Découvrir Fedora CoreOS, un système conçu pour faire tourner au mieux vos conteneurs

Timothée Ravier
Ingénieur CoreOS chez Red Hat

travier@redhat.com
@siosm:matrix.org
@siosm

Où héberger mes applications ?

- **Besoin :** Faire tourner des applications pour le développement et pour la production
- **Prérequis :** Une ou plusieurs applications packagées sous forme de conteneurs
- **Contraintes :**
  - Ne pas se lier complètement à un fournisseur de cloud
  - Docker seul ? plutôt Nomad ? déjà sur Kubernetes ?

travier@redhat.com

Programme

- Qu’est-ce que Fedora CoreOS ?
- Atouts pour le déploiement et la gestion des conteneurs
- Exemples : déploiement un seul noeud, avec Nomad ou Kubernetes

travier@redhat.com

Qu’est-ce que Fedora CoreOS ?

Une édition émergente de Fedora

- Résultat du **regroupement** de deux communautés :
  - Container Linux (de CoreOS Inc)
  - Atomic Host (du Project Atomic)

- Eléments importés de **Container Linux** :
  - La philosophie
  - La méthode de provisionnement
  - l'expertise Cloud Native

- Eléments importés de **Atomic Host** :
  - Basé sur Fedora
  - Le mécanisme de mise à jour
  - Sécurité apportée par SELinux

travier@redhat.com

Philosophie derrière Fedora CoreOS

- **Mises à jour automatiques**
  - Aucune interaction nécessaire pour les administrateurs

- **Provisionnement automatisé**
  - Tous les noeuds démarrent **d'un même point**
  - Configuration d'un noeud au **premier démarrage** via Ignition

- **Infrastructure immuable**
  - **Automatisation** du déploiement et configuration du système
  - Mise à jour des configurations puis **re-provisionnement**

- Applications utilisateur lancées dans des **conteneurs**
  - Rend les mises à jour de l'hôte plus **fiables**

travier@redhat.com

Plateformes & architectures supportées

- Disponible pour un grand nombre de plateformes de **cloud** ou **virtualisation** :
  - Alibaba, AWS, Azure, Azure Stack, DigitalOcean, Exoscale, GCP, IBM Cloud, Openstack, Vultr, VMWare, QEMU/KVM
  - Lancement direct sur AWS & GCP

- Plusieurs options pour le **Bare Metal**
  - ISO classique
  - Boot PXE (réseau)
  - Images disques standard et 4K natives

- Architectures **x86_64** et **aarch64**

travier@redhat.com

Atouts pour le déploiement et la gestion des conteneurs

Juste le nécessaire pour les conteneurs

- Construit à partir des paquets RPM de **Fedora**
  - Support matériel à jour, nouvelles fonctionnalités, etc.
- Uniquement les services essentiels et les outils d'administration
- Choix du gestionnaire de conteneurs :
  - **podman** ou **moby-engine** (**docker**)
- Pas d'interpréteur Python (Bash uniquement)

travier@redhat.com

Version et organisation du système

- Basé sur **rpm-ostree** pour gérer et mettre à jour le système
- **rpm-ostree** : Système hybride entre images et paquets
  - “Comme **Git** pour votre système d’exploitation”
  - Un seul identifiant pour une version donnée
    - Exemple: `32.20200615.2.0 - 86c0246`
- **Distinction claire** entre `/usr`, `/etc` et `/var`
  - Utilise des points de montage en **lecture seule**
  - Evite certains accidents (`rm -rf ...`) et bloque les attaques naïves

travier@redhat.com

Mises à jour automatiques par défaut

- Mise à jour automatiques → Mises à jour fiables
- Tests systématiques (CI) pour chaque changement
- Plusieurs flux de mise à jour pour valider en avance les futures versions
- Déploiement progressif des mises à jour
  - Arrêt possible si un problème est rencontré
- Si quelque chose se passe mal :
  - `rpm-ostree rollback` pour revenir en arrière

travier@redhat.com

Trois flux de mise à jour

- **next** - Changement de version de Fedora, fonctionnalités expérimentales
- **testing** - Ce qui va être prochainement dans **stable**
  - Image à moment précis des paquets stables de Fedora
- **stable** - Le flux le plus stable
  - Obtenu à partir du contenu testé dans le flux **testing**

- **Objectifs** :
  - Nouvelles versions publiées **toutes les deux semaines**
  - Trouver les bugs avec **next & testing** avant qu'ils arrivent dans **stable**

travier@redhat.com

Provisionnement automatisé

- Fedora CoreOS utilise Ignition pour **automatiser** le provisionnement d'un système au **premier démarrage**
- Centralise la configuration du système
  - Plus facile de **(re-)provisionner** de nouveaux noeuds
- **Même point de départ** et ce quelle que soit la plateforme :
  - Configuration avec Ignition **partout** au lieu d'avoir kickstart en bare metal et cloud-init pour le cloud

travier@redhat.com

Configuration Ignition

- Document JSON **déclaratif** fourni par l'intermédiaire des **user data** (clouds)
- Appliquée **une seule fois**, au **premier démarrage**, durant l'étape de l'initramfs
- Peut écrire des fichiers et units systemd, créer des utilisateurs et groupes, partitionner des disques, créer des grappes RAID, etc.
- **Si le provisionnement échoue, le démarrage échoue** (pas de système à moitié en place)
- Format de configuration fait pour les **machines**

```
{
 "ignition": {
  "config": {},
  "timeouts": {},
  "version": "3.0.0"
 },
 "passwd": {
  "users": [
   {
    "name": "core",
    "passwordHash": "$6$43y3tkl...",
    "sshAuthorizedKeys": [
     "ssh-ed25519 ..."
    ]
   }
  ]
 },
 "storage": {
  ...
 },
 "systemd": {
  ...
 }
}
```

Configuration Butane

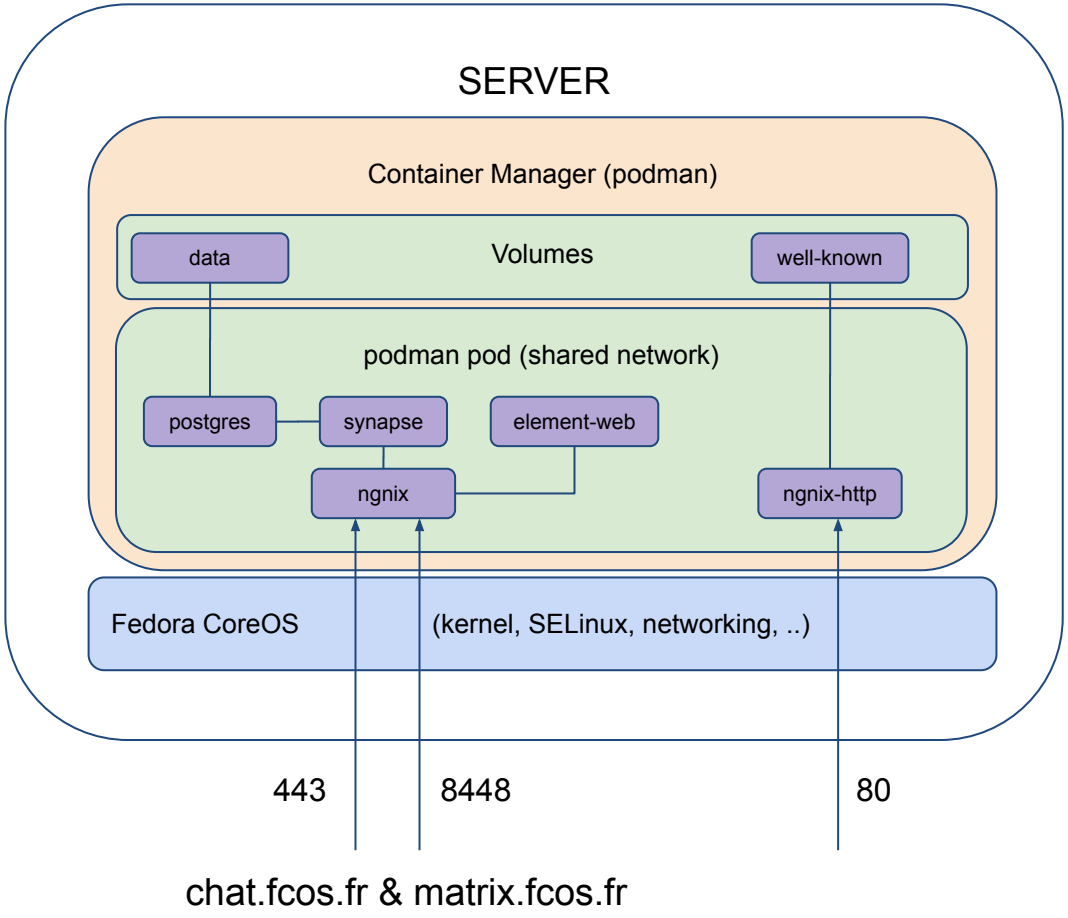
- **Butane** est un transpileur de configuration
- **Convertit** une configuration Butane en configuration Ignition
- Configurations Butane plus **lisibles pour les humains** (YAML)
- Même sémantique qu'Ignition avec du sucre syntaxique pour les opérations courantes
- Le Transpileur **détecte** les erreurs courantes

```
variant: fcos
version: 1.3.0
passwd:
 users:
   - name: core
     ssh_authorized_keys:
       - ssh-ed25519 ...
systemd:
 units:
   - name: docker.service
     enabled: false
     mask: true
   - name: docker.socket
     enabled: false
     mask: true
   - name:
storage:
 files:
   - path: /etc/chrony.conf
     overwrite: yes
     mode: 0644
     contents:
       local: chrony.conf
```

travier@redhat.com

Exemples : déploiement un seul noeud, avec Nomad ou Kubernetes

Déploiement d'un serveur Matrix



https://github.com/travier/fedora-coreos-matrix

Déploiement avec Nomad (Hashicorp)

https://github.com/travier/fedora-coreos-nomad

travier@redhat.com

Déploiement sur Kubernetes (OKD)

https://www.okd.io/installation/

travier@redhat.com

Rejoignez nous !

- Site web : https://getfedora.org/coreos
- Documentation : https://docs.fedoraproject.org/fr/fedora-coreos/
- Issues : https://github.com/coreos/fedora-coreos-tracker/issues
- Forum de discussion : https://discussion.fedoraproject.org/c/server/coreos
- Mailing list : coreos@lists.fedoraproject.org
- IRC/Matrix : #fedora-coreos (Libera.Chat) ou #coreos:fedoraproject.org (Matrix)
- Tutoriel : https://docs.fedoraproject.org/fr/fedora-coreos/tutorial-setup/
- Twitter : @FedoraCoreOS