

Setup 2 FreeBSD servers that sync data with full hdd encryption

Tags: `freebsd` `encryption` `hdd` `sync`

Zone: FreeBSD

I'am running these baby's for a few years now and i'am just very happy with them, i just wanted to share the manual that i have created for upgrades and other things. Ooohyes! FreeBSD makes me happy (as a server), no maintenance and i always use the hardware i do not need anymore.

The original is in dutch and i hope i can save this baby online a few times, while i'am listening to the Beasty Boys from my FreeBSD server.

I want to point out that al actions below will destroy all your data on your harddrive, you have been warned!

I have used this manual on FreeBSD 6.2 and now i'am rewriting it for FreeBSD 8.1, there are some slight changes.

Okay! Enough mumbo-Jumbo, Start this 100+ steps manual.

A word from the FreeBSD hood

The BSD02 Server is a big tower from 1995 (modified ofcourse) with a motherboard: Compaq: Compaq Deskpro EN (933 Mhz). My dad learned me to use the saw on metal, and the powerdrill.

The first time i encountered to following error:

Fatal trap 12: page fault while in kernal mode

fault virtual adress = 0x1

fault code = supervisor read, page not present

instruction pointer = 0x20:0xc06a6b14

stack pointer = 0x28:0xcbf3b670

frame pointer = 0x28:0xcbf3b670

code segment = base 0x0, limit 0xffff, type 0x1b
= DPL 0, pres 1, def32 1, gran 1

processor eflags = interrupt enabled, resume, IOPL = 0

current process = 2 (g_event)

trap number = 12

panic: page fault

What a drag and more time to listen to some more music.

I just did: **disable all power options in the bios** Who needs them anyway, just like cars, burn as much as you can!

And then the keyboard responded 50% of the time intermittedly:

>Number: 105368

>Category: kern

>Synopsis: geli passphrase prompt malfunctioning when mounting encrypted fs at boot time

>Confidential: no

>Severity: non-critical

>Priority: medium
>Responsible: freebsd-bugs
>State: open
>Quarter:
>Keywords:
>Date-Required:
>Class: sw-bug
>Submitter-Id: current-users
>Arrival-Date: Fri Nov 10 10:10:21 GMT 2006
>Closed-Date:
>Last-Modified:
>Originator: Jost Menke
>Release: 6.2-BETA3, also tested 6.1-RELEASE
>Organization:
>Environment:
FreeBSD 6.2-BETA3 FreeBSD 6.2-BETA3 #0: Mon Oct 30 22:04:37 UTC 2006 root at o
pus.cse.buffalo.edu:/usr/obj/usr/src/sys/GENERIC i386
>Description:
When running FreeBSD 6.2-BETA3 or 6.1-RELEASE in a VMware session with encrypted
root filesystem, the geli password prompt does not work when the root fs is mounted at boot
time. I put kern.geom.eli.visible_passphrase=1 into /boot/loader.conf to see what's wrong,
result: the keyboard doesn't work at all. When kbdmux is deactivated by putting
hint.kbdmux.0.disabled="1" into /boot/device.hints, the behaviour changes: Keyboard partly
works, but about 90% of all keystrokes are lost. The problem only seems to occur when
mounting encrypted volumes at boot time. Other people on the mailing list report similar
problems running FreeBSD on real hardware.
>How-To-Repeat:
- Install 6.2-BETA3 or 6.1-RELEASE with encrypted root fs in VMware player
- Put kern.geom.eli.visible_passphrase=1 into /boot/loader.conf
- Also try to put hint.kbdmux.0.disabled="1" into /boot/device.hints
>Fix:
>Release-Note:
>Audit-Trail:
>Unformatted:

The solution to all this grief is:

Stop: hint.kbdmux.0.disabled="1" in /mnt/boot/device.hints is the solution.

Also i put dcons_load="NO" in /mnt/boot/loader.conf

I Based my setup on:

<http://www.proportion.ch/index.php?page=31>

Configure future Harddisk

The harddisk that you are going to use to boot from in the future

1

Configuring hdd as Primary hdd

Ofcourse, at home, i use cheap hardware. Put your hdd that you are going to use as boot drive on the primary controller as Master and make sure the bios starts from a working cdrom drive.

Tip: Keep in mind that some hard drive with a special jumper setting will be seen as single harddrive.

2

Start FreeBSD installation

Start the FreeBSD Installation from CD/dvd
Choose your country, mine is Netherlands

3

Choose standard install

Choose the standard installation

4

You will be send to a FDISK-alike program

You will be send to a Fdisk alike program

5

Choose ad0 to configure

Choose **ad0** to configure.

6

Make a 12000 MB (becomes ad0s1)

Make a 12000 MB (this becomes ad0s1)

7

Becomes (becomes ad0s2)

Fill up the empty space on your hdd (becomes ad0s2)
Standard FreeBSD configures the following:

Part - Mount - Size - Newfs

- ad0s1a - / - 512MB - UFS2 - Y
- ad0s1b - swap - 732MB - SWAP -
- ad0s1d - /var - 1390MB - UFS2+S - Y
- ad0s1e - /tmp - 512MB - UFS2+S - Y
- ad0s1f - /usr - Rest - UFS2+S - Y

The numbers above are just too low for today's needs, so I change them to:

Part - Mount - Size - Newfs

- ad0s1a - / - 2000MB - UFS2 - Y
- ad0s1b - swap - 1000MB - SWAP -
- ad0s1d - /var - 2000MB - UFS2+S - Y
- ad0s1e - /tmp - 1000MB - UFS2+S - Y
- ad0s1f - /usr - Rest - UFS2+S - Y

if you need more you can fiddle around with these values.

9

Choose QUIT

Choose Q (Quit)

10

Choose BootMgr

Choose BootMgr

Don't choose the first options I always get an error
Invalid partition table

11

Choose OK

Choose OK

12

Time to setup seperate partitions

Now it is Time to setup seperate partitions, Choose ad0s1 (with your arrow keys)

14

Setup your hdd

Choose A for Defaultts

Part:	Mount:	Size:	Newfs
ad0s1a	/	512MB	UFS2
ad0s1b	swap	486MB	SWAP
ad0s1d	/var	1267MB	UFS2+S
ad0s1e	/tmp	512MB	UFS2+S
ad0s1f	/usr	1221MB	UFS2+S

If you got a bigger hdd than 10GB, change

ad0s1a to 10GB

ad0s1b to 3GB

ad0s1D to 10GB

ad0s1E to 10GB

ad0s1f to (the rest that is left)

(And yes you can just enter 10GB)

16

Press Q to Leave

Press Q to Leave

17

User (binaries and doc only)

Choose User (binaries and doc only)

Then choose your documentation language, i use en English Documentation

18

Say [Yes] on FreeBSD ports selection, choose [OK]

Say [Yes] on FreeBSD ports selection, choose [OK]

19

Kies Install from a FreeBSD CD/DVD

Choose Install from a FreeBSD CD/DVD

20

Choose OK

Choose [OK]

21

RU Sure?

Are you sure? [YES] (File system is written, and installation started)
Please wait until all is installed

22

Configure Ethernet or SLIP/PP network devices?

Configure Ethernet or SLIP/PP **network** devices? [NO]

23

function as a network gateway?

function as a **network** gateway? [No]

24

configure inetd and the network services that it provides?

configure inetd and the network services that it provides? [No]

25

like to enable SSH login? [YES]

like to enable SSH login? [YES] (Always handy to change configurations with SSH from a working machine)

26

Do you want anonymous FTP access?

Do you want anonymous FTP **access**? [No] (Never do this or the software kiddies will get you)

27

NFS Server? [NO]

NFS Server? [NO]

28

BFS Client [NO]

BFS Client [NO]

29

customize your system console settings? [NO]

customize your system console settings? [NO]

30

Time Zone? [YES]

Time Zone? [YES]

31

28. CMOS clock set to UTC... [NO]

28. CMOS clock set to UTC... [NO]

32

8. Europe

Choose 8. Europe (Or another continent, you will figure this out)

33

Netherlands

My country is Netherlands

34

CET reasonable? [YES]

CET reasonable? [YES]

35

enable Linux binary compatibility? [NO]

enable Linux binary compatibility? [NO] (I like to keep it as stable as possible)

36

PS/2, serial or BUS mouse? [NO]

PS/2, serial or BUS mouse? [NO] (Hardcore people use the keyboard)

37

FreeBSD package collection? [NO]

FreeBSD package collection? [NO] (We will install this on the encrypted partition later)

38

additional accounts to the system? [YES]

additional accounts to the system? [YES]

Add a user with the details you want

39

Set password for Root.

Set password for Root.

Remark! Use another root password in the unencrypted part (this part) than on the encrypted part.

Type your password {ENTER}

Type it again {ENTER}

40

Last chance

Visit the general configuration menu for a chance to set any last options? [No]

41

Exit install

[X] Exit install. {ENTER}

42

Exit - Reboot

Are you sure you wish to exit? The system will reboot [Yes]

CD will be ejected

[Ok]

Install X Windows

To successfully load: `vboxnetflt.ko` at bootup we first need to install x windows together with virtualbox on the unencrypted part.

95

Start the installation of Xwindows

```
1: cd /usr/ports/x11/xorg
2: make install clean
```

Options for libxslt

EXTRA_ENCODINGS = on

96

Options for libxslt

Use the standard options:

MEM_DEBUG = off

CRYPTO = on

[OK] to go on.

My machine is taking off at this moment. ;-) I will go downstairs and get some juice.

96a

Options for python

THREADS = on

UCS4 = on

PYMALLOC = on

IPV6 = on

Other options are off

Options for perl

PERL_64BITINT = on

USE_PERL = on

Options for m4

LIBSIGSEGV = off

97

Options for png

I use the default and that is APNG = off.

98

Options for xorg-apps 7.5

Also i use the standard, and that is all options = on.

99

Options for pixman

I don;t need MMX and SSE2 features and i have got AMD, so i leave SIMD = off.

1

Options Xorg-drivers

I have used the standard settings here.

2

Options for xorg-server

All Options on.

3

Options for HAL

Standard FIXED_MOUNTPOINTS = off and leave it that way.

4

Options for docbook-xsl

All options are on by default, that's a good thing.

5

Options for Glib

COLLATION_FIX = off

Docbook-xsl

All options on

Glib

COLLATION_FIX = off

6

GAM_POLLER

GAM_POLLER = off

7

Options for cairo

GLITZ = off

XCB = on

8

Options for xf86-video-radeonhd

UTILS = off

9

Finish installation of Xorg

Add two lines to /etc/rc.conf

```
1: vi /etc/rc.conf
```

Add the following lines at the bottom

```
1: hald_enable="YES"  
2: dbus_enable="YES"
```

10

Restart machine

```
1: shutdown -r NOW
```

11

Start X Windows

I don't need flashy graphics, so i don't configure. If i do i only get a black screen. Something to find out in the future, i just want to have a virtual machine.

```
1: startx
```

Install all sources

With sysinstall

12

Install Virtualbox

Install virtualbox inside X Windows on the unencrypted part of the hdd.

```
1: cd /usr/ports/emulators/virtualbox-ose-kmod
```

```
1: make install clean
```

Options virtualbox-ose-kmod

```
DEBUG = off
```

Install Second part Virtualbox

```
1: cd /usr/ports/emulators/virtualbox-ose
```

```
1: make install clean
```

13

Choose options for virtualbox-ose

```
QT4 = on  
DBUS = on  
X11 = on  
VNC = on  
NLS = on
```

Let the waiting begin!

14

Options for phonon

PULSAUDIO = off

15

Options for SQLite

FTS3 = on
METADATA = on
THREADSAFE = on

all other options are off.

16

Options for tcl

Only TCL_MODULES = on

17

Options for sdl

AALIB = on
NAS = on
OPENGL = on
OSS = on
VGL = on
XLIB = on

All other options are off.

18

Options for curl

CARES = on
OPENSSL = on
PROXY = on

All other options are off

19

Options for ca_root

ETCSYMLINK = off

Add vbox driver to /boot/loader.conf

Edit /boot/loader.conf

```
1: Vi /boot/loader.conf
```

Add the following line:

```
1: Vboxdrv_load="YES"
```

Add vbox to /etc/rc.conf

Edit /etc/rc.conf

```
1: Vi /etc/rc.conf
```

And add the following at the bottom:

```
1: Vboxnet_enable="YES"
```

Restart machine

Check if you see errors about vbox, this is necessary if you want bridget Network (own IP in your network).

43

Power down the machine

Power down the machine as soon as the bios screen is visible.

Configure temporary Harddisk

The harddisk that you are going to use for one or time

44

Switch hdd

Turn the computer off, disconnect the harddisk from the steps above and connect the other Temporary hdd als primary master slave.

45

Boot from cdrom

Boot drom the FreeBSD cdrom that you have used in the above steps.
Do not use a different FreeBSD version, there are differences in the versions!

46

Choose standard installation

Choose standard installation

47

You will be sent to Fdisk

You will be sent to a fdisk a like program. Create one slice [C], choose the default value (Whole harddisk). (If you are using a harddisk that is a bit broken, make this slice smaller).

48

Press Q to leave

Press [Q] to leave.

49

Select Boot Manager

Select Boot Manager and choose [OK]

50

Arrange the slices

Part - Mount - Size - Newfs

- * ad0s1a - / - 2000MB - UFS2 - Y
- * ad0s1b - swap - 1000MB - SWAP -
- * ad0s1d - /var - 2000MB - UFS2+S - Y
- * ad0s1e - /tmp - 1000MB - UFS2+S - Y
- * ad0s1f - /usr - Rest - UFS2+S - Y

51

Q to leave

Press Q to leave Fdisk

52

6-User

Select 6 User Average user.....
Select en English Documentation

53

No FreeBSD ports selection

Select [No] FreeBSD ports selection

54

Install from CD/DVD

Select CD/DVD - Install from a FreeBSD CD/DVD

55

Select yes to install

Select [Yes] to install

Wait a moment for FreeBSD todo the installation

56

Configure Ethernet or SLIP/PP network devices? [NO]

Configure Ethernet or SLIP/PP **network** devices? [NO]

57

function as a network gateway? [NO]

function as a **network** gateway? [NO]

58

***configure inetd and the network services that it provides?
[NO]***

configure inetd and the network services that it provides? [NO]

59

like to enable SSH login? [YES]

like to enable SSH login? [YES]

60

Do you want anonymous FTP access? [NO]

Do you want anonymous FTP **access**? [NO]

61

NFS Server? [NO]

NFS Server? [NO]

62

NFS Client [NO]

NFS Client [NO]

63

customize your system console settings? [NO]

customize your system console settings? [NO]

64

Time Zone? [YES]

Time Zone? [YES], Is this machine's CMOS clock set to UTC? [No]

65

8 - Europe

Select 8. Europe

66

34. Netherlands

34. Netherlands, Does the abbreviation `CEST` look reasonable? [Yes]

67

FreeBSD package collection

FreeBSD package collection [No]

68

additional accounts to the system? [YES]

Additional accounts to the system? [YES]

Enter the credentials for the extra user

69

Exit

[X] Exit

70

Set root password

Set root password, do not enter the same root password as the one you are going to use for the encrypted part.

71

Visit general configuration menu for a change to set any last options? [NO]

Visit general configuration menu for a change to set any last options? [NO]

72

Exit install

[X] Exit install, Are you sure you wish to exit? The system will reboot [Yes]

73

Are you sure you wish to exit

Are you sure you wish to exit [Yes], Sure to remove media from the drive: [Ok]

74

Turn off system when you see the BIOS screen

Turn off system when you see the BIOS screen

Make the encryption partition

75

Connect both harddisks to the system

Connect both harddisks to the system

Dont forget to set the harddisk to Master, if this harddisks has a seperate setting for single harddisk.

76

Go to the BIOS

Enter the BIOS and disbale booting from CDROM and make sure that you boot from harddisk temporary harddisk.

77

Log in under Root

Log in under Root

78

Check your devices

Check your devices

Type:

```
1: cd /dev
```

```
1: ls
```

Check if you see /ad0s2 (Harddisc 0 Slice 2). In some cases the device where you want to install your encrypted Freebsd can be /ad1s2, ad2s2 or even ad6s2. Be sure to check for s2.

79

Initialise the partition for encryption

Initialise the partition for encryption

Type:

```
1: geli init -b -s 4096 -l 256 /dev/ad0s2  
{ENTER}
```

Keep in mind that this can be different on your system, mostly my code will work without any problems

80

Enter new passphrase

You will be asked:

```
1: Enter new passphrase
```

Enter a long password for the encrypted partition that nobody knows. **You need to enter this everytime you start your system!**

81

Enter your passphrase a second time

Enter your passphrase a second time, if everything is ok you will be prompted:

```
1: Metadata backup can be found in /var/backups/ad0s2.eli and can be  
   restored.....
```

if not, enter the command again and try again.

Yes encryption is native

82

Attach the drive to FreeBSD

Attach the drive to FreeBSD

Type:

```
1: geli attach /dev/ad0s2
```

You can find the device (/dev/ad0s2) in /dev directory

83

Enter passphrase 1 time

Enter the passphrase that you have entered before to unlock the encrypted partition.

When everything goes well you will see:

```
1: GEOM_ELI: Device ad0s2.eli created.
2: GEOM_ELI: Encryption: AES-CBC 256
3: GEOM_ELI: Crypto: software
```

84

Arrange the partitions on the encrypted hdd

It's time to arrange the encrypted slice with partitions for the operating system.

```
1: bsdlablel -w /dev/ad0s2.eli
{ENTER}
```

```
1: bsdlablel -e /dev/ad0s2.eli
{ENTER}
```

Remember that ad0s2 can be something different on other systems, especially with IDE and Sata onboard

85

Edit partitions in slice with vi

An Editor will be started ([vi](#))

Enter the following!

```
# /dev/ad0s2.eli:
1: 8 partitions:
2: #      size          offset          fstype          [fsize    bsize
3: bps/cpg]
4: a:    500000          0              4.2BSD          0          0
5: b:    472656          500000         swap            0          0
6: c:    ??????          0              unused          0          0
7: # don't edit
8: d:    618164          972656         4.2BSD          0          0
9: e:    250000          1590820        4.2BSD          0          0
   f:      *            1840820        4.2BSD          0          0
```

I=Insert [ESC=end Insert], x = remove one character

Don't remove the character C, but MOVE the character c

Arrange everything with TABs to get it underneath eachother

86

Write the partitions

Press [ESC] to release insert, press **:w** to write the file, and then press **:q** to quit.
When no error appears all is well!

87

Check if the encrypted devices are made

To Check if the encrypted devices are made and visible to the system type:

```
1: cd /dev
```

```
1: ls
```

And search for ad0s2.eli, ad0s2.elia, ad0s2.elib, ad0s2.elid, ad0s2.elie, ad0s2.elif

88

Format the new encrypted partitions

It's time to format those new encrypted partitions

```
1: newfs -i 1024 /dev/ad0s2.elia
```

You will see some data over your devices and how many [inodes](#) your partition will have.

```
1: /dev/ad0s2.elia: 488.3 MB (1000000 sectors) block size 16384, fragment
2: size 4096
3:         using 4 cylinder groups of 122.08MB, 7813 blks, 31296 inodes.
4: super-block backups (for fsck -b #) at:
   160, 250176, 500192, 750208
```

The switch **-i 1024** will make it possible to write a lot of small files

89

Dont format swap, but the next

We don't need to format the swap partition (.elib), this is just a scratch disc so the next command will be:

```
1: newfs /dev/ad0s2.elid
```

90

Format tmp partition

After the /var we are going to format the /tmp partition:

```
1: newfs /dev/ad0s2.elie
```

91

format elif (the rest of the slice)

Format .elif, with this partition it is also very important to write a lot of files, especially because we are going to install the FreeBSD Ports collection.

```
1: newfs -i 1024 /dev/ad0s2.elif
```

No your screen will fill up with a lot of numbers (This is formatting under linux, it gives me peace of mind)

92

Installing the OS encrypted style

Now all encrypted partitions are formatted we are going to install the OS, again use the same OS version as used on all the other partitions.

The first step, make a directory:

```
1: mkdir /fixed
```

We can use this directory to mount the encrypted partition

93

Connect encrypted partition

We are going to connect the encrypted partition

```
1: mount /dev/ad0s2.elia /fixed
```

94

Create directorys for the OS

Create all the directory's that are needed for FreeBSD

```
1: mkdir /fixed/var
2: mkdir /fixed/tmp
3: mkdir /fixed/usr
```

95

Mount all partitions for OS

Mount all the OS partitions:

```
1: mount /dev/ad0s2.elid /fixed/var
2: mount /dev/ad0s2.elie /fixed/tmp
3: mount /dev/ad0s2.elif /fixed/usr
```

96

Copy FreeBSD System

Copy FreeBSD OS to encrypted partition.

Set the directory and switch from command-line shell

```
1: /bin/sh
2: export DESTDIR=/fixed/
3: /bin/csh
```

97

Mount cdrom

Insert the FreeBSD install cd/dvd and mount it

```
1: mount /cdrom
```

98

Install FreeBSD

Go to the FreeBSD release directory

```
1: cd /cdrom/8.1-RELEASE/base
```

```
1: ./install.sh
```

99

Are you sure to write to /fixed

You are about to extract the base distribution into /fixed/ - are you SURE you want to do this over your installed system (y/n)?

when it says /fixed/ [Y]

```
1
```

Install kernel files

The kernel files need to be installed seperately

```
1: cd /cdrom/8.1-RELEASE/kernels
2: ./install.sh GENERIC
```

2

Install the help pages

We need some info, so we install the help pages

```
1: cd /cdrom/8.1-RELEASE/manpages
2: ./install.sh
3: cd /cdrom/8.1-RELEASE/catpages
4: ./install.sh
```

Arrows up and down do the same as under dos, you can scroll through your commands

3

Mount the future boot drive

Mount the drive where we are going to boot from:

```
1: mount /dev/ad0s1 /mnt
```

4

Copy Boot directory

Copy the boot directory to the unencrypted partition:

```
1: cp -Rpv /fixed/boot /mnt
```

The files will roll over your screen

5

Speed Up Boot Process

To speed up the boot process we will get the 2 files that are needed to boot:

```
1: cd /mnt/boot/kernel
2: gzip kernel geom_eli.ko acpi.ko
```

6

Boot from encrypted partition please

All we need is installed on the unencrypted part. Now we are going to tell FreeBSD to boot from the encrypted partition.

```
1: vi /mnt/etc/fstab
```

7

Change fstab

Change the fstab file to the following (Mostly change s1? to s2.eli?):

#	Device	Mountpoint	Fstype	Options	Dump
	Pass#				
	/dev/ad0s2.elib	none	swap	sw	0
1:	0				
2:	/dev/ad0s2.elia	/	ufs	rw	1
3:	1				
4:	/dev/ad0s2.elie	/tmp	ufs	rw	2
5:	2				
6:	/dev/ad0s2.elif	/usr	ufs	rw	2
7:	2				
	/dev/ad0s2.elid	/var	ufs	rw	2
	2				
	/dev/acd0	/cdrom	cd9660	ro,noauto	0
	0				

In fstab you can tell FreeBSD what to mount at bootup, be carefull!! one mistake and you need to fix it in safe mode. I don;t like that!

If you have a floppydrive in your system, you can add:

/dev/fd0 /fdd ufs rw,noauto 0 0 to fstab

8

Write and close fstab

To save and close fstab, press [ESC], :w [ENTER], :q [ENTER]

9

Optional fdd mount directory

```
1: mkdir /fdd
2: mkdir /mnt/fdd
3: mkdir /fixed/fdd
```

10

Mount directory for cdrom

Make a mount directory for the cdrom

```
1: mkdir /cdrom
2: mkdir /mnt/cdrom
3: mkdir /fixed/cdrom
```

11

Copy fstab to the encrypted part

Copy fstab to the encrypted partition

```
1: cp /mnt/etc/fstab /fixed/etc
```

12

Disable kbdmux

Prevent problems by disabling "kbdmux", on my compaq my keyboard would only respond 50% of the time.

```
1: echo hint.kbdmux.0.disabled="\1\" >> /mnt/boot/device.hints
```

Kbdmux is responsible for caching FireWire

13

Get password request at bootup

Tell FreeBSD to ask for the password of the encrypted partition at bootup:

```
1: echo geom_eli_load="\YES\" >> /mnt/boot/loader.conf
```

14

All Steps Done?

ALL STEPS DONE!!!?????

15

Shutdown machine

Shutdown the machine

```
1: shutdown -h NOW
```

16

Remove slave hdd

Remove the power from the machine and disconnect the slave drive.

17

Start machine and goto Bios

Power on the machine and make sure the BIOS starts from your harddrive with the encrypted partition on it.

If everything goes right there will be asked for a password for ad0s2, Enter the password that you have provided to ELI and press Enter.

You have 3 changes to enter the correct code, if you fail 3 times you cannot access your encrypted partition anymore. Instead just power off the machine and try again

Attention If you have a PS/2 connection for your keyboard use a PS/2 Keyboard, USB will be initialized when you can login with your user name.

18

Login as Root

When you login as root and you don;t need to enter a password you are on the encrypted hdd.

For FreeBSD systems i always use Rocket Raid cards, these are always recognized by FreeBSD

19

Attach your big array

I mainly use the FreeBSD server for storing files, at this time i have an Array of 8 TB, so i want to attach and encrypt this also.

First step go to the /dev directory to check for devices

```
1: cd /dev
2: ls
```

Look for da0 or ar0

20

Make the big array encrypted

Encrypt your big drive also

```
1: geli init -b -s 4096 -l 256 /dev/da0
```

Enter the passphrase for this array twice.

If all goes well you will be told where you can find the metadata backup.

21

Attach the array

Lets attach this big encrypted array:

```
1: geli attach /dev/da0
```

Enter your Passphrase that you have provided.

If all goes well there will be printed:

```
1: GEOM_ELI: Device da0.eli created
2: GEOM_ELI: Encryption: AES-CBC 256
3: GEOM_ELI: Crypto: software
```

22

Make partitions

Make partitions on the encrypted slice:

```
1: bsdlabel -w /dev/da0.eli  
2: bsdlabel -e /dev/da0.eli
```

23

Change unused behind a:

[x] to delete characters, Press {I} to edit/insert, Change unused behind a: to 4.2BSD, [ESC], :w, :q

24

Format the big array

```
1: newfs /dev/da0.elia
```

A lot of numbers will come by.

My highest number is: 15626930752 ;-)

25

Create Mountpoint

Create a directory so we can mount the big array:

```
1: mkdir /encrypt_a
```

26

Mount big array

Type the following command to mount the big array:

```
1: mount /dev/da0.elia /encrypt_a
```

27

Check the size of your hdd

Once i head a RocketRaid card that would not go higher than 2TB, and i found out after a copy job of 1 week. So be sure to NOT make this mistake, check the harddives:

```
1: df -h
```

You will see the partition size, how much is available and the percentage that is used.

28

Edit fstab again

Now that we are sure all harddisk space is correct, change the fstab file so the array will be mounted on startup.

```
1: vi /etc/fstab
```

Add the following at the bottom of the fstab file:

```
1: /dev/da0.elia /encrypt_a ufs rw 2 2
```

29

Copy fstab to unencrypted

Mount and copy to the unencrypted part of the drive:

```
1: mount /dev/ad0s1a /mnt
2: cp /etc/fstab /mnt/etc
```

30

Reboot the machine

At startup you will be asked for the passphrase twice, one for ad0s2 and one for the da0

```
1: shutdown -r NOW
```

31

login as root

Enter the passphrases and login as root, further in this manual we will not login as root. I know this is not best practise.

Activate the Network

32

Check name of network device

We got to know the name of the network device, so we look at the file: messages

```
1: vi /var/log/messages
```

Look for Ethernet addres (You can search with /keyword), note the name, mine is: vr0

33

Activate network card

To activate the network card type:

1: sysinstall

34

Configure

Choose *Configure*

35

Networking

Choose *Networking*

36

Interfaces

Choose *Interfaces*

37

Choose vr0

In my case i choose vr0

38

Ipv6? No, DHCP [No].

Ipv6? No, DHCP [No].

39

Enter Network configuration

I use the following credentials:

Host: BSD0x

Ipv4 Gateway: 10.30.0.100

Nameserver: 10.30.0.100

Ipv4 Adress: 10.30.0.x

40

Bring xl0 interface up right now?

Bring xl0 interface up right now? [Yes]

41

Leave sysinstall

Press [X], [ENTER], Press [X], [ENTER], [X]

42

Restart system

1: Shutdown -r NOW

Creating Users and Groups

43

Add user

To add a user type:

1: adduser

Enter all fields, and use the default settings.

This is my list:

```
1: david:*:1001:
2: mariska:*:1002:
3: mysql:*:1003:rsync
4: ftp:*:1004:david
5: richard:*:1005:
6: speciaal:*:1006:david
7: locatedb:*:1007:
8: install:*:1008:rsync,locatedb,makelist
9: rsync:*:1009:
10: fotos:*:1010:david,mariska,rsync,locatedb,bezoeker,MCX1,tessa,makelist
11: readwww:*:1011:david,mariska,rsync,locatedb,MCX1,makelist
12: sound:*:1012:david,locatedb,rsync,makelist
13: emulator:*:1013:david,locatedb,rsync,makelist
14: bezoeker:*:1014:
15: copycopy:*:1015:
16: MCX1:*:1016:
17: tessa:*:1017:
18: bewoner:*:1018:david,mariska,rsync,locatedb,MCX1,makelist
19: makelist:*:1020:
20: copycop:*:1021:
21: rootmail:*:1022:
```

44

Add groups

When all users have been made, add the groups:

1: pw groupadd bewoner

Edit user groups

To edit the user groups use:

```
1: vi /etc/group
```

It will look like this:

```
bewoner:*:1018:david,mariska,rsync,locatedb,MCX1,makelist
```

After 1018: you can enter the user names that must have access to that group.

`/etc/group` Dump:

```
1: # $FreeBSD: src/etc/group,v 1.35.10.1.4.1 2010/06/14 02:09:06 kensmith
  Exp $
  #
  wheel:*:0:root,roland
  daemon:*:1:
  kmem:*:2:
  sys:*:3:
  tty:*:4:
  operator:*:5:root
  mail:*:6:
  bin:*:7:
  news:*:8:
  man:*:9:
  games:*:13:
  ftp:*:14:
  staff:*:20:
  sshd:*:22:
  smmsp:*:25:
  mailnull:*:26:
  guest:*:31:
  bind:*:53:
  proxy:*:62:
  authpf:*:63:
  _pflogd:*:64:
  _dhcp:*:65:
  uucp:*:66:
  dialer:*:68:
  network:*:69:
  audit:*:77:
  www:*:80:
  nogroup:*:65533:
  nobody:*:65534:
  roland:*:1001:
  mariska:*:1002:
  tessa:*:1003:
  makelist:*:1004:
  install:*:1005:
  bezoeker:*:1006:
  rootmail:*:1007:
  copycopy:*:1008:
  rsync:*:1009:
  messagebus:*:556:
  polkit:*:562:
  haldaemon:*:560:
```

```
vboxusers:*:920:
erotiek:*:1010:roland,mariska,locatedb,MCX1,rsync,makelist
fotos:*:1011:roland,mariska,locatedb,MCX1,rsync,makelist,tessa
movies:*:1012:roland,mariska,locatedb,MCX1,rsync,makelist,tessa
sound:*:1013:roland,locatedb,MCX1,rsync,makelist
emulator:*:1014:roland,locatedb,rsync,makelist
MCX1:*:1015:
Appz:*:1016:roland,mariska,locatedb,rsync,makelist
bewoner:*:1017:roland,mariska,locatedb,MCX1,rsync,makelist
ons:*:1018:roland,mariska,locatedb,rsync,makelist
locatedb:*:1019:
images:*:1020:roland,locatedb,rsync,makelist
copycop:*:1021:
```

Activate SSH

46

Activate SSH

Goto Sysinstall:
1: sysinstall

47

Configure, Networking, sshd

Configure, Networking, sshd, [OK], Exit, [Exit Install]

48

Check for ssh parameter

Edit rc.conf
1: vi /etc/rc.conf

Search for **sshd_enable="YES"**

If it is not present add it yourself.

49

Reboot to make fingerprint

Reboot so FreeBSD make the fingerprint for SSH
1: shutdown -r NOW

After this reboot i usually login with ssh, don't forget to add a username to the Wheel group.
FreeBSD does not accept external root acces.

Start sysinstall for the ports collection

50.

Type:

```
1: sysinstall
```

Choose Configure -> Distributions and place an "X" in front of Ports and select ok.

Install X Windows

Now we can reach the server with a windows machine we will install X-Windows. To get Virtualbox up and running we will install this in an early stage.

95

Start the installation of Xwindows

```
1: cd /usr/ports/x11/xorg
2: make install clean
```

Options for libxslt

```
EXTRA_ENCODINGS = on
```

96

Options for libxslt

Use the standard options:

```
MEM_DEBUG = off
```

```
CRYPTO = on
```

[OK] to go on.

My machine is taking off at this moment. ;-) I will go downstairs and get some juice.

96a

Options for python

```
THREADS = on
```

```
UCS4 = on
```

```
PYMALLOC = on
```

```
IPV6 = on
```

Other options are off

Options for perl

PERL_64BITINT = on

USE_PERL = on

Options for m4

LIBSIGSEGV = off

97

Options for png

I use the default and that is APNG = off.

98

Options for xorg-apps 7.5

Also i use the standard, and that is all options = on.

99

Options for pixman

I don;t need MMX and SSE2 features and i have got AMD, so i leave SIMD = off.

1

Options Xorg-drivers

I have used the standard settings here.

2

Options for xorg-server

All Options on.

3

Options for HAL

Standard FIXED_MOUNTPOINTS = off and leave it that way.

4

Options for docbook-xsl

All options are on by default, that's a good thing.

5

Options for Glib

COLLATION_FIX = off

Docbook-xsl

All options on

Glib

COLLATION_FIX = off

6

GAM_POLLER

GAM_POLLER = off

7

Options for cairo

GLITZ = off

XCB = on

8

Options for xf86-video-radeonhd

UTILS = off

9

Finish installation of Xorg

Add two lines to /etc/rc.conf

```
1: vi /etc/rc.conf
```

Add the following lines at the bottom

```
1: hald_enable="YES"  
2: dbus_enable="YES"
```

10

Restart machine

```
1: shutdown -r NOW
```

11

Start X Windows

I don't need flashy graphics, so i don't configure. If i do i only get a black screen. Something to find out in the future, i just want to have a virtual machine.

```
1: startx
```

When the following error appears: “error in locking authority file /root/.Xauthority” you need to delete .Xauth* files from the /root directory.

Install all sources

With sysinstall

12

Install Virtualbox

```
1: cd /usr/ports/emulators/virtualbox-ose-kmod
```

```
1: make install clean
```

Options virtualbox-ose-kmod

DEBUG = off

Install Second part Virtualbox

```
1: cd /usr/ports/emulators/virtualbox-ose
```

```
1: make install clean
```

13

Choose options for virtualbox-ose

QT4 = on

DBUS = on

X11 = on

VNC = on

NLS = on

Let the waiting begin!

14

Options for phonon

PULSAUDIO = off

15

Options for SQLite

FTS3 = on

METADATA = on

THREADSAFE = on

all other options are off.

16

Options for tcl

Only TCL_MODULES = on

17

Options for sdl

AALIB = on

NAS = on

OPENGL = on

OSS = on

VGL = on

XLIB = on

All other options are off.

18

Options for curl

CARES = on

OPENSSL = on

PROXY = on

All other options are off

19

Options for ca_root

ETCSYMLINK = off

Add vbox driver to /boot/loader.conf

Add the vbox driver to the unencrypted drive, first we mount the unencrypted drive.

```
1: Mount /dev/ad6s1a /mnt
```

Go to the unencrypted drive that you have mounted:

```
1: cd /mnt
```

Edit /mnt/boot/loader.conf

```
1: Vi /mnt/boot/loader.conf
```

Add the following line:

```
1: Vboxdrv_load="YES"
```

Copy Vbox Drivers to unencrypted part

To let FreeBSD load the vbox driver in loader.conf, we need to copy it to the unencrypted part

```
1: Cp vbox*.* /mnt/boot/modules
```

Add vbox to /etc/rc.conf

Edit /etc/rc.conf

```
1: Vi /etc/rc.conf
```

And add the following at the bottom:

```
1: Vboxnet_enable="YES"
```

Restart machine and Test Virtualbox

I could not seem to lose the error: “vboxnetflt.ko depends on netgraph”, my solution is not to mount the boot partition on the encrypted part, so fstab looks like this now:

#	Device	Mountpoint	Fstype	Options	Dump
	Pass#				
1:	/dev/ad0s2.elib	none	swap	sw	0 0
2:	0				
3:	/dev/ad0s1a	/	ufs	rw	1 1
4:	1				
5:	/dev/ad0s2.elie	/tmp	ufs	rw	2 2
6:	2				
7:	/dev/ad0s2.elif	/usr	ufs	rw	2 2
8:	2				
9:	/dev/ad0s2.elid	/var	ufs	rw	2 2
	2				
	/dev/acd0	/cdrom	cd9660	ro,noauto	0 0
	/dev/da0.elia	/encrypt_a	ufs	rw	2 2

Install Rsync (Synchronise data between systems)

50

Install rsyncd

To install rsyncd insert the FreeBSD cd/DVD in your drive.

Type:

```
1: sysinstall
```

51

Configure

Choose Configure -> Packages -> CD/DVD

52

Net

Choose Net -> rsync-x.x.x_x, place an X in front of it en choose [OK] and then [Install], [OK]

53

Leave Sysinstall

Leave sysinstall

54

Configuring Rsync

Edit the file to edit the RsyncDEAMON

```
1: vi /usr/local/etc/rsyncd.conf
```

Make it look like this

```
1: # rsyncd.conf - Example file, see rsyncd.conf(5)
2: #
3:
4: # Set this if you want to stop rsync daemon with rc.d scripts
5: pid file = /var/run/rsyncd.pid
6:
7: # Edit this file before running rsync daemon!!
8:
9: uid = rsync
10: gid = rsync
11: use chroot = no
12: max connections = 4
13: syslog facility = local5
14: pid file = /var/run/rsyncd.pid
15: #auth users =david, speciaal, copycop, copycopy
16: #secrets file = /usr/local/etc/rsyncd.secrets
17:
18: [test]
19:     path = /encrypt_a/tmp
20:     comment = Test to sync the samba tmp directory
21:
22: [encrypt_a]
23:     path = /encrypt_a
24:
25: [encrypt_a]
26:     path = /encrypt_a
27:     comment = Shared Directory Tree
28:     auth users = copycop
29:     hosts allow = 10.30.0.2
30:     secrets file = /usr/local/etc/rsyncd.secrets
31:
32: #[ftp]
33: #     path = /var/ftp/pub
34: #     comment = whole ftp area (approx 6.1 GB)
35:
36: #[sambaftp]
37: #     path = /var/ftp/pub/samba
38: #     comment = Samba ftp area (approx 300 MB)
39:
40: #[rsyncftp]
41: #     path = /var/ftp/pub/rsync
42: #     comment = rsync ftp area (approx 6 MB)
43:
44: #[sambawww]
45: #     path = /public_html/samba
46: #     comment = Samba WWW pages (approx 240 MB)
47:
48: #[cvs]
49: #     path = /data/cvs
50: #     comment = CVS repository (requires authentication)
51: #     auth users = tridge, susan
52: #     secrets file = /usr/local/etc/rsyncd.secrets
```

56

change the rights

Change the rights of the configuration file:

```
1: chmod 0640 /usr/local/etc/rsyncd.conf
```

57

Make a new password file

Make a password file for rsyncd:

```
1: vi /usr/local/etc/rsyncd.secrets
```

Enter username:password

```
1: tridge:mypass
```

```
2: susan:herpass
```

58

Edit the rights for secrets file

Also make this file not readable to the outside world:

```
1: chmod 0640 /usr/local/etc/rsyncd.secrets
```

When an error appears "Auth failed at module...." Then the rights for the configuration file and/or secrets file are wrong. Or check if you did not make a typo in the configuration file to the secrets file

59

Enter this in rc.conf if there is data

When you have data on your disc, you can add the following line to /etc/rc.conf:

```
1: rsyncd_enable="YES"
```

60

NTP

Sync your time with NTP

Since FreeBSD it is not needed to install NTP anymore, just open the file /etc/rc.conf.

```
1: vi /etc/rc.conf
```

```
2: ntp_enable="YES"
```

```
3: ntpd_enable="YES"
```

It takes about 17 minutes before windows clients can sync time with the FreeBSD NTP Daemon.

61

Make file /etc/ntp.conf

Make the file: /etc/ntp.conf

```
1: vi /etc/ntp.conf
```

62

Fill ntp file

File the NTP configuration file with:

```
1: # This is the configuration file for NTP
2: #   (Network Time Protocol).  More info at
3: #   www.NTP.org
4:
5: # This computer will act as a stratum 2 time
6: #   server, by referencing the following 4 or
7: #   more stratum 1 time servers:
8:
9: server nl.pool.ntp.org          iburst      # Netherlands
10: server be.pool.ntp.org         iburst      # Belgium
11: server de.pool.ntp.org         iburst      # Germany
12: server fr.pool.ntp.org         iburst      # France
13: server es.pool.ntp.org         iburst      # Spain
14:
15:
16: # Since the clock on most PCs drifts around
17: #   significantly, let's use a file to
18: #   keep track of that drift and compensate
19: #   for it:
20:
21: driftfile /etc/ntp.drift
22:
23: # Let's setup a log file for NTP:
24:
25: logfile /var/log/ntp.log
```

For alternate time servers visit: <http://www.pool.ntp.org/en/>

Other NTP usage

I did not get the windows machine's synchronize with the server and the NTP driftfile was empty. So I tried the port way.

First disable the default ntp with /etc/rc.conf

```
1: # -- sysinstall generated deltas -- # Fri Sep 24 19:01:22 2010
2: #rpcbind_enable="YES"
3: #nfs_server_enable="YES"
4: #ntpdate_enable="YES"
```

Goto the NTP port

```
1: cd /usr/ports/net/ntp/  
2: make install
```

Other NTP usage

Select the following modules

NTPSNMPD and ENABLE SSL

Select [OK]

Copy the NTP configuration file

Just to be save I copied the ntp configuration file.

```
1: cd /etc  
2: cp ntp.conf ntp_conf.bak
```

Edit ntp.conf

```
1: Vi /etc/ntp.conf
```

This is my /etc/ntp.conf file.

```
1: # This is the configuration file for NTP  
2: # (Network Time Protocol). More info at  
3: # www.NTP.org  
4:  
5: # This computer will act as a stratum 2 time  
6: # server, by referencing the following 4 or  
7: # more stratum 1 time servers:  
8:  
9: server nl.pool.ntp.org          iburst      # Netherlands  
10: server be.pool.ntp.org         iburst      # Belgium  
11: server de.pool.ntp.org         iburst      # Germany  
12: server fr.pool.ntp.org         iburst      # France  
13: server es.pool.ntp.org         iburst      # Spain  
14:  
15:  
16: # Since the clock on most PCs drifts around  
17: # significantly, let's use a file to  
18: # keep track of that drift and compensate  
19: # for it:  
20:  
21: driftfile /etc/ntp.drift  
22:  
23: # This server will broadcast NTP timing signals  
24: # over the Local Area Network (LAN)  
25:  
26: broadcast 10.30.0.255  
27:  
28:  
29: # Let's setup a log file for NTP:  
30:  
31: logfile /var/log/ntp.log  
32:
```

Add the following lines to /etc/rc.conf

First we make a backup of the rc.conf file.

```
1: cd /etc
2: cp rc.conf rc_conf.bak
```

Then we open rc.conf file

```
1: Vi /etc/rc.conf
```

We add the following lines at the bottom :

```
1: # Make sure that we don't use 'ntpdate'.  It is obsolete.
2: ntpdate_enable="NO"
3:
4: # NTP (Network Time Protocol) time-keeping program
5: # to set time on boot-up and adjust time while
6: # operating.
7: xntpd_enable="YES"
8:
9: # The NTP program is located here:
10: xntpd_program="/usr/local/bin/ntpd"
11:
12: # We want to run the NTP program with some options (flags).
13: #
14: # This is what they mean:
15: #
16: #     -A                = Disable authentication mode
17: #
18: #     -c /etc/ntp.conf  = The configuration file's location
19: #
20: #     -g                = Grab the correct time at startup
21: #
22: #     -N                = Notable Priority.  The OS should
23: #                        give ntpd highest permitted
24: #                        priority when scheduling tasks
25: #
26: #     -p /var/run/ntpd.pid = The Process ID will be found here
27: #
28: #     -l /var/log/ntpd.log = This where we will Log activities
29: #
30: #     Here's the command line:
31: #
32: xntpd_flags="-A -g -N -c /etc/ntp.conf -p /var/run/ntpd.pid -l
33: /var/log/ntpd.log"
```

Note: xntpd_flags are all on one line, so! Make sure it is all on one line!

Edit welcome Message

Change the welcome message

Yes i like to know where i log in with my machine, so we change the welcome message.

Open the motd

```
1: vi /etc/motd
```

64

Empty the original message

Press **dd** real quick to delete a line.

I add the following:

```
1: FreeBSD 8.1-RELEASE (BSD03) - 2010 /Node:3 (Original file:/etc/motd.bak)
2:
3: Running:
4: - Apache2, Php 5, Mysql 5
5: - Pure-FTPd, SSH
6: - Samba 3
7: - NFS
8:
9: IP: 10.30.0.4 / Gateway: 10.30.0.100
10:
11: - FreeBSD Handbook: http://www.FreeBSD.org
12: - Use sysinstall to install additional Packages
```

Save it and it's done!

Install NFS to copy data

65

Install NFS

To copy data the fastest way i use NFS, this is for FreeBSD the most efficient way.

66

Start system installer

```
1: sysinstall
```

67

NFS Steps

Choose [Configure] -> [Networking], put an X in front of NFS client & NFS server.and select [OK].

68

Warning to configure

There follows a warning that you have to configure: /etc/exports to allow hosts.

69

NFS Config file opened

The configuration file will be opened, add the following line at the bottom:

```
1: /encrypt_a -maproot=copycop 10.30.0.3
```

70

Exit the installer

Exit the installer.

71

Check the exports

```
1: vi /etc/exports
```

72

Check if NFS is startup at startup

Type:

```
1: vi /etc/rc.conf
```

There should be two lines with NFS in it.

```
1: nfs_server_enable="YES"  
2: rpcbind_enable="YES"
```

73

Restart the machine

74

Try to mount NFS share

Try to mount the NFS share from another (FreeBSD) machine.

```
1: mount 10.30.0.3:/encrypt_a /mnt
```

75

Copy files

To copy file use the following command:

```
1: cd /mnt
2: cp -Rpv * /encrypt_a
```

Remark The parameters: `-Rpv` will copy the owner and the date.

76

Absolutely sure

Want to be absolutely sure that all data is copied? Copy it twice with the command:

```
1: cp -Rpv * /encrypt_a
```

Remark The option "n" will prevent overwriting files that already exist.

77

Safety first

When everything is copied, i advice you to place a hashtag "#" infront of the share in the file `/etc/exports`

Install Samba

Install Samba so your window machine's can read the shares of FreeBSD.

I do not have much experience with samba 4, and there is not enough documentation about it, so this time i will choose samba3.

Set the kernel.maxfiles parameter higher

With windows 7 Screensaver in Media Center and Windows moviemaker I suggest to use a higher value for this, type:

```
1: sysctl kern.maxfiles=30000
```

80

Start samba installation

I assume that you have your network cable plugged in and have internet.

Type:

```
1: cd /usr/ports/net/samba34
```

```
1: make install clean
```

81

Choose the following options

LDAP
CUPS
WINBIND
SWAT
SYSLOG
POPT

Choose [OK]

82

(optional) pkg_delete tdb-1.2.0

I had a warning when i try to install Samba 34, i had to execute the command:

```
1: pkg_delete tdb-1.2.0
```

To delete a conflicting package.

83

Start the installation

```
1: make install clean
```

Wait for FreeBSD to finish.

84

Additional modules

There will be asked if you would like to install LIBSIGSEGV, i did not place an X.

85

GNUTLS

There will be asked to install a cups client, there is already an X and just leave it that way.
CUPS is for print services.

86

openldap-client

You will be asked to install openldap-client, standard SASL is off and FETCH is on, leave it that way.

87

Samba Install Finished

You will get a notification that Samba is installed.

This port has installed the following startup scripts which may cause these network services to be started at boot time.

/usr/local/etc/rc.d/samba

88

Edit the samba configuration file

```
1: vi /usr/local/etc/smb.conf
```

89

Fill in the following parameters

After workgroup: Your workgroup name, I use Wayward

After Server string: The description of your server, I use BSD04 Samba Server

Add the string: time server = yes

After host allow: Add the ip addresses that have acces, I use: 10.30.0. 127. (So machine's with 10.30.0.x have acces and the localhost has acces)

To make shares you have to add the following lines:

```
1: # This one is useful for people to share files
2: [tmp]
3:   comment = Temporary file space
4:   path = /encrypt_a/tmp
5:   writeable = no
6:   public = yes
```

Every user gets his own drive:

```
1: # Private-drives
2: #
3: [private]
4:   comment = Eigen Prive directory op de Server
5:   path = /encrypt_a/Private/%U
6:   public = no
7:   writeable = yes
8:   browseable = no
```

On the Appz drive force the right directory rights:

```
1: [appz]
2:   comment = Programma's, Games en dergelijke.
3:   path = /encrypt_a/Appz
4:   public = no
5:   writeable = yes
6:   browseable = no
```

```
7: force create mode = 0775
8: force directory mode = 0775
```

With the drive we share, i only want acces level user and group:

```
1: [ons]
2: comment = Gezamenlijke schijf
3: path = /encrypt_a/Ons
4: public = no
5: writeable = yes
6: browseable = no
7: force create mode = 0770
8: force directory mode = 0770
```

90

Start Samba at startup

Type:

```
1: vi /etc/rc.conf
```

and add the following lines:

```
1: nmbd_enable="YES"
2: smbd_enable="YES"
```

90

Restart machine

```
Shutdown -r NOW
```

91

Configure the user that may acces samba

```
1: smbpasswd -a username
```

You will be asked to enter the password for this user twice.

92

To only change the password drop -a parameter

Drop de **-a** parameter to change the password of that user.

I always use the same usernames that i made in FreeBSD, so the usernames will be attached to the files the user save in the shares.

An Error with Samba

This was kinda new to me, an error while accessing the drives from a windows machine. The error: *getpeername failed. Error was Socket is not connected*

A fast searched, and you just need to put the following line in /usr/local/etc/smb.conf:

```
1: smb ports = 139
```

Cups errors

Also a need error about Cups, i changed these lines in my smb.conf:

```
1: load printers = no
2: printing = bsd
3: printcap name = /dev/null
```

To make everything clear, here is a full dump of my smb.conf:

```
1:  # This is the main Samba configuration file. You should read the
2:  # smb.conf(5) manual page in order to understand the options listed
3:  # here. Samba has a huge number of configurable options (perhaps too
4:  # many!) most of which are not shown in this example
5:  #
6:  # For a step to step guide on installing, configuring and using samba,
7:  # read the Samba-HOWTO-Collection. This may be obtained from:
8:  # http://www.samba.org/samba/docs/Samba-HOWTO-Collection.pdf
9:  #
10: # Many working examples of smb.conf files can be found in the
11: # Samba-Guide which is generated daily and can be downloaded from:
12: # http://www.samba.org/samba/docs/Samba-Guide.pdf
13: #
14: # Any line which starts with a ; (semi-colon) or a # (hash)
15: # is a comment and is ignored. In this example we will use a #
16: # for commentry and a ; for parts of the config file that you
17: # may wish to enable
18: #
19: # NOTE: Whenever you modify this file you should run the command
20: "testparm"
21: # to check that you have not made any basic syntactic errors.
22: #
23: #===== Global Settings
24: =====
25: [global]
26:
27: # workgroup = NT-Domain-Name or Workgroup-Name, eg: MIDEARTH
28:     workgroup = Wayward
29:
30: # server string is the equivalent of the NT Description field
31:     server string = BSD03 Samba Server
32:
33: ## Samba Time Server?
34: #
35:     time server =yes
```

```

36:
37: ## getpeername failed. Error was socket is not connected, solution:
38: #
39: smb ports = 139
40:
41: # Security mode. Defines in which mode Samba will operate. Possible
42: # values are share, user, server, domain and ads. Most people will want
43: # user level security. See the Samba-HOWTO-Collection for details.
44:     security = user
45:
46: # This option is important for security. It allows you to restrict
47: # connections to machines which are on your local network. The
48: # following example restricts access to two C class networks and
49: # the "loopback" interface. For more examples of the syntax see
50: # the smb.conf man page
51:     hosts allow = 10.30.0. 127.
52:
53: # If you want to automatically load your printer list rather
54: # than setting them up individually then you'll need this
55:     load printers = no
56:
57: # you may wish to override the location of the printcap file
58:     printcap name = /dev/null
59:
60: # on SystemV system setting printcap name to lpstat should allow
61: # you to automatically obtain a printer list from the SystemV spool
62: # system
63: ;     printcap name = lpstat
64:
65: # It should not be necessary to specify the print system type unless
66: # it is non-standard. Currently supported print systems include:
67: # bsd, cups, sysv, plp, lprng, aix, hpux, qnx
68:     printing = bsd
69:
70: # Uncomment this if you want a guest account, you must add this to
71: /etc/passwd
72: # otherwise the user "nobody" is used
73: ;     guest account = pcguest
74:
75: # this tells Samba to use a separate log file for each machine
76: # that connects
77:     log file = /var/log/samba34/log.%m
78:
79: # Put a capping on the size of the log files (in Kb).
80:     max log size = 50
81:
82: # Use password server option only with security = server
83: # The argument list may include:
84: #     password server = My_PDC_Name [My_BDC_Name] [My_Next_BDC_Name]
85: # or to auto-locate the domain controller/s
86: #     password server = *
87: ;     password server = <NT-Server-Name>
88:
89: # Use the realm option only with security = ads
90: # Specifies the Active Directory realm the host is part of
91: ;     realm = MY_REALM
92:
93: # Backend to store user information in. New installations should
94: # use either tdbsam or ldapsam. smbpasswd is available for backwards
95: # compatibility. tdbsam requires no further configuration.
96: ;     passdb backend = tdbsam

```

```

97:
98: # Using the following line enables you to customise your configuration
99: # on a per machine basis. The %m gets replaced with the netbios name
100: # of the machine that is connecting.
101: # Note: Consider carefully the location in the configuration file of
102: #      this line. The included file is read at that point.
103: ;   include = /usr/local/etc/smb.conf.%m
104:
105: # Most people will find that this option gives better performance.
106: # See the chapter 'Samba performance issues' in the Samba HOWTO
107: # Collection
108: # and the manual pages for details.
109: # You may want to add the following on a Linux system:
110: ;   socket options = SO_RCVBUF=8192 SO_SNDBUF=8192
111:
112: # Configure Samba to use multiple interfaces
113: # If you have multiple network interfaces then you must list them
114: # here. See the man page for details.
115: ;   interfaces = 192.168.12.2/24 192.168.13.2/24
116:
117: # Browser Control Options:
118: # set local master to no if you don't want Samba to become a master
119: # browser on your network. Otherwise the normal election rules apply
120: ;   local master = no
121:
122: # OS Level determines the precedence of this server in master browser
123: # elections. The default value should be reasonable
124: ;   os level = 33
125:
126: # Domain Master specifies Samba to be the Domain Master Browser. This
127: # allows Samba to collate browse lists between subnets. Don't use this
128: # if you already have a Windows NT domain controller doing this job
129: ;   domain master = yes
130:
131: # Preferred Master causes Samba to force a local browser election on
132: # startup
133: # and gives it a slightly higher chance of winning the election
134: ;   preferred master = yes
135:
136: # Enable this if you want Samba to be a domain logon server for
137: # Windows95 workstations.
138: ;   domain logons = yes
139:
140: # if you enable domain logons then you may want a per-machine or
141: # per user logon script
142: # run a specific logon batch file per workstation (machine)
143: ;   logon script = %m.bat
144: # run a specific logon batch file per username
145: ;   logon script = %U.bat
146:
147: # Where to store roving profiles (only for Win95 and WinNT)
148: #      %L substitutes for this servers netbios name, %U is username
149: #      You must uncomment the [Profiles] share below
150: ;   logon path = \\%L\Profiles\%U
151:
152: # Windows Internet Name Serving Support Section:
153: # WINS Support - Tells the NMBD component of Samba to enable it's WINS
154: # Server
155: ;   wins support = yes
156:
157: # WINS Server - Tells the NMBD components of Samba to be a WINS Client

```

```

158: # Note: Samba can be either a WINS Server, or a WINS Client, but NOT
159: both
160: ; wins server = w.x.y.z
161:
162: # WINS Proxy - Tells Samba to answer name resolution queries on
163: # behalf of a non WINS capable client, for this to work there must be
164: # at least one WINS Server on the network. The default is NO.
165: ; wins proxy = yes
166:
167: # DNS Proxy - tells Samba whether or not to try to resolve NetBIOS
168: names
169: # via DNS nslookups. The default is NO.
170: dns proxy = no
171:
172: # Charset settings
173: ; display charset = koi8-r
174: ; unix charset = koi8-r
175: ; dos charset = cp866
176:
177: # Use extended attributes to store file modes
178: ; store dos attributes = yes
179: ; map hidden = no
180: ; map system = no
181: ; map archive = no
182:
183: # Use inherited ACLs for directories
184: ; nt acl support = yes
185: ; inherit acls = yes
186: ; map acl inherit = yes
187:
188: # These scripts are used on a domain controller or stand-alone
189: # machine to add or delete corresponding unix accounts
190: ; add user script = /usr/sbin/useradd %u
191: ; add group script = /usr/sbin/groupadd %g
192: ; add machine script = /usr/sbin/adduser -n -g machines -c Machine
193: -d /dev/null -s /bin/false %u
194: ; delete user script = /usr/sbin/userdel %u
195: ; delete user from group script = /usr/sbin/deluser %u %g
196: ; delete group script = /usr/sbin/groupdel %g
197:
198:
199: #===== Share Definitions
200: =====
201: [homes]
202: comment = Home Directories
203: browseable = no
204: writable = yes
205:
206: # Un-comment the following and create the netlogon directory for Domain
207: Logons
208: ; [netlogon]
209: ; comment = Network Logon Service
210: ; path = /usr/local/samba/lib/netlogon
211: ; guest ok = yes
212: ; writable = no
213: ; share modes = no
214:
215:
216: # Un-comment the following to provide a specific roving profile share
217: # the default is to use the user's home directory
218: ;[Profiles]

```

```

219: ;    path = /usr/local/samba/profiles
220: ;    browseable = no
221: ;    guest ok = yes
222:
223:
224: # NOTE: If you have a BSD-style print system there is no need to
225: # specifically define each individual printer
226: [printers]
227:     comment = All Printers
228:     path = /var/spool/samba34
229:     browseable = no
230: # Set public = yes to allow user 'guest account' to print
231:     guest ok = no
232:     writable = no
233:     printable = yes
234:
235: # This one is useful for people to share files
236: ;[tmp]
237: ;    comment = Temporary file space
238: ;    path = /tmp
239: ;    read only = no
240: ;    public = yes
241:
242: # A publicly accessible directory, but read only, except for people in
243: # the "staff" group
244: ;[public]
245: ;    comment = Public Stuff
246: ;    path = /home/samba
247: ;    public = yes
248: ;    writable = yes
249: ;    printable = no
250: ;    write list = @staff
251:
252: # Other examples.
253: #
254: # A private printer, usable only by fred. Spool data will be placed in
255: fred's
256: # home directory. Note that fred must have write access to the spool
257: directory,
258: # wherever it is.
259: ;[fredsprn]
260: ;    comment = Fred's Printer
261: ;    valid users = fred
262: ;    path = /homes/fred
263: ;    printer = fred_s_printer
264: ;    public = no
265: ;    writable = no
266: ;    printable = yes
267:
268: # A private directory, usable only by fred. Note that fred requires
269: write
270: # access to the directory.
271: ;[fredsdir]
272: ;    comment = Fred's Service
273: ;    path = /usr/somewhere/private
274: ;    valid users = fred
275: ;    public = no
276: ;    writable = yes
277: ;    printable = no
278:
279: # a service which has a different directory for each machine that

```

```

280: connects
281: # this allows you to tailor configurations to incoming machines. You
282: could
283: # also use the %U option to tailor it by user name.
284: # The %m gets replaced with the machine name that is connecting.
285: ;[pchome]
286: ; comment = PC Directories
287: ; path = /usr/pc/%m
288: ; public = no
289: ; writable = yes
290:
291: # A publicly accessible directory, read/write to all users. Note that
292: all files
293: # created in the directory by users will be owned by the default user,
294: so
295: # any user with access can delete any other user's files. Obviously
296: this
297: # directory must be writable by the default user. Another user could of
298: course
299: # be specified, in which case all files would be owned by that user
300: instead.
301: ;[public]
302: ; path = /usr/somewhere/else/public
303: ; public = yes
304: ; only guest = yes
305: ; writable = yes
306: ; printable = no
307:
308: # The following two entries demonstrate how to share a directory so
309: that two
310: # users can place files there that will be owned by the specific users.
311: In this
312: # setup, the directory should be writable by both users and should have
313: the
314: # sticky bit set on it to prevent abuse. Obviously this could be
315: extended to
316: # as many users as required.
317: ;[myshare]
318: ; comment = Mary's and Fred's stuff
319: ; path = /usr/somewhere/shared
320: ; valid users = mary fred
321: ; public = no
322: ; writable = yes
323: ; printable = no
324: ; create mask = 0765
325:
326: #----- My Shares -----
327: #####
328: # All drives on the backup server are read only
329: #
330:
331: # This one is useful for people to share files
332: [tmp]
333: comment = Temporary file space
334: path = /encrypt_a/tmp
335: writeable = no
336: public = yes
337:
338: # Log share
339: #
340: [log]

```

```
341:    comment = Log files of BSD03
342:    path = /var/log
343:    public = yes
344:    writeable = no
345:    browseable = no
346:
347: # Private-drives
348: #
349: [private]
350:    comment = Eigen Prive directory op de Server
351:    path = /encrypt_a/Private/%U
352:    public = no
353:    writeable = yes
354:    browseable = no
355:
356: # Appz Drive
357: #
358: [appz]
359:    comment = Programma's, Games en dergelijke.
360:    path = /encrypt_a/Appz
361:    public = no
362:    writeable = yes
363:    browseable = no
364:    force create mode = 0775
365:    force directory mode = 0775
366:
367: # Special Drive
368: #
369: [special]
370:    comment = Special Drives for: Ftp, Images, Sound, Apache
371:    path = /encrypt_a/Special
372:    public = no
373:    writeable = yes
374:    browseable = no
375:    force create mode = 0775
376:    force directory mode = 0775
377:
378: # Media
379: #
380: [media]
381:    comment = Media Audio, Video, Multimedia
382:    path = /encrypt_a/Media
383:    public = no
384:    writeable = yes
385:    browseable = no
386:    force create mode = 0775
387:    force directory mode = 0775
388:
389: # Ons
390: #
391: [ons]
392:    comment = Gezamenlijke schijf
393:    path = /encrypt_a/Ons
394:    public = no
395:    writeable = yes
396:    browseable = no
397:    force create mode = 0770
398:    force directory mode = 0770
399:
400: # Startup With batch files for connecting to BSD03
401: #
```

```

[startup]
    comment = Batch files to connect to the BSD03 FreeBSD Server
    path = /encrypt_a/Startup
    public = yes
    writeable = no
    browseable = yes

# Share to dump all the Ghost images from dos
[image]
    comment = Drive to dump all the Ghost image's to
    path = /encrypt_a/Images
    public = no
402:    writeable = yes
403:    browseable = yes
404:    force create mode = 0775
405:    force directory mode = 0775
406:
407: # Shares for the Media Center
408: #
409: [video]
410:    comment = Video Files for the media center
411:    path = /encrypt_a/Media/movies
412:    writeable = yes
413:    browseable = yes
414:    force create mode = 0775
415:    force directory mode = 0775
416:
417: [TV]
418:    comment = Alle the tv programs we like to keep
419:    path = /encrypt_a/Media/TV
420:    writeable = yes
421:    browsable = yes
422:    force create mode = 0775
423:    force directory mode = 0775
424:
425: [pictures]
426:    comment = All our pictures
    path = /encrypt_a/Media/pictures
    writeable = yes
    browseable = yes
    force create mode = 0775
    force directory mode = 0775

[audio]
    comment = All our avaible audio
    path = /encrypt_a/Media/audio
    writeable = yes
    browseable = yes
    force create mode = 0775
    force directory mode = 0775

```

Pure FTPd installeren (Php5, MySQL4.1, Apache22)

95

Install Mysql 4.1

The first step will be to install MySql 4.1 (PureFTPd cannot handle MySQL5).

```
1: cd /usr/ports/databases/mysql41-server
```

```
1: make install clean
```

96

Add 2 lines to rc.conf

```
1: vi /etc/rc.conf
```

```
1: mysql_enable="YES"  
2: mysqllimits_enable="NO"
```

Wijzig de locatie van de mysql Database naar de RAID harddisks.

```
vi /usr/local/etc/rc.d/mysql-server
```

Vul achter mysql_dbdir /encrypt_a/db/mysql in.

```
: ${mysql_dbdir="/encrypt_a/db/mysql"} .
```

97

Make the temp directory writable

```
1: chmod 0777 /tmp
```

98

Restart machine

Install PureFTPd

```
1: cd /usr/ports/ftp/pure-ftp
2: make - config
```

1

Select the following options

```
MYSQL
PRIVSEP
PERUSERLIMITS
THROTTLING
BANNER
```

2

Start the installation of PureFTPd

```
1: make install clean
```

3

Add PureFTPd to startup

Add PureFTPd to /etc/rc.conf to run it at startup.

```
1: /etc/rc.conf
```

```
1: # Pure-FTPd
2: pureftpd_enable="YES"
```

4

Download install script

```
1: fetch http://machiел.generaal.net/files/pureftpd/v2.x/script.mysql
```

Source: <http://machiел.generaal.net/index.php?subject=pureftpd>

5

Create mysql tables

```
1: mysql -u root -psecret < script.mysql
```

6

Go to the directory with the example file

Go to the directory where an example file of pure-ftpd is.

```
1: cd /usr/local/etc
```

7

Copy the example to use

```
1: cp pure-ftpd.conf.sample pure-ftpd.conf
```

Do not allow anonymous

Edit the configuration file of pure ftpd.

```
1: Vi /usr/local/etc/pure-ftpd.conf
```

Search the following line : NoAnonymous and set it to yes.

```
1: NoAnonymous          yes
```

8

Get the file for Mysql Needs

```
1: fetch http://machi1.generaal.net/files/pureftpd/v2.x/pureftpd-mysql.conf
```

9

Edit the Pureftp conf file

```
1: vi pureftpd.conf
```

10

Edit the following line

Search the following line and edit it

```
1: # MySQL configuration file (see README.MySQL)
2: MySQLConfigFile /usr/local/etc/pureftpd-mysql.conf
```


Add ftp account

```
1: adduser
```

Username: ftp and fill in the rest of the questions.

12

Start Pureftpd

```
1: /usr/local/etc/rc.d/pure-ftpd start
```

You can always stop Pureftp with: /usr/local/etc/rc.d/pure-ftpd stop

13

Install Apache

```
1: cd /usr/ports/www/apache22  
2: make install clean
```

Choose the standard options

14

Start apache at startup

```
1: vi /etc/rc.conf
```

Add the following lines at the bottom:

```
1: # Apache 2  
2: apache22_enable="YES"
```

Install Php5

```
1: cd /usr/ports/lang/php5
```

16

Choose php options

```
1: make config
```

Select [APACHE], and then [OK]

```
1: make install clean
```

Edit the configuration

```
1: vi /usr/local/etc/apache22/httpd.conf
```

Add the following two lines:

```
1: AddType application/x-httpd-php .php
2: AddType application/x-httpd-php-source .phps
```

18

Search Directory Index

Search for /DirectoryIndex

And replace it with:

```
1: DirectoryIndex index.htm index.php index.html
```

Save the configuration file.

Install php5 extensions

```
1: cd /usr/ports/lang/php5-extensions
2: make config
```

Select: MySQL, Posix, Session, and type:

```
1: make install clean
```

20

Select UTF-8 Support

Select UTF-8 Support and then [OK].

Make a symbolic link from root

Go to the root:

```
1: Cd /
```

Make the symbolic link to the Array drive

```
1: Ln -s /encrypt_a/Special/FTP /ftp
```

1. Ga naar de directory waar de webpagina staat.
`cd /usr/local/www/apache22`
2. Verwijder de directory zodat we hem kunnen vervangen voor een symbolic link:
`rm -R data`

Opmerking: de optie -R zorgt ervoor dat de directory word weggehaalt, ook als deze niet leeg is.

3. Maak een symbolische link aan naar de juiste locatie
`ln -s /encrypt_a/Special/www/html data`

Opmerking: Een symbolische link is beter dan het configuratie bestand aanpassen, op deze manier weet je 100% zeker dat alle verwijzingen kloppen.

4. Verwijder ook de cgi directory
`rm -R cgi-bin`

Maak vervolgens ook een symbolische link aan voor de cgi-bin directory.

```
ln -s /encrypt_a/Special/www/cgi-bin cgi-bin
```

Mail server installeren (Dovecot)

5. We gaan Dovecot gebruiken als onze IMAP mail server om al die mailboxen met informatie over de server uit te lezen. Ga naar de juiste directory:

```
cd /usr/ports/mail/dovecot
```

6. Installeer het pakket:
`make install clean`

7. Zodra het pakket niet gevonden kan worden, ga je naar de directory:
`cd /usr/ports/distfiles`

8. **(Optioneel)** En download je het bestand als volgt:
`fetch http://www.dovecot.org/releases/1.0/rc/dovecot-1.0.rc7.tar.gz`

Ga weer terug naar de dovecot directory en start de procedure opnieuw.

9. Ga naar de juiste directory:
`cd /usr/local/etc`

10. Open het bestand:
`vi /usr/local/etc/dovecot.conf`

11. Zorg dat de volgende regels op de volgende wijze in het configuratie bestand staan:
`protocols = imap pop3 imaps pop3s`
`disable_plaintext_auth = no`

12. Voeg het volgende toe aan het /etc/rc.conf bestand:
`dovecot_enable="YES"`

Start dovecot door het volgende commando:

```
/usr/local/etc/rc.d/dovecot start
```

Als er: *Starting dovecot* staat is het gelukt.

Forward root emails to account rootmail

Zorg ervoor dat het account rootmail bestaat en maak deze anders aan.

Wijzig het bestand: /etc/aliases en ga op zoek naar:

```
# Well-known aliases -- these should be filled in!
```

En voeg het volgende onder deze lijn toe:

```
root: rootmail  
manager: rootmail  
dumper: rootmail
```

Sla dit bestand op en start: `newaliases`

Installing FetchMail to collect mail from several email addresses

```
# cd /usr/ports/mail/fetchmail/  
# make install clean
```

Add the following line to:

/etc/rc.conf

```
fetchmail_enable="YES"
```

Put all your email accounts into: /usr/local/etc/fetchmailrc, like this:

Install Cacti for statistics:

Install net-snmp

```
# cd /usr/ports/net-mgmt/net-snmp; make install clean
```

Add a line to /etc/rc.conf

```
snmpd_enable="YES"
```

Edit snmpd.conf

```
cd /usr/local/share/snmp
cp snmpd.conf.example snmpd.conf
vi snmpd.conf
```

And edit the things you want to change.

Cacti is a powerful network graphing utility that front ends Rrdtool. This process will compile Rrdtool and all of its dependencies for you.

```
# cd /usr/ports/net-mgmt/cacti; make install clean
```

Go to the public_html directory: /encrypt_a/Special/www/html and make a symbolic link to cacti:

```
Ln -s /usr/local/share/cacti/ cacti
```

At this to /etc/contrab:

```
* /5 * * * * cacti /usr/local/bin/php /usr/local/share/cacti/poller.php > /dev/null 2>&1
```

Setup The Database

```
#mysqladmin --user=root create cacti
```

Set the passwd for the cacti user.

```
# passwd cacti
```

Changing local password for cacti

New Password: [cactipasswd]

Retype New Password: [cactipasswd]

Edit the /usr/local/share/cacti/include/config.php file for the proper database permissions:

```
$database_type = "mysql";
$database_default = "cacti";
$database_hostname = "localhost";
$database_username = "cacti";
$database_password = "cactipasswd";
$database_port = "3306";
```

Set the Cacti database's permissions.

```
#echo "GRANT ALL ON cacti.* TO cacti@localhost IDENTIFIED BY 'cactipasswd'; FLUSH PRIVILEGES;" | mysql
```

Import the default tables.

```
#mysql cacti < /usr/local/share/cacti/cacti.sql
```

Use the php.ini file.

```
Cd /usr/local/etc  
cp php.ini-production php.ini
```

Edit the file and set the correct timezone :

```
Vi php.ini
```

```
Search for: /dat.timezone
```

And enter behind it: "Europe/Berlin"

Restart the machine

Go to the ip address of your machine and follow the instructions of cacti.

For the first time there will be asked for username and password, this will be:

```
Admin  
admin
```

Then you will be forced to change the cacti password, I have used the same one as I entered with the installation routine.