Virtualization Forensics:
Acquisition and analysis of a clustered VMware ESXi servers

Dennis Cortjens
dennis.cortjens@os3.nl

PLAN
28th of February, 2014

Contents

1 Information ................................................................. 1
  1.1 Introduction .......................................................... 1
  1.2 Problem ............................................................... 1
  1.3 Position ............................................................... 2
  1.4 Questions .............................................................. 2
    1.4.1 Main .............................................................. 2
    1.4.2 Sub ............................................................... 2
  1.5 Goal ................................................................. 2
  1.6 Scope ............................................................... 3
1 Information

1.1 Introduction

Virtualization plays an important role in the world of IT. In enterprise IT infrastructures it has proven to be very efficient and cost effective. It reduces the amount of physical servers needed for the IT demand and with that the need for large energy consuming data centres.

In IT there are different forms of virtualization, but the well-known is the virtual machine. Simply described as a system within a system. It is often used for virtualizing operating systems and the is quite some software for this. This software can be divided in native (type 1) and hosted (type 2) hypervisors or virtual machine managers.

A native hypervisor runs directly on the hardware as a virtual machine operating system, where a hosted hypervisor is a virtual machine application on a operating system.

The well-known native (type 1) hypervisors are:

- Microsoft Hyper-V Server
- Oracle VM Server (Xen based)
- VMware ESXi

The well-known hosted (type 2) hypervisors are:

- Kernel-based Virtual Machine (KVM)
- Microsoft Windows Virtual PC
- Oracle VirtualBox
- VMware Fusion
- VMware Workstation
- Xen

Some of these hypervisors can be clustered, distributing and sharing virtual machines and storage across the IT infrastructure.

1.2 Problem

Over the last years virtualization has become increasingly popular. A lot of companies (small business and enterprise) adopted virtualization with the use of virtual machines in their IT infrastructure and even for personal use it is very popular. However, the world of digital forensics seems a little bit slow in this matter. It has been researched and documented, but not extensively. There are some books available with general knowledge about the workings of virtualization, but not on how to acquire and analyse it. Especially when it comes to the acquisition and analysis of large clusters of hypervisors with virtual machines and storage distributed across IT infrastructures.

ESXi is the widely adopted virtualization architecture by industry-leading virtualization software company VMware. Multiple ESXi servers can be clustered to distribute and share virtual machine and storage. Therefore it is adopted by a lot of companies as an efficient and cost effective solution for IT infrastructures. Besides that, ESXi is freely available and can be (mis)used for personal, small business and enterprise use.

With that the chance of computer crime experts and digital forensic investigators running into such systems has also increased. This is noticeable by a significant increase of searches at large data centres and running into clustered VMware ESXi servers last year (2013). A study into the acquisition and analysis of clustered VMware ESXi servers can provide a first guide line for computer crime experts and digital forensic investigators running into such situations.
1.3 Position

A literature study on the forensic acquisition and analysis of clustered VMware ESXi servers resulted in no information to that specific subject. However, there were a book, thesis and blog article related to the subject.

In 2010 Diane Barrett and Gregory Kipper wrote a (guide) book on virtual environments for digital forensic investigators. They describe virtualization in high detail. Even the acquisition and analysis of virtual environments, but from a desktop application perspective and not from a (clustered) hypervisor server perspective [1]. At the time of writing the book this wasn’t a well-known and popular solution yet. The book is somewhat outdated, but a good basis and reference for this research. It is a good book on virtualization forensics and a must have for all computer crime experts and digital forensic investigators with a specialization in this subject.

In 2011 Manish Hirwani researched the forensic analysis of VMware virtual hard disks and wrote a thesis about it. He describes the acquisition and analysis of VMware virtual disks using AccessData’s Forensic ToolKit, FTK Imager and Guidance Software’s EnCase [2]. The VMware virtual disk (VMDK) is still used within all of VMware’s product, similarly the VMware ESXi architecture. Nowadays there is full support for the VMDK format in the last versions of the mentioned forensic software. The thesis is somewhat outdated, but still a good basis and reference for this research.

In 2013 Phil Hagen wrote a article on his blog about VMware snapshots. He describes the calculation of snapshot creation times from the snapshot meta file (VMSD) with a python script (code published in the article). There is also a very good comment on this article with some links to software tools for analysing VMware snapshots and even the memory part of these snapshots [3]. This will be very useful for the analysis part of this research.

1.4 Questions

1.4.1 Main

How can clustered VMware ESXi servers be acquired and analysed in a forensic sound way within the least amount of time?

1.4.2 Sub

The main question is researched with the following sub questions:

1. How does VMware ESXi works?
2. What are the forensic artefacts of VMware ESXi?
3. How does a VMware ESXi cluster works?
4. What can be distributed within a cluster?
5. What are the additional forensic artefacts of a cluster?
6. What is the forensic and best way to freeze the virtual machines?
7. What is the forensic and fastest way of acquiring the virtual machines?
8. How can a cluster configuration be analysed?

1.5 Goal

The goals are set by the following sub questions:

How does VMware ESXi works? Determine the workings of VMware ESXi.

What are the forensic artefacts of VMware ESXi? Determine the forensic artefacts of of VMware ESXi.

How does a VMware ESXi cluster works? Determine the workings of a VMware ESXi cluster.

What can be distributed within a cluster? Determine what can be distribute and shared within a VMware ESXi cluster.
What are the additional forensic artefacts of a cluster? Determine the additional forensic artefacts of a VMware ESXi cluster (if different).

What is the forensic and best way to freeze the virtual machines? Determine the forensic and best way to freeze a virtual machine running on VMware ESXi. Forensic way above best way!

What is the forensic and fastest way of acquiring the virtual machines? Determine the forensic and best way to acquire a virtual machine on VMware ESXi. This will be measured by the time difference in acquiring the virtual machine over the IT network and acquiring the full hard disk drive of the VMware ESXi servers. Forensic way above fastest way!

How can a cluster configuration be analysed? Determine how the full cluster can analysed using (forensic) software.

1.6 Scope

This project is limited by the following scope:

- It focuses on being usable for the investigation of large scale IT infrastructures;
- The test environment cluster will consist of 3 physical servers (representable for large scale IT infrastructures, concept stays the same);
- It focuses on forensic value and validity;
- It focuses on version 5.5 of VMware ESXi;
- The measurement will be primary based on time, but speed will be mentioned;
- It will provide a first guide line for acquiring and analysing (clustered) VMware ESXi environments.
References


List of Figures

List of Tables