# FreeBSD Administration - Support #769

## Install FreeBSD With a GELI Encrypted ZFS Root The Hard Way

03/04/2016 04:13 PM - Daniel Curtis

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | 03/04/2016 |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | Daniel Curtis | **% Done:** | 100% |
| **Category:** | Installation | **Estimated time:** | 2.50 hours |
| **Target version:** | FreeBSD 10 | **Spent time:** | 6.00 hours |

**Description**

This is a guide on how I manually setup FreeBSD with a GELI encrypted hard drive underneath of a ZFS root on a GPT formatted hard drive, without the help of a GUI or bsdinstall. This guide is intended to install FreeBSD using the installation DVD and will work offline.

- When the FreeBSD Installer Welcome message appears, choose **Shell**.
- Get a list of available drives:

```
camcontrol devlist
```

- Create the boot partition and install bootcode:

```
gpart create -s gpt ada0
gpart add -l gptboot0 -s 512k -t freebsd-boot -a 4k ada0
gpart bootcode -b /boot/pmbr -p /boot/gptzfsboot -i 1 ada0
gpart set -a bootme -i 1 ada0
```

- Create the ZFS **bootpool**:

```
gpart add -l boot0 -t freebsd-zfs da1
mkdir -p /tmp/mnt/bootpool
zpool create -m none -o altroot=/tmp/mnt/bootpool bootpool /dev/gpt/boot0
mkdir -p /tmp/mnt/bootpool/boot/zfs
mount_nullfs /tmp/mnt/bootpool/boot/zfs /boot/zfs
```

- Create the **swap** and **disk0** slices:

```
gpart create -s gpt ada0
gpart add -s 4G -t freebsd-swap -a 4k -l swap0 ada0
gpart add -t freebsd-zfs -a 4k -l disk0 ada0
```

- Encrypt the swap space:

```
geli onetime -d -e AES-XTS -l 256 -s 4096 /dev/ada0p3
```

- Encrypt the OS slice:

```
mkdir /tmp/mnt/bootpool/boot/metadata_backup
geli init -b -s 4096 -e AES-XTS -l 256 -B /tmp/mnt/bootpool/boot/metadata_backup/ada0p4.eli /dev/ada0p4
```

- Attach the encrypted slice:

```
geli attach /dev/ada0p4
```

- Create the **xpool** ZFS pool on top of the GELI encrypted slice, then export it:

```
mkdir -p /tmp/mnt/xpool
zpool create -o altroot=/tmp/mnt/xpool -o cachefile=/tmp/zpool.cache -m none -f xpool /dev/ada0p4.eli
zpool export xpool
```

- Next import the **xpool** ZFS pool and create the root dataset and settings:

```
zpool import -o altroot=/tmp/mnt/xpool -o cachefile=/tmp/zpool.cache xpool
zpool set bootfs=xpool xpool
zfs set checksum=fletcher4 xpool
zfs set atime=off xpool
zfs create xpool/ROOT
zfs set mountpoint=/ xpool/ROOT
```

  - Then create some additional system datasets:

    ```
    zfs create -o canmount=off xpool/ROOT/usr
    zfs create -o canmount=off xpool/ROOT/var
    zfs create -o compression=on   -o exec=on  -o setuid=off xpool/ROOT/tmp
    zfs create -o compression=gzip -o setuid=off  xpool/ROOT/usr/ports
    zfs create -o compression=off  -o exec=off -o setuid=off xpool/ROOT/usr/ports/distfiles
    zfs create -o compression=off  -o exec=off -o setuid=off xpool/ROOT/usr/ports/packages
    zfs create -o compression=gzip -o exec=off -o setuid=off  xpool/ROOT/usr/src
    zfs create -o compression=lzjb xpool/ROOT/usr/obj
    zfs create -o compression=lzjb -o exec=off -o setuid=off xpool/ROOT/var/crash
    zfs create -o compression=off  -o exec=off -o setuid=off xpool/ROOT/var/empty
    zfs create -o compression=lzjb -o exec=on  -o setuid=off xpool/ROOT/var/tmp
    ```

- Set the permissions of the temp directories in the zfs mount:

```
chmod 1777 /tmp/mnt/xpool/tmp
chmod 1777 /tmp/mnt/xpool/var/tmp
```

- Remount the **bootpool**:

```
umount /boot/zfs
mkdir /tmp/mnt/xpool/bootpool
zfs set mountpoint=/tmp/mnt/xpool/bootpool bootpool
zpool export bootpool
zpool import bootpool
mkdir -p /tmp/mnt/xpool/bootpool/boot/zfs
mount_nullfs /tmp/mnt/xpool/bootpool/boot/zfs /boot/zfs
```

- Extract the base.txz and kernel.txz to the zfs root to install the base system:

```
cat /usr/freebsd-dist/base.txz | tar --unlink -xpJf - -C /tmp/mnt/xpool
cat /usr/freebsd-dist/kernel.txz | tar --unlink -xpJf - -C /tmp/mnt/xpool
```

# Post-Installation Setup

- Chroot into the xpool:

  ```
  chroot /tmp/mnt/xpool
  ```

- Copy the install bootload files over to the bootpool, then create a /boot symlink:

  ```
  cd /
  rm -r boot/zfs
  mv boot/* bootpool/boot/
  rm -r boot
  ln -sf bootpool/boot
  ```

- Set a root passwd:

  ```
  passwd root
  ```

- Add a new user:

  ```
  adduser
  ```

- Set timezone:

  ```
  tzsetup
  ```

- Create an fstab file:

  ```
  vi /etc/fstab
  ```

  - And add the swap partition definition:

    ```
    /dev/ada0p3        none    swap    sw    0   0
    ```

- Add the initial system configuration:

  ```
  echo 'zfs_enable="YES"' >> /etc/rc.conf
  echo 'sshd_enable="YES"' >> /etc/rc.conf
  ```

- And setup networking using DHCP:

  ```
  echo 'ifconfig_em0="DHCP"' >> /etc/rc.conf
  echo 'hostname="freebsd.example.com"' >> /etc/rc.conf
  ```

  - (Optional) Setup networking using a static IP address instead:

    ```
    echo 'ifconfig_em0="inet 192.168.10.70 netmask 255.255.255.0 broadcast 198.100.10.255"' >> /etc/rc.conf
    ```

```
echo 'defaultrouter="192.168.10.1"' >> /etc/rc.conf
echo 'hostname="freebsd.example.com"' >> /etc/rc.conf
echo 'nameserver 192.168.10.1' >> /etc/resolv.conf
```

- Add the bootloader config:

```
echo 'geom_eli_load="YES"' >> /boot/loader.conf
echo 'zfs_load="YES"' >> /boot/loader.conf
echo 'if_em_load="YES"' >> /boot/loader.conf
echo 'vfs.root.mountfrom="zfs:xpool/ROOT"' >> /boot/loader.conf
echo 'zpool_cache_load="YES"' >> /boot/loader.conf
echo 'zpool_cache_type="/boot/zfs/zpool.cache"' >> /boot/loader.conf
echo 'zpool_cache_name="/boot/zfs/zpool.cache"' >> /boot/loader.conf
```

- Exit from the chroot environment:

```
exit
```

- Setup the ZFS mountpoints

```
zfs set mountpoint=legacy xpool/ROOT
zfs set mountpoint=/tmp xpool/tmp
zfs set mountpoint=/usr xpool/usr
zfs set mountpoint=/var xpool/var
zfs set mountpoint=/bootpool bootpool
```

- Unmount the filesystems:

```
umount /boot/zfs
zfs unmount -a
zpool export xpool
zpool export bootpool
```

- Reboot the system and eject the FreeBSD install disc:

```
reboot
```

## Resources

- http://www.schmidp.com/2014/01/07/zfs-full-disk-encryption-with-freebsd-10-part-2/
- https://forums.freebsd.org/threads/42773/
- https://wiki.freebsd.org/RootOnZFS/GPTZFSBoot/9.0-RELEASE
- https://calomel.org/zfs_freebsd_root_install.html
- http://daemon-notes.com/articles/system/install-zfs/gpart
- http://daemon-notes.com/articles/system/install-zfs/zfs
- http://daemon-notes.com/articles/system/install-zfs/finish

### History

**#1 - 03/04/2016 05:03 PM - Daniel Curtis**

*- Description updated*

*- Status changed from New to Resolved*

*- % Done changed from 0 to 100*

**#2 - 03/04/2016 06:54 PM - Daniel Curtis**

*- Description updated*

**#3 - 03/07/2016 02:53 PM - Daniel Curtis**

*- Description updated*

**#4 - 04/22/2016 05:05 PM - Daniel Curtis**

*- Status changed from Resolved to Closed*