Digital Forensics, Incident Response, and Cloud Computing

Troy Larson
Azure | MSRC
Microsoft Corp.
Forensics, Response, Cloud Computing

• MSRC | Azure
  • Security incident response investigations.
    • Forensics @ Microsoft.
    • Compromise | Intrusion | Breach.
    • Forensics and incident response investigations for the cloud.
What is cloud computing?

• Insider’s view of cloud computing:
  • Technology overview.
  • Policy.
  • Forensics and Incident response.
    • Practices.
    • Challenges.
    • Opportunities.
What is cloud computing?
What is cloud computing?

• *Automated* datacenter, where *machines* are-
  • Deployed by machine.
  • Managed by machine.
  • Monitored by machine.
  • For services.
  • For tenants.
Azure Technical Overview

- Collection of automated datacenters.
  - Primary resources:
    - Compute.
    - Storage.
    - Network.
Azure Technical Overview

• Datacenters.
  • Clusters.
    • Nodes (blades).
Azure Technical Overview

• Compute node (host server).
Azure Technical Overview

- Virtual machine, from the host.
Azure Technical Overview

• The *persistent* virtual hard drive.
The virtual hard drive.

- To the host, *a file*.
- To the virtual machine, *a physical disk*.
  - Partitioned and formatted to create volumes and file systems.
  - Can be organized like physical hard drives:
    - Single disks.
    - Dynamic volumes—volumes spanning virtual disks.
    - RAID.
Azure Technical Overview

• Virtual machine memory.

Page File on VHD
Azure Technical Overview

- Virtual machine, from within.
Azure Technical Overview

• Different viewpoints.
  • On the host side of the hypervisor:
    • Memory is guest physical address space.
    • Disks are files.
  • On the guest side of the hypervisor:
    • Memory consists of virtual and physical address space.
    • Disk appear as physical and logical media.
Privacy: You own and control your data

For more than 20 years, Microsoft has been a leader in creating robust online solutions designed to protect the privacy of our customers. Our time-tested approach to privacy and data protection is grounded in our commitment to organizations’ ownership of and control over the collection, use, and distribution of their information.

We strive to be transparent in our privacy practices, offer you meaningful privacy choices, and responsibly manage the data we store and process. One measure of our commitment to the privacy of customer data is our adoption of the world’s first code of practice for cloud privacy, ISO/IEC 27018.

You own your own data. With Azure, you have ownership of customer data—that is, all data, including text, sound, video, or image files and software, that are provided to Microsoft by you, or on your behalf, through the use of Azure. You can access your customer data at any time and for any reason without assistance from Microsoft. We will not use customer data or derive information from it for advertising or data mining.

You are in control of your data. Because the customer data you host on Azure belongs to you, you have control over where it is stored and how it is securely accessed and deleted.
Policy

• Cloud administrators and security teams:
  • Extremely limited visibility into what is happening with tenant VMs.

• Tenant administrators and security teams:
  • Complete visibility into what is happening on their VMs.
  • No visibility into what is happening on other tenant VMs or host or infrastructure.

• Security responsibility follows ownership.
Policy

• Security.
  • Shared Security Model:
    • Management.
    • Ownership.
Policy

• Security incident.
Forensics, Response, Cloud Computing

Evidence Acquisition of Cloud-Based Machines
Forensics, Response, Cloud Computing

• Virtual machines, acquisition.
Forensics, Response, Cloud Computing

Host / VM
- Memory
  - As GPA.
  - As saved state file(s).
- Media
  - As files.
  - As blobs.
- Network
  - From virtual switch.

Guest / VM
- Memory
  - Live.
- Media
  - As physical or logical disks.
  - As blobs.
- Network
  - Live.
Forensics, Response, Cloud Computing

**Host / VM**
- Running or stopped.
- State can be frozen.*
- No collection artifacts.*
- Consistent memory and disk images.*

**Guest / VM**
- Running.
- State is dynamic.
- Collection artifacts.
- Inconsistent memory and disk images.

![Diagram showing Host / VM and Guest / VM with differences in storage and artifacts]
<table>
<thead>
<tr>
<th>Host / VM</th>
<th>Guest / VM</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Cloud provider.</td>
<td>• Tenant.</td>
</tr>
</tbody>
</table>
Forensics, Response, Cloud Computing

• Tenant evidence acquisition:
  • Standard remote collection procedures and tools should work for acquiring cloud-based VMs.*
  • Blob storage of virtual disks allows for quick acquisition or snapshots of virtual disks.
  • Equivalent to, or better than, current enterprise remote evidence collection capability.*
Forensics, Response, Cloud Computing

• Cloud infrastructure.
  • Consists of hundreds of thousands of physical machines.
    • Huge amounts of RAM.*
    • Huge amounts of disk storage.*
    • Novel disk storage technologies.*
    • Under extremely heavy load.*

• Can exceed the capability of current forensics tools and practices.
Forensics, Response, Cloud Computing

• Cloud infrastructure.
  • Network is not a standard corporate network.
    • No domain authentication.
    • Segmented.
    • Firewalled.

• Standard enterprise remote evidence tools and procedures often will not work.
Forensic Analysis
Of
Cloud-Based Machines
Forensics, Response, Cloud Computing

• Cloud machines:
  • Use standard operating systems.
  • Common, well known file systems, file types, structures, and strings.
  • Amenable to standard analytical tools and procedures.
  • Subject to compromise, breach, and other common sport.
Forensics, Response, Cloud Computing

• Security incident response and *stateless* virtual machines.
  • PAAS designed to be stateless.
    • Scalability and fault tolerance.
    • Persistent data goes to storage.
    • New instance starts clean.
  • Remediation by command line.

• What is the point of doing forensics or other in-depth security incident investigation?
Forensics, Response, Cloud Computing

• Cloud (virtual) machine advantages.
  • From host:
    • Fully consistent memory dumps.
    • Fully consistent drive (volume) images.
    • State files.

• By tenant:
  • Fully consistent drive images from storage.*
Forensics, Response, Cloud Computing

• Issues of scale and scalability.
  • Cloud infrastructure is vast.
  • Cloud environment is more vast.
  • Virtual entities can be dynamic, and endpoints ephemeral.

• Tenant deployments can be vast and dynamic, too.
Forensics, Response, Cloud Computing

• Cloud-ready incident response and forensics:
  • Must be able to work at scale.
  • Must be scalable—monitoring, triage, log analysis, forensics.*

• Problem:
  • DF/IR is dependent on subject matter expertise.
  • Subject matter experts do not scale well.*
Forensics, Response, Cloud Computing

Research topics.
Forensics, Response, Cloud Computing

• *What is normal?*

The analytical opportunities of scale.

*Jesse Kornblum*

Forensics, Response, Cloud Computing

• Cloud machines | “Roles” | \( n \) identical instances.
  
  • *Role instances:*
    • xyz-service-01_of_200
    • xyz-service-02_of_200
    • xyz-service-03_of_200
    • \ldots
    • xyz-service-56_of_200
Forensics, Response, Cloud Computing

• *Role Instances:*
  • Same OS VHD.
  • Same hardware and drivers.
  • Same configuration settings.
  • Same applications and services.
  • Same processes and command lines.
  • Same events.
Forensics, Response, Cloud Computing

• Processes creation event (Sec Event ID 4688):
  • New process name and path.
  • Parent process.
  • Command line.
  • Account that launches the process.

• What processes run in exactly the same way, on all role instances?
Forensics, Response, Cloud Computing

• Role-specific, event baselines:
  • Identical 4688 events, across all instances (per role), show what runs, how, by what account.
    • *What is normal for any instance of that role.*
    • Usage: *Compare individual to the herd.*
      • Detection and monitoring.
      • Live analysis and triage (e.g., Kansa).
      • Memory forensics.
      • Disk forensics.
Forensics, Response, Cloud Computing

• Role-specific, event baselines:
  • Signal to noise: non-identical 4688 events.
  • Unique for a role instance.
    • Anomalous, may indicate security issue.
  • Usage: *What stands out against the herd.*
    • Detection and monitoring.
    • Hunting.
Forensics, Response, Cloud Computing

• What other herd behavior can indicate normal or highlight anomalies?
  • Task scheduler and service events.
  • Object access events?
  • Logon, source IP address?
  • Error and failure events?
  • IPFIX?
  • Prefetch?
  • Amache.hve?
Forensics, Response, Cloud Computing

Questions?