses, including the GNU General Public License.
A copy of the GPL along with the other applicable Free Software Licenses, can be found in Appendix B.

Ownership and Copyright

The Open-E software is non-exclusive licensed and sold to you for use only as permitted by this License Agreement. Open-E GmbH reserves any rights not expressly granted to you. Copying of the software is prohibited by law unless specifically authorized in writing by Open-E GmbH. You may not use copy, modify, sell, lease, sublease or otherwise transfer Open-E software in whole or in part.

Intellectual Property Rights

The Open-E software contains intellectual property rights, and in order to protect them, you may not decompile, reverse engineer, disassemble or otherwise reduce the Open-E software to a human perceivable form.

Termination

This license will be automatically terminated without notice from Open-E GmbH if you fail to comply with any term or condition of this agreement. If you do not agree to be bound by these terms and conditions, you may not use the Open-E or any of its software components.

Disclaimer of Warranties

Open-E software are licensed "as is" without warrantee of any kind. Open-E GmbH hereby disclaims all warranties express and implied, relating to Open-E , the installation utilities and the embedded software including, without limitation, any implied warrantee of merchantability, fitness for a particular purpose or non-infringement.

Limitation of Liability

In no event will Open-E GmbH liability under this agreement exceed the price that you paid for your Open-E software. Furthermore, in no event will Open-E GmbH be liable for any lost profits, lost data, cost of procurement of substitute goods or services, or any special consequential, incidental, indirect or punitive damages arising out of or under this agreement.

The limitation of liability set forth in this paragraph will apply, whether or not Open-E GmbH was advised of the possibility of the loss, liability or damages and notwithstanding any failure of essential purpose of any limited remedy.

Waiver

No delay or failure of Open-E GmbH to exercise any right under neither this agreement nor any partial exercise thereof shall be deemed to constitute a waiver or any rights granted hereunder or under law.

Unlawful Provisions

If any provision of the agreement is held to be unenforceable for any reason, all other provisions of this agreement shall nevertheless be deemed valid and enforceable to the fullest extent possible.

Entire Agreement

This agreement constitutes the sole and exclusive agreement between the parties concerning the subject matter hereof.

LIMITED WARRANTY

Open-E warrants that the media on which the software is distributed will be free from defects for a period of ninety (90) days from the date of delivery of the software to you. Your sole remedy in the event of a breach of this warranty is that Open-E will, at its option, replace any defective media returned to Open-E within the warranty period, or refund the money you paid for the software. Open-E does not warrant that the software will meet your requirements, that operation of the software will be uninterrupted, or that the software will be error-free.

Authorized Service

Only an authorized service representative can service Open-E software. Failure to comply with this requirement will void the warranty.

Applicable Law

This agreement shall be governed by German law. You agree to jurisdiction and venue in the courts located in Munich, Germany for all claims, disputes and litigation arising under or related to this agreement.

8 Appendix B

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a
portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

   If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

   However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License.
   Section 6 states terms for distribution of such executables.

   When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

   If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

   Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6.
   Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

   You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions).

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

f) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

g) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. .Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

    Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

> *<one line to give the library's name and a brief idea of what it does.>*
> *Copyright (C) <year> <name of author>*
>
> This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.
>
> This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.
>
> You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

> Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!