MA Outline

Peter Okelmann
Supervisor: Jörg Thalheim

Motivation

Lambdas/Serverless Requirements:

- fast boot times
- small runtime overhead
- untrusted code from different parties

=> small boot images

=> containerization + virtualization

=> small containerization/virtualization services

Motivation

Inaccessible Lambdas:

- Small boot images
  - Almost no userland
  - No debugging
  - Difficult profiling
  - No security inspection
- Isolation: containerization + virtualization
  - Small interface: guest ⇔ hypervisor
- Small containerization/virtualization services
  - Offers no interactive shells

=> Accessibility through VMSH

Use cases

1. Interactive Debugging:
   - Big userland supported
   - No interaction with the guests userland
2. Status Probing:
   - Linux-perf profiling lambdas
   - Attaching monitors like Prometheus
   - Security scanning
3. Error Tracing:
   - Record request traces in selected pods
   - Less invasive than X-Trace

Problem Statement

Accessibility for Devs:

- **Interactive debugging**
- **Status probing**
- **Error tracing**

Design Goals:

- Isolation-platform agnostic
- Hypervisor debugging
- For serverless lambda deployments

=> create demo & evaluation system

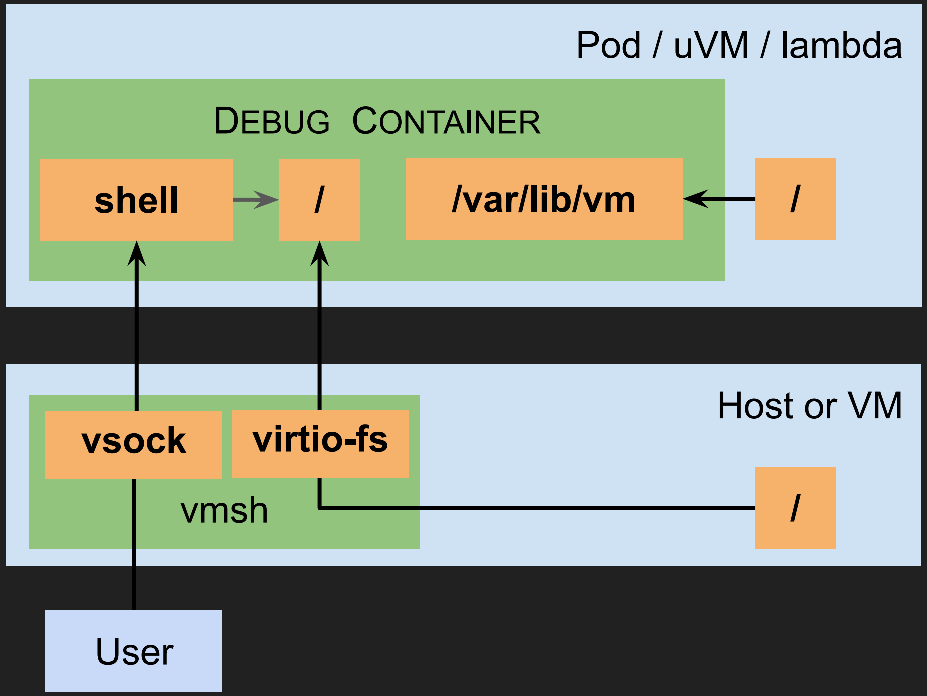
Design

Build evaluation system:

- VMSH
- Serverless: firecracker [4], kubernetes, vhive [10]

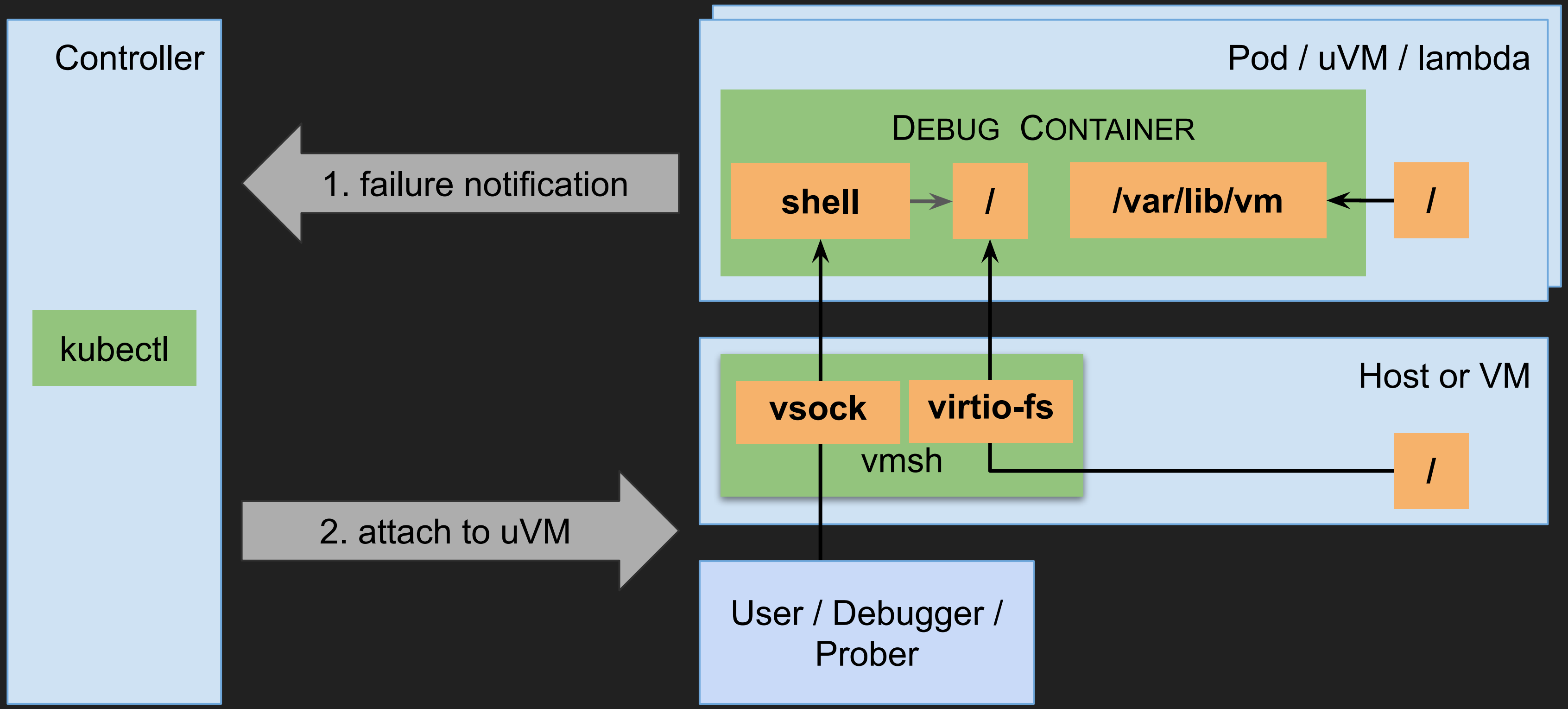
Limitations:

- KVM based hypervisor
- Linux based VM image

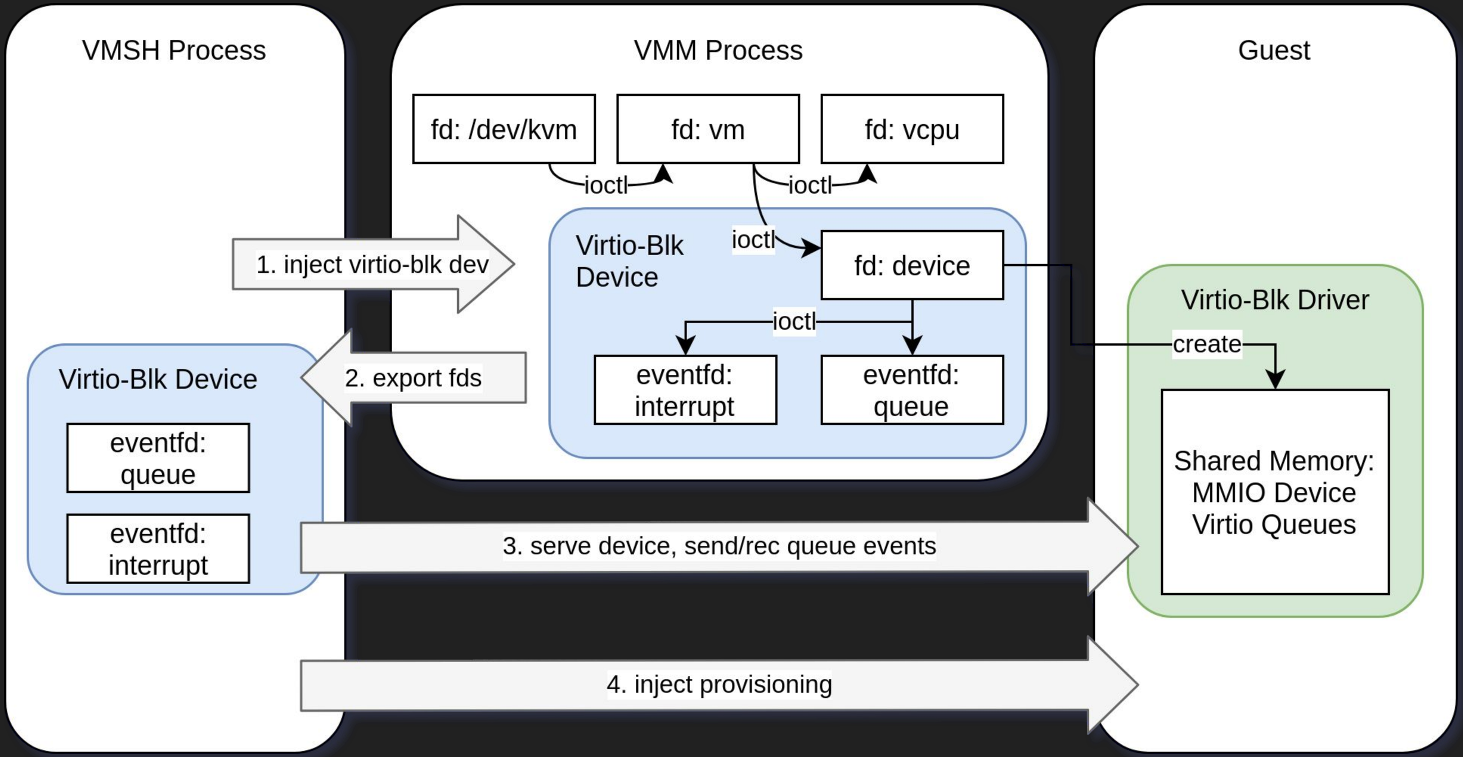


Author: Joerg Thalheim

Design: Eval System



Implementation: Virtio-Blk



Evaluation

- Building slim versions and comparing them:
  - App provisioning from ansible-galaxy
  - Vagrant boxes: only contain distro images
- Performance evaluation
  - Use cases
    - Debugging
    - Probing
    - Tracing
  - Measurements: naive big VM vs vmsh+uVM
    - Use case performance
    - Impact of use case on guest (invasiveness)
    - Startup performance
- Security: Principle of least privilege

Related Work

- Evaluation of Cntr [1]
  - Phoronix Test Suite
  - Docker tiny
- Introspection
  - Cntr: needs containerd-firecracker
  - X-Tier: VM introspection (for security scanners) [3]
  - Exterior: Introspection with secure VM [2]
  - KVM profiling: perf kvm
- Lambda Environments:
  - For eval: kubernetes, vhive [10], some open alternatives [11]
  - Firecracker [4], how to build elastic VMs for lambdas [12]
  - Cntr for container(d) based runtimes: docker, SAND [9]
- Tracing: Canopy [5], X-Trace [8], Dapper [6], Magpie [7]

Sources

[1] Cntr: Lightweight OS Containers, Usenix ATC Proceedings, 2018

[2] EXTERIOR : Using a Dual-VM Based External Shell for Guest-OS Introspection, Configuration, and Recovery, VEE, 2013

[3] X-TIER: Kernel Module Injection, NSS Proceedings, 2013

[4] Firecracker: Lightweight Virtualization for Serverless Applications, Usenix NSDI Proceedings, 2020

[12] My VM is Lighter (and Safer) than your Container, SOSP, 2017

[10] Benchmarking, Analysis, and Optimization of Serverless Function Snapshots, ASPLOS Proceedings, 2021

[5] Canopy: An End-to-End Performance Tracing And Analysis System, SOSP, 2017

[6] Dapper, a Large-Scale Distributed Systems Tracing Infrastructure, Google, 2010

[7] Magpie: online modelling and performance-aware systems, HotOS IX Proceedings, 2003

[8] X-Trace: A Pervasive Network Tracing Framework, Usenix NSDI, 2007

[9] SAND: Towards High-Performance Serverless Computing, Usenix ATC Proceedings, 2018

[11] An evaluation of open source serverless computing frameworks, IEEE CloudCom Proceedings, 2018

Thanks!

Questions?

Preliminary Schedule

- 15-02: Begin
- 15-03: virito-blk done
-
- 15-07: Complete Paper Draft, do eval?
- 01-08: Start revising the Draft
- 15-08: Final Deadline