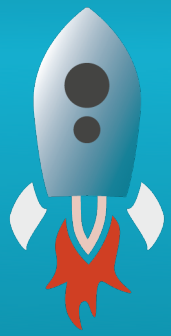
stackato by ActiveState

A Secure Cloud with Stackato Private PaaS



John Wetherill
Ho Ming Li
August 28, 2013

Today's Speakers

John Wetherill

Developer Evangelist

ActiveState®

Code to Cloud: Smarter, Safer, Faster™

stackato® by ActiveState®

NOTES:

Bart will tell a story of how we got into this space
Dan will provide a real-world service-provider perspective on HP's private cloud initiatives and vision

Topics

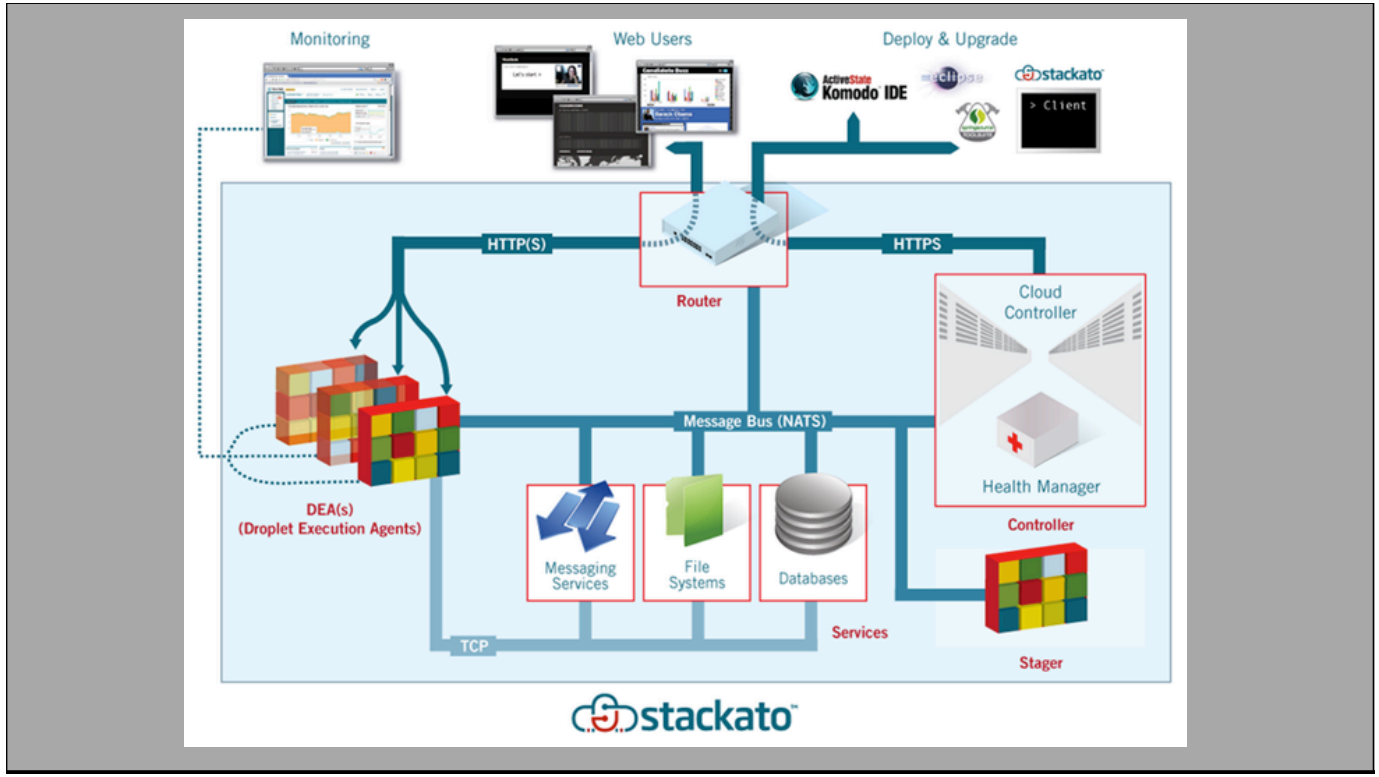
- LXC Containerization and App Isolation
- Private PaaS and Security
- SSL/SCP/DBShell
- Sudo
- Users/Groups
- Audit Features
- WebRTC

stackato by ActiveState

Recent Events

large enigneering teams
pain: integration
pain: security
diversity using opensource: children's hospital, largest anks healthcare, alzeimer's association, clothing stores, auto manufacturers, online retilers, utilities
graph databases

increased complexity


Monitoring
Web Users
Deploy & Upgrade
ActiveState Komodo IDE
eclipse
stackato
> Client
HTTP(S)
HTTPS
Router
Cloud Controller
Health Manager
Controller
Message Bus (NATS)
DEA(s)
(Droplet Execution Agents)
Messaging Services
File Systems
Databases
Services
TCP
Stager
stackato

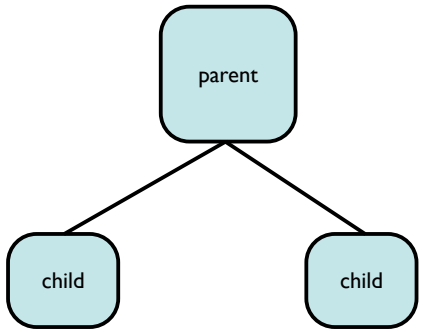
LXC Namespace Isolation

- isolate resources and processes
- pid
- net
- ipc
- mnt
- uts

stackato by ActiveState

pid namespace

- parent/child relationships
- child has its own pid numbering
- child has no visibility to parent
- child has no visibility to siblings
- each child has pid 1 (init-like)



net namespace

- each net namespace has its own network interfaces
- each net has its own loopback interface
- interface pairs can span multiple containers
- enables talking to “outside world”
- example: multiple apache instances binding to port 80

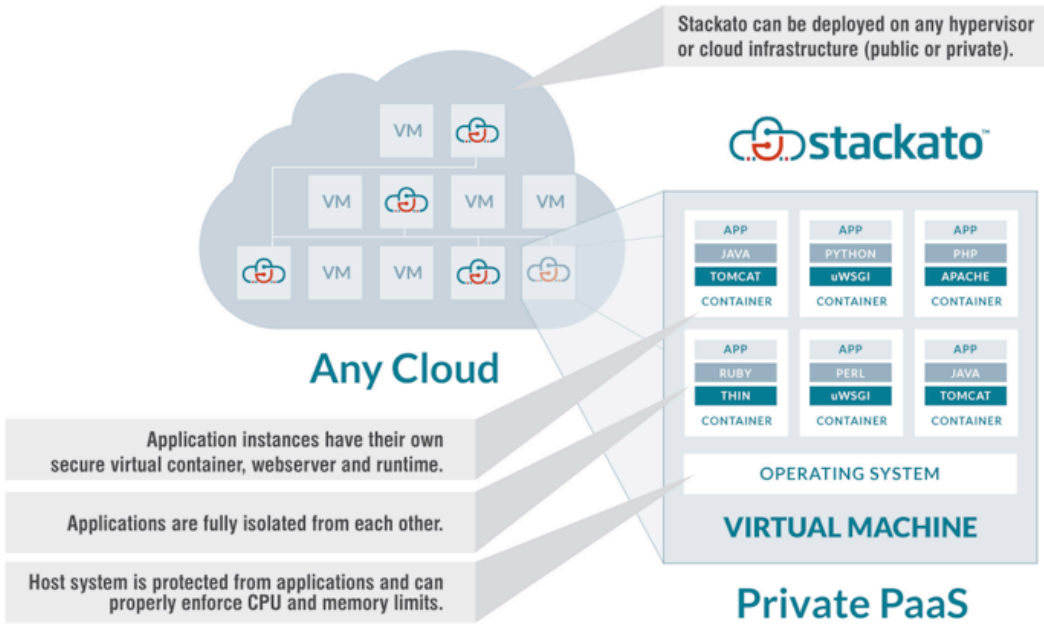
mnt namespace

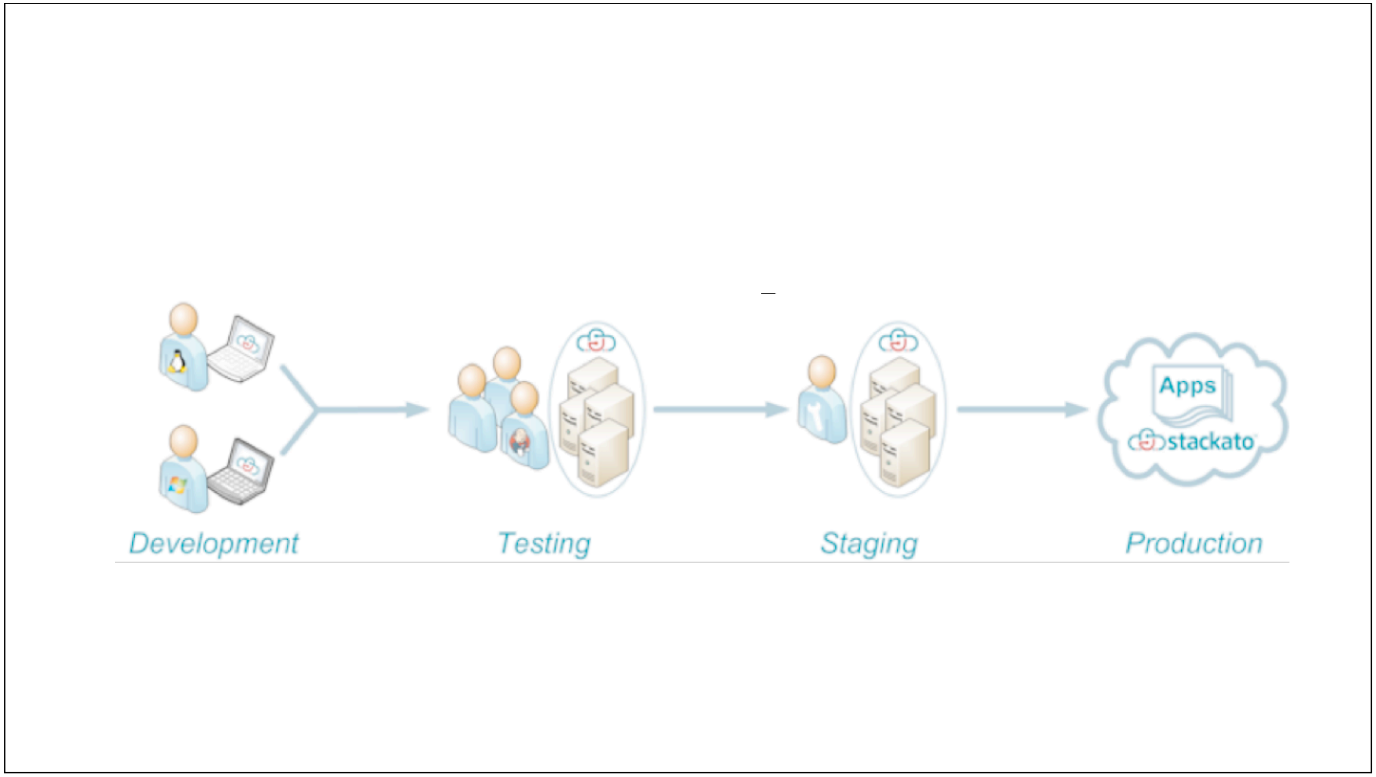
- chroot, on steroids
- sandbox a group of processes within a directory
- each container has its own mount points and root directory
- these are mapped into the top-level root filesystem
- no visibility or access to other containers' mount points

uts namespace

- deals with hostname
- each names has its own hostname
- system calls that access hostname will “see” the container hostname
- all processes in uds namespace see their own hostname

Private PaaS and Security


Stackato can be deployed on any hypervisor or cloud infrastructure (public or private).
stackato
VM
Any Cloud
APP
JAVA
TOMCAT
CONTAINER
APP
PYTHON
uWSGI
CONTAINER
APP
PHP
APACHE
CONTAINER
APP
RUBY
THIN
CONTAINER
APP
PERL
uWSGI
CONTAINER
APP
JAVA
TOMCAT
CONTAINER
OPERATING SYSTEM
VIRTUAL MACHINE
Application instances have their own secure virtual container, webserver and runtime.
Applications are fully isolated from each other.
Host system is protected from applications and can properly enforce CPU and memory limits.
Private PaaS


Apps
stackato
Development
Testing
Staging
Production

SSL and Stackato

- Stackato added SSL support to CloudFoundry
- Stackato API is accessed over SSL
- Web Console is accessed via SSL
- non-ssl access also available
- SSL terminates at router
- Stackato-deployed apps can talk SSL to outside using their own certs

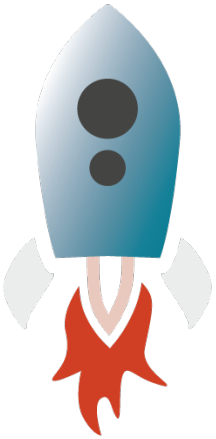
stackato by ActiveState

ssh and scp

- ssh and scp access to each container
- available only to container “owners” (users and admins)
- allows visibility to container’s:
  - process space
  - filesystems
  - environment
  - hostname
  - network

stackato by ActiveState

ssh scp



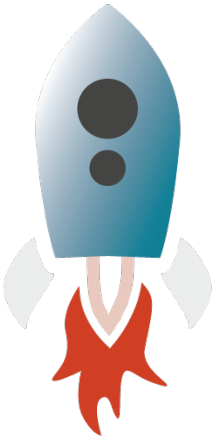
stackato by ActiveState

dbshell

- provides access to underlying database
- ssl tunnel is created to access interactive shell
- MongoDB, MySQL, PostgreSQL
- Useful for importing data:
- `$ stackato dbshell my-app mysql-service < mydata.sql`
- Cloud Foundry “tunnel” command is also available

stackato by ActiveState

dbshell

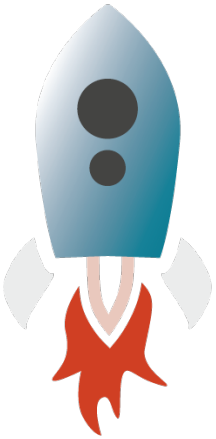


stackato by ActiveState

sudo access

- users can be granted sudo access
- allows root privileges, on container only
- useful for backups and other “system” tasks
- Stackato API exposes ability to grant/revoke sudo access
- Applies to users and groups
- Can be managed via WebConsole too

Demo: sudo

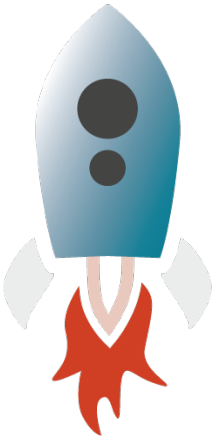


stackato by ActiveState

Miscellaneous Security Topics

- BREACH resilience
- Custom certs in Java apps
- WebRTC

Demo: WebRTC



stackato by ActiveState

stackato by ActiveState hp Cloud

Thank you!

Any questions?

John Wetherill – johnw@activestate.com
ActiveState