Singularity:

Simple.
Fast.
Secure.

Singularity

Singularity

Un peu d'histoire

- Inventé par Greg Kurtzer au LBNL pour répondre aux problèmes spécifiques au HPC
- Développement démarré en Octobre 2015
- Première release en Avril 2016
- Les retours de la communauté ont menés à la version 2.0 en Juin 2016
- Greg a crée **Sylabs.io** en Janvier 2018 : 25 employés en novembre 2018
- Sortie de la version 3.0 en Octobre 2018 avec une réécriture complète et de nouvelles fonctionalités

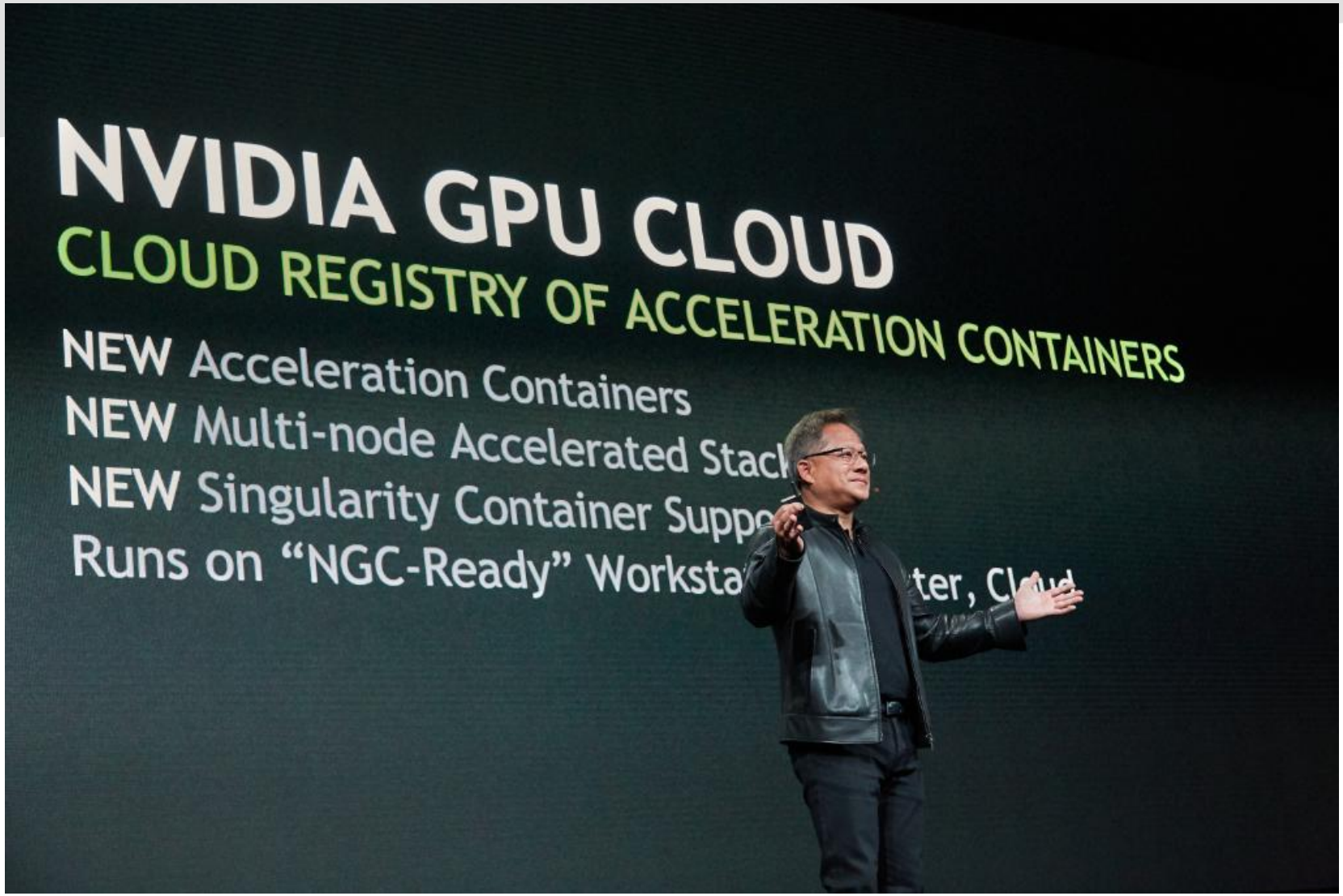
Qui l’utilise ?

Quelques exemples dans le HPC

- Summit @ Oak Ridge National Lab
- ABCI @ AIST
- Titan @ Oak Ridge National Lab
- Stampede & Stampede2 @ TACC
- Theta @ Argonne National Lab
- Astra (ARM!) @ Sandia National Lab
- MareNostrum @ Barcelona Supercomputing Center
- Comet & Gordon @ San Diego Supercomputing Center

Support officiel Nvidia

Nouvelles fraiches du matin



Les nouveautés de la 3.0 ?

- Migration de C vers Go (intégration avec les outils existants et les plugins)
- SIF est le format par défaut, apportant la **signature** et la **vérification**
- Infrastructure Cloud (Container Library, Remote Builder, et Keystore)
- Possibilité d’exécuter des images Docker et OCI
- Support/isolation réseau (plugins CNI / root uniquement)
- Support des Cgroups (version 1 / root uniquement)
- Sécurité : Linux capabilities, SELinux, AppArmor, seccomp

Migration vers Go

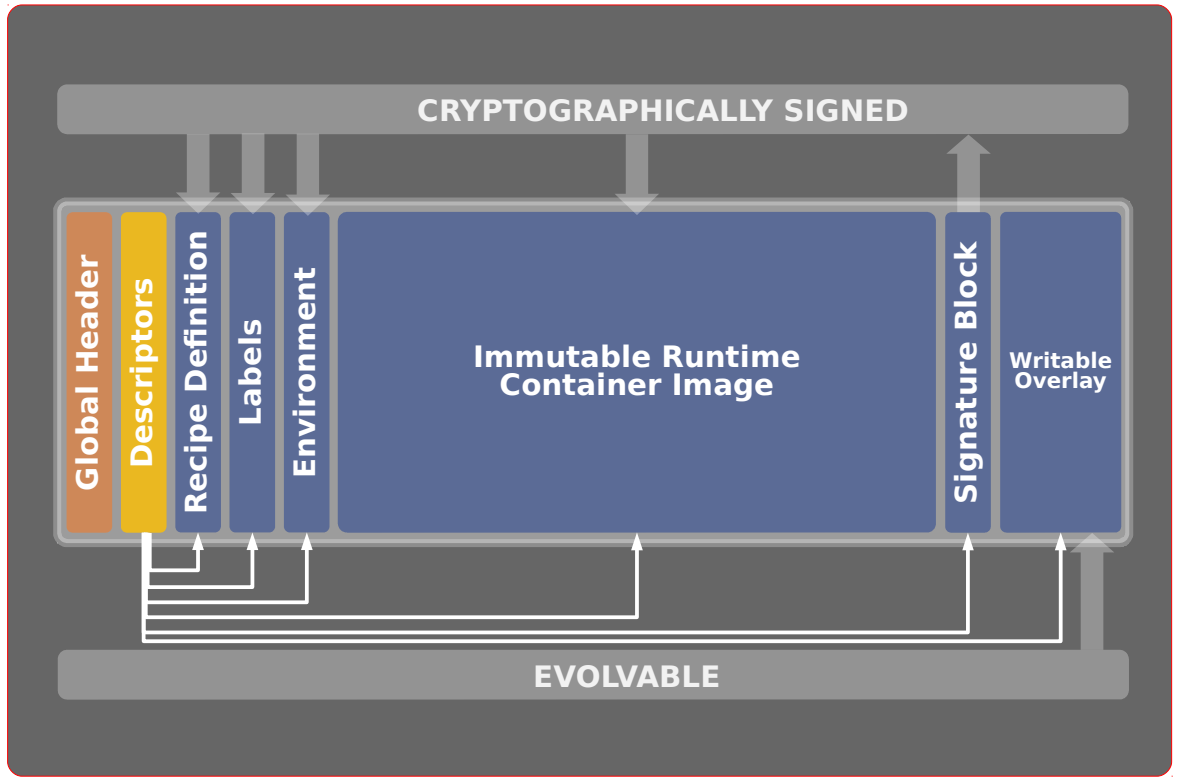
Motivations

- Eliminer shell et python de la ligne de commande
- La plupart des projets “conteneur” sont écrits en Go
- Bénéficier des dépendances de ces projets afin de ne pas réinventer la roue
- Langage facile à apprendre

Le format SIF

Singularity Image Format

- Les images Singularity se trouvent dans un fichier
- **Reproductibilité** complète de la pile logicielle
- Permet d'embarquer son **propre environnement**
- Un **format d'exécution** (pas d'archives)
- Signature / Vérification cryptographique
- **Simple**, intuitif, facile à utiliser (siftool)



Démo SIF

- **Gestion des clés avec Singularity (singularity keys)**
- **Signature d’une image SIF (singularity sign/verify)**
- **ECL (Execution Control List)**

Sylabs Cloud

- **Services de création de conteneur**
  - Local / Distant
  - Permet de créer des images sur des systèmes sécurisés
- **Bibliothèque de conteneur**
  - Service de stockage objet pour la distribution et le stockage
  - Scan, notification and gestion pour le DevSecOps
- **Gestion des clés cryptographiques**
  - Singularity supporte les conteneurs signés
  - Source de confiance des clés publiques (Keystore Sylabs)
  - Les clés des mainteneurs sont téléchargées automatiquement et testées à la demande pour la validation des conteneurs

Démo services Cloud

- **https://cloud.sylabs.io**
- **Création d’un conteneur (CLI)**
- **Création d’un conteneur (WEB)**

Singularity et le réseau ?

CNI !

- **CNI** : **C**ontainer **N**etwork **I**nterface
- Utilisé par plusieurs projets : Kubernetes, Mesos, Openshift, Amazon ECS
- Plugins de base dans Singularity : **bridge**, ptp (veth), ipvlan, macvlan
- Intégration du **port mapping**
- Entièrement **configurable**
- Utilisation de plugins tiers pour les configurations complexes

Démo réseau

- **Création d’un bridge**
- **Port mapping / Allocation statique addresse IP**
- **Plusieurs interfaces**
- **A quoi ressemble une configuration de réseau**

Sécurité

Un peu plus de confinement

- Support des **Cgroups**
- L’utilisateur root peut définir un set de **capabilities** à l’exécution
- L’administrateur peut gérer les capabilities des utilisateurs (avec précaution)
- Les utilisateurs peuvent passer un contexte d’exécution **SELinux**, ou un profil **AppArmor**
- Les utilisateurs peuvent passer leurs propres filtres d’appel système via **seccomp**
- Support d’exécution avec des **UID/GID** différents pour l’utilisateur root

Démo

- **Les capabilities**
- **Confinement et lancement d’un serveur Nginx**

Roadmap

Le futur ... à court terme ?

- Singularity 3.1 intégrera un **système de plugin** pour l’ajout d’outils tiers
- **Conteneurs cryptés (SIF)**
- **OCI** compliance
- Intégration à **Kubernetes** avec la possibilité d’exécuter des conteneurs cryptés (SIF)
- Améliorations au niveau de construction des images

Sylabs et SingularityPRO

- Engagement dans l’open source
- SingularityPRO est à Singularity ce que RHEL est à Fedora
- Support long terme pour plusieurs releases
- Stabilité avec le portage des corrections de bug et des fonctionnalités
- Patch de sécurité
- Accès aux services Sylabs Cloud avec option d’hébergement on-prem

Features	Singularity	Singularity Pro
SIF: Single File Container Format	✓	✓
Cryptographically Verifiable	✓	✓
No Persistent Global Daemon Process	✓	✓
Supports Non-root Users Running Containers	✓	✓
Blocks Privilege Escalation within Container	✓	✓
“Bring Your Own Environment” Usage Model	✓	✓
Supports AI/HPC Workflows and Architectures	✓	✓
Supports GPUs Natively	✓	✓
Code Curation		✓
Streamlined Security Updates		✓
Sylabs Cloud Features		✓
Signed Packages and Repositories		✓
Additional Self Service Help		✓
Container Build Services		✓
Cryptographic Key Service		✓
Container Library		✓

@SylabsIO
@SingularityApp

Sylabs.io