RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Survey of the Operating Landscape Investigating Incidents in the Cloud

SESSION ID: CSV-T09

Paul A. Henry
Security & Forensics Analyst
vNet Security, LLC
@phenrycissp

Jacob Williams
Chief Scientist
CSRgroup Security Consultants
@MalwareJake

A Lot To Cover Here In Just An Hour…

- We simply can not cover all cloud platforms in an hour so…..
- Private Cloud
  - VMware
- Public Cloud
  - Amazon
  - Rackspace

A Little Perspective…

- What are you trying to accomplish?
  - Are you going to image the entire storage system to access a single VM for forensic analysis?
- A better, more business (and privacy) friendly approach may be to only copy the specific VMDK container for the respective VM you are targeting

Forensicating In A Private Cloud

- Moving from the physical realm to private cloud introduces several challenges
  - Unsupported disk format
  - No file undelete capability
  - No down time

Storage Considerations

- Underlying disk format
  - VMFS
    - Cluster aware sharable file system
    - Enables multiple ESX servers to have access to the same LUNS
    - Enabler of capabilities like vMotion, HA and DRS
    - Undocumented by VMware and not supported by commercial forensics tools
  - RDM
    - Used when high performance - direct storage access is required
    - Directly mounted by the VM and typically formatted by the respective operating system

A Few Words On VMFS

- File recovery
  - Version 4.x thru 5
    - Official statement from VMware:
      - *"vmfs-undelete utility is not available for ESX/ESXi 4.0 ESX/ESXi 3.5 Update 3 included a utility called vmfs-undelete, which dd be used to recover deleted .vmdk files. This utility is not available with ESX/ESXi 4.0. Workaround: None. Deleted .vmdk files cannot be recovered"*
    - Hope your client has a VMFS backup… prior to deletion
    - Undocumented files system with little 3rd party support…

Understanding The VMDK

- VMware encapsulates the entire virtual machine within the respective VMDK (think of it as a container)
  - Everything associated with a particular VM is stored within the respective VMDK
  - If your focus is a given VM then life just got easier for you…

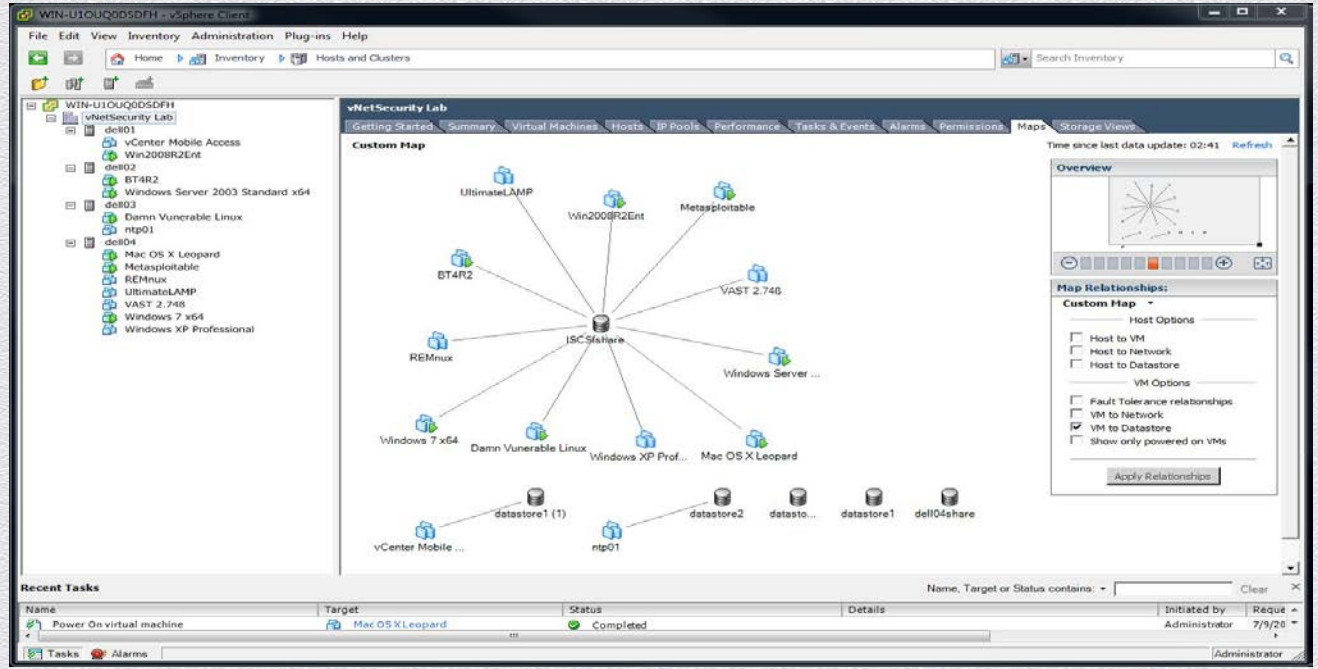
VMDK Files

- The files within a VMDK for a respective VM include but are not limited to:
  - *.vmx: VM config file
  - *.vmdk: Virtual disk config file
  - *-flat.vmdk: Actual VM hard disk
  - *.nvram: VM's BIOS file
  - *.log: VM log files
  - *.vmsn: Running state of virtual machine

Locating a VMDK

- Locating a specific VM VMDK
  - Working within vSphere
  - Using the vSphere Client connected ESX / ESXi
  - Using SSH connected to ESX / ESXi
  - Using A Third Party Product FastSCP

vCenter Maps (1)



SANS

#RSAC

RSACONFERENCE2014

vCenter Maps (2)

Datastore Browser - [ISCSIshare]

Folders | Search

/
- Windows Server 2008 R2 x64_1
- W2KR2x64-02
- veeam_fastscp_3.0.3.272
- BT4R2
- Metasploitable
- UltimateLAMP
- Windows XP Professional
- REMnux
- Windows 7 x64
- Windows Server 2003 Standard
- Mac OS X Leopard
- VAST 2.74+w58
- Damn Vunerable Linux
- Quest
- Win2008R2Ent

[ISCSIshare] Windows Server 2003 Standard x64

Name	Size	Type	Path	Modified
Windows Server 2003 Standard x64.vmx	3.38 KB	File	[ISCSIshare] Windows Server 2003 Standard x64	7/9/2011 6:08:15 AM
Windows Server 2003 Standard x64.vmxf	1.61 KB	File	[ISCSIshare] Windows Server 2003 Standard x64	7/9/2011 6:01:58 AM
Windows Server 2003 Standard x64.vmsd	0.04 KB	File	[ISCSIshare] Windows Server 2003 Standard x64	1/25/2011 10:14:06 AM
Windows Server 2003 Standard x64.vmdk	41,943,04	Virtual Disk	[ISCSIshare] Windows Server 2003 Standard x64	1/24/2011 5:37:41 PM
vmware-1.log	29.17 KB	Virtual Machine log file	[ISCSIshare] Windows Server 2003 Standard x64	1/24/2011 6:09:36 PM
vmware-2.log	60.87 KB	Virtual Machine log file	[ISCSIshare] Windows Server 2003 Standard x64	1/24/2011 6:25:47 PM
Windows Server 2003 Standard x64 Edition.nvram	8.48 KB	Non-volatile memory file	[ISCSIshare] Windows Server 2003 Standard x64	7/9/2011 6:07:40 AM
Windows Server2003 Standardx64-ctk.vmdk	2,560.50	File	[ISCSIshare] Windows Server 2003 Standard x64	1/25/2011 11:55:01 AM
vmware-3.log	100.83 KB	Virtual Machine log file	[ISCSIshare] Windows Server 2003 Standard x64	1/25/2011 2:02:58 PM
vmware.log	58.25 KB	Virtual Machine log file	[ISCSIshare] Windows Server 2003 Standard x64	7/9/2011 6:08:43 AM
Windows Server 2003 Standard x64-4a5f83ed.vswp	1,048,576	File	[ISCSIshare] Windows Server 2003 Standard x64	7/9/2011 6:06:02 AM

Three Approaches to Imaging

1. Shutdown the VM and image
2. Suspend the VM and image
3. Snapshot the VM and image

The method chosen will of course vary with the given circumstances found within the virtual environment

Snapshot the VM and Image

- A snapshot preserves the state and data of a virtual machine at a specific point in time.
  - State includes the virtual machine's power state (powered-on, powered-off, suspended, etc.).
  - Data includes all the files that make-up the virtual machine, including disks, memory, and other devices, such as virtual network interface cards.

Snapshot the VM (1)

WIN-U1OUQ0DSDFH - vSphere Client

File Edit View Inventory Administration Plug-ins Help

Home ▸ Inventory ▸ Hosts and Clusters

Search Inventory

- WIN-U1OUQ0DSDFH
  - vNetSecurity Lab
    - dell01
      - vCenter Mobile Access
      - Win2008R2Ent
    - dell02
      - BT4R2
      - Windows Server 2003 Standard x64

Windows Server 2003 Standard x64

Getting Started | Summary | Resource Allocation | Performance | Tasks & Events | Alarms | Console | Permissions | Maps | Storage Vie

General

Guest OS:	Microsoft Windows Server 2003, Standard E...
VM Version:	7
CPU:	1 vCPU
Memory:	1024 MB
Memory Overhead:	118.70 MB
VMware Tools:	OK
IP Addresses:	192.168.1.209
DNS Name:	win2k3-83ea69cd
EVC Mode:	N/A
State:	Powered On
Host:	dell02
Active Tasks:	Create virtual machine snapshot

Commands

Open Console

Resources

Consumed Host CPU:	23 MHz
Consumed Host Memory:	359.00 MB
Active Guest Memory:	20.00 MB
	Refresh Storage Usage
Provisioned Storage:	42.02 GB
Not-shared Storage:	42.02 GB
Used Storage:	42.02 GB

Datastore	Status	Capacity	
ISCSIshare	Normal	676.25 GB	309.1

Network	Type	St
Production	Standard switch network	

Image the Snapshot Procedure (1)

- Create a new folder on the NAS and connect to it using esxcfg-nas
- Create a hash set for the respective VM over SSH
- Copy the folder to the NAS with FastSCP
- Hash all files in the copied folder and compare to the original hashes

Image the Snapshot Procedure (2)

```
/vmfs/volumes # esxcfg-nas -a -o 192.168.1.11 -s /nfs/LABNFS3 NASLAB3
Connecting to NAS volume: NASLAB3
NASLAB3 created and connected.
/vmfs/volumes # ls
3c3693e8-f77a642a-1910-5c6bdcb26d3a  Hypervisor2
4d3b2f90-8f87fd37-7ac9-0019b9f34d56  Hypervisor3
4d3b6c95-95d1b576-1590-001372f82a57  ISCSIshare
4d3b6c96-68c9e3de-cdc1-001372f82a57  NASLAB3
54314f7d-e45002a6-a747-e419ff05c9d7  c28da578-4f1a2b1c-8f1e-90603fb2577a
942fa076-89461742                    datastore1
Hypervisor1
/vmfs/volumes # 
```

Image the Snapshot Procedure (3)

```
/vmfs/volumes/4d3b2f90-8f87fd37-7ac9-0019b9f34d56/Windows Server 2003 Standard x
/vmfs/volumes/4d3b2f90-8f87fd37-7ac9-0019b9f34d56/Windows Server 2003 Standard x
/vmfs/volumes/4d3b2f90-8f87fd37-7ac9-0019b9f34d56/Windows Server 2003 Standard x
64 # find * -type f -print0 | xargs -0 md5sum >> origfiles.md5
md5sum: can't open 'Windows Server 2003 Standard x64-000001-delta.vmdk': Device
or resource busy
md5sum: can't open 'Windows Server 2003 Standard x64-4a5f83ed.vswp': Device or r
esource busy
/vmfs/volumes/4d3b2f90-8f87fd37-7ac9-0019b9f34d56/Windows Server 2003 Standard x
64 #
```

Image the Snapshot Procedure (4)

Veeam Backup and FastSCP

File Edit View Tools Help

Back Forward Refresh Up View Add Server Scheduled Copy

- Backup
  - Jobs
  - Sessions
- Servers
  - My Computer
    - Boot - Win7 160 GB SSD (C:)
    - Win 7 Page File 60 GB SSD (D:)
    - Win / FTK Temp Files 2SSD RAID 0 (E:)
    - CD-ROM (F:)
    - Paul Henry (G:)
    - Images ASUS 2SATA III RAID 0 (H:)
    - Oracle Adaptec 8 Drive RAID 0 (I:)
    - Storage Adaptec 8 Drive RAID 5 (J:)
    - Removable (K:)
    - CD-ROM (L:)
    - LABNFS (X:)
    - LABNFS3 (Y:)
      - Windows Server 2003 Standard x64
    - LABNFS2 (Z:)
  - vc
    - vNetSecurity Lab
      - Datastores

Name	Type	Size	Modified
vmware-1.log	log	29.17 KB	7/11/2011 2:09:...
vmware-2.log	log	60.87 KB	7/11/2011 2:09:...
vmware-3.log	log	100.83 KB	7/11/2011 2:09:...
vmware-4.log	log	68.50 KB	7/11/2011 2:09:...
vmware-5.log	log	61.99 KB	7/11/2011 2:09:...
Windows Server 2003 Standard x64 Edition.nvram	nvram	8.48 KB	7/11/2011 2:09:...
Windows Server 2003 Standard x64.vmdk	vmdk	0.71 KB	7/11/2011 2:09:...
Windows Server 2003 Standard x64.vmsd	vmsd	0.53 KB	7/11/2011 1:54:...
Windows Server 2003 Standard x64.vmx	vmx	3.41 KB	7/11/2011 1:54:...
Windows Server 2003 Standard x64.vmxf	vmxf	1.56 KB	7/11/2011 1:54:...
Windows Server 2003 Standard x64-ctk.vmdk	vmdk	2.50 MB	7/11/2011 2:09:...
Windows Server 2003 Standard x64-flat.vmdk	vmdk	40.00 GB	7/11/2011 2:09:...

12 objects 40.00 GB veeam

Image the Snapshot Procedure (5)

Administrator: Command Prompt

```
Y:\Windows Server 2003 Standard x64>c:\md5deep-3.9.1\md5deep *.*
3eed6c12ef1332e9daba5ed01f4aeb7e  Y:\Windows Server 2003 Standard x64\Windows Server 2003 Standard x64.vmx
9216c87694d6a4d23e416286060eea6d  Y:\Windows Server 2003 Standard x64\Windows Server 2003 Standard x64.vmxf
0de866afdd27e62a0b146d476f88624b  Y:\Windows Server 2003 Standard x64\Windows Server 2003 Standard x64.vmsd
de55452597af9129bacb19cfe00f2316  Y:\Windows Server 2003 Standard x64\Windows Server 2003 Standard x64-flat.vmdk
047bd4f5f8664703b8ffcc18806f2700  Y:\Windows Server 2003 Standard x64\Windows Server 2003 Standard x64.vmdk
f437e93a71f474162780098acef5d2aa  Y:\Windows Server 2003 Standard x64\vmware-1.log
e20eb7494cd24e8904993686bc87700d  Y:\Windows Server 2003 Standard x64\vmware-2.log
8f15665ec02153285f05708c9abed98e  Y:\Windows Server 2003 Standard x64\Windows Server 2003 Standard x64 Edition.nvram
9a1b829088f87
e54ac35c58d78
a79851ab03c34
bdfad0c9492ab
```

dell02 - PuTTY

```
/vmfs/volumes/4d3b2f90-8f87fd37-7ac9-0019b9f34d56/Windows Server 2003 Standard x
64 # cat origfiles.md5
8f15665ec02153285f05708c9abed98e  Windows Server 2003 Standard x64 Edition.nvram
9ab41e1070ea3e2575afcfbade0c762b  Windows Server 2003 Standard x64-000001-ctk.vm
dk
70ad93c0001810e16e2d3ce38364d56d  Windows Server 2003 Standard x64-000001.vmdk
164d05993acf3c743d0720c9b81d5bb6  Windows Server 2003 Standard x64-Snapshot4.vms
n
9a1b829088f879720a0f9880161f0c45  Windows Server 2003 Standard x64-ctk.vmdk
de55452597af9129bacb19cfe00f2316  Windows Server 2003 Standard x64-flat.vmdk
047bd4f5f8664703b8ffcc18806f2700  Windows Server 2003 Standard x64.vmdk
0de866afdd27e62a0b146d476f88624b  Windows Server 2003 Standard x64.vmsd
3eed6c12ef1332e9daba5ed01f4aeb7e  Windows Server 2003 Standard x64.vmx
9216c87694d6a4d23e416286060eea6d  Windows Server 2003 Standard x64.vmxf
79641ec4f01df56fbb9ee40dd4631ecb  origfiles.md5
f437e93a71f474162780098acef5d2aa  vmware-1.log
e20eb7494cd24e8904993686bc87700d  vmware-2.log
e54ac35c58d78ce1e451bfc60daba8a1  vmware-3.log
a79851ab03c345a080c9fa9eb5af33b8  vmware-4.log
bdfad0c9492abd5975c3847ab14becd1  vmware-5.log
1ff3bc13d44d8ed1fcf5a075d7ac74dc  vmware-6.log
ba29d2d0a27f9baa6c64c3016eea891b  vmware.log
/vmfs/volumes/4d3b2f90-8f87fd37-7ac9-0019b9f34d56/Windows Server 2003 Standard x
/vmfs/volumes/4d3b2f90-8f87fd37-7ac9-0019b9f34d56/Windows Server 2003 Standard x64 #
```

Additional Snap Shot Considerations

- What if snapshots already exist before imaging?
  - There are currently no tools available to handle the forensic analysis of the individual child disks created in a snapshot <VMname>-0000xx.vmdk
    - Be sure to create an image of all files before beginning any snapshot consolidation
    - Each snapshot will have to be reverted and imaged separately
    - Simply consolidating all snapshots in bulk could cause the loss of potential evidence

Going Old School With DD

- We know where the files are but we need the complete path to enter into our dd command line
  - Use the ESX / ESXi command

    "esxcfg-info –s"
- Remember the label that was assigned to the data store "VMFS Store"

DD Imaging VMFS (1)

```
\==+Vm FileSystem :
   |----Volume UUID.............................................4e1b18e5-d3bbada8-2df7-0019b9f34d56
   |----LVM Name................................................4e1b18e3-f1c4ec0c-d7e2-0019b9f34d56
   |----Type....................................................VMFS
   |----Head Extent.............................................naa.5000c50003d27e93:2
   |----Console Path............................................/vmfs/volumes/4e1b18e5-d3bbada8-2df7-0019b9f34d56
   |----Block Size..............................................1048576
   |----Total Blocks............................................1792
   |----Blocks Used.............................................885
   |----Size....................................................1879048192
   |----Usage...................................................927989760
   |----Volume Name.............................................VMFS Store
   |----Lock Mode...............................................public
   |----Major Version...........................................3
   |----Minor Version...........................................46
   |----Is Force Mounted........................................false
   |----Is Accessible...........................................true
   |----Something Offline.......................................false
   \==+Extents :
      \==+Disk Lun Partition :
         |----Name..............................................naa.5000c50003d27e93:2
         |----Partition Number..................................2
         |----Start Sector......................................8402048
         |----End Sector........................................12594960
         |----Partition Type....................................251
         |----Console Device..................................../vmfs/devices/disks/naa.5000c50003d27e93:2
         |----DevFS Path......................................../vmfs/devices/disks/naa.5000c50003d27e93:2
         |----Size..............................................2146770944
         |----Type..............................................0x000000fb
```

SANS

#RSAC

RSACONFERENCE2014

DD Imaging VMFS (2)

```
942fa076-89461742                    datastore1 (1)
/vmfs/volumes # cd VMFS\ Store/
/vmfs/volumes/4e1b18e5-d3bbada8-2df7-0019b9f34d56 # ls
ntp01
/vmfs/volumes/4e1b18e5-d3bbada8-2df7-0019b9f34d56 # cd ntp01/
/vmfs/volumes/4e1b18e5-d3bbada8-2df7-0019b9f34d56/ntp01 # ls
ntp01-flat.vmdk   ntp01.vmdk        ntp01.vmx        vmware.log
ntp01.nvram       ntp01.vmsd        ntp01.vmxf
/vmfs/volumes/4e1b18e5-d3bbada8-2df7-0019b9f34d56/ntp01 # find * -type f -print0
 | xargs -0 md5sum >> origfiles.md5
/vmfs/volumes/4e1b18e5-d3bbada8-2df7-0019b9f34d56/ntp01 # cat origfiles.md5
68d32e294be7f2bb58f8e6a076bef743  ntp01-flat.vmdk
7aaf58d9d8b67950d2b8919cc538059d  ntp01.nvram
b6dbebc6a8b2265622b603b93d4b6eb9  ntp01.vmdk
d41d8cd98f00b204e9800998ecf8427e  ntp01.vmsd
93b3ce90dfda2fda3b5ba98e8eb3a78f  ntp01.vmx
6eccac733134ff774475a1eed44e3e36  ntp01.vmxf
d41d8cd98f00b204e9800998ecf8427e  origfiles.md5
9e407366411c85a9622f2f262372cad3  vmware.log
/vmfs/volumes/4e1b18e5-d3bbada8-2df7-0019b9f34d56/ntp01 # dd if=/vmfs/devices/di
sks/naa.5000c50003d27e93:2 of=/vmfs/volumes/NASLAB3/vmfs_partition.dd
4192912+0 records in
4192912+0 records out
/vmfs/volumes/4e1b18e5-d3bbada8-2df7-0019b9f34d56/ntp01 #
```

SANS

#RSAC

RSACONFERENCE2014

Copy the VM from VMFS

```
C:\>java -jar fvmfs.jar y:\vmfs_partition.dd filecopy /ntp01/ntp01-flat.vmdk J:/ntp01_vm/ntp01-flat.vmdk
VMFSTools (C) by fluid Operations (v0.9.8.18 r95 / 2010-01-25_15-57-35)
http://www.fluidops.com

Size = 600.00 MB
Copying file -- bytes left=545259520 throughput=33527 KB/s ETA=16s
Copying file -- bytes left=474480640 throughput=30846 KB/s ETA=15s
Copying file -- bytes left=394788864 throughput=31147 KB/s ETA=12s
Copying file -- bytes left=311427072 throughput=31642 KB/s ETA=9s
Copying file -- bytes left=234356736 throughput=31477 KB/s ETA=7s
Copying file -- bytes left=145752064 throughput=32074 KB/s ETA=4s
Copying file -- bytes left=66584576 throughput=31981 KB/s ETA=2s
Copied 629145600 bytes in 19s throughput was 31701 KB/s

C:\>java -jar fvmfs.jar y:\vmfs_partition.dd filecopy /ntp01/ntp01.nvram J:/ntp01_vm/ntp01.nvram
VMFSTools (C) by fluid Operations (v0.9.8.18 r95 / 2010-01-25_15-57-35)
http://www.fluidops.com

Size = 8.48 KB
Copied 8684 bytes in 0s throughput was 542 KB/s

C:\>java -jar fvmfs.jar y:\vmfs_partition.dd filecopy /ntp01/ntp01.vmdk J:/ntp01_vm/ntp01.vmdk
VMFSTools (C) by fluid Operations (v0.9.8.18 r95 / 2010-01-25_15-57-35)
http://www.fluidops.com

Size = 606.00 Bytes
Copied 606 bytes in 0s throughput was 60 KB/s

C:\>java -jar fvmfs.jar y:\vmfs_partition.dd filecopy /ntp01/ntp01.vmsd J:/ntp01_vm/ntp01.vmsd
VMFSTools (C) by fluid Operations (v0.9.8.18 r95 / 2010-01-25_15-57-35)
http://www.fluidops.com

Size = 0.00 Bytes
Copied 0 bytes in 0s throughput was 0 KB/s

C:\>java -jar fvmfs.jar y:\vmfs_partition.dd filecopy /ntp01/ntp01.vmx J:/ntp01_vm/ntp01.vmx
VMFSTools (C) by fluid Operations (v0.9.8.18 r95 / 2010-01-25_15-57-35)
http://www.fluidops.com

Size = 2.82 KB
Copied 2883 bytes in 0s throughput was 205 KB/s

C:\>java -jar fvmfs.jar y:\vmfs_partition.dd filecopy /ntp01/ntp01.vmxf J:/ntp01_vm/ntp01.vmxf
VMFSTools (C) by fluid Operations (v0.9.8.18 r95 / 2010-01-25_15-57-35)
http://www.fluidops.com
```

Forensicating In A Public Cloud

- Moving from the physical realm to public cloud introduces several challenges
  - Where is my server?
  - No “VMware-like” snap-shot capability
  - Terminating an instance really terminates it (oh my)

Inventory Running Instances

- Always inventory running instances
- Before taking a suspect EC2 instance offline, verify the termination behavior
  - EBS backed instances that are terminated are gone forever

```
C:\>aws ec2 describe-instances
-----------------------------------------------------------------------------------------
|                                   DescribeInstances                                   |
+---------------------------------------------------------------------------------------+
||                                    Reservations                                     ||
|+-------------------------------------+-------------------------------------------------+|
||  OwnerId                            |  [redacted]                                     ||
||  ReservationId                      |  r-82ba858b                                     ||
|+-------------------------------------+-------------------------------------------------+|
||                                     Instances                                       ||
|+-----------------------+-------------------------------------------------------------+|
||  AmiLaunchIndex       |  0                                                          ||
||  Architecture         |  x86_64                                                     ||
||  ClientToken          |  [redacted]                                                 ||
||  EbsOptimized         |  False                                                      ||
||  Hypervisor           |  xen                                                        ||
||  ImageId              |  ami-1e53c82e                                               ||
||  InstanceId           |  i-ba8db5b3                                                 ||
||  InstanceType         |  t1.micro                                                   ||
```

SANS

#RSAC

RSACONFERENCE2014

EBS Volumes

- EBS Volumes are like disks that can be attached to a running EC2 instance
- Each running EC2 instance will have a volume for its root disk
- Users may add additional storage to EC2 instances
  - Without stopping them if the OS supports hot swapping file systems

```
C:\>aws ec2 describe-volumes
-----------------------------------------------------------
|                     DescribeVolumes                     |
+---------------------------------------------------------+
||                        Volumes                        ||
|+----------------------+--------------------------------+|
||  AvailabilityZone    |  us-west-2b                    ||
||  CreateTime          |  2014-02-10T04:23:21.497Z      ||
||  Size                |  30                            ||
||  SnapshotId          |  snap-f41961cb                 ||
||  State               |  in-use                        ||
||  VolumeId            |  vol-b5a41d9d                  ||
||  VolumeType          |  standard                      ||
|+----------------------+--------------------------------+|
||                      Attachments                      ||
```

SANS

#RSAC

RSACONFERENCE2014

EBS Snapshots

- Always inventory snapshots present in an AWS account
- Snapshots may not be assigned to a volume
- Snapshots may contain
  - Data from instances that have been terminated
  - Log files that have since rotated off

```
C:\>aws ec2 describe-snapshots --filter Name=volume-id,Values=vol-b5a41d9d
-----------------------------------------------
|               DescribeSnapshots               |
+-----------------------------------------------+
||                  Snapshots                  ||
|+--------------+-----------------------------+|
||  Description |  suspect image, case 152321 ||
||  OwnerId     |  568446001437               ||
||  Progress    |  100%                       ||
||  SnapshotId  |  snap-c85de539              ||
||  StartTime   |  2014-02-14T01:25:40.000Z   ||
||  State       |  completed                  ||
||  VolumeId    |  vol-b5a41d9d               ||
||  VolumeSize  |  30                         ||
|+--------------+-----------------------------+|
```

EC2 Volumes

- Enumerate the volumes associated with suspect account
- Note any extra volumes that are not root volumes for EC2 instances
  - Note any extra volumes without “attachments” (currently unmounted)
  - If not based on a snapshot, may contain relevant data not available elsewhere
- Use the ‘aws ec2 describe-volumes’ command to list

What About Analyzing It In The Cloud?

- Transferring data out of the AWS cloud for analysis is time consuming and expensive
- Analyze it in the Cloud: Newly launched EC2 instances can be used to perform analysis on suspect EC2 instances
  - Faster acquisition time
  - Saves money (over transferring out of the cloud)

Using a Linux AMI

- Standard Linux AMIs can also be used for forensic acquisition in EC2
  - The two key tools required are mount and dd
- Linux AMIs also include an SSH server
  - Any files acquired can be securely copied out of the AWS cloud for offline analysis
- A SANS SIFT Workstation for the cloud is coming soon !

Imaging EC2 Instances

- The snapshot feature can be used to obtain disk images of running EC2 instances
- Tools such as F-Response can be used to acquire or analyze EC2 instance images in-band
- EC2 snapshots can also be copied and used outside of the cloud

EC2 Disk Image Steps

1. Launch Linux (forensic) EC2 instance
2. Snapshot suspect EC2 instance
3. Create volume based on snapshot
4. Attach volume to Linux (forensic) instance
5. Create empty volume to capture snapshot
6. Use dd to create an exact bitwise copy

AWS Command Line Steps

1. aws ec2 describe-instances
   - Get instance ID of forensics machine and volume ID of suspect drive
2. aws ec2 create-snapshot
   - Create a snapshot of the suspect volume
3. aws ec2 create-volume
   - Create a new volume based on the suspect volume snapshot
4. aws ec2 attach-volume
   - Mount the volume containing suspect data to investigator machine

What About Amazon S3

- S3 is Amazon's 'Simple Storage Service'
- Supports file sizes of up to 5TB
- Supports HTTP, HTTPS, and Bit torrent transfer
- Users may interact with S3 via
  - APIs
  - AWS Control Panel
  - Third party apps

Amazon S3 (2)

- Data transfer from S3 is relatively fast
  - But limited by your network connection
  - Transfer prices high for full disk images
- Amazon offers a data loading service
  - Send them a hard drive with files, and they load it on S3

S3 Transfer vs. Export (1)

- Suppose you have 2TB of forensic data in S3 you want to download to perform offline analysis
  - See chart below to estimate download time

Available Internet Connection	Theoretical Min. Number of Days to Transfer 1TB at 80% Network Utilization	When to Consider AWS Import/Export?
T1 (1.544Mbps)	82 days	100GB or more
10Mbps	13 days	600GB or more
T3 (44.736Mbps)	3 days	2TB or more
100Mbps	1 to 2 days	5TB or more
1000Mbps	Less than 1 day	60TB or more

S3 Transfer vs. Export (2)

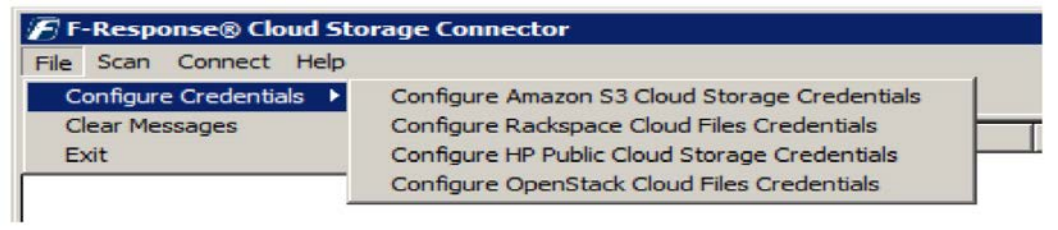
- The Amazon Import/Export (sneaker-net) calculator estimates that for 2TB of data
  - Total cost: $158.71
  - Loading time: 26 hours
  - Chain of Custody ?
  - Expedited return shipping included
- Note that regular S3 transfer charges for bandwidth are between $102.40 and $245.76
  - Depending on your overall S3 usage tier

Forensicating In The Cloud

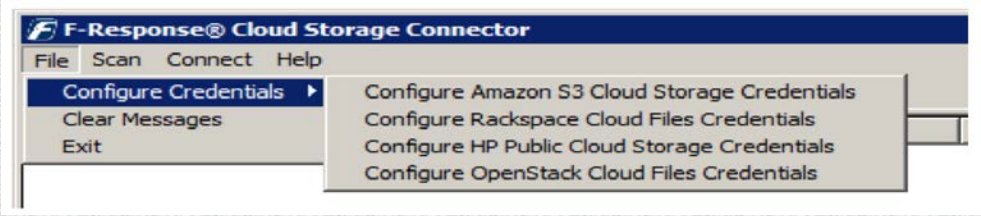
- Easy to setup an EBS Backed Windows 2008 / 2012 forensic workstation running FTK 4.x
- Handle the license dongle with USB to Ethernet
  - Don’t forget to open a firewall rule !
- Easily connect r/o to your to target dd image
- Want faster forensicating performance
  - How about using multiple FTK “Worker” machines !
- On going testing of other popular IR & Forensic tools

More On Cloud Connector…

- You knew that F-Response Cloud Connector worked with Amazon S3 but did you know it also works with Rackspace, HP and OpenStack?
  - Just like on Amazon you connect to storage containers and work with them as if they were local to your forensic workstation



Cloud Connector -> Rackspace (1)

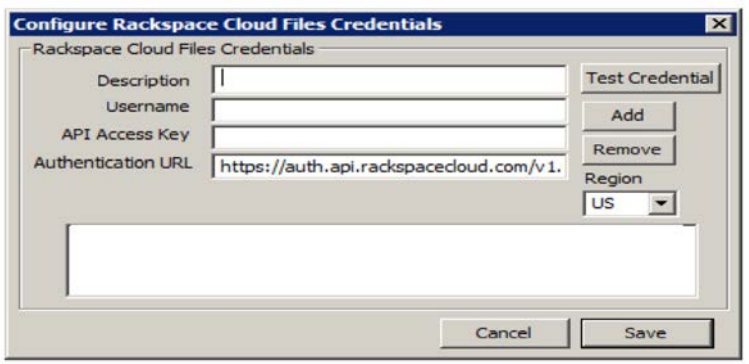


Step 1

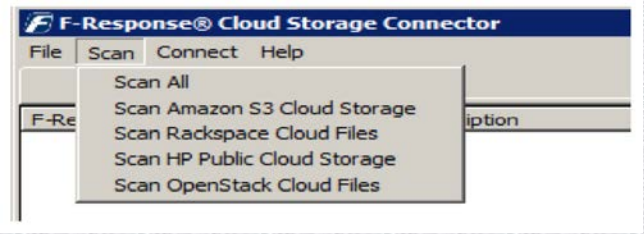
Step 2

Step 3

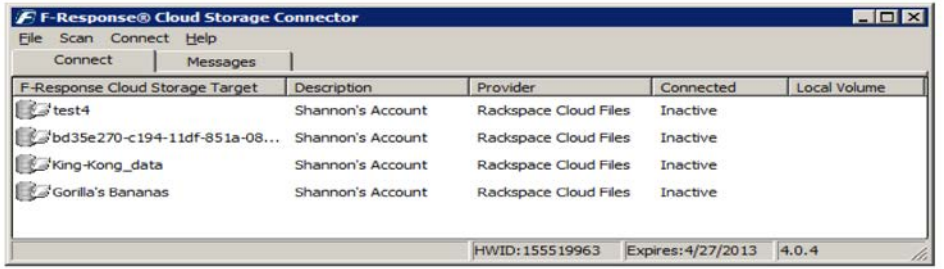
Cloud Connector -> Rackspace (2)



Step 4

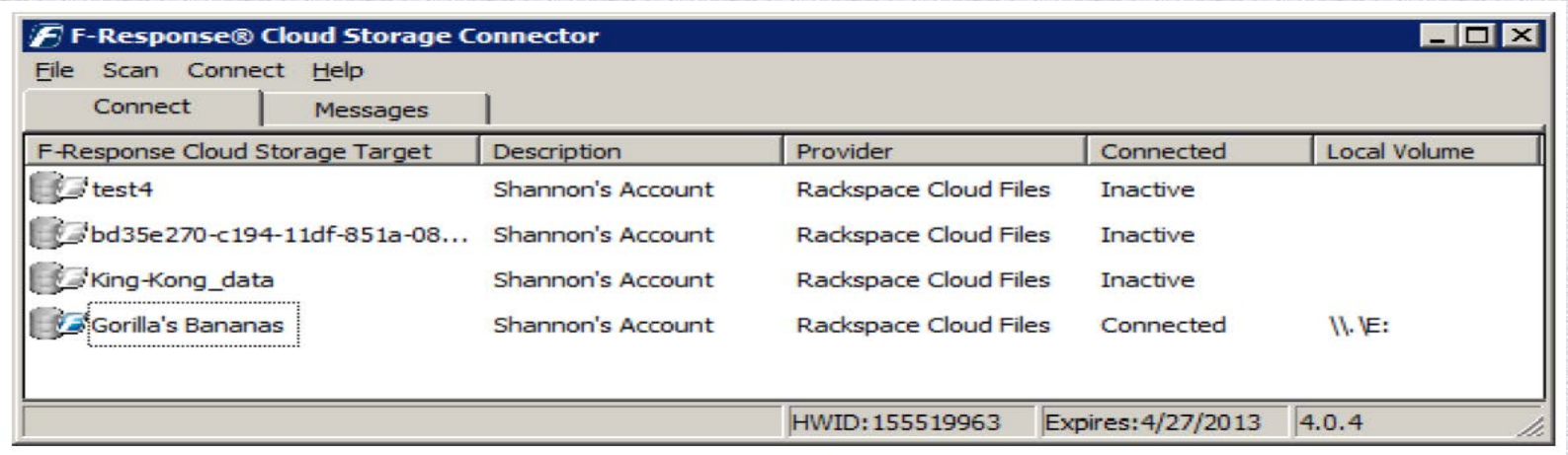


Step 5



Step 6

Cloud Connector -> Rackspace (3)



Step 7

Now simply run your IR & Forensics tools against Rackspace Storage as if it were a local read-only physically connected hard drive….

How To Apply This Knowledge

- Armed with this knowledge a sound forensics process can be applied in a private or public cloud environment
  - In a Private Cloud environment platforms such as VMware while much more complex then a physical environment can actually make some aspects of IR & Forensics easier.
  - In a Public Cloud environment platforms such as Amazon AWS can be handled with careful planning. Remember snapshots in AWS are not the same as VMware – no RAM image and no revert to previous snapshot.