Ambient IT
128 Boulevard Macdonald
75019 Paris

Mail : formation@ambient-it.net
Tél : +33 (0)1 40 34 11 53

AMBIENT-IT

Formation Firecracker

3 jours (21 heures)

Présentation

Créée et développée par Amazon en 2018, Firecracker est une technologie au design minimaliste de virtualisation open source sous Apache 2.0. Elle peut créer et gérer des conteneurs sécurisés et multi-locataires ainsi que des services fonctionnels. Cela permet d'utiliser des services sécurisés tout en combinant la vitesse, l'efficacité des ressources et les performances offertes par les conteneurs avec la sécurité et l'isolation offerts par les machines virtuelles traditionnelles.

Grâce à la multiplication des périphériques minimalistes, il exclut les périphériques inutiles et les fonctionnalités invitées pour réduire l'empreinte mémoire et la surface d'attaque de chaque microVM. Cela améliore la sécurité, diminue le temps de démarrage, augmente l'utilisation du matériel et permet un environnement en sandbox sécurisé pour chaque conteneur.

FireCracker combine temps de démarrage rapide/à haute intensité et sécurité basée sur la virtualisation matérielle.

Les microVM offrent une sécurité et une isolation de charge de travail améliorées par rapport aux machines virtuelles traditionnelles, tout en permettant la vitesse et l'efficacité des ressources des conteneurs.

Si vous souhaitez approfondir sur la sécurité pour les services AWS Lambda et Fortgate je vous invite à regarder ces slides.

Firecracker prend actuellement en charge les processeurs Intel, il est intégré aux conteneurs Kata, Weave FireKube (via Weave Ignite) et containerd (via firecracker-containerd). Firecrecker fonctionne également sur Linux.

Objectifs

- Savoir utiliser Firecracker
- Créé des conteneurs sécurisés et multi-locataires
- Maîtriser les sandbox
- Créer et gérer des MicrosVM

Public visé

- Développeurs AWS & Apache
- Développeurs Rust

Pré-requis

- Connaissance de AWS et de Apache
- Connaître et développé sur Rust

Programme de notre formation Firecracker

API REQUEST

- ACTIONS : Instance Start/ Flush Metrics/ SendCtrlAltDel
- Logers API REQUEST
- Mettre à jour un Block Device
- Mettre à jour l'Interface Réseau
- Removing Rate Limiting Supression de la Limitation de Débit

DESIGN DE FIRECRACKER

- SCOPE
  - Qu'est ce que FireCracker ?
  - Features
  - Specifications
  - Integration de l'hôte
  - Intégration du Réseau Hôte
  - Stockage
- ARCHITECTURE INTERNE
  - Confinement des menaces
- COMPONENTS AND FEATURES
  - Modèle de Machine : Disposition/Exposition du CPU de l'invité/Clocksources disponible pour les invités
  - I/O: Stockage, Mise en réseau et Limitation de débit
  - MicroVM Metadata Service : Jailling/ Cgroups et quotas/ Monitoring

Configuration d'un Environnement de Développement pour FireCracker

- Local : Local Bare-Metal Machine / Machine Virtuelle Locale (macOS avec VMware Fusion)
- Cloud : AWS/GCP/Addemdum/Microsoft Azure

Premiers pas avec FireCracker

- Conditions préalables
- Obtenir le binaire FireCracker
- Exécution de FireCracker
- Construire à partir de la source
- Exécution à la suite de Test d'Intégration
- Annexe A : Configuration de l'Accès KVM
- Annexe B : Configuration de Docker

Le gardien FireCracker

- Le gardien FireCracker
- L’utilisation du gardien
- Les Opérations du gardien
- Exemple d’Exécution et de Notes
- Observations
- Avertissements

Micro VM Metadata Services

- Le BackEnd MMDS : Exemple d’utilisation: Rotation des Informations d’Identifications
- Le Magasin de Données (Data store)
- Dumbo : Pile réseau MMDS / Gestionnaire TCP/ Point de terminaison MMDS/ Connexion

Reactive FormsConfiguration du réseau Firecracker

- Pour l'hôte
- Configuration de FireCracker
- Pour l’invité
- Nettoyer

Recommandations de configuration de l'hôte de Production

- Configuration du gardien
- Configuration de la sécurité de l’hôte : Host Security Configuration : Atténuation des problèmes de canaux latéraux / Problèmes connues du noyau

Création de roofts personnalisés et d'images du noyau

- Création d’une image du noyau (Kernel)
- Création d’une image Rootfs

Utilisation du dispositif Firecracker Virtio-vsock

- Utilisation du dispositif Firecracker Virtio-vsock
- Prérequis
- Firecracker Virtio-vsock Design (Connexions initiés Hôte/Invité)
- Configuration de l’appareil Virtio-vsock
- Exemples (Utilisation d’outils de prises internes (nc-vsock and socat))

Sociétés concernées

Cette formation s’adresse aux entreprises, petites ou grandes, souhaitant former ses équipes à une

nouvelle technologie informatique avancée.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiple permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.