Retrospecting VM Images

Wolfgang Richter

Glenn Ammons*, Jan Harkes, Adam Goode, Vasanth Bala*, Nilton Bila+, Eyal de Lara+, Mahadev Satyanarayan

PARALLEL DATA LABORATORY
Carnegie Mellon University
Roadmap

• What is the retrospection problem?
• What are the main challenges?
• How can we solve them?
Retrospection

- VM Collections Growing
  - 300% Year over Year, IBM Research RC2

- System, Application, and User Content

- Searchable History
  - Debugging Opportunities
  - Legal Data or Code Origin
  - Malware Tracking
  - License Violations
A search computation should only be performed on demand for a specific query, and its scope should be restricted to the smallest relevant subset of VM images.

PRINCIPLE 1
Control of policy for retrospection should reside with the owners of VM images and their delegates.

PRINCIPLE 2
The retrospection mechanism should place as few constraints as possible on the code used for search computations.

PRINCIPLE 3
Find The Picture

• Rich Content-Based and Application-Specific Queries

• 10 Images OK

• 100 Images OK

• 1000+ Images ?
OpenDiamond Platform

- Distributed, Unindexed Search
- Focuses on the principle of early discard
- Enables Arbitrary Search Queries
  - Arbitrary x86 Binary Code
Available Structured Data

• VM’s have Attributes and Metadata
  • Owners
  • Files
  • File Systems

• Files have Attributes and Metadata
  • Owners
  • File Type
  • Permissions
Scoping Solution

- Metadata MySQL Database
- Scope Server
  - Manage Access to Data
- Scope Cookie
  - X.509 Signed Cookie
  - Determines Accessible Data
Problem: VM Sprawl

![Graph showing the relationship between VM Images and Files (Thousands)]
Problem: VM Sprawl

![Graph showing the growth of VM images in GB over time](image-url)
Solution: Deduplication

![Graph showing deduplication process]

Files (Thousands) vs. VM Images over Time

- Raw
- Deduplicated

Wolfgang Richter © October 10
http://www.pdl.cmu.edu/
Solution: Deduplication

![Graph showing space usage by VM images with and without deduplication]
IBM Research Mirage

- Deduplicates Files
  - Referenced by SHA-1 Tag

- Reads VM Image Partitions and File Systems

- On-Disk Deduplicated Format

- Centralized VM Store
Network Bottlenecks

Concurrent Retrievers vs MB/Sec

Carnegie Mellon
Parallel Data Laboratory
http://www.pdl.cmu.edu/
Network Bottlenecks

![Graph showing network bottlenecks](image-url)
Dataretriever

• Abstract Data Source

• Interface with Deduplicated Data Efficiently

• Enable Partitioning of Data if Needed
  • Compute on Local Data
Architecture

Client → Scope → Mirage

Server → Dataretriever → Mirage

Server → Dataretriever

MySQL
Remember Network Bottlenecks
CPU-Bound Search Process

[Bar chart showing Objects per Second for different storage architectures and plug-ins]

- Raw Random
- Raw Linear
- Null Plug-in
- RGB Plug-in

Storage Architecture:
- Single HDD
- RAID1 HDD
- Single SSD
Achievable Efficient Retrospection

Interarrival time (seconds)

Probability

Local

Mirage

http://www.pdl.cmu.edu/
Current Research: Principle 2

• Control of Policy to Owners via Encryption

• **Proof of Concept**: Convergent Encrypt /home
  • Encrypt Files Using File Hash as Key

• Future Direction: Key Escrow?
  • Support Investigations
Recap

• **Retrospection** – Search VM Image Content

• **Main Challenges**
  1. Get Data Efficiently
  2. Handle Big and Growing Data

• Introduced **Scoping** and **Dataretriever**
Questions?