Agentless Cloud-wide Monitoring of Virtual Disk State

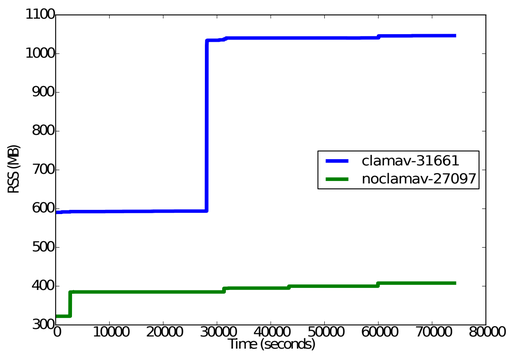
Wolfgang Richter*, Canturk Isci †, Benjamin Gilbert*, Jan Harkes*, Vasanth Bala †, Mahadev Satyanarayanan*
(*Carnegie Mellon University, †IBM Research)

Problem

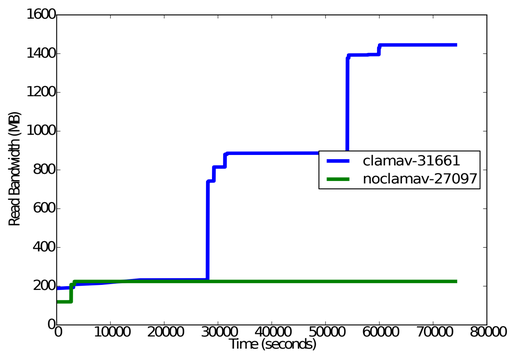
Can we **externalize** virus scanning, log monitoring, and **common administrative processes**?
Can we gain anything by observing **collections of similar VMs**?

Potential Quantitative Gains

Memory (2.6x)



Read BW (6.4x)

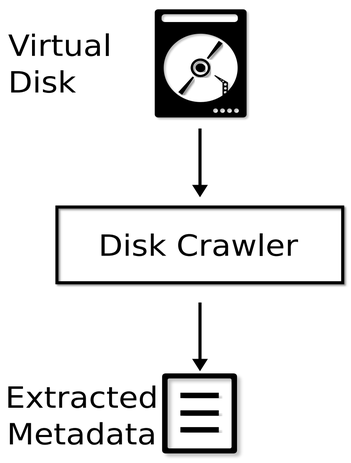


Qualitative Gains

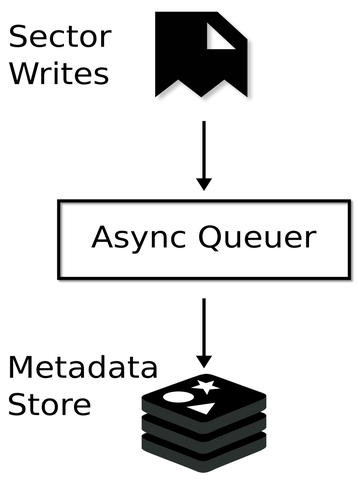
- Reduce attack surface
- Failure independent from VM instances
- Security independent from VM compromise
- Centralized monitoring reducing duplicated in-VM work
- Decouple monitor resource usage from production workloads

Distributed Streaming Virtual Machine Introspection

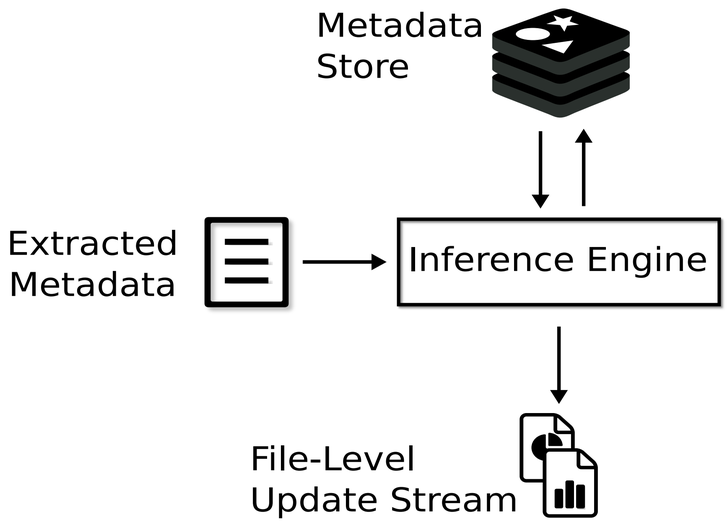
1. Crawl Virtual Disk



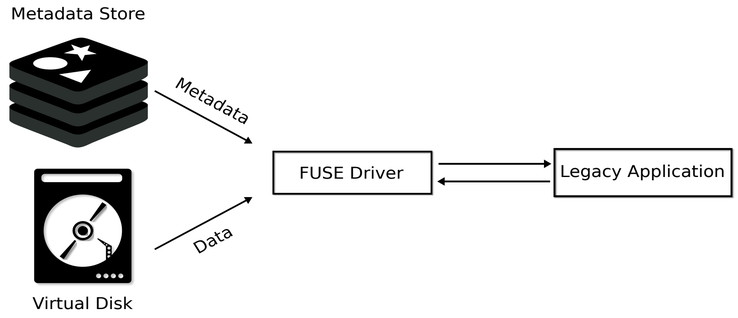
2. Intercept Virtual Writes



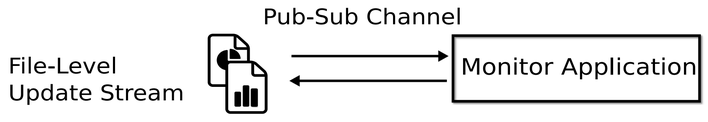
3. Infer File-Level Updates



4a. Interface: `/cloud`



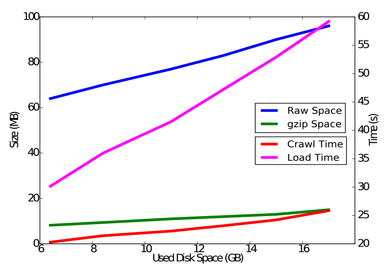
4b. Interface: `cloud-inotify`



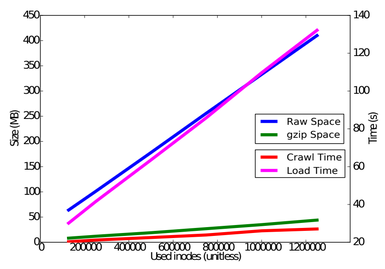
Evaluation

Crawl Overhead

vs Used Space

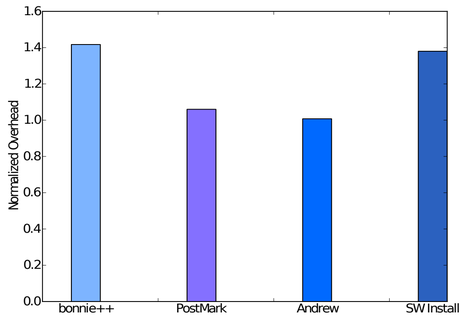


vs Used Inodes

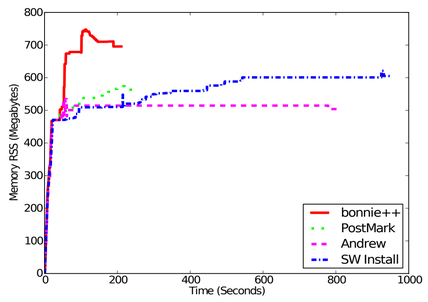


VM/VMM Overhead

Benchmarks

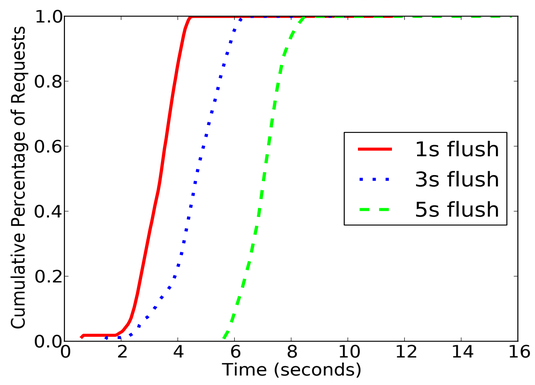


Redis Memory Usage

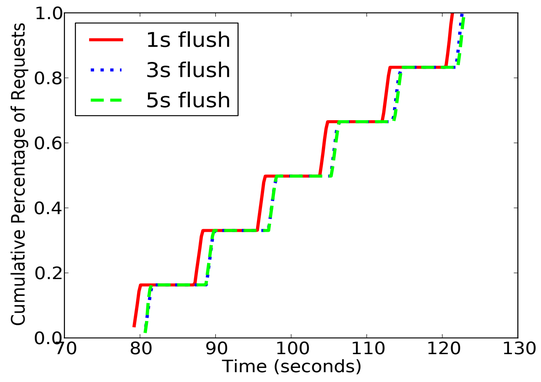


Crawl Overhead

Tuned Guest



Untuned Guest



Intel Science & Technology Center for Cloud Computing

Carnegie Mellon University · Georgia Tech · intel · Princeton University · UC Berkeley · University of Washington