Design and Implementation of FROST - Digital Forensic Tools for the OpenStack Cloud Computing Platform

By

Josiah Dykstra and Alan Sherman

Presented At

The Digital Forensic Research Conference

DFRWS 2013 USA Monterey, CA (Aug 4th - 7th)

Design and Implementation of FROST:

Digital Forensic Tools for the OpenStack Cloud Computing Platform

Josiah Dykstra and Alan T. Sherman

August 6, 2013

UMBC
Cyber Defense Lab

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.

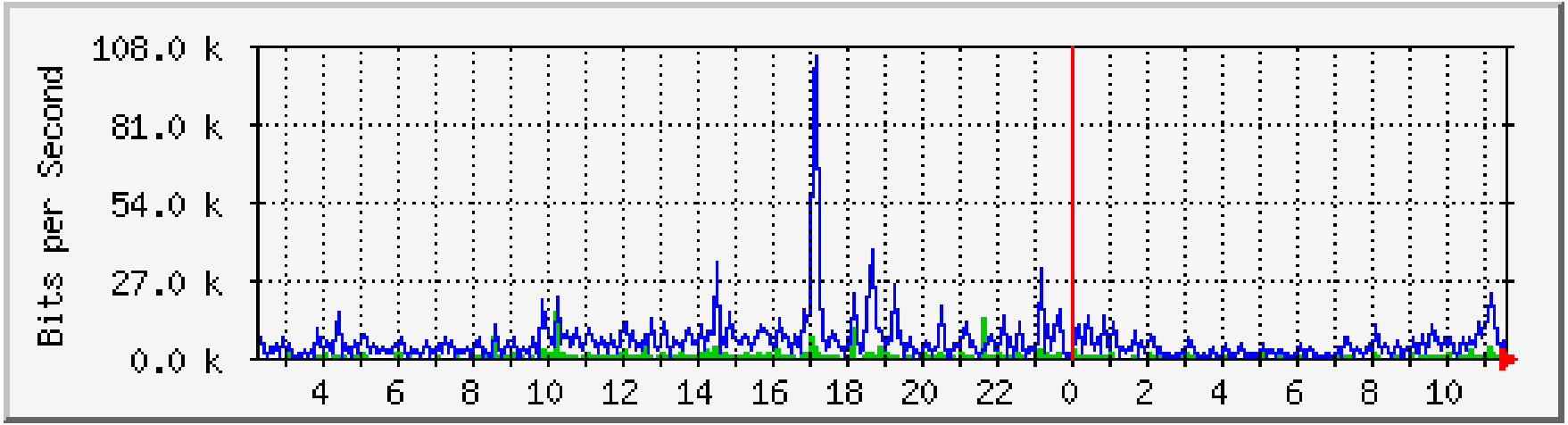
Takeaway

FROST provides carrier-grade, user-driven, trustworthy forensic acquisition of cloud-based:

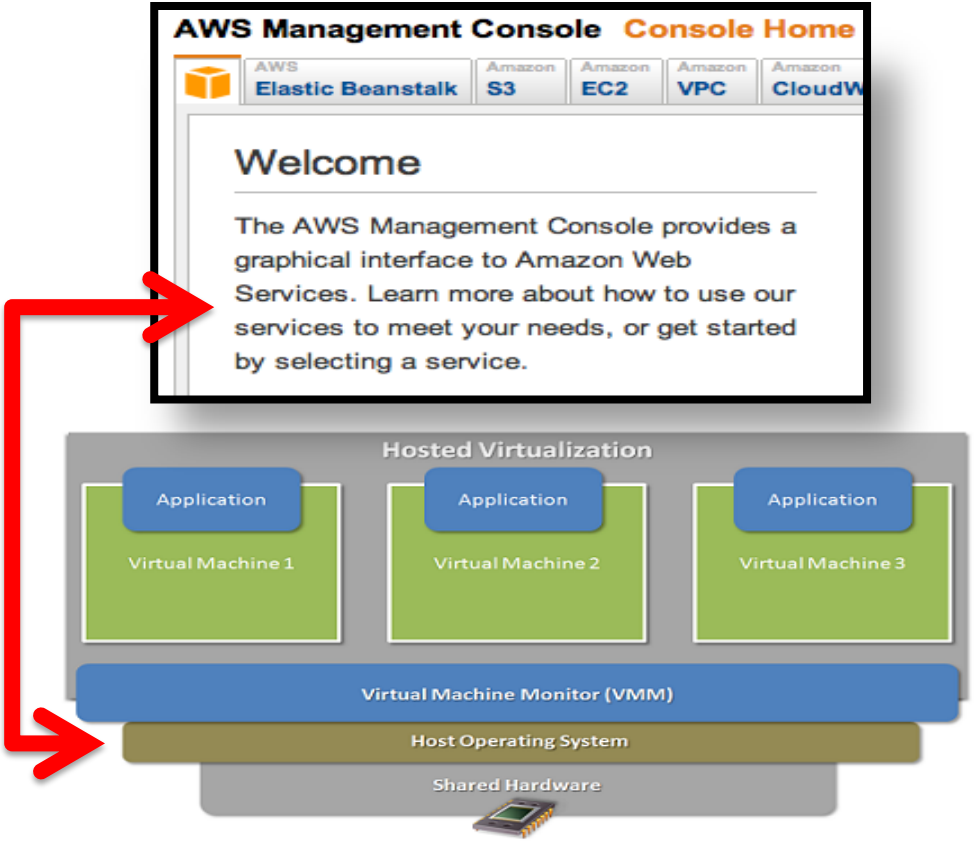
INTRODUCTION

An Investigator's View

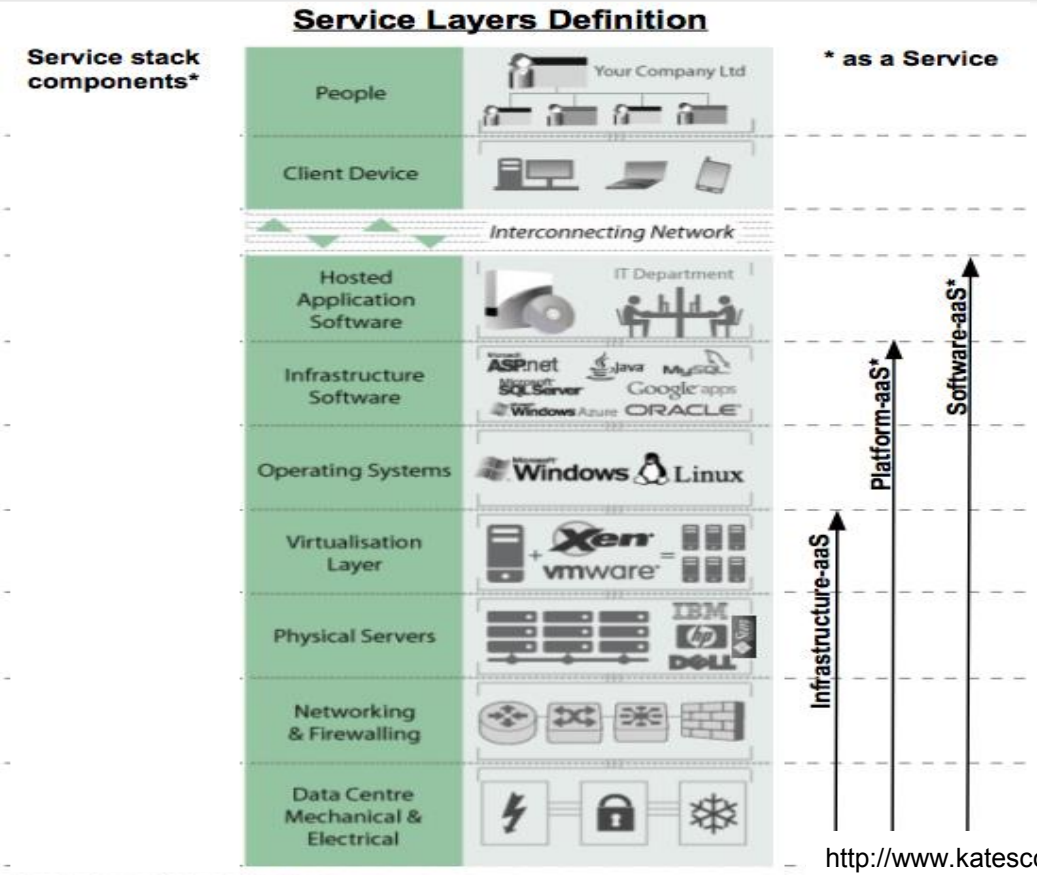
Setting the Stage



The Management Plane

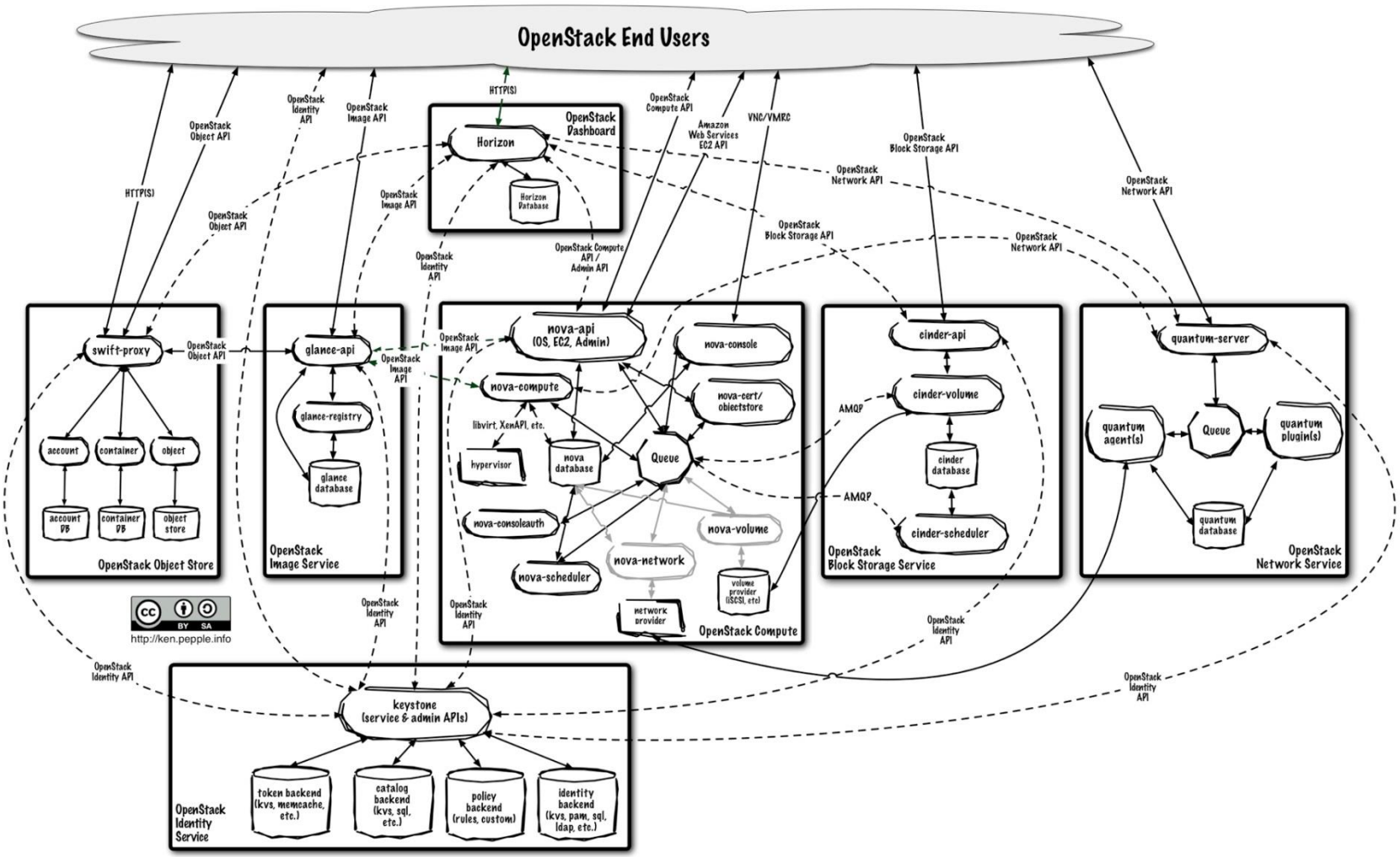


Cloud Layers



http://www.katescomment.com/iaas-paas-saas-definition/

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


OpenStack End Users
HTTP(S)
OpenStack Dashboard
Horizon
Horizon Database
OpenStack Object API
OpenStack Identity API
OpenStack Image API
OpenStack Compute API
Amazon Web Services EC2 API
VNC/VMRC
OpenStack Block Storage API
OpenStack Network API
OpenStack Compute API / Admin API
swift-proxy
account
container
object
account DB
container DB
object store
OpenStack Object Store
glance-api
glance-registry
glance database
OpenStack Image Service
nova-api (OS, EC2, Admin)
nova-console
nova-compute
nova-cert/ objectstore
libvirt, XenAPI, etc.
hypervisor
nova database
Queue
nova-consoleauth
nova-volume
nova-network
nova-scheduler
volume provider (iSCSI, etc)
network provider
OpenStack Compute
cinder-api
cinder-volume
cinder database
cinder-scheduler
AMQP
OpenStack Block Storage Service
quantum-server
quantum agent(s)
Queue
quantum plugin(s)
quantum database
OpenStack Network Service
keystone (service & admin APIs)
token backend (kvs, memcache, etc.)
catalog backend (kvs, sql, etc.)
policy backend (rules, custom)
identity backend (kvs, pam, sql, ldap, etc.)
OpenStack Identity Service
http://ken.pepple.info

ec2-184-72-135-102.compute-1.amazonaws.com/project/instances/

openstack DASHBOARD

Project

CURRENT PROJECT
demo

Manage Compute

Overview

Instances

Volumes

Images & Snapshots

Access & Security

Instances

Logged in as: demo Settings Sign Out

Instances

Launch Instance

Instance Na	te	Actions

Displaying 1 item

Launch Instance

Details | Access & Security | Volume Options | Post-Creation

Instance Source

Image

Image

cirros-0.3.0-x86_64-uec

Instance Name

My First Instance

Flavor

m1.tiny

Instance Count

1

Specify the details for launching an instance.

The chart below shows the resources used by this project in relation to the project's quotas.

Flavor Details

Name	m1.tiny
VCPUs	1
Root Disk	0 GB
Ephemeral Disk	0 GB
Total Disk	0 GB
RAM	512 MB

Project Quotas

Number of Instances (0) 10 Available

Number of VCPUs (0) 20 Available

Total RAM (0 MB) 51,200 MB Available

Cancel Launch

ec2-184-72-135-102.compute-1.amazonaws.com/project/instances/

openstack
DASHBOARD

Project

CURRENT PROJECT
demo

Manage Compute

- Overview
- Instances
- Volumes
- Images & Snapshots
- Access & Security

Instances

Logged in as: demo

Success: Launched instance na
"My First Instance".

Instances

Launch Instance | Term

	Instance Name	IP Address	Size	Keypair	Status	Task	Power State	Actions
☐	My First Instance	10.0.0.3	m1.tiny | 512MB RAM | 1 VCPU | 0 Disk	-	Active	None	Running	Create Snap

Displaying 1 item

REQUIREMENTS

Technical 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 the 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.

Legal Requirements

Rule 901. AUTHENTICATING OR IDENTIFYING EVIDENCE

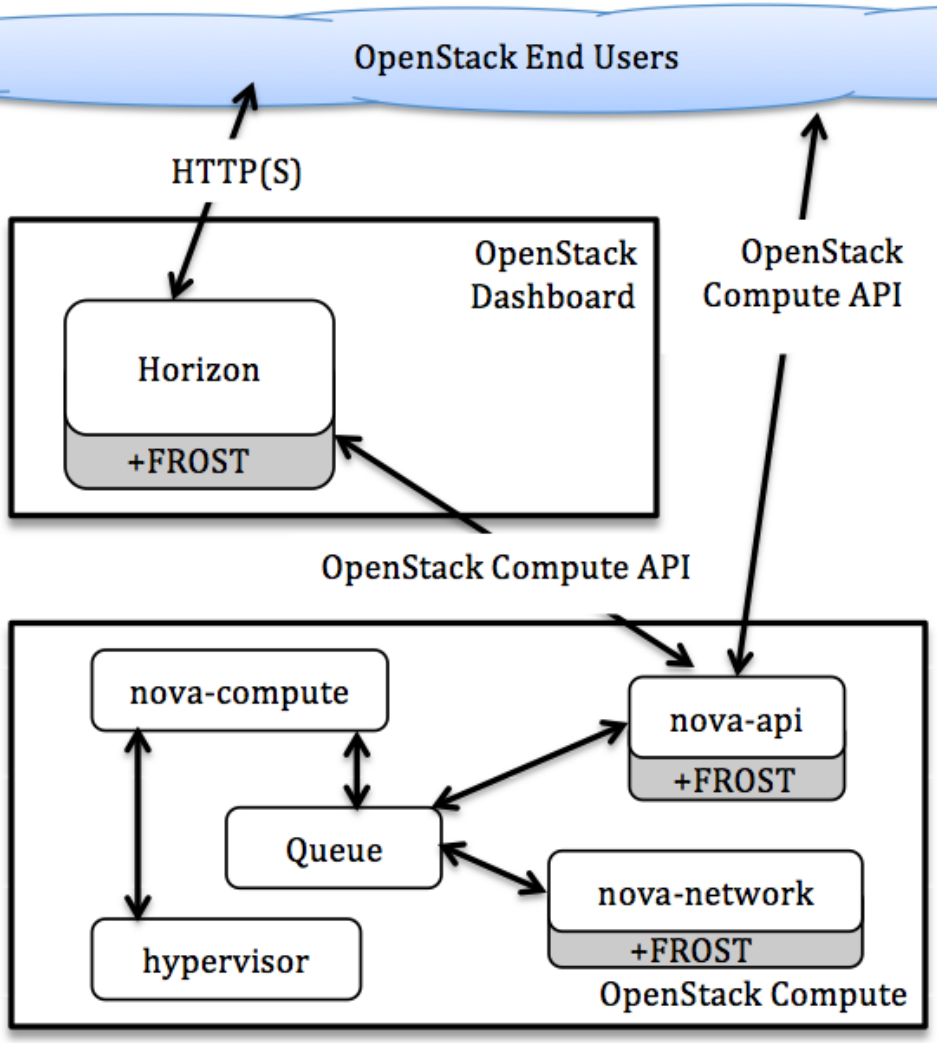
(a) In General. To satisfy the requirement of authenticating or identify an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.

(b) …

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

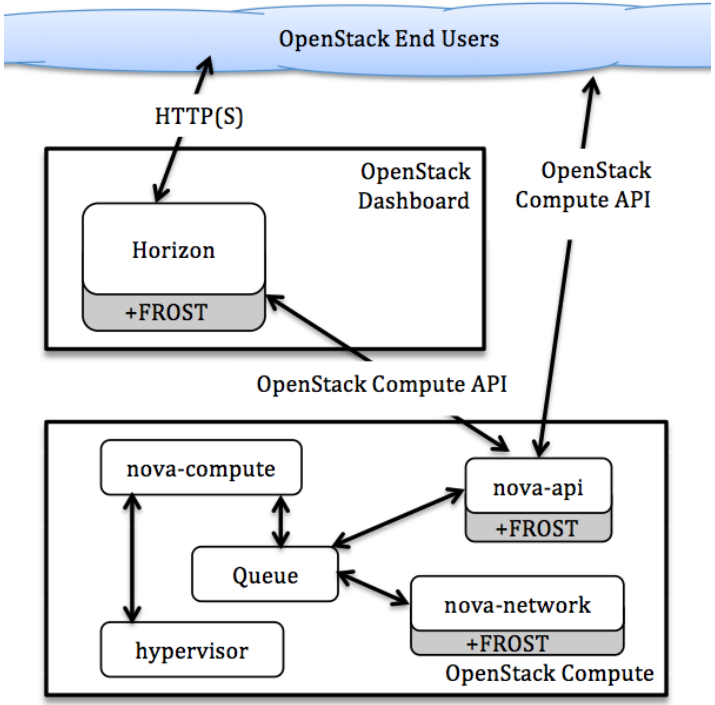
Federal Rules of Evidence
http://www.law.cornell.edu/rules/fre/rule_901

DESIGN


OpenStack End Users
HTTP(S)
OpenStack Dashboard
Horizon
+FROST
OpenStack Compute API
OpenStack Compute API
nova-compute
nova-api
+FROST
Queue
nova-network
+FROST
hypervisor
OpenStack Compute

Data Retrieval

- Virtual Disk Images
- Host Firewall Logs
- API Logs



Logs

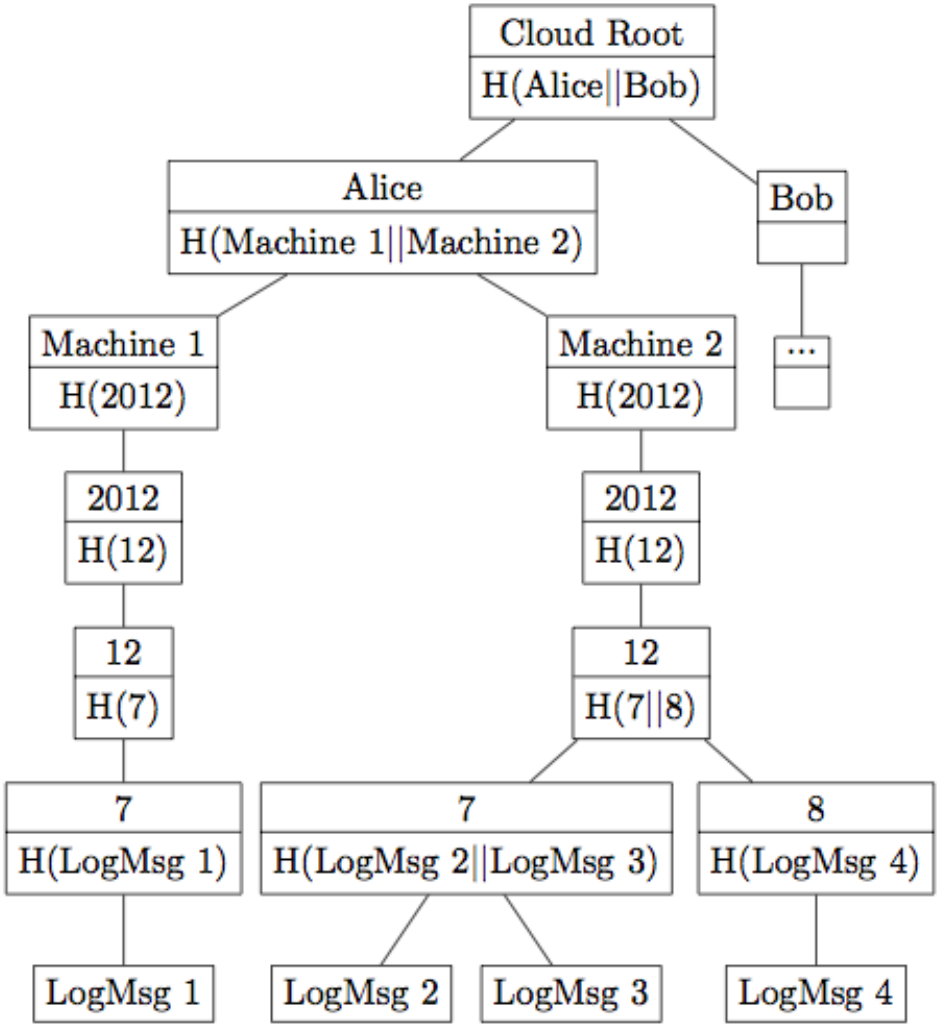
2012-12-01 13:30:49 INFO nova.api.openstack.wsgi [req-0afcfbcd-b836-4593-a02c-25d8d3a94b00 admin demo] POST http://10.34.50.142:8774/v2/5ee30[illegible]8387f56111576cf819/servers

2012-12-01 13:30:49 DEBUG no[illegible]fbcd-b836-4593-a02c-25d8d3a94b00 admin demo] Created reserva[illegible]4091-8b75-3b555961ec3e', '72c39d24-0a96-42ca-96f1-5[illegible]-872b-4b40-a853-2aa7c730262e'] from (pid=16036) reserve /o[illegible]a.py:697

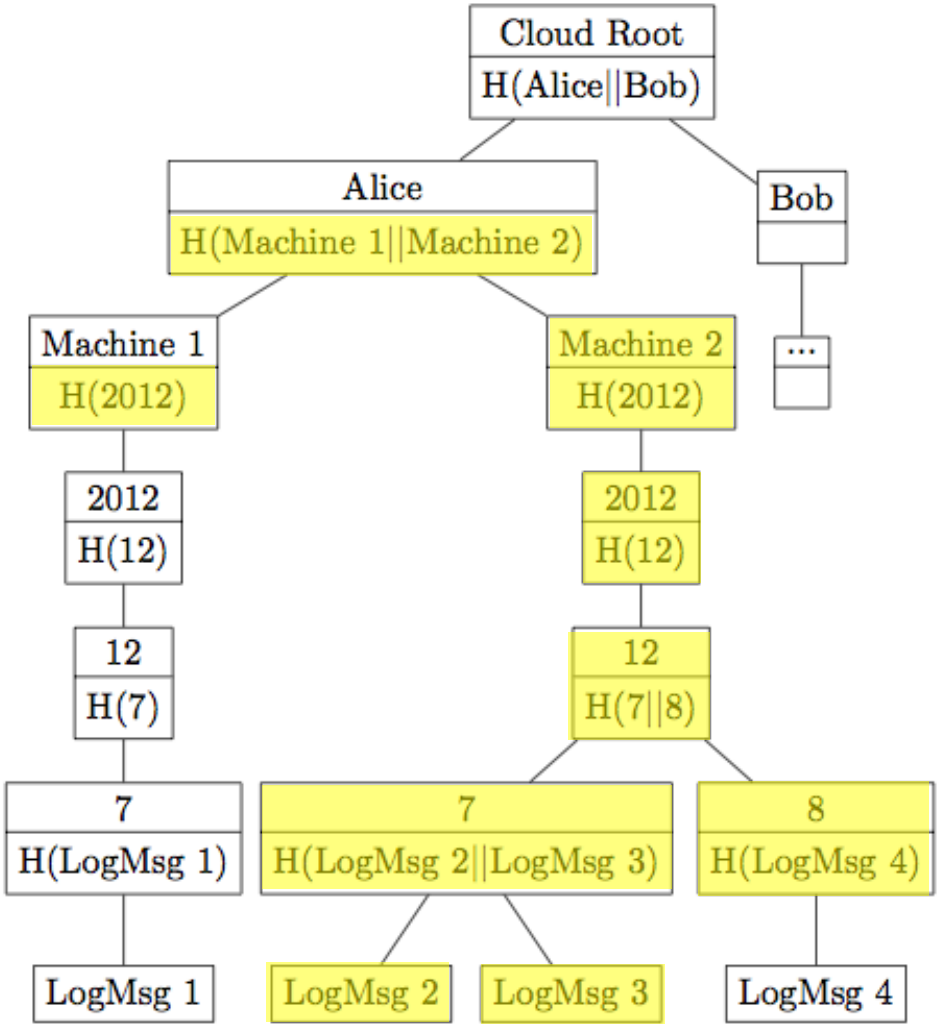
2012-12-01 13:30:50 DEBUG [illegible]0afcfbcd-b836-4593-a02c-25d8d3a94b00 admin demo] G[illegible]ces... from (pid=16036) _create_instance /opt/stack/nova/[illegible]e/api.py:492

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

ALS


Cloud Root
H(Alice||Bob)
Alice
H(Machine 1||Machine 2)
Bob
Machine 1
H(2012)
Machine 2
H(2012)
...
2012
H(12)
2012
H(12)
12
H(7)
12
H(7||8)
7
H(LogMsg 1)
7
H(LogMsg 2||LogMsg 3)
8
H(LogMsg 4)
LogMsg 1
LogMsg 2
LogMsg 3
LogMsg 4

ALS


Cloud Root
H(Alice||Bob)
Alice
H(Machine 1||Machine 2)
Bob
...
Machine 1
H(2012)
Machine 2
H(2012)
2012
H(12)
2012
H(12)
12
H(7)
12
H(7||8)
7
H(LogMsg 1)
7
H(LogMsg 2||LogMsg 3)
8
H(LogMsg 4)
LogMsg 1
LogMsg 2
LogMsg 3
LogMsg 4

IMPLEMENTATION

Web Interface

Instance Detail: My First Instance

Overview | Log | VNC | Incident Response

Instance Incident Response Tasks

Download Nova API Logs
Download Host Firewall Logs
Download Disk Image

DFXML


```
<?xml version='1.0' encoding='UTF-8'?>
<dfxml xmloutputversion='1.0'>
<creator version='1.0'>
   <program>FROST</program>
   <version>1.0</version>
<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>
```

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>
```

API Logs API

```
$ 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 URGP=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
```

Evaluation

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