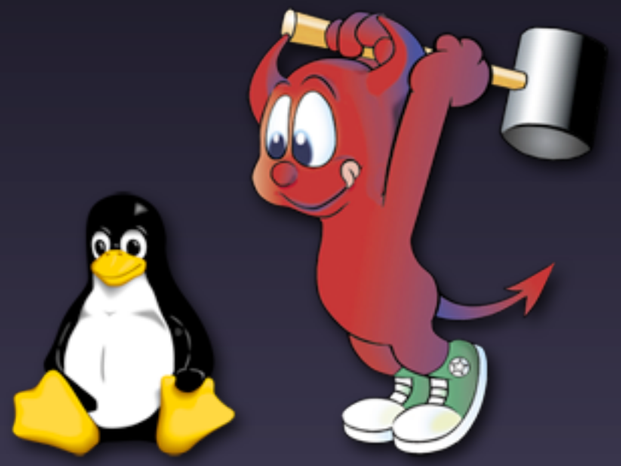
WO on FreeBSD

Miguel Arroz
Global Village Consulting, Inc.
WOWODC 2011


Nigi Nigi Nu Noos 'e' Nu Nu Noo
Seafood
and Oriental
Restaurant
TRY OUR
FRESH DELI
Sandwiche's
MADE WITH
IMPORTED
EUROPEANS
MEAT AND CHEESE

WO on FreeBSD



WOWODC!

FreeBSD overview

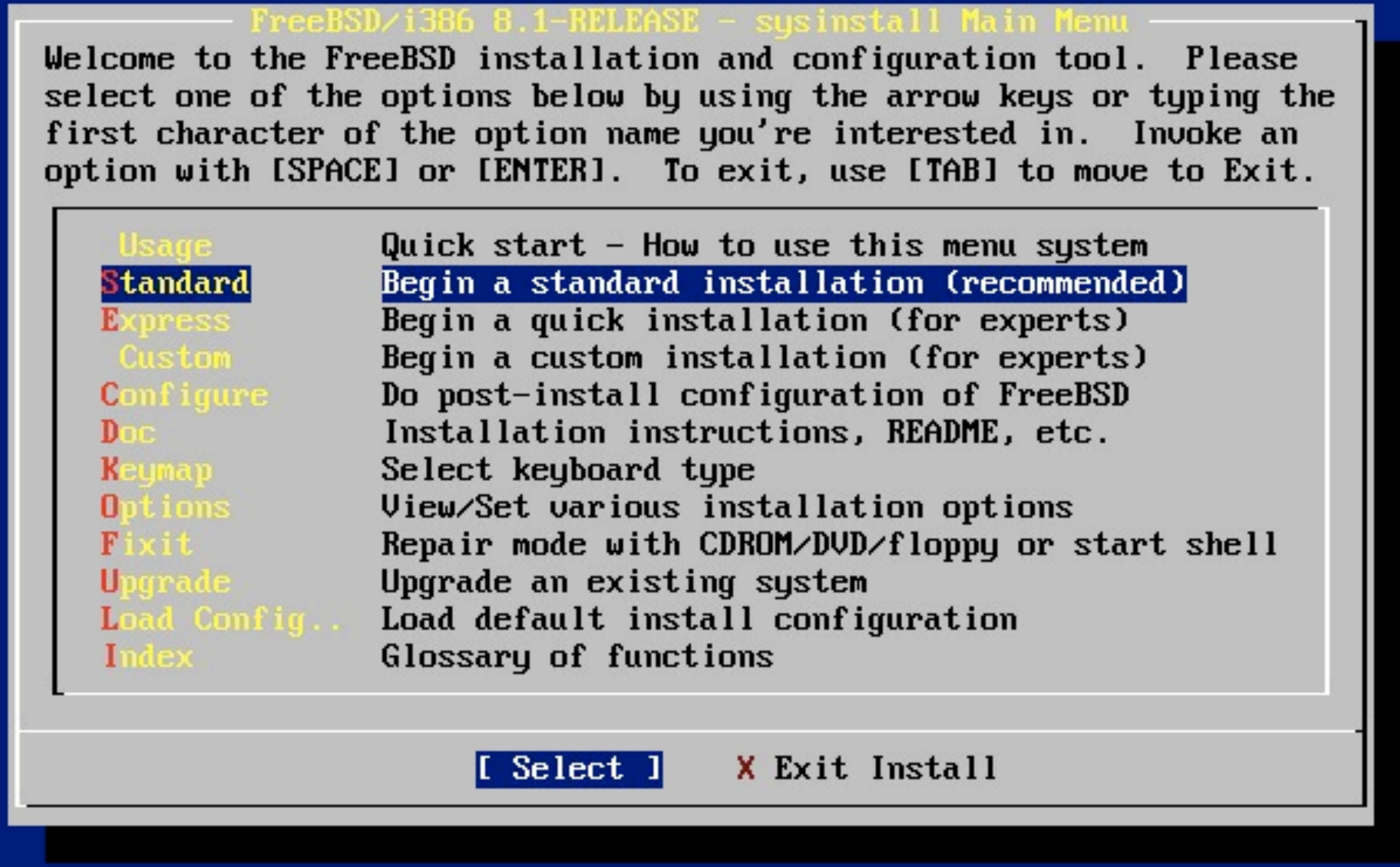
- UNIX System
- BSD License (of course!)
- Supports x86, amd64, pc98 as Tier 1
- Distributed and installed via FTP, HTTP, CD/DVD, etc.

FreeBSD overview

- Integration and consistency
- The same team handles the Kernel and user-land tools
- Release engineering team

Installation

- Pseudo-graphical installation
- Very fast, low footprint
- Installs only the essential, the rest is up to you


FreeBSD/i386 8.1-RELEASE - sysinstall Main Menu
Welcome to the FreeBSD installation and configuration tool. Please select one of the options below by using the arrow keys or typing the first character of the option name you're interested in. Invoke an option with [SPACE] or [ENTER]. To exit, use [TAB] to move to Exit.
Usage Quick start - How to use this menu system
Standard Begin a standard installation (recommended)
Express Begin a quick installation (for experts)
Custom Begin a custom installation (for experts)
Configure Do post-install configuration of FreeBSD
Doc Installation instructions, README, etc.
Keymap Select keyboard type
Options View/Set various installation options
Fixit Repair mode with CDROM/DVD/floppy or start shell
Upgrade Upgrade an existing system
Load Config.. Load default install configuration
Index Glossary of functions
[Select]
X Exit Install

Networking

- Everything you would expect from an UNIX system
- Reference (KAME) IPv6 implementation

Documentation

- FreeBSD Handbook (free, on freebsd.org)
- Mail-lists

WOWODC!

Security

- Most software installs with safe default configuration
- Installing a port prints a message with security information if appropriate
- Easy to configure daily scan for security advisors on OS and installed ports
- http://security.freebsd.org/

Security

```
The following files will be updated as part of
updating to 7.1-RELEASE-p16:
/usr/lib/libssl.a
/usr/lib/libssl.so.5
/usr/lib/libssl_p.a
/usr/src/crypto/openssl/ssl/s3_clnt.c
/usr/src/sys/conf/newvers.sh

WARNING: FreeBSD 7.1-RELEASE-p15 HAS PASSED ITS
END-OF-LIFE DATE.
Any security issues discovered after Tue Feb  1
00:00:00 WET 2011
will not have been corrected.
```

WOWODC!

FreeBSD versions

- Major versions
  - May break binary and source compatibility.
  - Used to introduce new features, deprecate or remove unused stuff.

FreeBSD versions

- Minor versions:
  - Maintain binary and source compatibility (main goal)
  - Bug fixes, mostly
  - New features (usually, small ones) if baked enough

FreeBSD versions

- Security advisors and erratas:
  - Released for all the currently supported versions
  - Very easy to install, specially if you use GENERIC kernel
  - Fix security vulnerabilities and show-stopper bugs
  - Don’t break binary or source compatibility
  - Never introduce new features
  - Kernel and OS source is updated too if installed

Release cycles

- Security advisors and erratas are only made available for currently supported FreeBSD releases
- The life-time of each release depends on a few factors

Branch	Release	Type	Release Date	Estimated EoL
RELENG_7	n/a	n/a	n/a	February 28, 2013
RELENG_7_3	7.3-RELEASE	Extended	March 23, 2010	March 31, 2012
RELENG_7_4	7.4-RELEASE	Extended	February 24, 2011	February 28, 2013
RELENG_8	n/a	n/a	n/a	last release + 2 years
RELENG_8_1	8.1-RELEASE	Extended	July 23, 2010	July 31, 2012
RELENG_8_2	8.2-RELEASE	Normal	February 24, 2011	February 29, 2012

Minor versions

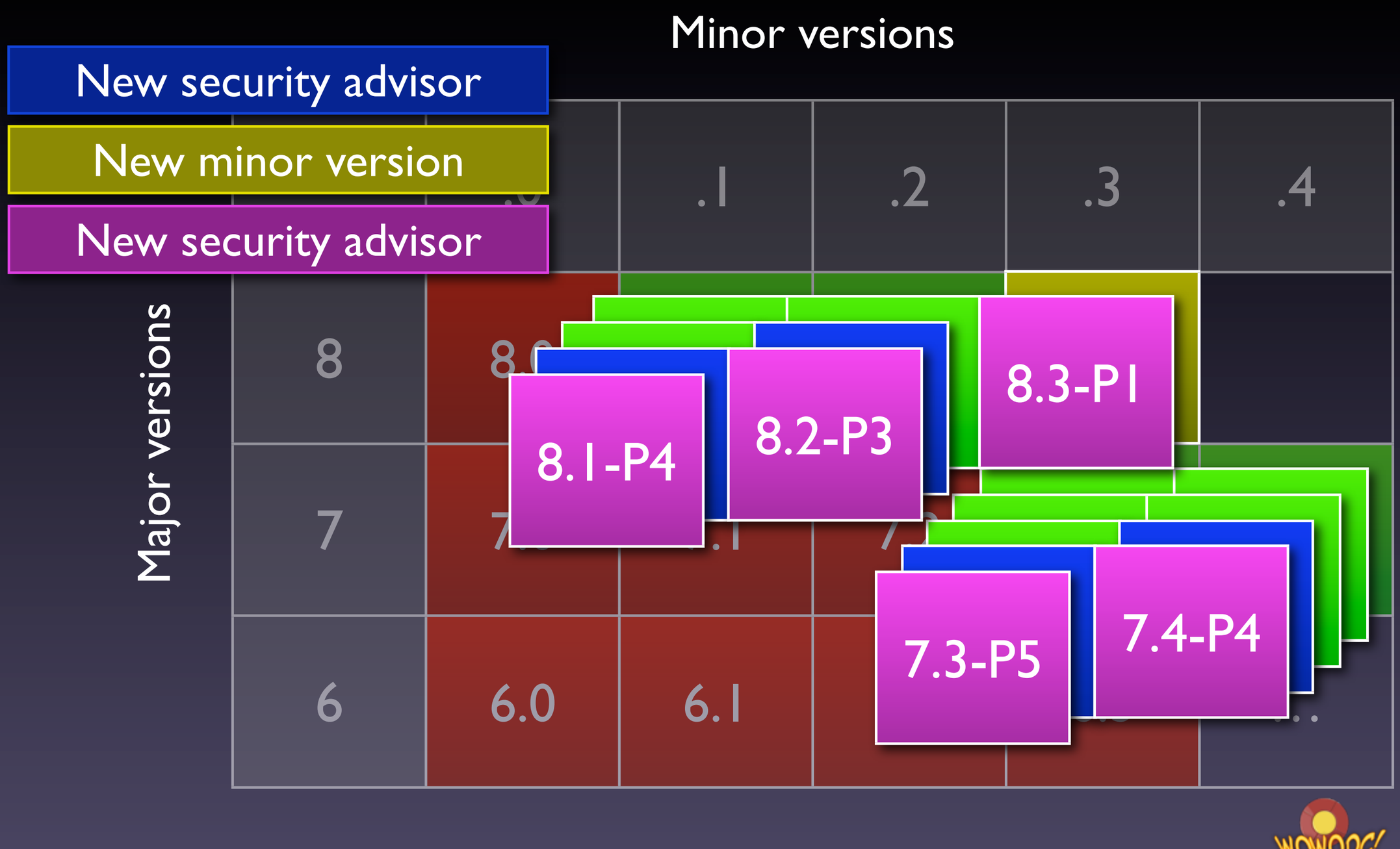
Major versions

	.0	.1	.2	.3	.4
8	8.0	8.1	8.2		
7	7.0	7.1	7.2	7.3	7.4
6	6.0	6.1	6.2	6.3	…

Minor versions

Major versions

	.0	.1	.2	.3	.4
8	8.0	8.1	8.2		
7	7.0	7.1	7.2	7.3	7.4
6	6.0	6.1	6.2	6.3	…


New security advisor
New minor version
New security advisor
Minor versions
Major versions
.1
.2
.3
.4
8
6
6.0
6.1
8.1-P4
8.2-P3
8.3-P1
7.3-P5
7.4-P4

Updating

- If using GENERIC kernel, errata or security advisor is trivial:
  - freebsd-update fetch
  - freebsd-update install
  - reboot
- If stuff happens:
  - freebsd-update rollback

Updating

- Put this on cron to be warned when there's a patch to install:
  - @daily root freebsd-update cron
- Minor and major version updates can be done remotely, but are more complex
  - Check FreeBSD Handbook (24.2 - FreeBSD Update)
  - May need to recompile installed software
  - May need console access

Installing software

- Packages
- Ports
- Traditional UNIX way (configure, make, make install)

Packages

- Binary distributions
- Usually smaller than source archives
- No compilation required
  - Much faster, specially when there are many dependencies
- pkg_add -r <package>

Ports

- Packages are compiled with conservative options (must run on all hardware). Ports can be tuned.
- Ports allow compile-time options configuration.
- Some software licenses force source-only distribution.
- May apply local patches.
- The source is with you.

Port Tree

- The port tree stays in /usr/ports
- Installation using portsnap:
  - portsnap fetch
  - portsnap extract
- Updating:
  - portsnap fetch
  - portsnap update

Installing a Port

- Browser for ports: http://www.freebsd.org/ports/
- Install port (typical):
  - cd /usr/ports/<path to port>
  - make install clean
- make config to see configuration menu

Updating ports

- The easiest way to upgrade a port and it's dependencies is using one of these utilities:
  - portupgrade
  - portmanager
  - portmaster
- See Handbook (4.5.4 - Upgrading Ports)

Port security scan

- Install ports-mgmt/portaudit
- After installing, FreeBSD makes daily security scans on installed ports and notifies you of any released security advisors.

```
Checking for a current audit database:

Database created: Wed Apr 21 03:10:01 WEST 2010

Checking for packages with security vulnerabilities:

Affected package: sudo-1.7.2.5
Type of problem: sudo -- Privilege escalation with sudoedit.
Reference: <http://portaudit.FreeBSD.org/1a9f678d-48ca-11df-85f8-000c29a67389.html>

Affected package: gtar-1.22
Type of problem: gtar -- buffer overflow in rmt client.
Reference: <http://portaudit.FreeBSD.org/c175d72f-3773-11df-8bb8-0211d880e350.html>

2 problem(s) in your installed packages found.

You are advised to update or deinstall the affected package(s) immediately.
```

Jails

- OS-level virtualization system
- More isolation than chroot, less isolation than VM
- Jail has its own kernel structures, binded IPs and superuser
- Can be used to test software or isolate deployed services
- Can’t use a different kernel
- No live-migration

BSD Hypervisor

- http://wiki.freebsd.org/201105DevSummit?action=AttachFile&do=get&target=BHyVe.pdf

Status

- Guest
  - FreeBSD/amd64 releases 7.2 and 8.1
  - SMP - up to 8 virtual cpus
  - I/O - virtio or pci passthru
  - Minor kernel patches required
- Host
  - FreeBSD/amd64 release 8.1
  - Unmodified GENERIC kernel
- Hardware
  - Requires hardware virtualization assist with Nested Page Tables
  - Intel VT-x is supported
  - AMD-V support in progress

Init scripts

- Shares a lot with Mac OS X startup items
- /etc/rc.conf - switches and configurations
- /etc/rc.d/<*servicename*> <*action*>
  - /etc/rc.d/sshd restart
- /usr/local/etc/rc.d/<*servicename*> <*action*>
- Scripts can specify provided and required services

```
hostname="andromeda.example.com"
defaultrouter="XXX.XXX.XXX.XXX"

ifconfig_em0="inet X.X.X.X netmask X.X.X.X"
ifconfig_em0_alias0="inet X.X.X.X netmask 255.255.255.255"

ifconfig_em1="inet X.X.X.X netmask X.X.X.X"
ifconfig_em1_alias0="inet X.X.X.X netmask 255.255.255.0"

static_routes="service multicast"
route_service="-net X.X.X.X/8 X.X.X.X"
route_multicast="-net X.X.X.X X.X.X.X"

sshd_enable="YES"
ntpdate_enable="YES"
ntpdate_flags="time.service.example.com"
syslogd_enable="YES"
syslogd_flags="-ss"
ntpd_enable="NO"
```

WO on FreeBSD

Kernel Tuning

- File /etc/sysctl.conf:

```
# Increase the number of maximum open file descriptors
kern.maxfiles=65535

# Enough space to cache the full java launch command line,
# so that we can see it in "ps" output instead of [java]
kern.ps_arg_cache_limit=1024

# Limits the number of logging lines per logging rule
net.inet.ip.fw.verbose_limit=5
```

Java

- Diablo distribution (Sun JVM)
- Port java/diablo-jdk16
- Installation may include time-zone updaters and JCE Policy files
- All files must be downloaded manually due to licensing
  - The port will guide you

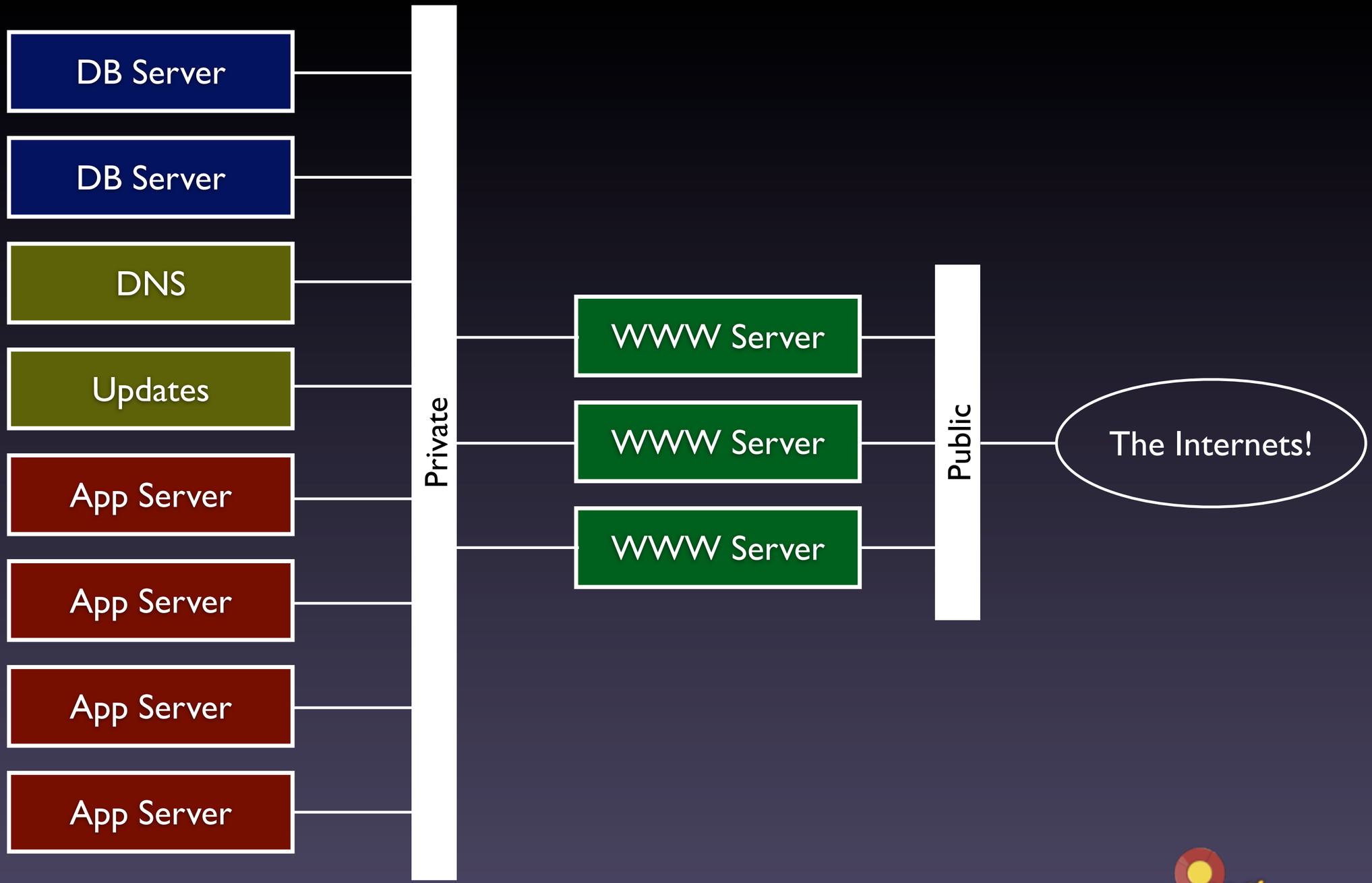
Apache

- Port www/apache22

WebObjects

- Two ways to install the WO frameworks on FreeBSD:
  - Using the WOPort
  - Manually
    - http://wiki.objectstyle.org/confluence/display/WO/Deploying+on+FreeBSD+8.2+and+WebObjects+5.4.3

Dual-network configurations


DB Server
DB Server
DNS
Updates
App Server
App Server
App Server
App Server
Private
WWW Server
WWW Server
WWW Server
Public
The Internets!

Why?

- Security
  - Data between wotaskd and other components
  - Data (RR) between adaptors and apps
  - Broadcasted and other custom data between apps
  - Hide database and other services from the public network
- Save public IPs

Why?

- Ideally, you should only expose ports 80 and 443

Network configuration

- em0 with private IP
- em1 with public IP
- Add as much services as you can to private network

Software configuration

- On file /usr/local/etc/rc.d/wotaskd:
  - command_args="${log_args} -WOHost 10.1.2.3"
- On JavaMonitor:
  - Add hosts using their private IPs
  - Add -WOHost argument with private IP to apps

WOHostUtilities

- WO Apps need to make sure requests for stats, shutdown, refuse new sessions, etc, are legit
- Those requests must *not* came from web server, and their source must be localhost.
- Problem is… private IPs are not considered localhost IPs by Java.

WOHostUtilities

- Use Wonder, set er.extensions.WOHostUtilities.localhostips

```
er.extensions.WOHostUtilities.localhostips=(10.1.2.1,10.1.2.2,10.1.2.3)
```

SoftLayer

- Dual network configuration by default
- VPN access to the private network
- Free IPv6 for every server
- Amazing support staff

One small detail…

- FreeBSD + Adaptec 5405 RAID card = pain
  - Must use firmware 17574 or newer.
  - SoftLayer use this cards, request updated firmware or older card.

Q&A