
Josiah Dykstra and Alan T. Sherman

August 6, 2013
The views expressed in this presentation are mine alone. Reference to any specific products, process, or service do not necessarily constitute or imply endorsement, recommendation, or favoring by the United States Government or the Department of Defense.
Takeaway

FROST provides carrier-grade, user-driven, trustworthy forensic acquisition of cloud-based:
INTRODUCTION
An Investigator’s View
Setting the Stage

![Graph showing network traffic over time. The graph has a y-axis labeled 'Bits per Second' with values up to 108.0 k, and an x-axis with a range from 4 to 10. The graph displays peaks and valleys representing network activity.]
The AWS Management Console provides a graphical interface to Amazon Web Services. Learn more about how to use our services to meet your needs, or get started by selecting a service.
Cloud Layers

Service Layers Definition

Notes:
Brand names for illustrative / example purposes only, and examples are not exhaustive.

http://www.katescomment.com/iaas-paas-saas-definition/
<table>
<thead>
<tr>
<th>Instance Name</th>
<th>IP Address</th>
<th>Size</th>
<th>Keypair</th>
<th>Status</th>
<th>Task</th>
<th>Power State</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>My First Instance</td>
<td>10.0.0.3</td>
<td>m1.tiny</td>
<td>512MB RAM</td>
<td>1 VCPU</td>
<td>0 Disk</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
REQUIREMENTS
“Digital Evidence submitted for examination should be maintained in such a way that the integrity of the data is preserved. The commonly accepted method to achieve this is to use a hashing function.” (SWGDE 2005)
Technical Requirements

“The two critical measurable attributes of the acquisition process are completeness and accuracy. Completeness measures if all the data was acquired, and accuracy measures if the data was correctly acquired.” (NIST 2004)
Requirements

- Be compatible with existing forensic formats.
- Be easy to generate.
- Be open and extensible.
- Be scalable.
- Follow existing practices and standards.
Rule 901. AUTHENTICATING OR IDENTIFYING EVIDENCE

(a) In General. To satisfy the requirement of authenticating or identify an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.

(b) ... 

9) Evidence about a Process or System. Evidence describing a process or a system and showing that it produces an accurate result.

Federal Rules of Evidence
http://www.law.cornell.edu/rules/fre/rule_901
DESIGN
Data Retrieval

- Virtual Disk Images
- Host Firewall Logs
- API Logs
2012-12-01 13:30:49 INFO nova.api.openstack.wsgi [req-0afcfbcd-b836-4593-a02c-25d8d3a94b00 admin demo] POST
http://10.34.50.142:8774/v2/5ee3040fa890428387f56111576cf819/servers
2012-12-01 13:30:49 DEBUG nova.quota [req-0afcfbcd-b836-4593-a02c-25d8d3a94b00 admin demo] Created reservations ['915e9c89-b3bc-4091-8b75-3b555961ec3e', '72c39d24-0a96-42ca-96f1-56-872b-4b40-a853-2aa7c730262e'] from (pid=16036) reserve /opt/stack/nova/nova/quota.py:697
2012-12-01 13:30:50 DEBUG nova.compute.api [req-0afcfbcd-b836-4593-a02c-25d8d3a94b00 admin demo] Going to run 1 instances... from (pid=16036) _create_instance /opt/stack/nova/nova/compute/api.py:492
2012-12-01 13:30:50 DEBUG nova.openstack.common.rpc.amqp [-] Making asynchronous cast on scheduler... from (pid=16036) cast /opt/stack/nova/nova/openstack/common/rpc/amqp.py:376
IMPLEMENTATION
Web Interface

Instance Detail: My First Instance

Instance Incident Response Tasks

- Download Nova API Logs
- Download Host Firewall Logs
- Download Disk Image
<?xml version='1.0' encoding='UTF-8'?>
<dfxml xmloutputversion='1.0'>
  <creator version='1.0'>
    <program>FROST</program>
    <version>1.0</version>
  </creator>
  <execution_environment>
    <os_sysname>Linux</os_sysname>
    <os_release>3.2.0-25-virtual</os_release>
    <os_version>#40-Ubuntu SMP Thu Nov 29 22:20:17 UTC 2012</os_version>
    <host>domU-12-31-39-17-29-5D</host>
    <arch>x86_64</arch>
  </execution_environment>
</dfxml>
<fileobject>
  <filename>/opt/stack/data/nova/instances/instance-00000003/disk</filename>
  <filesize>6946816</filesize>
  <ctime>2012-11-29T11:51:49Z</ctime>
  <mtime>2012-11-29T11:51:49Z</mtime>
  <atime>2012-11-29T11:52:07Z</atime>
  <hashdigest type='SHA1'>8891608acfc13472bd2ca7dc409e973bf112bce3</hashdigest>
</fileobject>

<rusage>
  <utime>0.036002</utime>
</rusage>
$ nova get-nova-logs 0afcfbcd-b836-4593-a02c-25d8d3a94b00 verify.xml

[truncated]
2012-12-01 13:30:49 INFO nova.api.openstack.wsgi [req-0afcfbcd-b836-4593-a02c-25d8d3a94b00 admin demo] POST http://10.34.50.142:8774/v2/5ee3040fa890428387f56111576cf819/servers
2012-12-01 13:30:49 DEBUG nova.quota [req-0afcfbcd-b836-4593-a02c-25d8d3a94b00 admin demo] Created reservations ['915e9c89-b3bc-4091-8b75-3b555961ec3e', '72c39d24-0a96-42ca-96f1-593da3aa9f81', '57843316-872b-4b40-a853-2aa7c730262e'] from (pid=16036) reserve /opt/stack/nova/nova/quota.py:697
2012-12-01 13:30:50 DEBUG nova.compute.api [req-0afcfbcd-b836-4593-a02c-25d8d3a94b00 admin demo] Going to run 1 instances... from (pid=16036) _create_instance /opt/stack/nova/nova/compute/api.py:492
[truncated]
Firewall Logs API

$ nova get-firewall-logs 0a18799f-c198-4dbb-b369-b49184e3dfbc verify.xml

0a18799f-c198-4dbb-b369-b49184e3dfbc: Nov 28 11:13:38 domU-12-31-39-17-29-5D kernel: [ 310.765760] IPTables-Dropped: IN=eth0 OUT=
MAC=12:31:39:17:29:5d:fe:ff:ff:ff:ff:ff:08:00 SRC=130.85.36.72 DST=10.97.42.171 LEN=52 TOS=0x00 PREC=0x00 TTL=48 ID=29222 DF Proto=TCP SPT=55739 DPT=443 WINDOW=1002 RES=0x00 ACK URG=0

0a18799f-c198-4dbb-b369-b49184e3dfbc: Nov 28 11:13:36 domU-12-31-39-17-29-5D kernel: [ 309.623023] IPTables-Dropped: IN=eth0 OUT=
MAC=12:31:39:17:29:5d:fe:ff:ff:ff:ff:ff:08:00 SRC=172.16.0.23 DST=10.97.42.171 LEN=103 TOS=0x00 PREC=0x00 TTL=64 ID=42188 Proto=UDP SPT=33905 DPT=53 LEN=83
[truncated]
Disk Image API

$ nova get-disk myvol-e9a5612d report.xml
MD5:   b17ee04095b2a3d81eed98628072eab6
SHA1:  399f5ffaccd09fe43d642d5f0d996875ca650c9f

$ sha1sum myvol-e9a5612d
399f5ffaccd09fe43d642d5f0d996875ca650c9f
Tests for functionality and scalability

- 100 fake users
- 5 VMs per user
- Scan ports 1-1024 on each VM
- Randomly try to stop VMs
- For 20 users download API logs, FW logs, disk images

Live evaluation with users/admins of gov’t cloud
Other Uses

- Data preservation
- E-discovery
- Real-time monitoring
- Metrics
- Auditing
- Other acquisition capabilities
Summary

- Investigators need forensic data
- FROST enables:
  - Independent data acquisition
  - No need to trust Guest OS
  - Scalable to cloud environments
  - Platform for future tools
Questions

dykstra@umbc.edu