FreeBSD Planning, Installation and Security Tips

This document acts as a condensed "cheat sheet" to help you to install FreeBSD as a server at your location. If you are new to FreeBSD and/or UNIX you may find this document useful. Even if you are an experienced user you may wish to quickly review the guidelines set forth here to ensure that your installation will be secure and able to grow with future use. As much of this advice comes from experience we are always interested in hearing your comments about how well this works in the real world. You can send information and comments to nsrc@nsrc.org.

Step 1: Plan Your Installation

- **Supported Hardware:** The file, 'HARDWARE.TXT', located at the top level of the FreeBSD CD-ROM, or at the FreeBSD ftp site (ftp://ftp.freebsd.org/), contains a comprehensive list of supported hardware for each version of FreeBSD. Use this file to ensure that the hardware you have available will work with FreeBSD. Most current and "standard" hardware is supported.

- **Hardware Inventory:** Take a detailed inventory of the hardware on the machine on which you plan to install FreeBSD. If you have legacy ISA cards you should note the IRQ, I/O addresses, and possibly DMA addresses in use by the card. If they are not the default addresses, then you will need to specify these during installation. FreeBSD uses manufacturer default IRQ, I/O, and DMA settings during installation unless otherwise specified.

- **Hard Drive Configuration (RAID):** Your toughest decision is likely to be your hard drive configuration. Whether to use RAID, individual drives for certain file systems, how to partition the drives, etc. RAID is nice as it can grow if needed, and your data is protected against individual driver failures. You should read Chapter 12 of the FreeBSD Handbook for a discussion of RAID and methods for backing up your data. If you use the FreeBSD software RAID solution this is actually the Vinum Volume Manager that you can read about at http://www.vinumvm.org/. An excellent HOWTO for implementing Vinum software RAID under FreeBSD can be found at http://www.daemonnews.org/200002/vinum.html. If you are installing a server that will require additional space (i.e. for user's home directories, growing databases, email storage, etc.), then plan your initial installation to make this easier. A good discussion about planning your hard drive configuration can be found at http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/dirstructure.html. Very quickly here a few comments about some of the file system choices you are likely to make:
    - / (root) : This can be quite small. 64MB is often enough. The root file system contains the bootable kernel of FreeBSD.
    - /var : This is where log files go. If you plan on allowing log files to grow large, then leave enough space, otherwise this can be fairly small (100MB). *But*, if you plan on having users on your system with email space, then this partition is the default location for user's email (under /var/mail), and you will need to make this large enough to accommodate user email on your system.
    - /usr : This is where the rest of FreeBSD generally goes. You'll want at least 500MB if not considerably more space set aside for this partition.
    - "/usr/home" : This directory will need to be large enough to accommodate your entire user base, and you should be prepared to grow this in the future. One trick to consider is setting aside a separate disk for your user home directories, and then creating a logical link between that disk and /usr/home. That is, if you have /d1 as a separate disk, then changing directory to /usr/home, will actually place you in /d1.

- **Services to Run or Not:** Decide what services you plan to run. Only install, or activate, these services. Additional services that you do not use only create security risks and potentially reduce the stability of your machine. For instance, if you are not going to creating network file shares, then do not run the nfs daemons and do not run portmap (required by nfs). Both are insecure. In addition, Telnet, FTP, POP, and IMAP are all insecure. See "Step 3: Secure Your Installation" for more information.

- **GUI or Not:**If you don't need to run X Windows, then don't install it and it's associated software. Generally for a server box X Windows is not necessary. You can do whatever work you need to do on your server via shell access through services such as ssh. This is one of the great strengths of FreeBSD (and UNIX in general).

Step 2: Install FreeBSD

- Before you install FreeBSD read, in it's entirety, Chapter 2 of the FreeBSD Handbook. You can read this at http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/. This is pretty much a requirement. If you skip this step it's likely you'll just end up reinstalling FreeBSD.

- Be ready, the two hardest parts of installation are likely to be deciding on your disk layout, and specifying your hardware - particularly if you have older hardware (see above for discussions on both these topics).

- Don't worry if you end up installing FreeBSD several times. This is a great learning process! And, it's typical as you learn how to use the product. If you create original data or difficult to create configurations, just be sure to back these up before reinstalling.

- If you are used to Linux or Windows installations you'll probably want to have a printout of Chapter 2 of the FreeBSD Handbook available the first few times you install.

- Installation starts automatically if you boot from a FreeBSD install CD-ROM. Otherwise see Chapter 2 of the

- After installation you can run /stand/sysinstall to start the installation program again. This is one way to reconfigure systems, but more importantly, this allows you to install additional software once FreeBSD is installed.

- During installation we recommend installing the entire "ports" collection (about 5,000 software titles as of Feb, 2002). This takes up about an additional 100MB, but allows you to pick and choose programs you may need at your leisure. This does not install all these programs, but rather pointers to where they can be found on the Internet, and descriptions of what they do. You can, later, use cvsup to keep this collection current.

Step 3: Secure Your Installation

Security is a *big* topic. It is essential that you plan on following these steps to *secure* your server immediately upon installation. Do not leave it up without first securing it. If you have not had to secure a server before, then spend some time reading up on security before proceeding. First, here are the basic concepts you need to do in order to secure your server:

- Run only the services you plan on using.
- Use only the services that are necessary.
- Use secure passwords.
- Force users on your machine to use secure passwords.
- Restrict root access to a minimal set of services.
- Restrict access to these services via inetd and tcpwrappers.
- Restrict access to your box using IP Firewall services (ipfw).
- Use ssh and sftp instead of telnet and ftp.
- Log events on your machine and understand what logs are being kept.
- Install some type of system change detection software so that you can tell if your server has been compromised.
- Back up your server's data so that if it is compromised you can reinstall from scratch, but still have your data available.
- Finally, physical security is important. The more people who have physical access to the machine, the less secure your server is.

Some services you just should not run. At the top of this list is Telnet. You should access your box using Secure Shell (ssh) as all information passed is encrypted. Telnet passes all information in clear text across the network, and this is very insecure. In addition, other common services with this problem include FTP, POP, and IMAP. If you are just starting out as an ISP this is your chance to work with SSH and SCP clients for your users, as well as encrypted POP and IMAP email clients, or secure Webmail servers using SSL.

You should not allow your root user to access your server via FTP. You can always ftp from your box as root to another box to get files. Or, better yet, use scp (Secure CoPy, part of the standard ssh installation) to copy files to and from other servers.

To get started with implementing the security steps mentioned above you should read and understand the following:

- An introduction to FreeBSD security can be found at:
  http://www.freebsd.org/security/index.html
- You should read Chapter 10 of the FreeBSD Handbook, which deals with Security:
  http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/
- An excellent place to look for a general overview of UNIX security is:
  http://ns.uoregon.edu/security/tools.html
- inetd overview from the FreeBSD Handbook:
  http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/inetd.html#INETD-OVERVIEW
- More detailed inetd discussion from the FreeBSD inetd man (manual) page at:
  http://www.freebsd.org/cgi/man.cgi?query=inetd&sektion=8,
  or just type "man inetd" after you've installed FreeBSD.
- tcpwrapper (host access restrictions) overview at:
  http://www.freebsd.org/cgi/man.cgi?query=hosts_access&sektion=5,
  or just type "man hosts_access" after you've installed FreeBSD.
- IP Firewall or ipfw facility under FreeBSD:
  http://www.freebsd.org/cgi/man.cgi?query=ipfw&apropos=0&sektion=0&manpath=FreeBSD+4.5-R
  ,
  or, just type "man ipfw" after you've installed FreeBSD.
- To learn more about logging of events begin with Chapter 6 of the FreeBSD Handbook.
- Consider using something like Tripwire as a change detection system. You can find Tripwire at:
  http://www.tripwire.org/
  In addition this comes as one of the ports packages under /ports/tripwire.

You'll need to stay on top of security alerts as well in case your services are affected and need to be patched. As a minimum you should register for the FREEBSD-SECURITY-NOTIFICATIONS mailing list. This list is not an email discussion list, but rather just posts security problems and fixes. To subscribe to this list send email to majordomo@FreeBSD.org and in the body of the message place:

subscribe freebsd-security-notifications

Remember to not include a signature as this will be processed as well. There are several other excellent Security email bulletins and resources as well. Two to consider are -

- SANS (System Administration, Networking, and Security) Institute.
  SANS email lists list:
  http://server2.sans.org/sansnews
  Wiew the SANS BSD alerts page:
  http://www.sans.org/newlook/digests/SAC/BSD.htm
- CERT (Computer Emergency Response Team):
  CERT Advisory Mailing List:
  http://www.cert.org/contact_cert/certmaillist.html

If you were to look around on these sites and read some of the available material there you would find a considerable amount of security information, tips, and strategies that you might apply to securing your own server or network.

Finally, remember bad passwords are an easy security target. Current cracking software can cycle through millions of language based combinations of words in a matter of seconds. You should pick passwords that do not contain words of any kind and that include non-alphanumeric tokens, such as $, !, @, &, and mix in upper and lower case letters as well.

Step 4: Administer and Update Your Installation

This is another big topic, and one that you'll learn about as long as you are administering a server. Chapters 6 through 20 of the FreeBSD Handbook come under the "System Administration" heading. If you have to pick two chapters to read first you should go to chapters 6 and 8, or "Configuration and Tuning," and "Users and Basic Account Management" respectively. Chapter 10, "Security," has already been mentioned in the previous section. Naturally some of these chapters may be more relevant to what you are trying to accomplish, so be sure to review all of them.

If your server will have multiple users be sure you read about user administration before you start creating accounts, and consider how you want to implement password restrictions, access restrictions, and possible disk quotas among other things.

In addition, if you are not on your FreeBSD system, or you prefer reading information in your web browser instead, the entire FreeBSD manual pages are available at http://www.freebsd.org/cgi/man.cgi.

Finally, to update your system you can use CVS Update. This allows you to entirely update a server (all packages) at once, or to update individual packages as you see fit. You can read about this in more detail at http://www.freebsd.org/cgi/man.cgi?query=cvs&apropos=0&sektion=0&manpath=FreeBSD+4.5-RELEAS is one way to upgrade your current FreeBSD system to the latest version without needing to re-install the operating system.

Back to Top

| NSRC Home | International Networking Developments Database | Networking Technology and Tools |
| Network Administration | General Computer Networking Info | Networking Tips and FAQs | Workshops |

Search: Match: All Format: Long Search

Network Startup Resource Center

Last Update
May 5, 2002
Created by hervey@nsrc.org