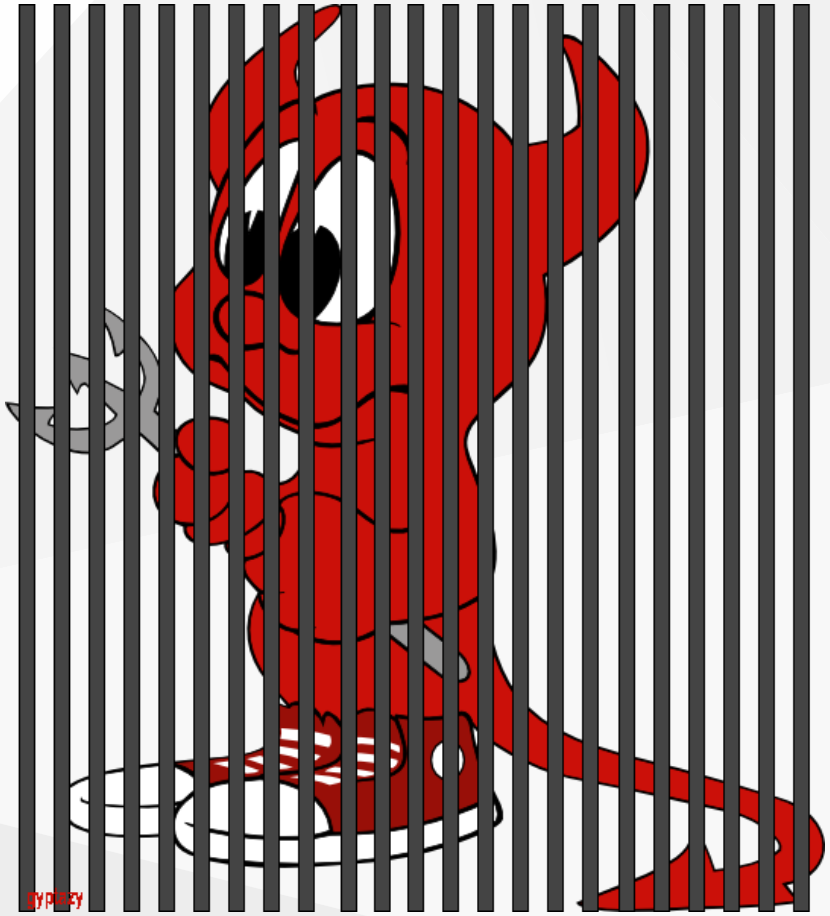
FreeBSD Jails (basics)

What are Jails & why everyone loves them?!



TOC

Introduction

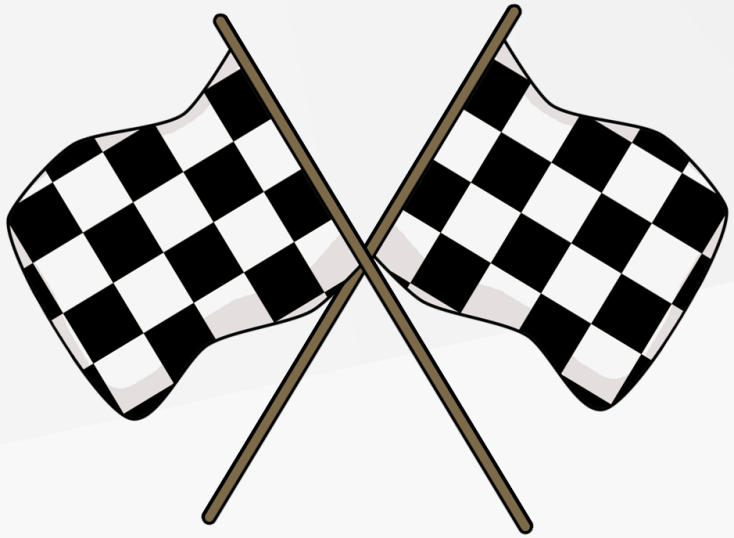
- Introduced in FreeBSD 4 in 1999 by Poul-Henning Kamp
- Implementation of OS-level virtualization
- Providing independent mini FreeBSD subsystems by
  - Sharing the same kernel
  - Different userland
  - Small overhead

What does it provide?

- Initialized by a system call `jail`
- Dedicated environments decapsulated from the main system
- Based on chroot environment
  - But there've been possibilities to break out
- Improved:
  - The behaviour of traditional chroots
  - Extended the support of user/network separation
- Own subset of users (including root user)

Goals

- Virtualization
- Security



Goals: Virtualization

- Internally a Jail looks like a real system
- Providing a fully usable environment:
  - Creating "customer" systems
  - Running processes in encapsulated environments

But...

- No real virtualization
- No different kernels
- No support for clustering

Goals: Security

- Modifying kernel, loading modules, etc. is not possible
- Modifying network configuration is not possible
  - Bound to (a) specific IP(s)
    - Can not access divert or alter routing
    - Raw sockets may additional be enabled
- Interactions between Jails is restricted
- (Un)mounting is not possible
- Accessing file system above their root directory is not possible

Jail Types (1/2)

- Thick Jails
  - Fully copy of base system
  - High isolation
  - Flexibility in different versions of libs, configs and software
- Thin Jails
  - Based on OpenZFS snapshots or NullFS mounts
  - Less resources overhead
  - Faster deployment
  - Easier maintenance

Jail Types (2/2)

- VNET Jails
  - vEnv for isolation & control of network resources
  - Provides high level of network segmentation
- Linux Jails
  - Support for Linux binaries
  - Compatibility layer for certain Linux sys calls

Usage: Creating a (classic) Jail

- Preparing the host
- Networking
- Creating Jail directory tree
- Creating Jail config files
- Creating Jail userland

Usage: Tools

Instead of doing everything by hand - use a manager:

- BastilleBSD (sysutils/bastille)
- AppJail (sysutils/appjail)
- iocage (sysutils/iocage)
- ezjail (sysutils/ezjail)

Resources

Documentations

- FreeBSD: https://docs.freebsd.org/en/books/handbook/jails/

Presentation

- GitHub: https://github.com/gyptazy/tech-talks

Notes

This tech-talk is a single part of multiple ones. Please see also:

- 01: Basics - What is it, why, general functionality
- 02: Deeper insights - How the things work internally
- 03: Setting up a Jail from scratch manually
- 04: Setting up a Jail with tooling & manager (ezjail)
- 05: Custom things of Jails (vnet, pf, Jail audit)

Thanks!

Web: https://gyptazy.ch
Twitter: @gyptazy
Fediverse: gyptazy@bsd.cafe