Role Based Package Management for FreeBSD

Rubber stamp package deployment
Introduction
About Your Presenter

Previously

▪ Senior Network Architect with Mintel International Ltd.
  • Responsible for maintaining ~200 physical FreeBSD systems and 400+ Jails spread across 7 sites
  • Providing tools for the system administration team to perform their day to day duties.

Currently

▪ Research Engineer with the Vulnerability Research Team at Sourcefire Inc.
  • Working on Razorback
    http://razorbacktm.sourceforge.net/
A Quick Survey

Please raise your hand if..

- You manage more than 5 FreeBSD boxes
- You have some form of automated deployment system
  - You have binary deployment system
- You use some form of configuration management tool
  - CfEngine (2 or 3)
  - Puppet
  - Chef
  - Home Grown Tool or other
System Overview
System Goals

- Build a package
- Install on multiple systems
- Have none standard options

- Save you time
- Deployment
- Updates
- Maintenance

- Centralized Management
The Tools

- A database server
- MarcusCom Tinderbox
  (http://tinderbox.marcuscom.com/)
- An automation tool
  - CfEngine
  - Puppet
  - Cron
- A Web Server
- Some scripts (pmanager)
System Architecture
Key Concepts – The Fundamentals

Ports Tree
• A snapshot of a FreeBSD tree

Build
• Target FreeBSD Release
• Target System Architecture
• Target Ports Tree

Package
• A binary package of a single port build in a Build definition

Server
• A full FreeBSD instance or Jail
The ‘Role’ concept - What is a role?

- A group of services required to perform a function.
  - E.g. Web Server, Database Server
- A group of packages required for a service
  - Apache, PHP with PCRE and MySQL modules
  - MySQL, p5-DBD-MySQL
- A group of hosts to run the service
System Setup
System Requirements

- A build host
  - 4GB Ram
  - Dual Core CPU
  - Fast Disk Subsystem (500Gb + space)

- Per site mirrors
  - Package Mirrors
  - Database Mirrors

- A day or 2 for system setup
The Build Host

- **OS**
  - Highest Supported Target Release

- **Packages**
  - databases/mysql51-server
  - databases/mysql51-scripts
  - devel/p5-Config-General
  - devel/p5-Getopt-Long
  - textproc/p5-Text-ASCIITable
  - ports-mgmt/tinderbox
    - Follow the installation instructions but don’t create anything
  - devel/subversion
Getting the Code

Check out from SVN:

```
svn co http://svn.tomjudge.com/freebsd/tinderbox /usr/local/pmanager
```

A port for this will be coming soon™
Setting up the database

Log into MySQL:

```
cd /usr/local/pmanager
mysql -u root -p
```

Setup the DB:

```
CREATE DATABASE package_management;
USE package_management;

./db.sql

GRANT ALL ON package_management.* TO pmanager@localhost IDENTIFIED BY 'pmanager';
GRANT ALL ON tinderbox.* TO pmanager@localhost IDENTIFIED BY 'pmanager';
```
Create the build environment

In tinderbox:

```bash
cd /usr/local/tinderbox/scripts
./tc createJail -j 8.2-RELEASE -t 8.2-RELEASE -u LFTP -H ftp.freebsd.org
./tc createJail -j 7.4-RELEASE -t 7.4-RELEASE -u LFTP -H ftp.freebsd.org
```
Create a ports tree

In tinderbox:

cd /usr/local/tinderbox/scripts
./tc createPortsTree -p production -u CSUP -d "Production Ports Tree"

In pmanager:

cd /usr/local/pmanager
./pmanager addPortsTree --name=production \
   --path=/usr/local/tinderbox/portstrees/production/ports
./pmanager updatePortsTree --name=production
Create the builds

In tinderbox:

```
cd /usr/local/tinderbox/scripts
./tc createBuild -b 8.2-Production -j 8.2-RELEASE -p production-ports \
    -d "8.4 Production Build"
./tc createBuild -b 7.4-Production -j 7.4-RELEASE -p production-ports \
    -d "7.4 Production Build"
```

In pmanager:

```
cd /usr/local/pmanager
./pmanager addBuild --name=8.2-Production --ports-tree=production
./pmanager addBuild --name=7.4-Production --ports-tree=production
```
Using none standard options

Setup the directory structure:

```
   cd /usr/local/tinderbox
   mkdir -p options/\{8.2,7.4\}-Production/php5
```

Add an options file:

```
   echo "WITH_APACHE="\"YES\"" > options/7.4-Production/php5/options
   echo "WITH_APACHE="\"YES\"" > options/8.2-Production/php5/options
```

Enable options:

```
   cd /usr/local/tinderbox/scripts
   ./tc
```
Day to Day Operations
Example Roles

● Web Server
  ▶ Apache
  ▶ PHP 5.3
  ▶ PHP MySQL

● MySQL Database Server
  ▶ MySQL Server
  ▶ MySQL Scripts
Creating the roles

Create the roles:

```bash
cd /usr/local/package_management
./pmanager addRole --name="Web Server"
./pmanager addRole --name="Database Server"
```
Setup the Web Server Role

Add the packages:

```bash
./pmanager addPackageToRole --role="Web Server" --package=lang/php5 \
    --build=7.4-Production

./pmanager addPackageToRole --role="Web Server" \
    --package=databases/php5-mysql --build=7.4-Production

./pmanager addPackageToRole --role="Web Server" --package=lang/php5 \
    --build=8.2-Production

./pmanager addPackageToRole --role="Web Server" \
    --package=databases/php5-mysql --build=8.2-Production
```
Setup the Database Server Role

Add the packages:

```bash
./pmanager addPackageToRole --role="Database Server" \
  --package=databases/mysql51-server --build=7.3-Production

./pmanager addPackageToRole --role="Database Server" \
  --package=databases/mysql51-scripts --build=7.3-Production

./pmanager addPackageToRole --role="Database Server" \
  --package=databases/mysql51-server --build=8.1-Production

./pmanager addPackageToRole --role="Database Server" \
  --package=databases/mysql51-scripts --build=8.1-Production
```
Scheduling the builds:

One off build:

    cd /usr/local/pmanager
    ./pmanager cron

Automated builds:
Add the following to /etc/crontab

    @hourly root /usr/local/pmanager/cron.sh
Adding Hosts to Roles

Setup the directory structure:

```bash
cd /usr/local/pmanager
```

Add an options file:

```bash
echo "WITH_APACHE="YES"" > options/7.4-Production/php5/options
```

```bash
echo "WITH_APACHE="YES"" > options/8.2-Production/php5/options
```

Enable options:

```bash
cd /usr/local/tinderbox/scripts
./tc
```
Configuring the Hosts
Host Role Assignment

- Web Server
  - web1.example.com
  - web2.example.com
  - dev.example.com

- Database Server
  - db1.example.com
  - db2.example.com
  - dev.example.com
Register the hosts

cd /usr/local/pmanager
./pmanager addServer --name=web1.example.com
./pmanager addServer --name=web2.example.com
./pmanager addServer --name=db1.example.com
./pmanager addServer --name=db2.example.com
./pmanager addServer --name=dev.example.com
Adding Hosts to Roles – Web Servers

Web Servers

```
cd /usr/local/pmanager
./pmanager addServerToRole --server=web1.example.com \  --role="Web Server"
./pmanager addServerToRole --server=web2.example.com \  --role="Web Server"
./pmanager addServerToRole --server=dev.example.com \  --role="Web Server"
```
Adding Hosts to Roles – Database Servers

Database Servers

```bash
cd /usr/local/pmanager
./pmanager addServerToRole --server=db1.example.com \
    --role="Database Server"
./pmanager addServerToRole --server=db2.example.com \
    --role="Database Server"
./pmanager addServerToRole --server=dev.example.com \
    --role="Database Server"
```
Setting up the agents
Installation

Dependencies

- databases/p5-DBD-mysql
- devel/p5-Config-General
- devel/p5-Getopt-Long

Getting the code:

```
svn co http://svn.tomjudge.com/freebsd/tinderbox /usr/local/pmanager
```

A port for this will be coming soon™
Database Access

GRANT USAGE ON `package_management`.*
  TO 'pmanager_agent'@'192.168.0.0/255.255.255.0'
  IDENTIFIED BY 'pmanager_agent';

GRANT SELECT ON `package_management`.*
  TO 'pmanager_agent'@'192.168.0.0/255.255.255.0';

GRANT SELECT ON `tinderbox`.*
  TO 'pmanager_agent'@'192.168.0.0/255.255.255.0';
Setup

- Copy `pmanager_agent.conf` from `/usr/local/pmanager` to `/usr/local/etc`
- Update `/usr/local/etc/pmanager_agent.conf`
- Add `/usr/local/pmanager/pmanager_agent` to cron or your management tool.
Live Demo
Did it work?
The Important Bits
The License

"THE BEER-WARE LICENSE" (Revision 42): <tom@tomjudge.com> wrote this file. As long as you retain this notice you can do whatever you want with this stuff. If we meet some day, and you think this stuff is worth it, you can buy me a beer in return Tom Judge.
Information

Tutorial:
http://www.tomjudge.com/index.php/FreeBSD/Role_Based_Package_Management

Tracking ports in a production environment:
http://www.tomjudge.com/index.php/FreeBSD/Tracking_Ports_In_A_Production_Environment

Tinderbox:
http://tinderbox.marcuscom.com/

Contact:
- Email: tom@tomjudge.com
- IRC: t_j on FreeNode and EFNet
Questions
The VRT is hiring.

- Research Engineer
  - Ninja Flavor C Coders
- Manager, Attack Detection Team
- Research Analyst
- Research Systems Engineer