A new concept in storage management
Open Source
Storage, Inc

# OSVault User Manual

First Edition

***OSVault Users Manual, First Edition***

# 1 About OSVault

## 1.1 Introduction

This document is intended to aid the reader in installing and using an OSVault appliance. We have assumed that you have purchased an optical library with an attached appliance (server) that already has the OSVault software installed.

## 1.2 How OSVault Works

OSVault is both a set of software to automatically mount and dismount DVD and ProData media when needed, and a system configuration, based on LINUX, that creates a dedicated storage appliance to offer Network Accessible Storage (NAS) services.

OSVault consists of the following major software packages:

- LINUX 2.6.3 – the appliance operating system that supports Network File System (NFS) access by UNIX and LINUX systems and allows the other various software packages to share the appliance hardware
- SAMBA 3.1 – allows Microsoft Windows systems to access files stored on the OSVault appliances
- autofs 2.4.6 – An auto-mounting file system that recognizes when file systems on different physical media are required and issues the robotic commands to move the needed media into an available drive slot
- webmin – A web (HTML) based system administration package that allows all needed configuration parameters in the appliance to be specified or queried

When fully configured, OSVault looks like a network file server such as a Network Appliance Filer, a Windows 2000 Server, or a LINUX file server. OSVault allows client computers to connect via either of two protocols, CIFS or NFS, to create, read, write, or delete files and directories on the appliance. An OSVault appliance allows direct access to each piece of media in the ASACA library as if it were a hard disk drive *x*, or the client system can read and write to the /cache directory and OSVault will move files, after a pre-determined period of time, to an available DVD or ProData disc in the ASACA library.

For example, if a Windows XP user can access the OSVault appliance over a network, then that user can right-click on the My Computer icon, select Map Network Drive..., type in \\OSVAULT\CACHE, and click on the Finish button. The Windows XP system will then create a new disk drive number that maps into the OSVault appliance and will open an Explorer window showing the contents of the OSVault /cache file system. Files can then be copied into and out of the /cache file system, and application programs, such as Word or Excel, can directly save or open files in that file system.

The /cache file system is periodically scanned by OSVault, and older files are "migrated" from the hard disk onto an available piece of optical media. A link is created between the /cache file name and the new location for the file on the optical media. In this way, files that are no longer resident on the hard disk inside OSVault can still be opened by the original name. When the original name is opened, OSVault will mount the required piece of optical media before the client system is returned the data it is requesting, or notified that the data has been written successfully.

By default, any uninitialized optical media in the ASACA library is formatted and labeled with a label composed of the string "ASACA" followed by the slot number and side of the media in the library. For example, the second piece of media in the library, if unformatted, will be labeled ASACA4097A on the top side, and ASACA4097B on the bottom side. That piece of media can then be directly accessed, bypassing the /cache, by referencing the name /archive/ASACA4097A. Windows users can map a network drive to a particular piece of media by entering \\OSVAULT\archive\ASACA4097A.

## 1.3 Where to Find This Software

The software that makes up the OSVault appliance is completely open-source. This means that the software source code can be freely downloaded from various sources, including web sites. The following web sites have the software components.

- http://dvdvault.sourceforge.net – The changes to the autofs software for an ASACA library and the migration software
- http://fedora.redhat.com – the LINUX operating system distribution used by OSVault
- http://www.samba.org – the SAMBA software for Microsoft Windows "share" access
- http://www.webmin.com – the web-based administration software
- http://www.osstorage.com/OSVault – the complete RPM software package that makes up the appliance

Other components are resident on the distribution DVD, including the KICKSTART configuration for installation and the post-LINUX-installation configuration script.

One note about open source software: open source software can be freely downloaded and changed or customized in accordance with the copyrights on the various modules. Support from Open Source Storage for installations is not free and requires the purchase of a support contract.

## 1.4 About Open Source Storage Inc.

Open Source Storage Inc. is a professional services company that develops and maintains the OSVault software. Since OSVault is open-source, OSS Inc. does not actually sell the software. Open Source Storage makes revenue to fund continuing development by assisting customers (end-users and manufacturers) with the installation, deployment and support of OSVault.

# 2 Installing OSVault

OSVault is intended to run as an appliance on an Intel or AMD processor system. Certain assumptions are made including:

- The appliance will not be used for other purposes
- The hard disk drives on the appliance do not contain data that will be preserved, other than OSVault specific data
- The hardware meets the hardware prerequisites given below

## 2.1 Hardware Requirements

OSVault is usually shipped to a customer site as a pre-configured appliance. However, this document also shows the steps needed to install the OSVault Library Appliance distribution on DVD onto a generic hardware platform. OSVault has been tested on various hardware platforms and is officially supported on hardware that contains the following hardware components:

- Intel Pentium 4 processor (single processor is acceptable, dual CPU configurations have also been tested)
- 1GByte of RAM memory (more memory is acceptable)
- Two ATA or SATA disk drives with at least 500GBytes of storage on each disk
- Adaptec 79xx, 29160 or 39160 SCSI Host Bus Adapter (HBA) or LSI Logic SCSI Host Bus Adapter (HBA)
- A LINUX(Fedora)-support Gigabit Ethernet Interfaces

Expected system performance is somewhat dependant on the hardware used in the appliance. For example, a properly configured Pentium 4 system with 10,000RPM SATA disk drives connected to a Gigabit Ethernet switch should be able to read and write data in cache at around 40Mbytes per second. The limiting factor is the throughput to the hard disk drive in the cache, not the network connection, the memory or the CPU. Adding or trunking a second gigabit ethernet link to the appliance will not increase performance, since the magnetic disk is still the limiting factor. Using a RAID-0 configuration on two or more disks for the cache can increase performance substantially, and the appliance will be able to move around 75Mbytes per second through a single Gigabit Ethernet link to a single client system.

The type of data moved over the network can also impact performance. The megabyte per second numbers given previously assumes that large files are transferred sequentially into or out of the cache. If a number of small files are transferred, throughput will drop considerably due to the overhead involved in creating directory entries for new files in the cache. A large number of very small files all stored in a single directory can drop performance below 1Mbyte per second, even with fast magnetic disks.

The migration of data out of the cache to the optical drives imposes a performance penalty of around 4.5Mbytes per second per ProData optical drive used, or less than 1Mbyte per second per DVD-RAM optical drive used. So an appliance configured to migrate from a single magnetic disk cache to three ProData optical drives will then only be able to move around 20Mbytes per second between the client systems and the cache.

Reading files from a client system that resides on optical media can take various amounts of time to complete. The factors that impact that amount of time are:

- Type of optical media -- DVD-RAM media takes approximately 30 seconds to load and be recognized, while ProData media takes approximately 15 second to accomplish the same load.
- Number of drives in use in the ASACA library -- If all drives are busy fulfilling other client reads or writes to other pieces of media, this particular read or write will have to wait for a drive to become available.
- Transfer rates of optical media -- ProData writes at around 4.5 Mbytes per second and reads at around 10 Mbytes per second, while DVD media reads at around 2Mbytes per second and writes at around 1Mbyte per second.
- Other cache based reads or writes at rates high enough to use a significant percentage of the network bandwidth -- A single client blasting data to or from the cache can use 90% of the network bandwidth for periods of time.

Although complex, the performance of the OSVault appliance is predictable and your sales representative can help you with expected system performance for your application.

## 2.2 Booting the Distribution DVD and Loading the Software

Quick Start Checklist

1. Unpack the ASACA library according to the directions. Make sure to remove the internal retaining items.
2. Load the ASACA library with media. You MUST put a piece of media in the first slot in the library (top of the "A1" magazine). This piece of media is used for backups of the appliance during operation. Media

loaded must only be DVD-RAM or ProData media. DVD-R and DVD-RW media is not supported by the ASACA drive firmware.

3. If a separate server is being installed, place the server within 6 feet of the ASACA library to attach it to the library.
4. BEFORE TURNING ON POWER, Install a 68-pin SCSI cable between the server SCSI port and the ASACA SYSCON (system controller). Run a short SCSI cable between the SYSCON and the DVD-RAM or ProData drive connection on the back of the ASACA library. Make sure the SCSI cable is 6 feet (2 meters) long or less. Longer SCSI cables (or inferior cables) will result in chronic I/O errors during operation.
5. Determine an IP (Internet Protocol) address for the server and make a note of it.
6. Determine an IP address for the ASACA library and set the address on the ASACA library via the library's front panel.
7. Install CAT-5 network cables between the library and your network switch, and between the server and your network switch. Wireless (802.11a/b/g) is not supported.
8. Install the power cables to the server and the library, being careful to keep the power cables and the SCSI cables from running parallel in close proximity.
9. Attach a keyboard and monitor to the server. Some servers support serial port BIOS settings and you can use another computer with the “minicom” or HyperTerminal software on it in place of the keyboard and monitor.
10. Power up the ASACA library.
11. Power up the server.
12. Place the distribution DVD into the server DVD-ROM drive and reboot the server if necessary.
13. KEEP IN MIND THAT INSTALLING THE DVD DISTRIBUTION SOFTWARE WILL ERASE THE HARD DRIVES ON THE SERVER.
14. When the monitor on the server displays the “Boot:” prompt and waits for input, type in the following command:

    ```
    linux ks=cdrom:/ks.cfg
    ```

15. The above command will load the OSVault software onto the server and will format the boot disk and cache disk for operation. The IP address of the server will initially be set to 10.1.1.2, which you can change after installation completes.
16. You will be prompted to indicate where the distribution media resides. Select CDROM with the arrow keys. Press the TAB key until the OK button is highlighted, and then press return.

17. Software installation will take approximately 30 minutes (longer on some servers). If the distribution media is on multiple pieces of media, for example CD, you will be prompted to switch to the other pieces of media.
18. After software installation, the now-configured appliance will perform a hardware inventory on the ASACA library (15 minutes per 250 slots) and will then load every piece of media in the library and examine it. It takes about a minute for each piece of media to be formatted or checked. If the media is unformatted, OSVault will put a UDF file system on each side of each piece of media. If the media is formatted, the volume label on the media will be used to create a directory (using the volume name) in /archive.
19. OSVault will then reboot the server and all services on the server will be started. You can configure the appliance via a web browser (http://10.1.1.2:10000) or via the attached keyboard/monitor. The web interface is preferred unless you are an expert LINUX administrator.

## 2.3 Power for the Appliance

THIS DEPENDS ON CONFIGURATION. Check the manuals that came with the server hardware.

## 2.4 Hooking up Cables

The following cables must be attached to the appliance:

1. SCSI cables from the VHDCI connector on the back of the appliance to the SYSCON Micro-68 connector on the ASACA Library
2. SCSI cables from the SYSCON Micro-68 connector to the Micro-68 connector for the drive bus on the back of the ASACA library
3. Power cables from a power source (100-240 volt) to the appliance and to the library
4. Network cables from the customer's network facility to the appliance Gigabit Ethernet port (RJ-45) and to the ASACA library 10/100BaseT port (RJ45). This cable must be at least CAT-5 compliant.

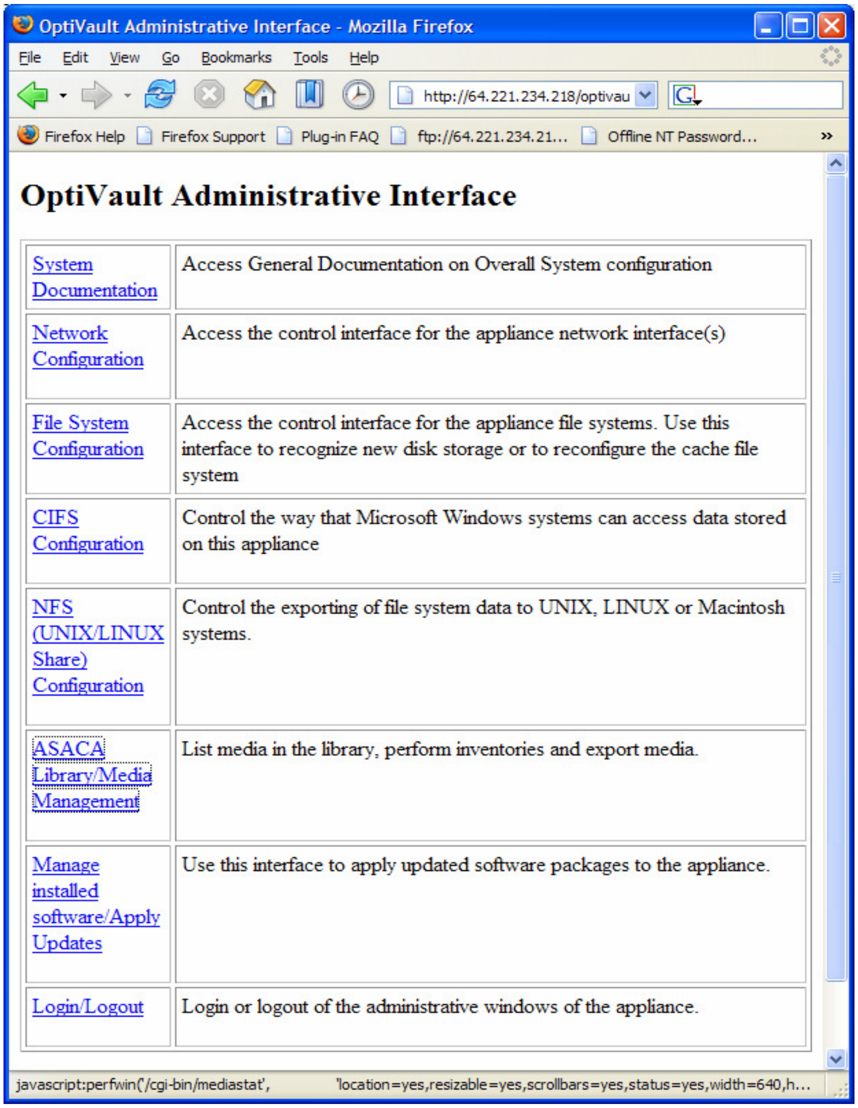
## 2.5 Plugging into Your Network

The ASACA-provided OSVault appliance has two 10/100/1000BaseT network interfaces. During installation, the RJ-45 connector labeled “0” should be plugged into the local area network. The RJ-45 connector labeled “1” should be plugged into the RJ-45 connector on the DVD or PD library. The cable used to plug between the appliance and the library should be a Cat-5 (or better) cross-over cable. The cabling from connector “0” and the premise's network switch should be a straight-thru cable, CAT-5 or better.

The network interface will automatically determine what speed to run based on the network switch capabilities, the quality of the cabling used, and the length of the cable. With a limited number of network switches, it may be necessary to lock down the duplex of the link to either half or full.

## 2.6 Accessing the Web-Based Interface

The OSVault appliance has a web portal (main page) at the default address on the appliance. When first installed, the appliance is at http://10.1.1.2. Any web browser on another system in the same 10.1.1.x network can type the link into the web browser and be presented with the following screen:



OptiVault Administrative Interface

| | |
|---|---|
| System Documentation | Access General Documentation on Overall System configuration |
| Network Configuration | Access the control interface for the appliance network interface(s) |
| File System Configuration | Access the control interface for the appliance file systems. Use this interface to recognize new disk storage or to reconfigure the cache file system |
| CIFS Configuration | Control the way that Microsoft Windows systems can access data stored on this appliance |
| NFS (UNIX/LINUX Share) Configuration | Control the exporting of file system data to UNIX, LINUX or Macintosh systems. |
| ASACA Library/Media Management | List media in the library, perform inventories and export media. |
| Manage installed software/Apply Updates | Use this interface to apply updated software packages to the appliance. |
| Login/Logout | Login or logout of the administrative windows of the appliance. |

```
javascript:perfwin('/cgi-bin/mediastat',          'location=yes,resizable=yes,scrollbars=yes,status=yes,width=640,h...
```

## 2.7 Accessing the Command Line Interface

### Using Secure Shell

Secure shell, referred to as SSH, allows the entry of commands in a line or text mode into the appliance, with all data encrypted so that others cannot snoop on what you are doing. This is particularly important when using an external Internet connection to control the appliance, since external Internet data can be intercepted while transiting networks outside of your local office. Also, anyone within a company with physical access to your company network can, with relative ease, intercept any communications to the appliance. Therefore, SSH is recommended for all command line interface activities and is the only interface, other than the appliance console, enabled for command line access.

SSH is available on all Windows, LINUX, Macintosh and UNIX systems. For Windows systems, a copy of CYGWIN can be downloaded from http://www.cygwin.com. See Appendix A for instructions on installing CYGWIN on a Windows system.

Installing CYGWIN with its default settings on a Microsoft Windows system will allow you to invoke SSH in a command window. Just double click on the CYGWIN desktop icon on your Microsoft Windows system and then type the following command:

```
ssh root@10.1.1.2
```

You will then be prompted for the "root" password, which by default is "password". Your local system will then store keys used for encrypting the communications with the OSVault appliance. If you later change the IP address for the OSVault appliance, the next time you use SSH, a new set of keys will be generated.

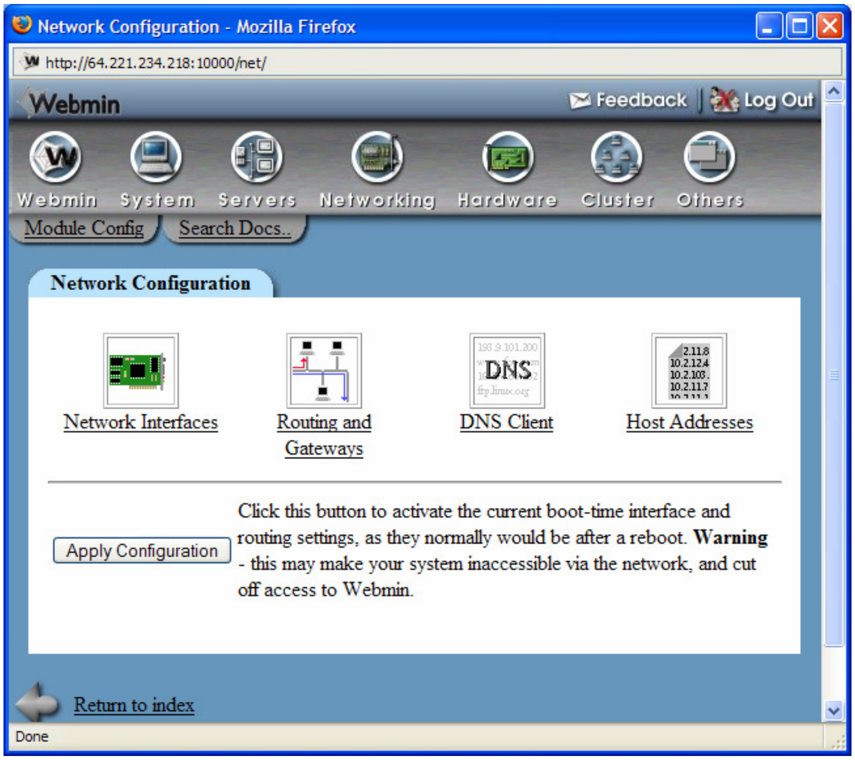
### Using TELNET

TELNET is disabled by default on the OSVault appliance.

# 3 Configuring OSVault

## 3.1 Setting the IP Address

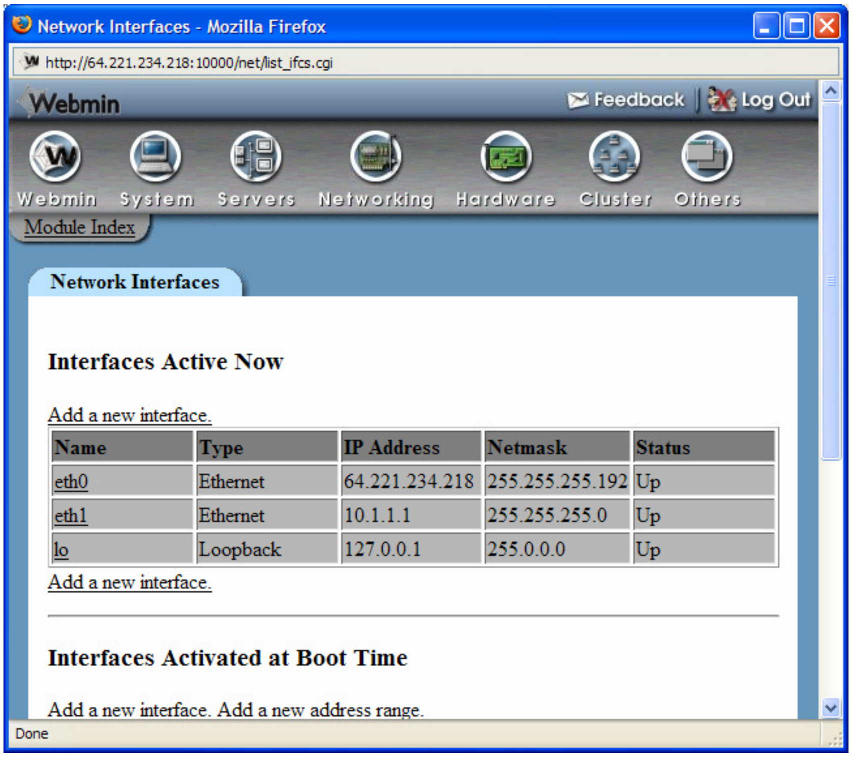
You can use the "Network Configuration" link to change the appliance network address to work in your local network. For example, if you wish to change the OSVault appliance address to 192.168.2.14, click on the "Network Configuration" link and you will see the following screen:



Network Configuration

Click this button to activate the current boot-time interface and routing settings, as they normally would be after a reboot. **Warning** - this may make your system inaccessible via the network, and cut off access to Webmin.

You can then click on the "Network Interfaces" icon to go to the screen that will allow you to set the IP address of the appliance, as follows:



Network Interfaces

**Interfaces Active Now**

Add a new interface.

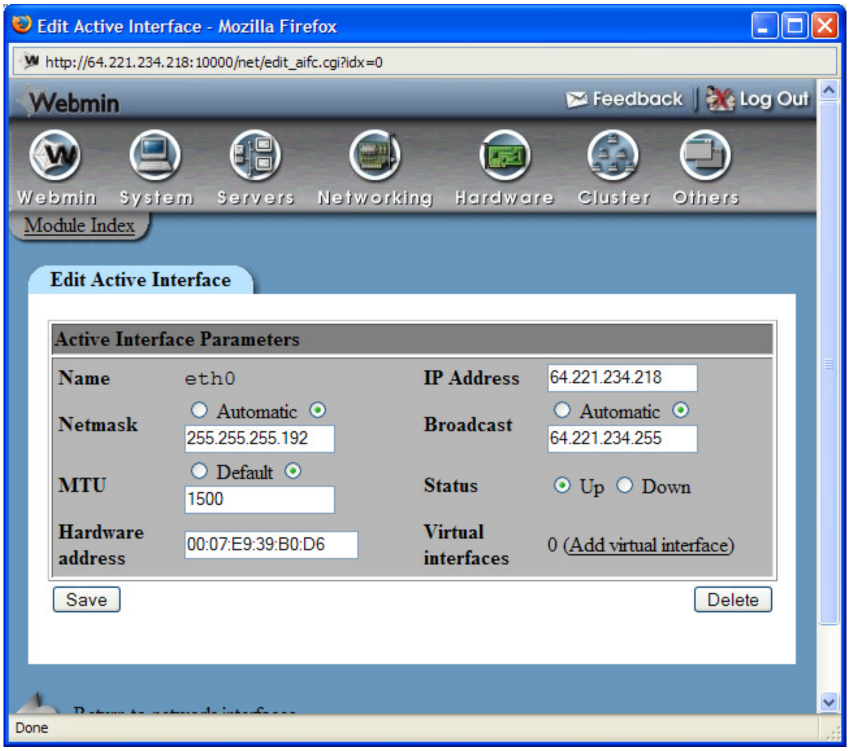
| Name | Type | IP Address | Netmask | Status |
|---|---|---|---|---|
| eth0 | Ethernet | 64.221.234.218 | 255.255.255.192 | Up |
| eth1 | Ethernet | 10.1.1.1 | 255.255.255.0 | Up |
| lo | Loopback | 127.0.0.1 | 255.0.0.0 | Up |

Add a new interface.

**Interfaces Activated at Boot Time**

Add a new interface. Add a new address range.

In the above screen, there are two Ethernet interfaces on the appliance, eth0 and eth1. To change eth0 to the desired IP address, click on the name “eth0”, and use the following screen to set the information:



Edit Active Interface

Active Interface Parameters

| | | | |
|---|---|---|---|
| Name | eth0 | IP Address | 64.221.234.218 |
| Netmask | ○ Automatic ● 255.255.255.192 | Broadcast | ○ Automatic ● 64.221.234.255 |
| MTU | ○ Default ● 1500 | Status | ● Up ○ Down |
| Hardware address | 00:07:E9:39:B0:D6 | Virtual interfaces | 0 (Add virtual interface) |

## 3.2 Performing a Library Inventory

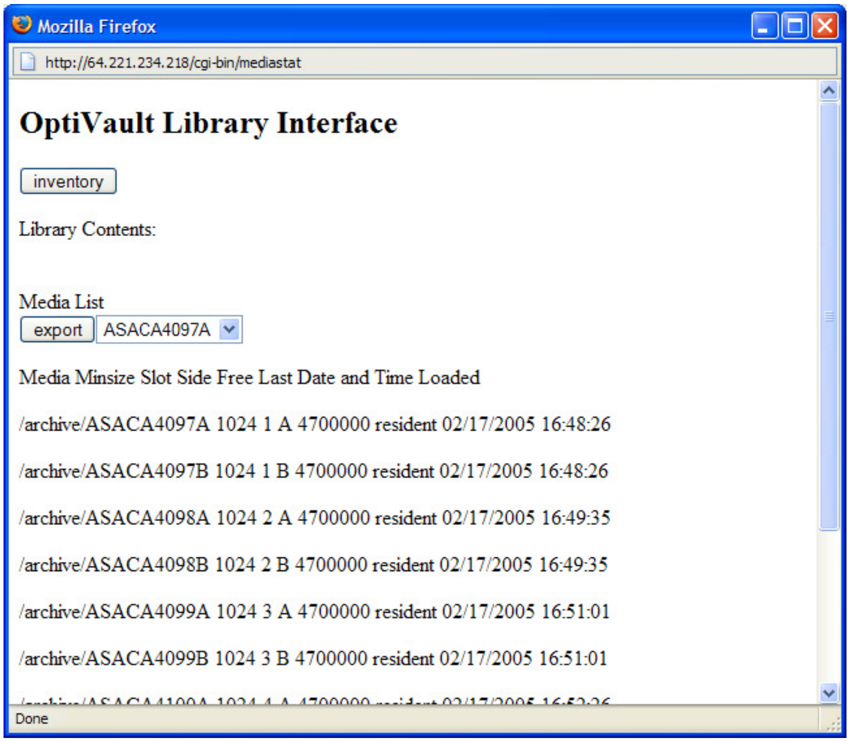
OSVault, during installation, will perform a full inventory of the library. This inventory includes having the library use its internal intelligence to check for the presence of media in each slot (called an Initialize Element command), and then a load of all detected media into an optical drive to see if the media is formatted. If unformatted media is encountered, OSVault will format the media.

Media formatting involves the placement of a Universal Data Format (UDF) file system on the optical media. UDF is the standard file system that is an extension of the same file system used on CDs and also the same file system used on DVD movies. UDF can be read and written on every major file system in use today. Media formatted and written to by the OSVault appliance can be exported and read on just about any computer with a DVD drive. The ProData (sometimes referred to as Blue Laser) media can only be read or written in a ProData compliant drive (most DVD drives are not blue laser capable as of this writing).

Please keep in mind that this process can take a long time. A full hardware inventory takes approximately twenty minutes per 250 slots, regardless of the number of media installed in the library. The format verification and formatting can take one minute per piece of media installed in the library. So, for example, an ASACA AM250-PD with 100 pieces of media will take about two hours to finish a full inventory.

## Web Inventory of the Library

Use a web browser to type in the IP address of the OSVault appliance. You can then select the library control by clicking on ASACA Library/Media Management . That will present the following window:



OptiVault Library Interface

Library Contents:

Media List

```
Media Minsize Slot Side Free Last Date and Time Loaded

/archive/ASACA4097A 1024 1 A 4700000 resident 02/17/2005 16:48:26

/archive/ASACA4097B 1024 1 B 4700000 resident 02/17/2005 16:48:26

/archive/ASACA4098A 1024 2 A 4700000 resident 02/17/2005 16:49:35

/archive/ASACA4098B 1024 2 B 4700000 resident 02/17/2005 16:49:35

/archive/ASACA4099A 1024 3 A 4700000 resident 02/17/2005 16:51:01

/archive/ASACA4099B 1024 3 B 4700000 resident 02/17/2005 16:51:01

/archive/ASACA4100A 1024 4 A 4700000 resident 02/17/2005 16:52:26
```

Clicking on the "Inventory" button will initiate a full library inventory. On a 250-slot library that is full of media, this can take as long as 4.5 hours to run. Each piece of media in the library will be loaded into a drive and have the label read and stored in the appliance. Also, directories for direct-media access, usually /archive/*medialabel*, will be created; *medialabel* is the label read from the media. Any media that is found in the library that is unformatted (does not have a valid UDF file system) will be formatted with a file system and labeled with a label of the form of "ASACA" followed by the slot number and side; for example *ASACA4097A* would the name for a piece of media in the second slot, top side. ASACA libraries start slot numbers at 4096.

### Command Line Inventory of the Library

```
inventory -o /dev/sg0 -p ASACA -f -a /etc/auto.archive \-o /etc/migration.conf
```

The above command uses the /dev/sg0 device entry to issue commands to the robot to mount all media for format checks. You can determine the device name with the mcstat command.

Inventory will mount each side of each piece of media in the library unless the -n flag is given. The "-n" flag tells inventory to only use a single side (side 0, or the upside as you look at the media in the magazine) of each piece of media.

## 3.3 Formatting All Media

In some cases, it may be necessary to format all of the media in the library, regardless of data already stored on the media. If the "format all" option is selected on the inventory command, all (REPEAT ALL!!!) data in the library will be erased.

### Web-Based Method Not Available

To avoid the possibility of mistakenly formatting all media and wiping out current data, a web interface to accomplish a full format is not implemented.

### Command Line Method

There is a command line interface option to the inventory command that will cause the inventory command to ignore any existing UDF label on the media, and to format all pieces of media (both sides) with a new UDF file system. To indicate that "inventory" should format all media, the "-x" flag must be given twice to the "inventory" command, as shown below:

```
inventory -o /dev/sg0 -p ASACA -x –x
```

# 4 Initializing OSVault

Once the OSVault appliance software is installed, the system will prompt you to reboot the appliance. The appliance will then restart with the newly installed software and will start a series of initialization tasks, including:

Startup of the network interfaces, and setup of CIFS (Windows SHARE) and NFS services

- Startup of the web-based system control (ports 80 and 10000 by default)

- Mounting of the magnetic drives for cache space
- Scheduling of the migration task to relocate files written to cache onto optical media
- (One time only) Having the library perform a hardware initialization to determine what media is stored in the library
- (One time only) Loading each piece of media into a drive and formatting the media if it is not already formatted -- Note that media not previously written in standard UDF format is considered unformatted and will be overwritten. Several software packages such as DiskXtender from EMC and AMASS from ADIC do not use a standard optical format.
- Initialization of the Relational Database that tracks media moves from cache to optical media and the contents of each file moved.

Once the OSVault appliance has finished its one-time inventory and format process, any references to files stored on optical media or to files migrated from the cache to optical media will cause the ASACA library to load the appropriate media to fulfill that reference. Assuming a standard installation on an ASACA 250, 750 or 1450 slot library, you can verify proper operation of the OSVault appliance with a single SSH command line:

```
ssh root@10.1.1.2 ls –l /archive/ASACA4097A
```

This command, run from a Windows (with CYGWIN), LINUX or UNIX client, will cause OSVault to load the second piece of media, top side up, from its storage slot into a drive slot. With DVD-RAM media, this will take about thirty seconds. With ProData media, this will take about fifteen seconds.

# 5 Administering OSVault

You can access all of the OSVault administration capabilities via a network interface. Additionally, if a standard PS/2 keyboard and VGA (or better) monitor is attached to the appliance, you can perform the command line utilities via that interface.

## 5.1 Web-Based Appliance Administration

OSVault uses a customized installation of the Webmin software, a web-based system administration utility. Since the underlying operating system for OSVault is LINUX, a LINUX implementation of Webmin allows for advanced system configuration beyond the defaults set by the OSVault installation.

### Logging In

Logging into Webmin is easy. Open a web browser, like Netscape or Internet Explorer, on any machine that has network access to the server that you wish to login on. Browse to port 10000 on the IP or hostname of the server.

Webmin will then respond with either an authentication window, or an authentication web form, where you can enter the administrator user name (usually "root") and password. After successful authentication, you will be greeted with the Webmin index page. The type of login form you receive (either on a web page or in a popup window) depends on the configuration of the Webmin server. The differences between session authentication and standard HTTP authentication will be discussed later in this book. In general, all of the web interface screens required to perform system administration have been previously discussed. However, OSVault contains a full suite of system administration web tools that allow for further customization. Documentation on the general system web interfaces are contained in Section 10 of this document.

## 5.2 Command Line Interface Administration

The OSVault appliance allows for the use of command line administration via either Secure Shell (ssh) or TELNET. The command line interface is a full LINUX command shell and can be used to set any system configuration, to reconfigure hardware or to reinitialize the system. The command line interface should be used with care, as it is possible to destroy data stored in the appliance if the commands are used incorrectly.

## 5.3 Basic CLI Commands

### mcstat

Mcstat is a command line program that locates the library interface in the appliance. The library interface has a name such as /dev/sg0 and mcstat will print out that name when run. Mcstat also prints out information on the library vendor and product string, as retrieved via the SCSI or Fibre Channel interface, as well as the addressing information of the library. The output from mcstat is as follows:

```
[root@OSVAULT ~]# mcstat
SCSI Media Changer Status Command
Medium changer found on /dev/sg3
Vendor ASACA
Product AM250DVD
  2 transports starting at 1
  250 storage elements starting at 4096
  3 data devices starting at 64
  1 import slots starting at 128
[root@OSVAULT ~]#
```

In the above listing, the library attached to the appliance is an ASACA 250 slot DVD-RAM library. Since the library can be virtualized or be missing magazines, the storage element count is important. In this case, there is a standard dual picker, 250 slots for media in magazines of 50 each and 3 DVD-RAM drives.

## readvol

Readvol is a command line utility to report which slots are occupied in the ASACA library. Readvol will retrieve the hardware inventory from the library and use that information to determine what media is present. If media in the library has been removed or added without performing an “initelem” command, the results reported by readvol will not be correct.

You need to use the identifier returned from mcstat as the only argument to readvol, for example /dev/sg3. A sample run of readvol is shown below:

```
[root@OSVAULT ~]# readvol /dev/sg3

Querying ASACA   , AM250DVD

Volume in slot 4096 (relative slot 0)

Volume in slot 4097 (relative slot 1)

Volume in slot 4098 (relative slot 2)

Volume in slot 4099 (relative slot 3)

Volume in slot 4100 (relative slot 4)

Volume in slot 4101 (relative slot 5)

Volume in slot 4102 (relative slot 6)

Volume in slot 4103 (relative slot 7)

Volume in slot 4146 (relative slot 50)

Volume in slot 4147 (relative slot 51)

Volume in slot 4148 (relative slot 52)
```

## inventory

The inventory command line utility is the overall workhorse utility for OSVault. Running inventory at any time will reload all media present in the library and make sure  the OSVault directory of media loaded in the library is correct.

An example of inventory output is shown below:

```
[root@OSVAULT ~]# !255

inventory -l /dev/sg3 -p ASACA -f -a /etc/auto.archive -o /etc/migration.conf

Querying ASACA   , AM250DVD

Drive device name not specified, autoconfiguring

Using /dev/scd2 as the drive to format in
```

```
Skipping 1 slot(s) for backups
Media in slot 4097, side 0 has label ASACA4097A
Media in slot 4097, side 1 has label ASACA4097B
Media in slot 4098, side 0 has label ASACA4098A
Media in slot 4098, side 1 has label ASACA4098B
Media in slot 4099, side 0 has label ASACA4099A
Media in slot 4099, side 1 has label ASACA4099B
Media in slot 4100, side 0 has label ASACA4100A
Media in slot 4100, side 1 has label ASACA4100B
Media in slot 4101, side 0 has label ASACA4101A
Media in slot 4101, side 1 has label ASACA4101B
Media in slot 4102, side 0 is uninitialized
Volume in slot 4102, formatting with mkudffs --vid=ASACA4102A –lvid=ASACA4102A  /dev/scd2
```

You can see in the above example that “inventory” can locate the order of optical drives in the library by itself. It does this by loading the first piece of media in the library into each drive and then seeing which drive reports a “media present” condition.

## chkconfig

Chkconfig provides a simple command-line tool for maintaining the /etc/rc[0-6].d directory hierarchy by relieving system administrators of the task of directly manipulating the numerous symbolic links in those directories.

This implementation of chkconfig was inspired by the chkconfig command present in the IRIX operating system. Rather than maintaining configuration information outside of the /etc/rc[0-6].d hierarchy, however, this version directly manages the symlinks in /etc/rc[0-6].d. This leaves all of the configuration information regarding what services init starts in a single location.

Chkconfig has five distinct functions: adding new services for management, removing services from management, listing the current startup information for services, changing the startup information for services, and checking the startup state of a particular service.

When chkconfig is run without any options, it displays usage information. If only a service name is given, it checks to see if the service is configured to be started in the current runlevel. If it is, chkconfig returns true; otherwise it returns false. The –level option may be used to have chkconfig query an alternative runlevel rather than the current one.

If either on, off, or reset is specified after the service name, chkconfig changes the startup information for the specified service. The on and off flags cause the service to be started or stopped, respectively, in the runlevels being changed. The reset flag resets the startup information for the service to whatever is specified in the init script in question.

By default, the on and off options affect only runlevels 2, 3, 4, and 5, while reset affects all of the runlevels. The –level option may be used to specify which runlevels are affected.

Note that for every service, each runlevel has either a start script or a stop script. When switching runlevels, init will not re-start an already-started service, and will not re-stop a service that is not running.

## putaway

Putaway is a command line utility to restore media that is located in drives, or in the import/export slot, back into a storage slot. It is actually a renamed version of “inventory”, since “inventory” will perform the same function prior to starting the loading of media into drives. When “inventory” is renamed to “putaway”, it will exit prior to starting the load of media.

The format for putaway is

```
putaway -l /dev/sg3
```

where /dev/sg3 is the name of the library device inside the appliance. An example follows:

```
[root@OSVAULT ~]# putaway -l /dev/sg3

Querying ASACA   , AM250DVD

Volume in drive 64

putting cart in drive 64 in slot 4096

[root@OSVAULT ~]#
```

## initelem

Initelem is a utility to tell the ASACA library to check each slot and see if media is present. Due to the mechanical nature of checking for media (each slot is pulled out and a light beam checks if media is present), a full hardware initialization will take a considerable amount of time. A 250-slot ASACA library takes fifteen minutes to complete this operation; a 1450 slot ASAC library takes almost 1.5 hours to complete a full hardware initialization. Initelem has one argument, the device name of the library interface that is returned by the mcstat command.

```
[root@OSVAULT ~]# initelem /dev/sg3

SCSI Media Changer Status Command

Vendor ASACA

Product AM250DVD

Setting timeout to 720000
```

## mm

Mm which is short for “move medium”, is a utility to move a piece of media within the ASACA library. The format of the “mm” command is:

```
mm from to invert picker device
```

Where “from” is the library slot to move from; “to” is the library slot, drive or import/export slot to move to; “invert” is a “1” (meaning to flip the media during the move) or “0” (do not flip); “picker” is the library picker to use to move the media (use “0” for best results); and “device” is the library device name inside the appliance (for example “/dev/sg3”).

As an example, the following command will move the media from the second drive (slot 65) to the 10th storage slot (slot 4106) using the default picker without flipping it, and then move it back again. The third command is an error where there is no media in the drive:

```
[root@OSVAULT ~]# mm 4096 65 0 0 /dev/sg3
[root@OSVAULT ~]# mm 65 4096 0 0 /dev/sg3
[root@OSVAULT ~]# mm 65 4096 0 0 /dev/sg3
Source slot is empty
Could not move medium
[root@OSVAULT ~]#
```

## sourceslot

Sourceslot is a utility to display the slot that a piece of media belongs in. The one argument required is a drive number (starting at 0, not 1) that has a piece of media loaded into it. Running “sourceslot /dev/sg3 0” will return the slot number the library pulled the media from. The following is an example of three commands you can run to empty the media from a drive, back to the slot it came from.

```
[root@OSVAULT mclib]# mcstat
SCSI Media Changer Status Command
Medium changer found on /dev/sg3
Vendor ASACA
Product AM250DVD
  2 transports starting at 1
  250 storage elements starting at 4096
  3 data devices starting at 64
  1 import slots starting at 128
[root@OSVAULT mclib]# mm 4096 64 0 0 /dev/sg3
[root@OSVAULT mclib]# sourceslot /dev/sg3 0
```

```
Querying ASACA   , AM250DVD
Volume in drive 64 came from 4096
[root@OSVAULT mclib]# mm 64 4096 0 0 /dev/sg3
```

## migration

The “migration” command is used to move files from the “/cache” file system to an appropriate optical media based on rules given as arguments. Usually, the “migration” command is invoked from the automatic job scheduler, “cron”, so that the “/cache” file system is emptied frequently enough so that it does not fill completely.

The “migration” command has several arguments:

- -t# – Don't migrate files that are not at least “#” minutes old
- --source-name – The name of the file system root directory to search for candidate files to relocate to optical media
- --low-water # – Don't start migrating files from the “source-name” to the optical media until the file system that contains “source-name” has more than “#” percent used.
- --high-water – Stop migrating files from “source-name” to optical media when the file system that contains “source-name” is less than “#” percent used
- --force-mig (or -f) – Migrate all files from the /cache file system to optical media without checking for high water or low water marks; works the same as if the high water and low water marks are both set to 0
- --nounlink – Don't unlink the file from the /cache directory after moving to optical media; **do not** use this in a scheduled migration, as the files will continue to be copied every time migration is run
- --debug-level level – Print out different levels of information; valid values for “level” are “critical”, “serious”, “error”, “warning”, “debug”, and “everything” (Use “--debug-level everything” to show the most information.)

The default entry in the scheduler (cron) for migration is:

```
0-55/5 * * * * migration -t10 --source-name /cache --high-water 30 --low-water 20 –f
```

## stage

The “stage” command called automatically by the operating system to restore files from optical media, back to hard disk cache when a file is opened for reading.

Stage can also be invoked manually from the command line to restore files back into hard disk cache. You can restore files by file name (as they would appear in the /cache directory) or by inode number. The inode number is an internally generated, unique number that uniquely identifies the file, even when renamed. The system uses this version of stage to restore files; users generally use the file name to restore a file.

The syntax of a stage by filename might be:

```
stage --filename /cache/userdata/music/recording.mp3
```

The syntax of a stage by inode number might be:

```
stage--inode 32
```

# 6 Importing and Exporting

## 6.1 Individual Media

### Import

Media to be imported must first be placed into the Import/Export slot (I/E slot) in the ASAC library. Use the front panel on the library to insert the media into the I/E slot. Refer to the ASACA User Manual on how to accomplish this. The media must be inserted into the library BEFORE telling OSVault to import it.

When importing media, OSVault will perform the following operations:

- Check to see if media is present in the I/E slot; if not an error is returned and processing of the import operation stops
- Moves the piece of media to an unoccupied slot in the ASACA library; if no empty slots are available in the library an error is returned and processing of the import operation stops
- Indicate success of the operation when complete.

### Export

Exporting media from the library makes the files on that media unavailable for I/O in the OSVault appliance, so requests for files on that media (or to files that were migrated from cache to that media) will result in an error being returned to the requesting application. **Please note** that exporting a media label will also export the media label located on the other side of that piece of media.

Attempting to export media that is currently in use, i.e. mounted in an optical drive, will probably fail with an error such as “Unmount failed, device in use”.

If you receive this error, wait until the media is no longer in use and retry the export operation.

To removed the media from the I/E slot after exporting, refer to the ASACA Library Users Manual for directions on use of the library front panel.

## 6.2 Magazines

The ASCA AM-series of optical libraries organizes all of their media into groups of 50 pieces, called a magazine. A magazine in the library can be removed and replaced with another magazine, causing up to 50 pieces of media to move in or out of the library.

If you remove a magazine without telling OSVault, you may get errors when trying to access files on that media. If you add a magazine full of media to the library without telling OSVault, the files on that media may not be accessible until you perform an inventory.

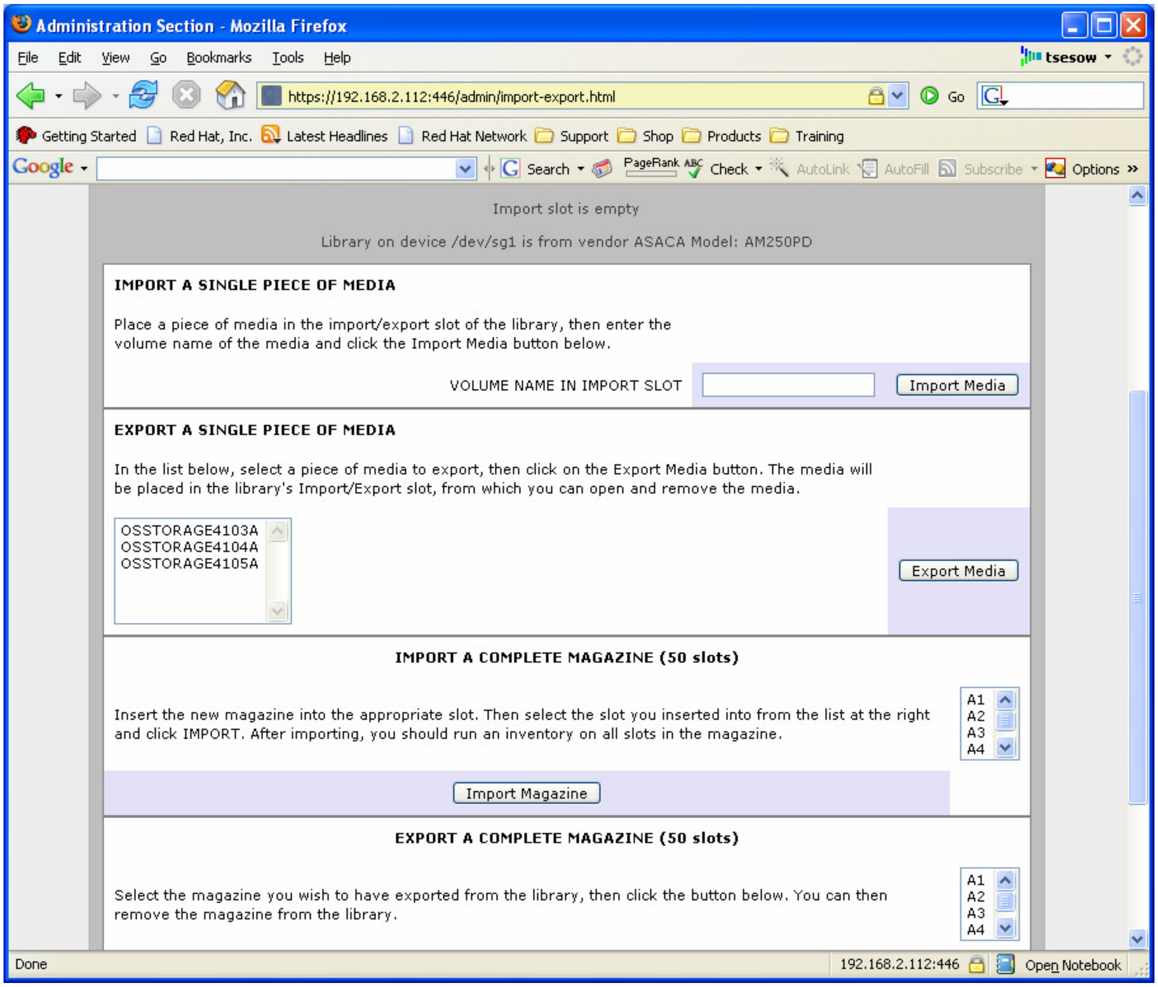
A picture of an ASACA AM-series magazine is shown below:

In the ASACA AM-series libraries, magazines are numbered from A1 to A7, B1 to B7, C1 to C8 and D1 to D7. The exact magazines labels in each model are shown in the following table.

| | |
|---|---|
| AM-250 | Magazines A1, A2, B1, B2, C1 (C1 is not easily removable) |
| AM-750 | Magazines A1 thru A4, B1 thru B4, C1 thru C4 and D1 thru D3. The number of D magazines depends on the number of drives installed. |
| AM-1450 | Magazines A1 thru A7, B1 thru B7, C1 thru C8 and D1 thru D7. The number of D magazines depends on the number of drives installed. |

## 6.3 Web-Based Import/Export

If you open a web browser at http://10.1.1.2 (the default OSVault IP address), you will be presented with the following screen:



Import slot is empty

Library on device /dev/sg1 is from vendor ASACA Model: AM250PD

IMPORT A SINGLE PIECE OF MEDIA

Place a piece of media in the import/export slot of the library, then enter the volume name of the media and click the Import Media button below.

VOLUME NAME IN IMPORT SLOT

EXPORT A SINGLE PIECE OF MEDIA

In the list below, select a piece of media to export, then click on the Export Media button. The media will be placed in the library's Import/Export slot, from which you can open and remove the media.

OSSTORAGE4103A
OSSTORAGE4104A
OSSTORAGE4105A

IMPORT A COMPLETE MAGAZINE (50 slots)

Insert the new magazine into the appropriate slot. Then select the slot you inserted into from the list at the right and click IMPORT. After importing, you should run an inventory on all slots in the magazine.

A1
A2
A3
A4

EXPORT A COMPLETE MAGAZINE (50 slots)

Select the magazine you wish to have exported from the library, then click the button below. You can then remove the magazine from the library.

A1
A2
A3
A4

## Import Media

Once the media is inserted into the I/E slot (see above), click on the IMPORT button on the web browser. This will move the piece of media out of the import/export slot, place it in an empty slot in the library and update the inventory of media.

## Export Media

Using the ASACA Library/Media Management screen in your web browser, selected the media name that you wish to export. Clicking on the export button will then start the media export process, which performs the following operations:

- The I/E slot in the library is checked to verify that it is currently empty, if it is occupied the export operation is terminated with an error and the media selected for export remains in the library
- The media is moved from its storage slot to the I/E slot
- The directory entry for the media in the /archive directory is removed so that references to files on the library will return an error to the client requesting the data
- The database (/etc/migration.conf) is updated to show that the media is no longer present in the library

To remove the media from the I/E slot after exporting, refer to the ASACA Library Users Manual for directions on use of the library front panel.

## Import a Magazine

Insert the magazine into the appropriate slot. Select the slot identifier on the screen and click IMPORT. If the magazine has been previously seen by OSVault, the media in it is set back to RESIDENT in the library. If the user moved media around or this is a completely new magazine, an inventory must be run on the magazine. New magazines will create new database entries.

## Export a Magazine

Select the slot identifier on the screen and click EXPORT. The OSVault system will update the internal appliance database to mark all media in the library as absent and inform you when it is safe to remove the magazine.

## 6.4 Command Line Import/Export

### Import Media

Use the "importmedia" command to import media into the ASACA library. Media to be imported must first be placed into the Import/Export slot (I/E slot) in the ASAC library.

For example, to import a piece of media that was originally labeled "DATA4100A" and put it into slot 4100, use the following command after inserting the media into the import/export slot of the optical library:

```
importmedia –volume_label DATA4100A –store_slot 4100
```

This will move the piece of media out of the import/export slot in the library, place it is slot 4100 (which for an ASACA library is the 5th slot) and update the inventory of media to show that DATA4100A is now back in the library.

### Export Media

To export media from the library, use the "exportmedia" command. The "exportmedia" command takes one argument which is the media label on the media, e.g. ASACA4097A. To removed the media from the I/E slot after exporting, refer to the ASACA Library Users Manual for directions on use of the library front panel.

For example, to export the optical media labeled DATA4100A from the library, use the command:

```
exportmedia DATA4100A
```

This will move the media from its storage slot to the import/export slot in the optical library and will update the OSVault inventory to show that DATA4100A is absent from the library.

### Import a Magazine

Insert the magazine into the appropriate slot. Use the importmedia command with the "-m" option, followed by the slot identifier. For example, to import a magazine into the first 50-slot magazine (magazine A1) in the library, type the following command:

```
importmedia –m A1
```

If the magazine has been previously seen by OSVault, the media in it is set back to RESIDENT in the library. If the user moved media around or this is a completely new magazine, an inventory must be run on the magazine. New magazines will create new database entries.

### Export a Magazine

To export an entire magazine from a library, use the exportmedia command with the “-m” option, followed by the magazine identifier. For example, to export the first 50-slot magazine (magazine A1) from a library, type the following command:

```
exportmedia –m A1
```

The OSVault system will update the internal appliance database to mark all media in the library as absent and inform you when it is safe to remove the magazine.

# 7 Attaching Client Systems to OSVault

## 7.1 Windows 98/2000/XP/2003 Clients

OSVault appears on your network as a Windows 2000 server. The “cache” share is automatically created when the appliance starts up. Writing to the “cache” share will always result in the files being created on hard disk first. After a period of time, older files will be moved to optical media and all further I/O operations will work directly against the optical media.

If your Windows machine is on the same subnet as your OSVault appliance, you should now be able to connect to the OSVault server by clicking on Start / Run and typing:

```
\\MYSERVER\pub
```

**Mangling Method**

Name mangling is a method where Windows allows long filenames to retain a short filename equivalent. For example, C:\Program files can also be referred to as C:\PROGRA~1. There are two algorithms available, hash and hash2. If you store a lot of files on your server, you can help to avoid name collisions by adjusting your global parameter section with mangling method = hash2. This is set in the OSVault Advanced Web Interface.

**Oplocks**

Opportunistic locking essentially means that the client is allowed to download and cache the file on their hard drive while making changes; if a second client wants to access the file, the first client receives a break and must sync the file back to the server. This can give significant performance gains in some cases; in others, some programs insist on syncing back the contents of the entire file for a single change. Level1 Oplocks (aka just plain "oplocks") is another term for opportunistic locking.

Level2 Oplocks is a fancy way of saying that you are providing opportunistic locking for a file that will be treated as "read-only". Typically this is used on files that are read-only or on files that the client has no intention to write to (at least, not initially).

Kernel Oplocks are essentially a method that allows the Linux kernel to co-exist with Samba's oplocked files, although this is simplifying things a bit. SGI IRIX and Linux are the only two UNIX's that are oplock aware at the moment. Unless your system supports kernel oplocks, you should disable oplocks if you are accessing the same files from both Unix/Linux and Smb clients.

Regardless, oplocks should always be disabled if you are sharing a database file (e.g., Microsoft Access) between multiple clients, as any break the first client receives will result in the entire file needing to be synced (not just the single record), which will result in a noticeable performance delay and, more likely, problems accessing the database in the first place. Notably, Microsoft Outlook's personal folders (*.pst) react very badly to oplocks. If in doubt, disable oplocks and tune your system from that point. If client-side caching is desirable and reliable on your network, you will benefit from turning on oplocks. If your network is slow and/or unreliable, or you are sharing your files among other file sharing mechanisms (e.g., NFS) or across a WAN, or multiple people will be accessing the same files frequently, you probably will not benefit from the overhead of your client sending oplock breaks and will instead want to disable oplocks for the share. Another factor to consider is the perceived performance of file access. If oplocks provide no measurable speed benefit on your network, it might not be worth the hassle of dealing with them.

## Windows 98/ME

Fortunately, both Windows 98 and Windows ME use encrypted passwords by default. All that's left is to configure your Network properties in the Control Panel. Make sure you have Client for Microsoft Networks and TCP/IP installed along with your network adapter. If you're not using a DHCP server, you'll probably need to configure the TCP/IP settings as well.

Under the properties for Client for Microsoft Networks, check the box for Log on to Windows NT domain and specify the domain name that your Samba server is using. Finally, under the second tab labeled Identification, give your computer a unique name and specify the name of the workgroup (which should match the name of the domain, although not strictly necessary).

## Windows XP/2000

You'll need to enable TCP/IP on your system, as well as configure a WINS server, from the control panel. The IP address of the WINS server should be your OSVault appliance server (where the nmbd daemon is running). To map a drive using the Windows GUI, open My Computer. On the toolbar are many options; look for one that provides a list that includes the phrase Map

Network Drive (under Windows XP this option is under the Tools menu). Once selected, a new box will open up. In the Drive box, click a drive letter that you wish to use. In the Folder box, type the path for the server and path that you wish to connect to.

Alternately, from a Command Prompt, you can type:

```
NET USE F: \\MYSERVER\PUB /YES
```

## 7.2 LINUX Clients

Before beginning, you should double-check to make sure your mount program is new enough (version 2.10m if you want to use Version 3 NFS), and that the client machine supports NFS mounting, though most standard distributions do. If you are using a 2.2 or later kernel with the /proc filesystem you can check the latter by reading the file /proc/filesystems and making sure there is a line containing nfs. If not, typing **insmod nfs** may make it magically appear if NFS has been compiled as a module; otherwise, you will need to build (or download) a kernel that has NFS support built in. In general, kernels that do not have NFS compiled in will give a very specific error when the **mount** command below is run.

To begin using a machine as an NFS client, you will need the portmapper running on that machine; and to use NFS file locking, you will also need **rpc.statd** and **rpc.lockd** running on both the client and the server. Most recent distributions start those services by default at boot time.

With **portmap**, **lockd**, and **statd** running, you should now be able to mount the remote directory from your server just the way you mount a local hard drive, with the mount command. Suppose our server is called *OSVault*, and we want to mount the /cache directory on *slave1.foo.com*. Then all we have to do from the root prompt on *slave1.foo.com* is type:

```
mount OSVault:/cache /mnt/home
```

and the directory /cache on master will appear as the directory /mnt/home on *slave1*. (Note that this assumes we have created the directory /mnt/home as an empty mount point beforehand.)

You can get rid of the file system just like you would for a local file system,

by typing:

```
umount /mnt/home
```

## Getting NFS Servers Mounted at Boot Time

NFS file systems can be added to your /etc/fstab file the same way local file systems can, so that they mount when your system starts up. The only difference is that the file system type will be set to **nfs** and the dump and fsck order (the last two entries) will have to be set to zero. So for our example above, the entry in /etc/fstab would look like:

```
none    10.1.1.2:/cache       /OSVAULT_CACHE    nfs   defaults  0 0
```

See the manual pages (using the *man* command) for *fstab* if you are unfamiliar with the syntax of this file. If you are using an automounter such as amd or autofs, the options in the corresponding fields of your mount listings should look very similar if not identical.

At this point you should have NFS working, though a few tweaks may still be necessary to get it to work well.

## Soft vs. Hard Mounting

There are some options you should consider adding at once. They govern the way the NFS client handles a server crash or network outage. One of the cool things about NFS is that it can handle this gracefully, if you set up the clients correctly. There are two distinct failure modes:

**soft**

If a file request fails, the NFS client will report an error to the process on the client machine requesting the file access. Some programs can handle this with composure, most won't. We do not recommend using this setting; it is a recipe for corrupted files and lost data. You should especially not use this for mail disks, if you value your mail.

**hard**

The program accessing a file on an NFS mounted file system will hang when the server crashes. The process cannot be interrupted or killed (except by a "sure kill") unless you also specify **intr**. When the NFS server is back online the program will continue undisturbed from where it was. We recommend using **hard,intr** on all NFS mounted file systems.

Picking up from the previous example, the fstab entry would now look like:

```
# device    mountpoint  fs-type    options    dump fsckord

  ...

master.foo.com:/home  /mnt/home   nfs     rw,hard,intr  0     0

  ...
```

## Setting Block Size to Optimize Transfer Speeds

The **rsize** and **wsize** mount options specify the size of the blocks of data that the client and server pass back and forth.

The defaults may be too big or to small; there is no size that works well on all, or most, setups. On the one hand, some combinations of Linux kernels and network cards (largely on older machines) cannot handle blocks greater than 128Kbytes. On the other hand, if they can handle larger blocks, a bigger size might be faster.

Getting the block size right is an important factor in performance and is a must if you are planning to use the NFS server in a production environment.

### 7.3 Solaris Clients

Not yet tested.

### 7.4 HP-UX Clients

Not yet tested.

### 7.5 MacIntosh OS X Clients

OS X supports both the Network File System and the CIFS (Windows) Share.

If you wish to access the OSVault appliance via the CIFS protocol, first make sure that you've enabled SMB support in the Macintosh Directory Access Utility (in the Applications/Utility folder). Select SMB and then click Configure. You can now enter in your preferred workgroup and WINS server information. Next, activate the Finder (e.g., click on the Finder in the Dock). Select Go, then Connect to Server. In the Server Address field, type in your server address. For example:

```
smb://ServerName/ShareName
```

After clicking Connect, you may be prompted for your authentication.

### 7.6 AIX Clients

Not yet tested.

## 8 Media Duplication and Replication

Media duplication and replication are not included in the current version of the OSVault appliance. They will be implemented in a future release.

## 9 Automatic Backups

### 9.1 How Automatic Backups Work

According to the schedule set in the “cron” schedule, a backup will run periodically (at 1am by default) where the cache directory will be backed up to the first piece of optical media in the library. Also backed up at this time is certain system configuration information.

The purpose of the backup is to enable the restoration of operation after a hard disk failure without needing to full read all media in the optical library. Even if the backup media is not used, it is possible to restore the full system operation after a hard disk failure by reinstalling the system software and performing a full inventory.

The automatic backup does not make a copy of the /cache file system data, so migration must run frequently enough to ensure that data is stored on the more reliable optical media. If migration is running less frequently, or if a higher level of reliability is required, then the /cache file system should be placed on a RAID hard drive system with RAID-1 or RAID-5 level configured. OSVault has been tested with the Engenio RAID systems (marketed by STK, SGI, and IBM), the Xyratex RAID systems (with Chaparral RAID controllers) and the Nstor RAID systems.

## 9.2 How to Restore a System Backup

The backup on the first optical media is a “tar” file that needs to be restored via the command line interface with the following commands:

```
mcstat
putaway 0
mm 4096 64 0 0 /dev/sg3
tar xvf /dev/scd2
```

The above steps assume that /dev/scd2 is the name of the first drive (topmost) in the library. /dev/sg3 is assumed to be the device name of the library interface.

# 10 Advanced Web-Based Administration Utilities

See the OSVault Advanced Web Adminstration Manual.