RHEL/Fedora + Docker

Maciej Lasyk

Kraków, devOPS meetup #3

2014-02-26

Google + Docker + Fedora?

Google + Docker + Fedora?

Google + Docker + Fedora?

We won't talk about this :)

So.. why Docker?

So.. why Docker?

Looking for some dev-env..

So.. why Docker?

Looking for some dev-env..

What about XEN/KVM/Virtualbox?

So.. why Docker?

Looking for some dev-env..

What about XEN/KVM/Virtualbox?

So if looking for lightweight solution – why not LXC?

So.. why Docker?

Looking for some dev-env..

What about XEN/KVM/Virtualbox?

So if looking for lightweight solution – why not LXC?

Answer is simple – LXC is sitting on lower level

And also – it need more sysop work

Docker **just** works – it's simpler so devs are :)

Read this for more: http://stackoverflow.com/questions/17989306/what-does-docker-add-to-just-plain-lxc

So.. why RHEL/Fedora?

So.. why RHEL/Fedora?

So.. why RHEL/Fedora?

No it's not about flame ;)

So.. why RHEL/Fedora?

No it's not about flame ;)

RHEL (CentOS) just does the job like Ubuntu / Debian / Gentoo...

So.. why RHEL/Fedora?

No it's not about flame ;)

RHEL (CentOS) just does the job like Ubuntu / Debian / Gentoo...

Oh maybe in a more mature & stable & secure way

So.. why RHEL/Fedora?

No it's not about flame ;)

RHEL (CentOS) just does the job like Ubuntu / Debian / Gentoo...

Oh maybe in a more mature & stable & secure way

CVE-2014-0038 & https://github.com/saelo/cve-2014-0038

"Red Hat has previously been paged by its users to enable x32 support in Fedora 18; however, it refused to include it, citing security concerns.

It affects every user by potentially exposing them to as-yet-unfound security bugs for zero gain," Red Hat kernel developer Dave Jones said at the time.

"In addition to this, it increases the potential attack surface for all users, 99.9 percent of which will never even use this feature unless we enable it for additional packages."

LXC 1.0 released

[Posted February 21, 2014 by jake]

From:	Stéphane Graber <stgraber-AT-ubuntu.com>
To:	lxc-devel-AT-lists.linuxcontainers.org, lxc-users-AT-lists.linuxcontainers.org, containers-AT-lists.linux-foundation.org
Subject:	LXC 1.0 has been released!
Date:	Thu, 20 Feb 2014 14:20:09 -0500
Message-ID:	<20140220192009.GT2689@castiana>

LXC 1.0 released

[Posted February 21, 2014 by jake]

From:	Stéphane Graber <stgraber-AT-ubuntu.com>
To:	lxc-devel-AT-lists.linuxcontainers.org, lxc-users-AT-lists.linuxcontainers.org, containers-AT-lists.linux-foundation.org
Subject:	LXC 1.0 has been released!
Date:	Thu, 20 Feb 2014 14:20:09 -0500
Message-ID:	<20140220192009.GT2689@castiana>

Unprivileged containers - we should talk about it @Infosec

More important – ready for production!

A little bit of Fedora/RHEL + Docker history

Fedora/RHEL:

first request: 2013-08-23

rls: 2013-11-28/docker-io-0.7.0-6.fc20 (Fedora + EPEL 6)

https://bugzilla.redhat.com/show_bug.cgi?id=1000662

A little bit of Fedora/RHEL + Docker history

Fedora/RHEL:

first request: 2013-08-23

rls: 2013-11-28/docker-io-0.7.0-6.fc20 (Fedora + EPEL 6)

https://bugzilla.redhat.com/show_bug.cgi?id=1000662

What had to be done?

AUFS replacement with device-mapper (SELinux)

libvirt-lxc in order to integrate with libvirt

Openshift integration (RHEL PaaS)

http://blog.docker.io/2013/09/red-hat-and-docker-collaborate/

Current status of Docker / RHEL / Fedora

Current status of Docker / RHEL / Fedora

Fedora 19/20/RawHide + Epel 6:

    lxc-0.9.0-2.fc20.x86_64

    docker-io-0.8.0-3.fc20.x86_64

https://github.com/dotcloud/docker

    v.0.8.1

https://github.com/lxc/lxc

    lxc-1.0.0

Quickstart

Quickstart

```
if (centos || rhel):
    install_epel_repo()

yum -y install docker-io

systemctl enable docker || chkconfig –add docker

systemctl start docker || chkconfig –add docker

docker pull mattdm/fedora

docker run -t -i mattdm/fedora /bin/bash
```

Fedora Dockerfiles

https://git.fedorahosted.org/cgit/dockerfiles.git/tree/
https://github.com/scollier/Fedora-Dockerfiles

What's there?

apache,couchdb,firefox,hadoop,memcached,
mongodb,mysql,nginx,nodejs,postgresql,rabbitmq,
ssh,wordpress

Fedora Dockerfiles

https://git.fedorahosted.org/cgit/dockerfiles.git/tree/
https://github.com/scollier/Fedora-Dockerfiles

What's there?

    apache,couchdb,firefox,hadoop,memcached,
    mongodb,mysql,nginx,nodejs,postgresql,rabbitmq,
    ssh,wordpress

Installation:

    docker build -rm -t docent/nginx \
        git://github.com/scollier/dockerfiles-fedora-nginx.git

    or just download Dockerfile and docker build .

Fedora Dockerfiles

https://git.fedorahosted.org/cgit/dockerfiles.git/tree/
https://github.com/scollier/Fedora-Dockerfiles

What's there?

    apache,couchdb,firefox,hadoop,memcached,
    mongodb,mysql,nginx,nodejs,postgresql,rabbitmq,
    ssh,wordpress

Installation:

    docker build -rm -t docent/nginx \
        git://github.com/scollier/dockerfiles-fedora-nginx.git

    or just download Dockerfile and docker build .

Trusted builds (index accounts linked with GitHub)

Docker / Fedora / JBoss

It's all about Dockerfile...

Docker / Fedora / JBoss

It's all about Dockerfile...

```
FROM mattdm/fedora
RUN yum install -y jboss-as
ENTRYPOINT /usr/share/jboss-as/bin/launch.sh \
                    standalone standalone.xml 0.0.0.0
```

Docker / Fedora / JBoss

It's all about Dockerfile...

```
FROM mattdm/fedora
RUN yum install -y jboss-as
ENTRYPOINT /usr/share/jboss-as/bin/launch.sh \
                    standalone standalone.xml 0.0.0.0
```

than just:

JBOSS_DOCKER=$(docker build -t my_freakin_jboss .)

docker run -i -t $JBOSS_DOCKER

https://asciinema.org/a/7912

Internal docker registry / shipyard

So we'd like to host our own registry

https://github.com/dotcloud/docker-registry

yum install docker-registry (epel: 0.6.3, github 0.6.5)

Internal docker registry / shipyard

So we'd like to host our own registry

https://github.com/dotcloud/docker-registry

yum install docker-registry (epel: 0.6.3, github 0.6.5)

or just use this samalba/docker-registry

YO DAWG, I HEARD U LIKE DOCKER
SO I PUT A DOCKER IN UR DOCKER SO YOU CAN USER DOCKER IN DOCKER

Internal docker registry / shipyard

So we'd like to host our own registry

https://github.com/dotcloud/docker-registry

yum install docker-registry (epel: 0.6.3, github 0.6.5)

or just use this samalba/docker-registry

Collaboration?

```
docker export internal_registry > internal_registry.tar
gzip internal_registry.tar
mv internal_registry.tar.gz /vagrant
```

Or simply host it ;)

Docker + SELinux

f20 policy: https://git.fedorahosted.org/cgit/selinux-policy.git/tree/docker.te?h=f20-contrib

What's there?

seinfo -t -x | grep docker

sesearch -A -s docker_t (and the rest)

or just unpack docker.pp with semodule_unpackage

Docker + SELinux

f20 policy: https://git.fedorahosted.org/cgit/selinux-policy.git/tree/docker.te?h=f20-contrib

What's there?

    seinfo -t -x | grep docker

    sesearch -A -s docker_t (and the rest)

    or just unpack docker.pp with semodule_unpackage

How to use it?

    man docker_selinux :)

Docker + SELinux

f20 policy: https://git.fedorahosted.org/cgit/selinux-policy.git/tree/docker.te?h=f20-contrib

What's there?

    seinfo -t -x | grep docker

    sesearch -A -s docker_t (and the rest)

    or just unpack docker.pp with semodule_unpackage

How to use it?

    man docker_selinux :)

Permissive domains! semanage permissive -a docker_t

It's only in targeted policy (not for MCS)

And seriously...

Do you know this guy?

And seriously...

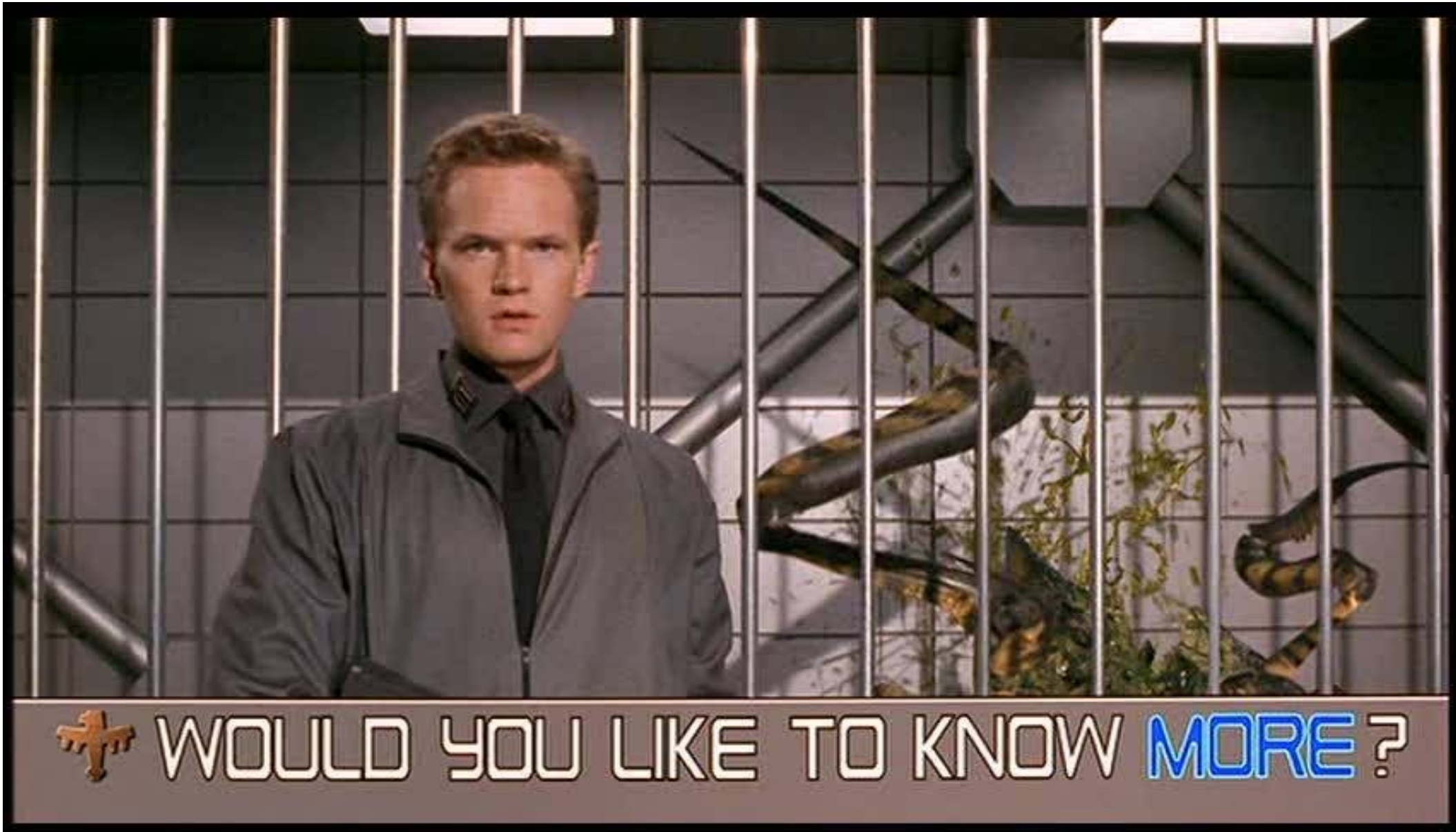Do you know this guy?

So he has something to tell you...

http://www.youtube.com/watch?v=o5snlP8Y5GY

stopdisablingselinux.com

stopdisablingselinux.com

or...

Infosec meetup

Thank you :)

RHEL/Fedora + Docker

Maciej Lasyk

Kraków, devOPS meetup #3

2014-02-26

http://maciek.lasyk.info/sysop

maciek@lasyk.info

@docent-net