Centre de Calcul de l'Institut National de Physique Nucléaire et de Physique des Particules

Singularity au CC-IN2P3

Vanessa HAMAR

Disclaimer

- Les informations contenues dans cette présentation ont été compilées à partir des différents sites Web, principalement les sites : Singularity, Docker, OSG et WLCG.

Plan

- Pour quoi containers ?
- Bref comparaison entre containers
- Singularity
  - Définition
  - Rôles
    - Environnement de création
    - Environnement de production
- Sécurité
- Singularity au CC
  - Installation
  - Distribution des images
  - Expériences
- Conclusions
- Liens utiles

Pour quoi containers ?

- “Containers are a solution to the problem of how to get software to run reliably when moved from one computing environment to another. This could be from a developer's laptop to a test environment, from a staging environment into production and perhaps from a physical machine in a data center to a virtual machine in a private or public cloud.”*

*cio.com

Bref comparaison entre containers

- **Docker :**
  - Micro services.
  - Enterprise applications.
  - Développeurs/DevOps

- **Shifter :**
  - Utilise un grand nombre d'applications docker.
  - Fournit un moyen de les exécuter dans HPC après un processus de conversion.
  - Il supprime également toutes les exigences de root afin qu'ils soient exécutable en tant que utilisateurs.
  - Utilisateurs des applications scientifiques

- **Singularity :**
  - Portabilité des applications (fichier image unique, contenant les dépendances)
  - Reproductibilité, exécution multiplateforme, prise en charge des systèmes d'exploitation hérités et des applications.
  - Utilisateurs de l'applications scientifiques

http://geekyap.blogspot.fr/2016/11/docker-vs-singularity-vs-shifter-in-hpc.html

Singularity

Singularity est une solution de containérisation, créée pour répondre à des besoins des applications scientifiques

Containers pour la Science !

Singularity

- Singularity permets aux utilisateurs:
  - De leurs laisser le plein contrôle de leur environnement.
  - De gérer leurs *workflows*, leurs piles logicielles et librairies.
  - De gérer leurs données.
  - D'utiliser les ressources des plateformes sous-jacentes.
    - Interconnecte HPC.
    - Systèmes des fichiers.
    - GPU/Accélérateurs divers.
    - Etc.

Cela signifie que:

- Les utilisateurs n'ont pas besoin de demander aux administrateurs des clusters d'installer quoi que ce soit pour eux – ils peuvent le placer dans un conteneur Singularity et l'exécuter.
- Aucun changement du système de batch est nécessaire

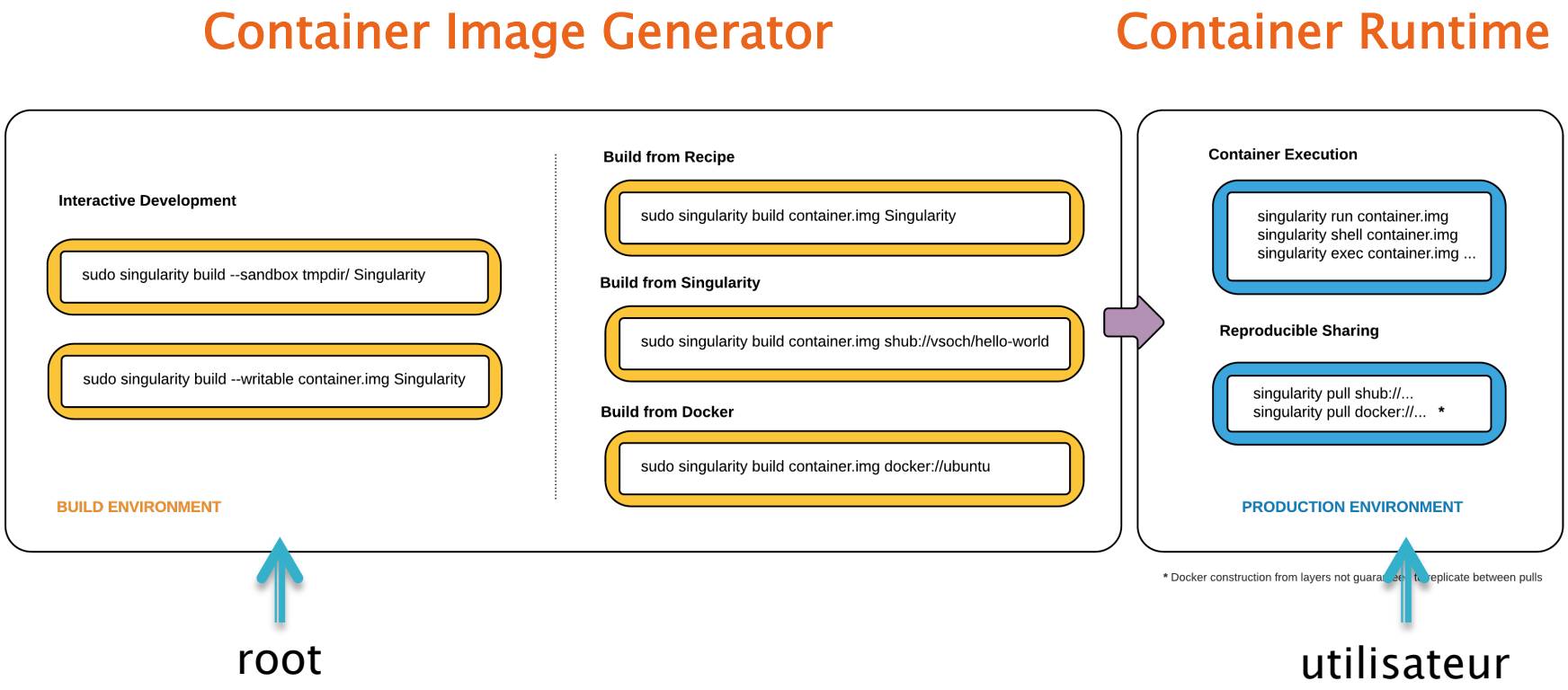
Singularity

- Singularity réalise cela :
  - En encapsulant l'environnement d'exécution.
  - En se basant sur des images.
  - En ne modifiant rien au niveau de l'environnement exécution de l'utilisateur.
  - En interdisant toute possibilité de gain de privilèges.
  - En ne nécessitant pas de processus daemon.
  - Il n'a pas besoin de gérer le réseau, est transparent.
  - Les cgroups ne sont pas touchés par Singularity, tout est géré par le système batch.
  - Support MPI (OpenMPI, MPICH, IntelMPI)

Un utilisateur à l'intérieur d'un conteneur Singularity est le même utilisateur qu'à l'extérieur du conteneur

Singularity rôles

- Singularity a deux rôles principales:



Les utilisateurs peuvent créer et personnaliser des conteneurs localement, puis les exécuter sur une ressource partagée

Environnement de création

Interactive Development

```
sudo singularity build --sandbox tmpdir/ Singularity
```

```
sudo singularity build --writable container.img Singularity
```

BUILD ENVIRONMENT

Build from Recipe

```
sudo singularity build container.img Singularity
```

Build from Singularity

```
sudo singularity build container.img shub://vsoch/hello-world
```

Build from Docker

```
sudo singularity build container.img docker://ubuntu
```

Environnement de création

- Formats des images :
  - **squashfs:** est un système de fichiers en lecture seule compressé qui est largement utilisé pour les live CDs, clés USB, et les OS des téléphones portables
  - **ext3**:(également appelé *writable*) est un fichier contenant un système de fichiers ext3 ou c'est possible écrire
  - **directory**: (également appelé *sandbox*) est un répertoire Unix standard contenant une image root
  - **tar.gz**: zlib fichier compressé tar zlib
  - **tar.bz2**: fichier archive tar bzip2
  - **tar**: fichier tar

Format de conteneur par défaut:
Squashfs >= version 2.4
Ext3 < 2.4

Environnement de création

- The Singularity Recipe

Header

Bootstrap

From (shub, docker, localimage, yum, et autres)

Sections

%help

%setup

%files

%labels

%environment

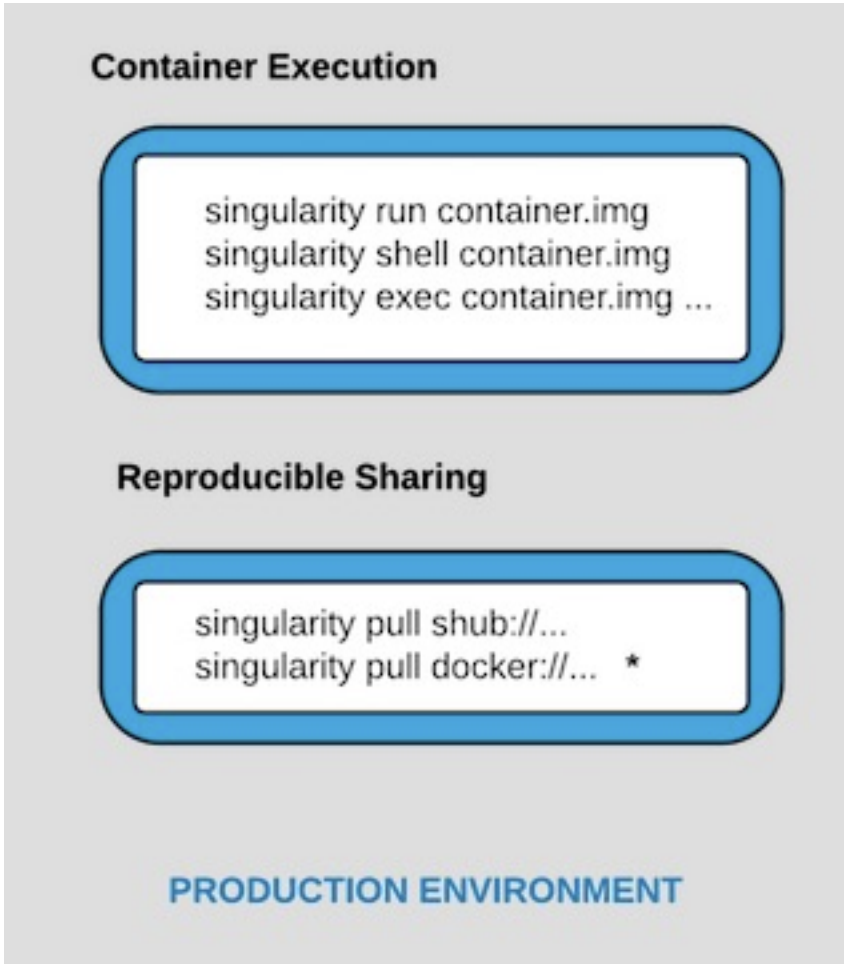
%post

%runscript

https://github.com/singularityware/singularity/tree/master/examples

DEMO: Build a centos 7 singularity image

Environnement de production



Environnement de production

- Singularity permet de faire un mapping entre un point de montage de la machine hôte et un répertoire dans le container. Pour faire cela il y a deux approches :
  - Le mapping du point de montage est définit dans l'image du container elle-même et donc seul l'administrateur peut le faire.
  - L'utilisateur peut lui même définir depuis le container des points de montages correspondants à des espaces de la machine hôte. Cela nécessite que des droits particuliers lui aient été donnés.
- Selon la complexité des workflows applicatifs ces points sont sources d'importantes difficultés.
  - Nécessite de configure singularity dans un mode dit setUID ou bien de s'appuyer sur des fonctionnalités kernel (namespace) qui ne sont pas encore présentes dans le kernel fournit par défaut.

DEMO

Environnement de production

- Submitting a job in the computing cluster

Un simple script:
mon_job_singularity.sh

```
#!/bin/bash
singularity exec /cvmfs/singularity.in2p3.fr/images/cc/official/sl/x86_64/6/6.9/ $HOME/my_script.sh
```

Normal submission:

```
qsub -q long -l os=cl7 mon_job_singularity.sh
```

Securité

- **User Namespace:** Singularity supporte nativement l'espace de nommage de l'utilisateur et peut fonctionner complètement sans privilège («rootless») depuis la version 2.2 (octobre 2016) mais les fonctionnalités sont sévèrement limitées.

- **SetUID:** Il s'agit du modèle d'utilisation par défaut de Singularity, car il offre le plus de flexibilité en termes de fonctionnalités prises en charge.

Pour cette raison, Singularity a été développé avec la transparence à l'esprit.

Securité

- Mais les derniers mois nous avons reçu des alertes de sécurité liées à singularity autant pour le mode User Namespace, comme pour le setuid !!!

Singularity au CC

- Singularity est disponible depuis quelques mois sur l'ensemble des nœuds de calcul de nos fermes.
  - Version 2.5.0
  - Déployé dans le mode setUID.

- Nous proposons aux utilisateurs un ensemble d'images "de bases" dans CVMFS.
  - Debian.
  - SL6.
  - CentOS7.
  - Ubuntu.

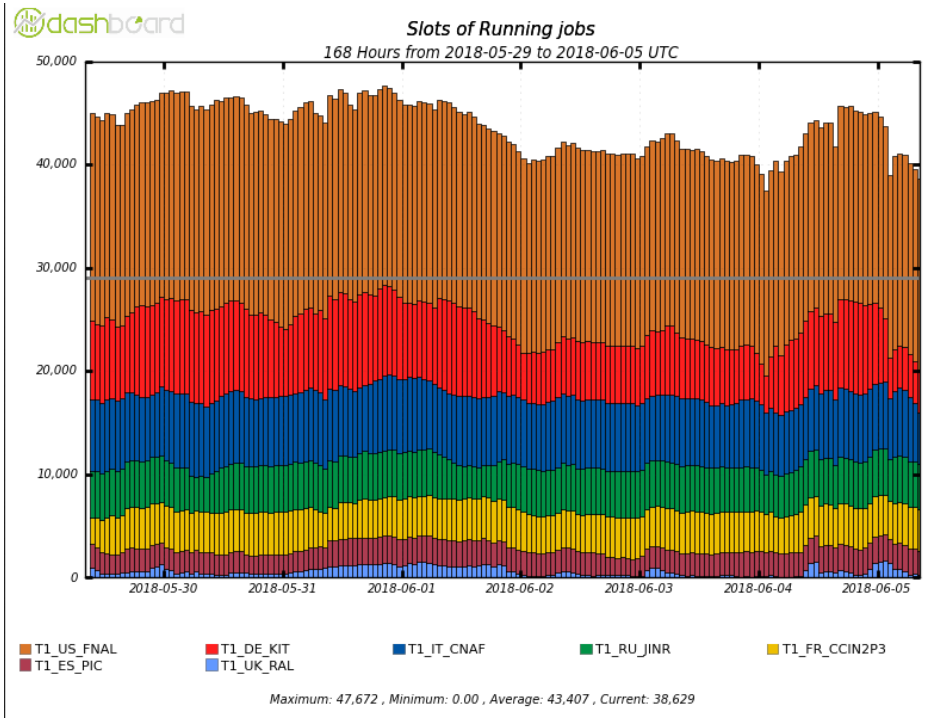
Singularity – Image distribution

- Dans la présentation de Brian Bockelman, pre-GDB, July 2017 :
  - Given our heavy investment in CVMFS, it seems very natural to leverage it for image distribution.
    - Given CVMFS implementation details, images should be distributed as flat directories - Cache will work at the individual file level.

- Au CC nous avons un repo cvmfs pour stocker des images singularity.

- Certaines applications/expériences qui sont organisées au niveau mondial proposent leurs propres images via le système CVMFS.
  - C'est notamment le cas de l'expérience de physiques des hautes énergies qui exige singularity (CMS).
  - Cette expérience exécute quotidiennement des centaines de taches avec singularity.

Singularity au CC



- CMS Un des quatres expériences LHC utilise déjà singularity pour executer sa production.

- Test par l'expérience CMS de la disponibilité de singularity
  - Ce test est jugé critique du coté applicatif.

Detailed output of Metric Result

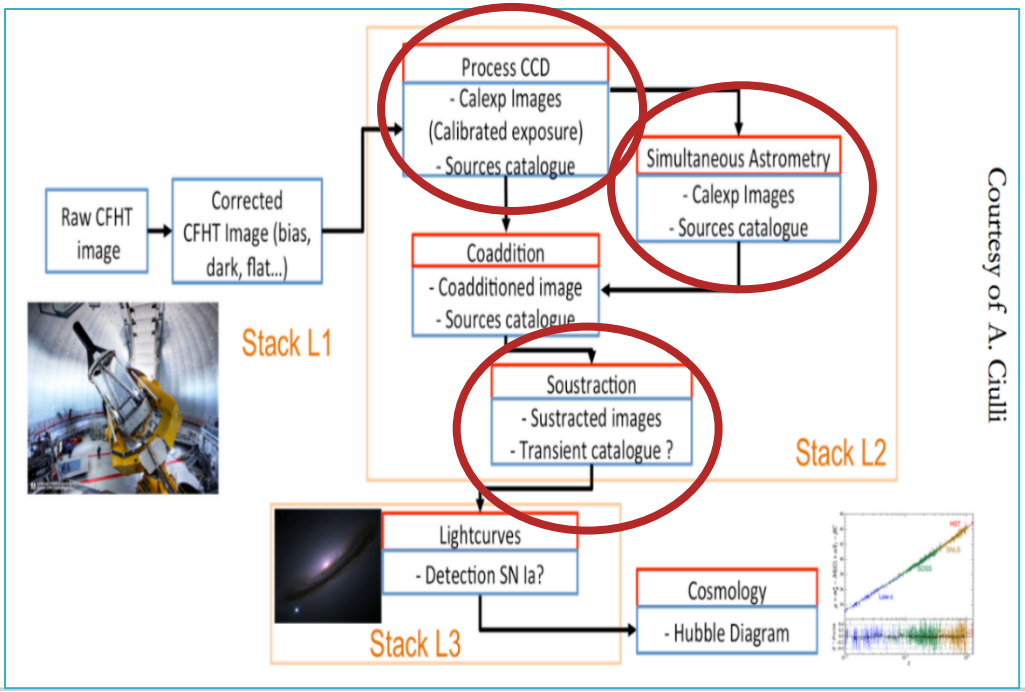
Field	Value
Hostname	cccreamceli04.in2p3.fr
Metric	org.cms.WN-isolation
VOFQAN	/cms/Role=pilot
Service Flavour	CREAM-CE
Timestamp	2018-05-30T14:26:02Z
Status	OK
Summary	ccwsge1102: OK: OK
Details	/usr/bin/singularity exec --home /scratch/43018761.1.mc_long/tmp.YVSMhODsp4:/srv --bind /cvmfs --pwd /srv --contain --ipc --pid /cvmfs/singularity.opensciencegrid.org/bbockelm/cms:rhel6 echo Hello World OR grep Hello World WARNING: Container does not have an exec helper script, calling 'echo' directly Hello World

Singularity au CC

- Singularity est également utiliser au CC pour tester valider des workflows applicatifs ou bien réaliser des challenges.

- LSST – Deep Learning Challenge
  - Ici c'est l'aspect maitrise de l'environnement d'exécution qu'a permis singularity.
  - Les frameworks nécessaires au code machines learning sont très dépendants des librairies GPU. Singularity à permit de décorréler les aspects implémentation des librairies GPU des applicatifs (tensor flow)

- LSST : validation du workflow et impact sur les performance de stockage.



Conclusions

- A very nice idea ☺

Pour les utilisateurs

- Facile a utiliser
- Bonne documentation
- Un mailing liste réactive

Pour les administrateurs systèmes

- Un nouveau projet qui avance vite
- Quelques problèmes de compatibilité avec les anciennes versions
- Attention aux alertes de sécurité

Questions

Where to find information

- Links:
  - Singularity - User guide
  - HPC Containers singularity
  - Docker vs Singularity vs Shifter

- Mailing lists:
  - “Singularity” singularity@lbl.gov