Imperial College London

LSDS
Large-Scale Data & Systems Group

Serverless Confidential Containers: Challenges and Opportunities

Carlos Segarra

(w/ Tobin Feldman-Fitzthum and Daniele Buono)

Large-Scale Data & Systems (LSDS) Group - Imperial College London

Visiting IBM TJ Watson (Sep'23 – Nov'23)

https://carlossegarra.com
<cs1620@ic.ac.uk>

CLOUD STARS

9th International Workshop on Serverless Computing (WOSC)

Introduction: Characterizing Serverless Functions

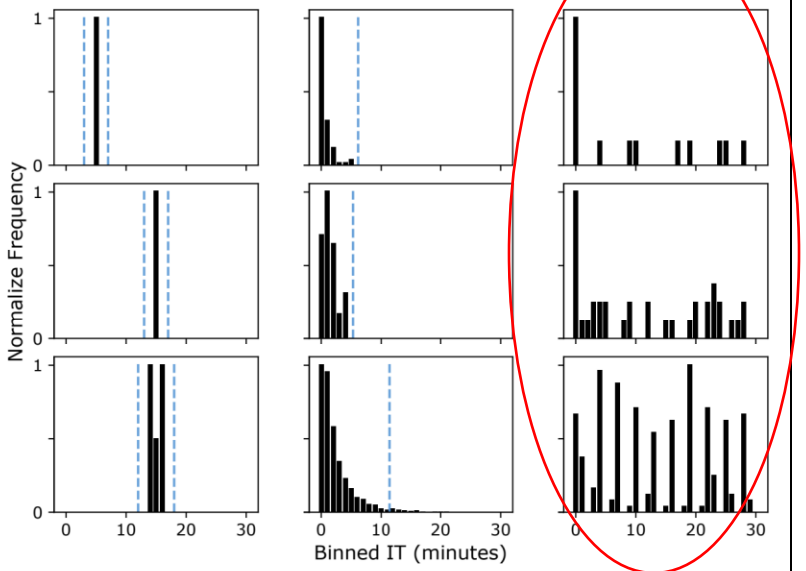


Figure 12: Nine normalized IT distributions from real FaaS workloads over a week.

Functions are bursty!

Functions are short-lived!
(90% shorter than 10s)

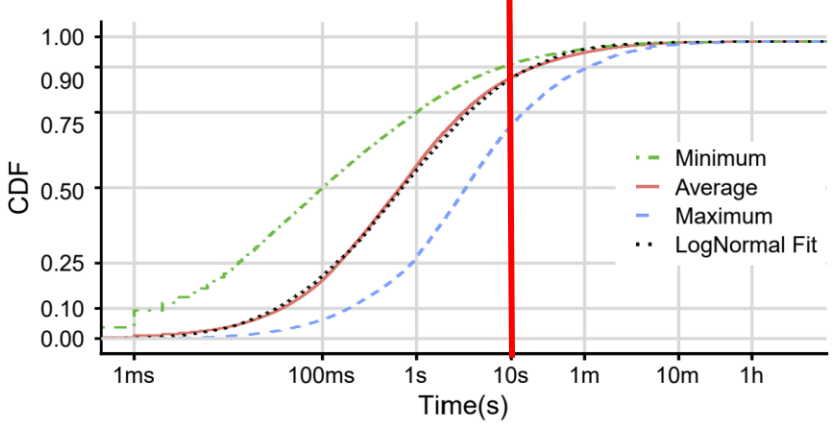


Figure 7: Distribution of function execution times. Min, avg, and max are separate CDFs, and use independent sorting.

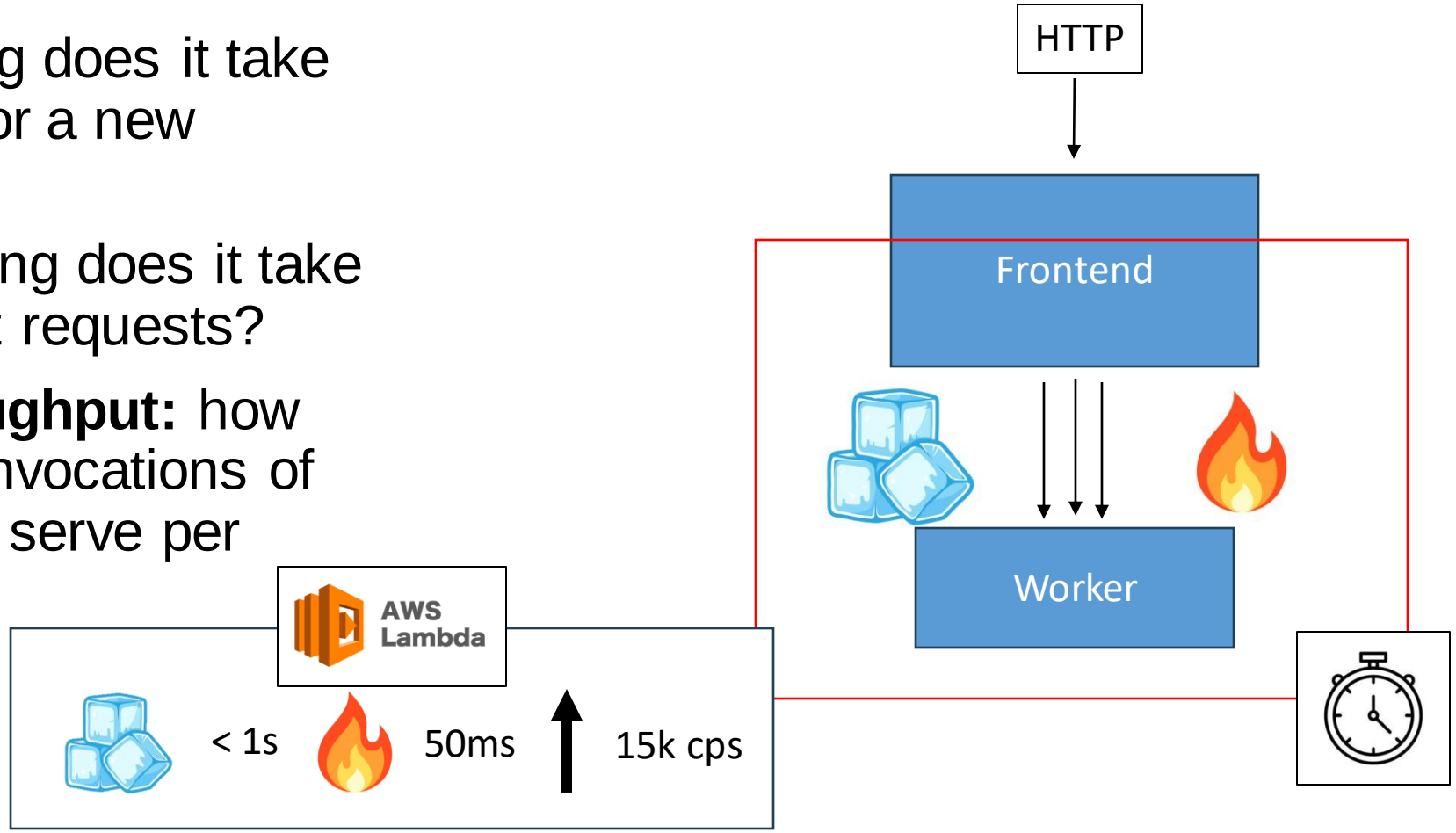
[ATC'20] Serverless in the Wild: Characterizing and Optimizing the Serverless Workload at a Large Cloud Provider

Introduction: Problems in Serverless

Cold-Start: how long does it take to serve a request for a new function?

Warm-Start: how long does it take to serve subsequent requests?

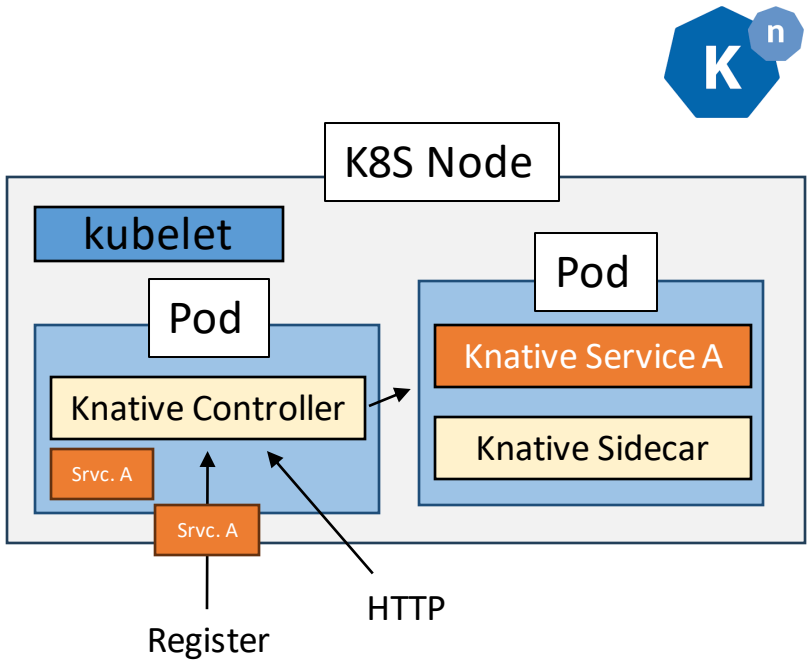
Instantiation Throughput: how many (concurrent) invocations of this function can we serve per second?



[ATC'23] On-demand Container Loading in AWS Lambda

Introduction: More Problems in Serverless!

Inter-function isolation is fine, but not enough!

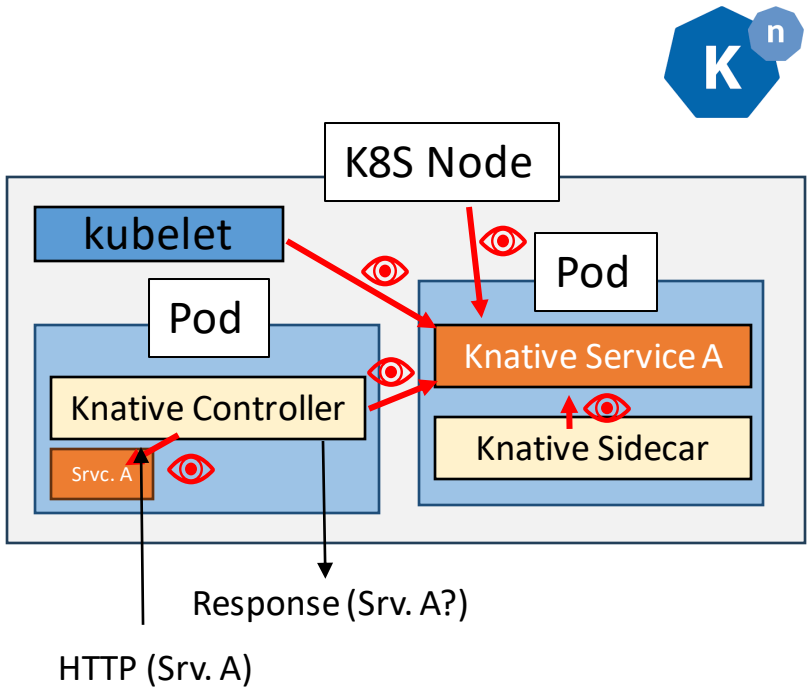


Introduction: More Problems in Serverless!

Inter-function isolation is fine, but not enough!

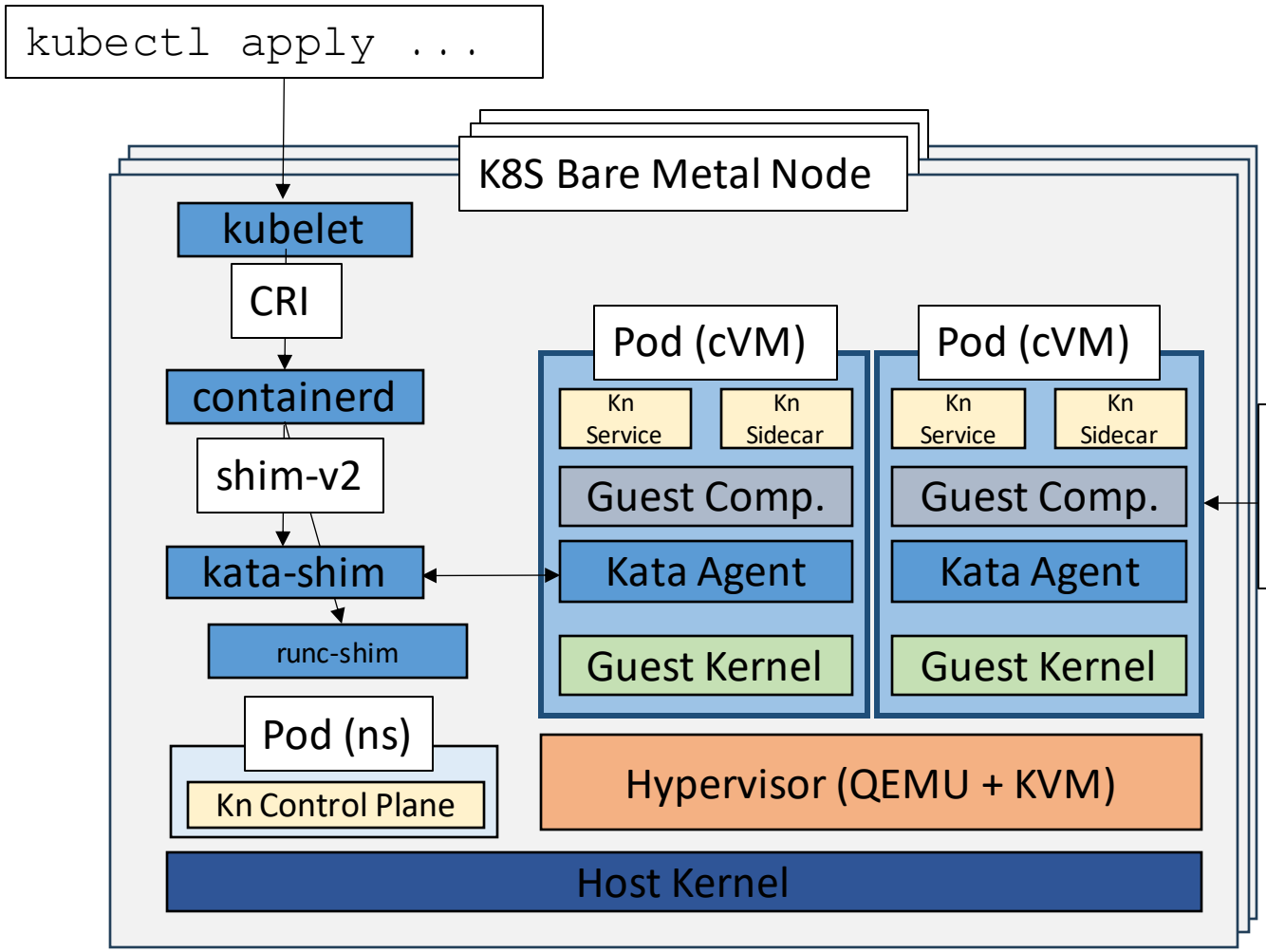
We need isolation from the host environment to guarantee...

- Data Confidentiality
- Code Confidentiality
- Execution Integrity



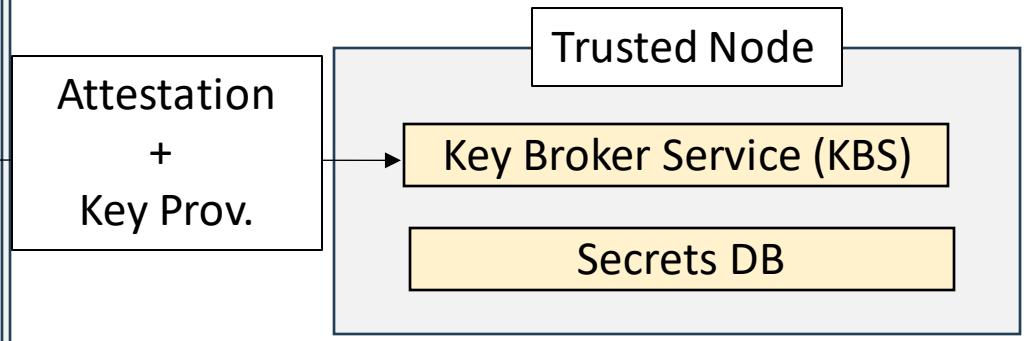
Confidential Computing

PoC: Knative on Confidential Containers



CONFIDENTIAL CONTAINERS

https://github.com/confidential-containers

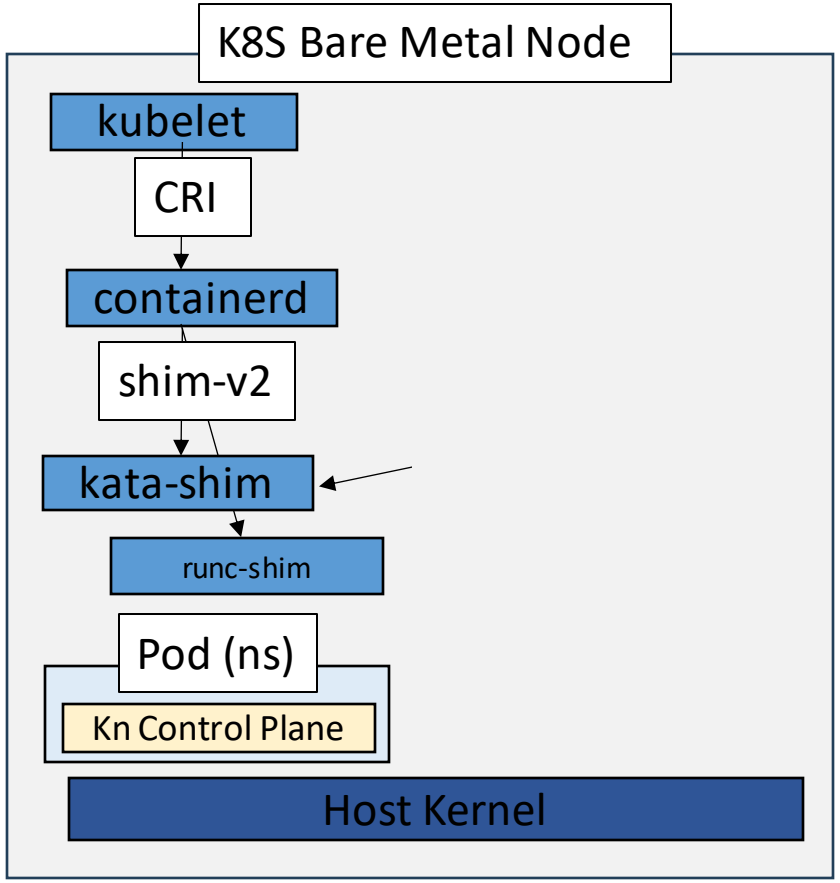


Evaluation

We want to evaluate the feasibility of our PoC according to the three key metrics we identified for serverless:

	1. Cold Start Times	2. Warm Start Times	3. Instantiation Throughput
RUNC	6s	1s	1 fps
kata containers	7s	2s	0.5 fps
CONFIDENTIAL CONTAINERS	??	??	??

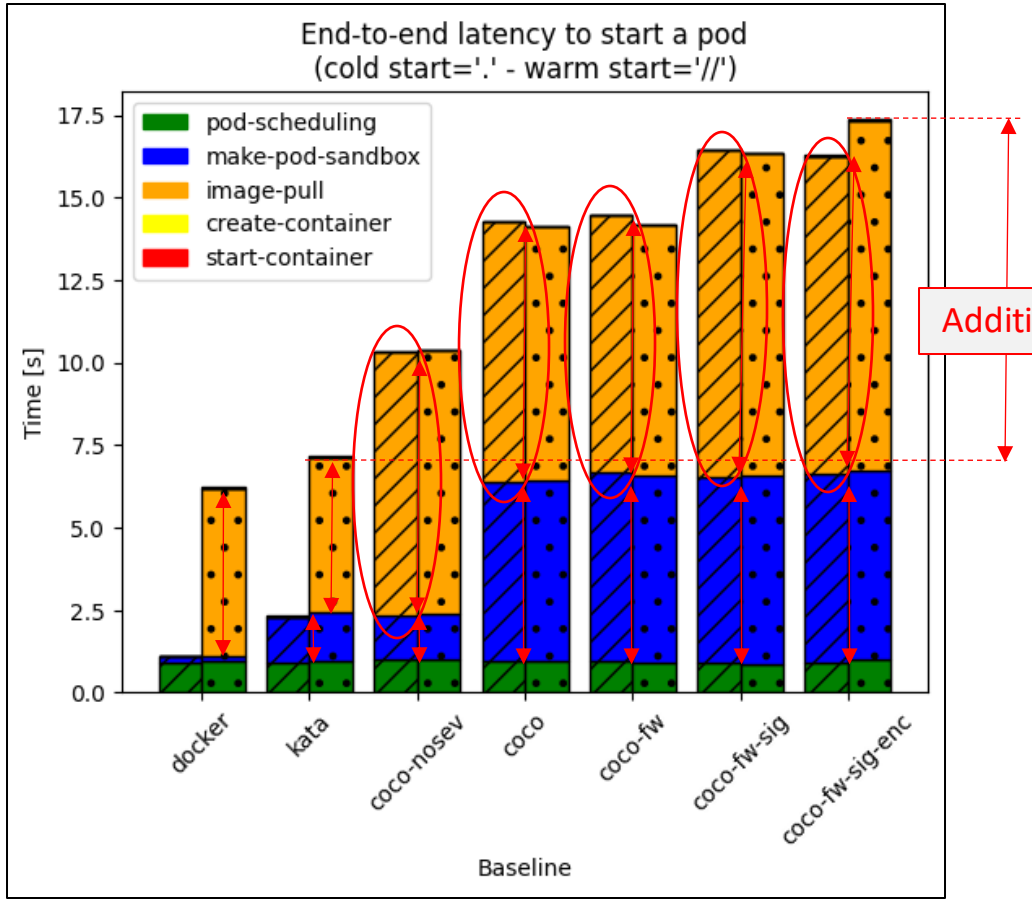
Evaluation: Baselines



0. **docker (i.e. runc):** no VMs
1. **kata:** VMs
2. **coco-nosev:** + pull in guest
3. **coco-nosev-ovmf:** + OVMF
4. **coco:** + SEV
5. **coco-fw:** + HW att
6. **coco-fw-sig:** + image signature
7. **coco-fw-sig-enc:** + image enc.

Knative Service is a simple "Hello World" in Python

Evaluation: Cold/Warm Starts



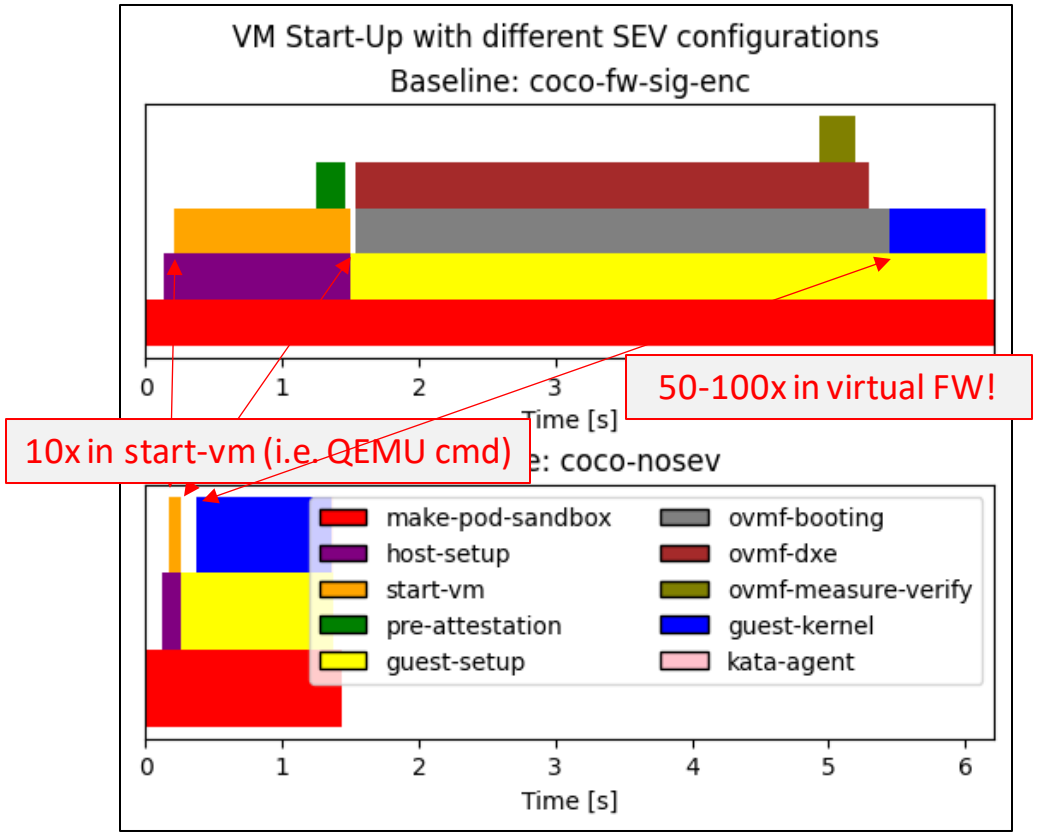
Additional 10 s!

Observations:

1. Why is VM start-up 4x slower with SEV?
2. Why is image pulling 2-3x slower w.r.t docker?
3. Why are there no warm starts?

Let us address these questions one by one

Evaluation: VM Start-Up in detail

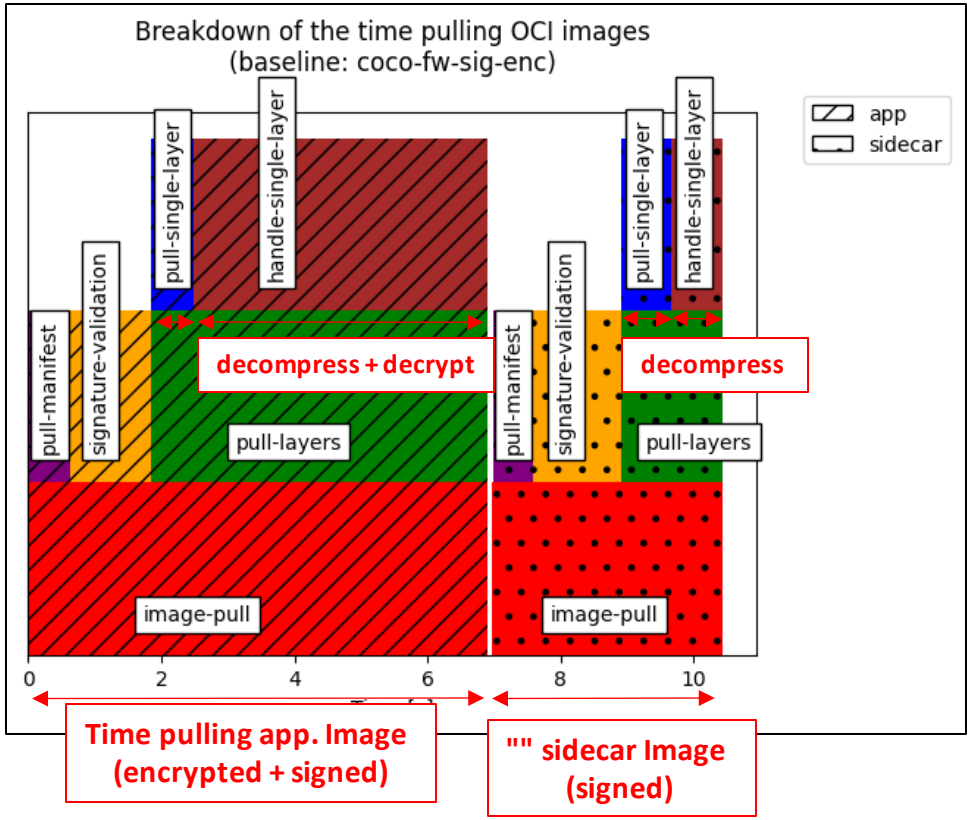


Q1: Why is VM start-up 3x slower with SEV?

start-vm: Provisioning guest memory (pages introduces 1-2 extra seconds (for 2GB of memory)

virtual-fw: OVMF DXE driver initialization introduces 3-4 extra seconds

Evaluation: VM Start-Up in detail

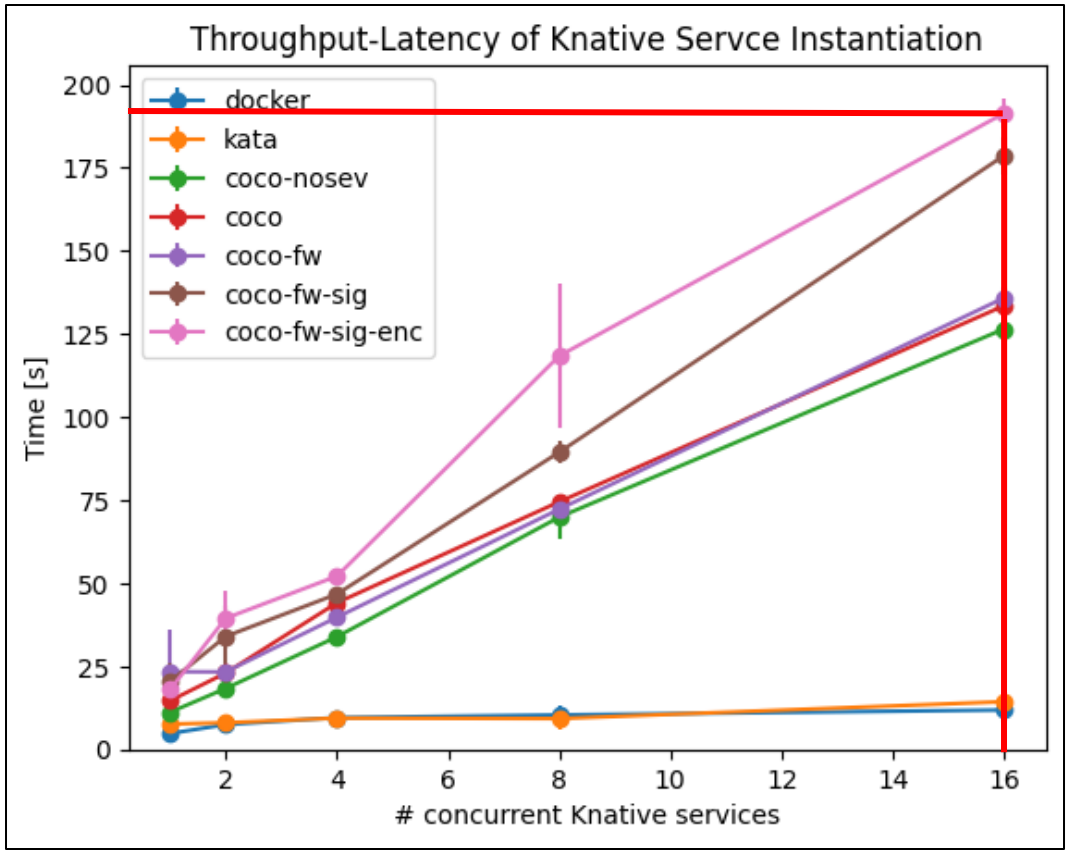


Q2: Why is image-pulling 2x slower w.r.t Docker?

A: containerd's PullImage becomes blocking!

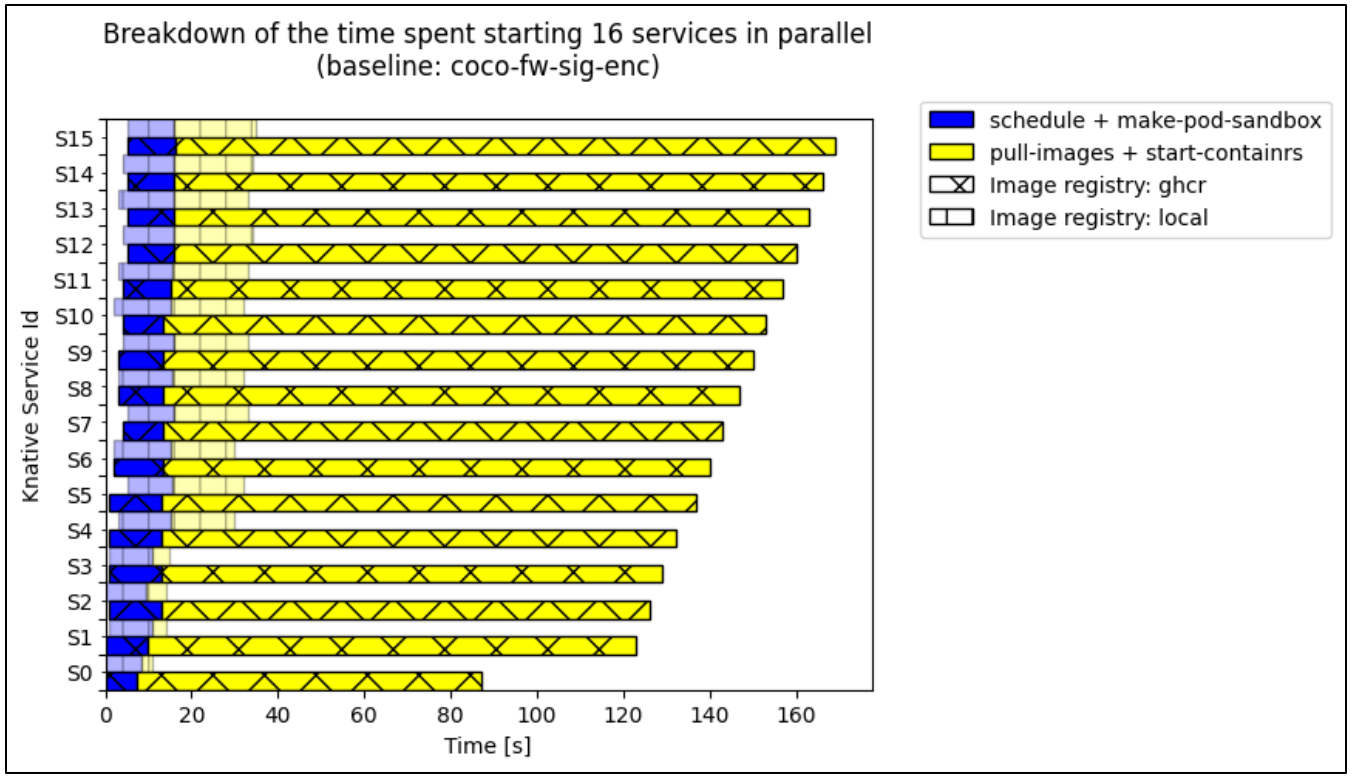
A(ctd): Decrypting image layers is the bottleneck!

Evaluation: Instantiation Throughput



Starting 16 concurrent functions takes > 3' !!

Evaluation: Instantiation Throughput (ctd.)



Q: Why Starting 16 concurrent functions takes > 3'?

A: We are being throttled by the registry!

Evaluation

We want to evaluate the feasibility of our PoC according to the three key metrics we identified for serverless:

	1. Cold Start Times	2. Warm Start Times	3. Instantiation Throughput
RUNC	6s	1s	1 fps
kata containers	7s	2s	0.5 fps
CONFIDENTIAL CONTAINERS	17.5 s	17.5 s	~ 0.1 cps

Imperial College London

LSDS
Large-Scale Data & Systems Group

Serverless Confidential Containers: Challenges and Opportunities

Carlos Segarra

(w/ Tobin Feldman-Fitzthum and Daniele Buono)

Large-Scale Data & Systems (LSDS) Group - Imperial College London

Visiting IBM TJ Watson (Sep'23 – Nov'23)

https://carlossegarra.com
<cs1620@ic.ac.uk>

CLOUD STARS

IBM TJ Watson – Thursday, November 16th 2023