

**SINGIDUNUM UNIVERSITY
DEPARTMENT OF POSTGRADUATE STUDIES**



**STUDY COURSE
CONTEMPORARY INFORMATION TECHNOLOGIES**

**ESTABLISHING PROACTIVE DIGITAL FORENSICS
INFRASTRUCTURE IN PRIVATE COMPUTER CLOUD**

- MASTER'S THESIS -

Mentor:

prof. dr Gojko Grubor

Student:

Ljubomir Ivaniš

410026/2013

Beograd, 2014.

PROLOGUE

This thesis primarily relies on prior knowledge gained through years of work that is based on the use of virtual environments, starting from 2004 to the present. Virtual solutions have progressed over the years, and therefore have increased in their complexity. Today's solutions, with which virtual Clouds can be created, represent the culmination of current development that is based on those virtual platforms. Given the increasing complexity of these environments, there is a need for more precise definition of Cloud environments.

I wish to emphasize that currently there is a relatively small number of research papers that deal with the topic of Cloud Computing with emphasis on digital forensics. Main motive of this master's thesis is to bring Cloud Computing platform closer to the user, to explain its components, and allow for easier understanding of the complexity of these environments when it comes to digital forensics.

Given that digital forensics is a very exact science, and that Cloud Computing is not easy to precisely define as a term, we have a very big problem. That's why I've tried to explain in this master's thesis the way in which individual components within Cloud Computing platform can be used for proactive preparation of forensic investigation, the problems that forensics may encounter, as well as suggestions of ways in which these problems might be avoided or minimized. This thesis presents experiences I've gained through practical use of virtualization and Cloud technologies. All examples and figures that are displayed in the thesis, I have created using test environments.

While writing the thesis, I have had the precious help of professors from my study course. Firstly, I would like to give thanks to all the help I received from my mentor, Professor Dr. Grubor, who enabled me to write a thesis on this topic. I would also like to thank other professors who have helped me in creating this thesis with their suggestions, tips, ideas and guidance.

I would also like to thank all the professors of the Singidunum University who participated in my education, during my academic and master studies, and my family for their support and understanding.

ABSTRACT

The idea for this thesis comes out of necessity for better explanation of problems facing digital forensic in Cloud environments. It tries to describe the ways in which individual components within Cloud Computing platform can be used for proactive preparation of forensic investigation, the problems that forensics may encounter, as well as suggestions of ways in which these problems might be avoided or minimized.

The goal of the thesis is to present abilities of current technologies and the use of those technologies in a proactive manner, to bring Cloud Computing platform closer to the user, to explain its components, and allow for easier understanding of the complexity of these environments when it comes to digital forensics.

KEY WORDS

Cloud, IaaS, PaaS, SaaS, NaaS, **Digital forensics**, Server, Client, **Virtualization**, System Center, **Networking**, Monitoring, Auditing, **Log collecting**

CONTENTS

1. Research methodology	- 1 -
1.1. Introductory remarks	- 1 -
1.2. Thesis subject	- 1 -
1.3. Aims and objectives of research.....	- 2 -
1.4. Hypothetical framework of research	- 2 -
1.5. Methods, techniques and course of research process	- 3 -
2. Types of services offered using Cloud technology	- 4 -
2.1. Infrastructure as a service (IaaS)	- 4 -
2.2. Software as a service (SaaS)	- 7 -
2.3. Platform as a service (PaaS).....	- 9 -
2.4. Network as a service (NaaS)	- 10 -
3. Description of components and their functionality within Cloud solution	- 11 -
3.1. Virtualization using Hyper-V hosts.....	- 14 -
3.2. Virtualization using VMM	- 15 -
3.3. Virtualization of presentation.....	- 16 -
3.4. Application virtualization.....	- 18 -
3.5. Network virtualization on Hyper-V hosts	- 19 -
3.6. Network virtualization using VMM	- 20 -
3.7. Description of hardware and software configuration of master's thesis.....	- 21 -
4. Basic principles of digital forensics.....	- 23 -
4.1. Problems faced by digital forensics.....	- 24 -
4.2. Description of the environment used in master's thesis	- 28 -
5. Log configuration for event monitoring within virtual and physical computers ..	- 33 -
6. Log files	- 37 -
6.1. Description of a solution for collecting log files	- 38 -
6.2. Description of solution for centralized collecting of log files.....	- 42 -
7. Case Study: Examples of proactive digital forensics in the Cloud	- 46 -
7.1. Types of virtual networks and physical network infrastructure	- 54 -
7.2. Methods and tools for collecting information from physical network equipment....	- 59 -
8. Conclusion	- 65 -
9. LITERATURE.....	- 67 -

1. Research methodology

1.1. Introductory remarks

This thesis describes problems that can be encountered when performing digital forensics within Cloud systems based on IaaS platforms and offers solutions that can facilitate it. Starting from the assumption that it is necessary to determine who did what and when, and to have enough evidence for those claims, great care has to be given to tools for auditing (monitoring and logging) events.

This thesis is based on the use of Microsoft private Cloud solution built on System Center 2012 R2 platform and the corresponding operating system Windows Server 2012 R2. Given that this platform allows running and executing large number of clients and server operating systems from different manufacturers, it is also used for providing public Cloud services.

The final version of Windows Server 2012 R2 was released on 18th November 2013 together with product package called System Center 2012 R2.

Since this platform allows launching and executing large number of clients with operating systems from different manufacturers, it is also used to facilitate public Cloud services. In other words, public Cloud is just a service that can be offered to third parties through implementation of private Cloud solutions. Public Cloud is nothing more than private Cloud to the provider, and public Cloud to the customer, i.e. service user.

1.2. Thesis subject

The thesis addresses the methods for monitoring and collecting information, as well as positive and negative aspects of existing solutions for collecting logs. This thesis attempts to show the complexity of monitoring events within Cloud Computing, and limitation factors of current technologies. The thesis also tries to put into perspective possible events and places from which they can be traced. Information obtained are centralized for easier viewing and processing. This is very complex task that has not been adequately documented in published works in world literature. This thesis also tries to combine knowledge and experience of the author and his colleagues.

1.3. Aims and objectives of research

Main objective

The main objective of this thesis is to present the components of Cloud environment, explain their possible use, and draw attention to advantages and disadvantages of each, and present necessary elements of Cloud environment. Additional objective is to describe current situation when it comes to digital forensics in Cloud systems, to explain possible uses of existing forensic tools and draw attention to the advantages and disadvantages of each, as well as to introduce new tools and their potential uses within the Cloud environment. The third goal is to present a practical view of these tools and information that can be gathered with their help.

Specific objective

The specific objective of this thesis is to take the intricate and complex area of Cloud environment monitoring and bring it closer to the average user by explaining basic functionalities of forensic tools and their use within Cloud service.

1.4. Hypothetical framework of research

1st hypothesis

The literature is very vague and imprecise in describing Cloud environment. There is relatively high degree of confusion related to the essential elements required to create a Cloud environment.

There is a need to define the elements of Cloud environment, to explain their purpose, present pros and cons of each, to describe possible uses of parts of Cloud solutions, and to create connections between these elements and thus explain the elements necessary for creating Cloud solutions.

2nd hypothesis

Large number of elements that constitute Cloud environment present a problem during its creation. Choosing a good solution when creating suitable Cloud environment is very challenging for most companies.

It is necessary to define the elements needed to create appropriate Cloud environment according to the needs of specific company, explain pros and cons of individual components when it comes to the need for high level of automation within Cloud solution, and explain possible uses of each of these elements and benefits that can be achieved by linking them together.

3rd hypothesis

Monitoring events within Cloud system in terms of digital forensics can be a challenge especially when very large number of components that make up the Cloud are taken into account. In addition to the complexity of the environment, one limitation factor can be the legislation. Problems of legislation are reflected in the fact that provider and buyer of Cloud services may not reside in the same state or country.

It is necessary to define ways and tools which can facilitate access to information needed for digital forensics.

Working hypothesis

Large number of elements that constitute Cloud environment present a problem for the successful performance of digital forensics. Choosing the correct solution for digital forensics is a big problem and a challenge. It is therefore necessary to define necessary procedures, as well as necessary tools, and explain possible ways of keeping track of each of these elements, and to explain pros and cons of individual components. Using different tools and approaches depend on specific case or specific company that is the object of the investigation.

1.5. Methods, techniques and course of research process

Scientific research methods are systematic, critical, controlled and repeatable processes of acquiring new skills necessary to identify, define and solve a scientific problem.

Main principles of scientific research are presented through:

- systematisation - research arrangement that allows creation of natural and logical sequence of processes that are monitored,
- control - conducting research in as specific and controlled conditions as can be achieved to avoid or exclude alternative conclusions,
- criticality - indicates that all claims of events, processes, relationships, and properties must be seriously, honestly and rigorously validated, verified and substantiated.

There are several divisions of scientific research. According to the nature of research there are theoretical and empirical, according to research goals there are fundamental and applied, according to research function there are exploratory research and research aimed at verifying the hypothesis.

Specifically, this research paper uses fundamental and applied research. Fundamental research is used to acquire new knowledge within the field of Cloud systems solutions, while applied research is used to acquire new knowledge and to form a hypothesis for solving the given problem.

Methods of synthesis and generalization are applied in this thesis, as well as basic logical methods of induction and deduction, analytically-descriptive method of virtualization and Cloud service functionality research. Towards the end, the experimental method of verification of basic functionality of Cloud service in a controlled environment is applied.

Note:

The work is divided into three logical sections. The first part explains Cloud system infrastructure (chapter 2), the second section deals with principles of digital forensics (chapter 4), and the third part presents practical examples of information-gathering tools (chapters 5 - 7).

2. Types of services offered using Cloud technology

To better understand what constitutes a Cloud, it is best to start from the beginning and explain what types of Clouds there are. In other words, it would be good to explain what counts as Cloud Computing platform and define which services can be created using Cloud technologies.

Services often identified with Cloud technologies are:

- Infrastructure as a Service (IaaS)
- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Network as a Service (NAAS)

2.1. Infrastructure as a service (IaaS)

*"In the most basic cloud-service model, providers of IaaS offer computers – physical or (more often) virtual machines – and other resources. (A hypervisor, such as Hyper-V or Xen or KVM or VMware ESX/ESXi, runs the virtual machines as guests. Pools of hypervisors within the cloud operational support-system can support large numbers of virtual machines and the ability to scale services up and down according to customers' varying requirements.)"*¹

Also, some other principles are given in the text that deals with Cloud monitoring. They are described in the document: *"SecLaaS Secure Logging-as-a-Service for Cloud."*²

Since the main theme of this thesis is proactive preparation for forensics in private Cloud (IaaS), it is necessary to define the segments that constitute one such environment.

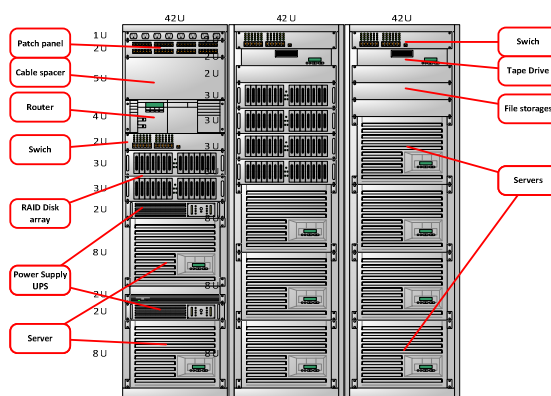


Fig. 1 –Example of presumed physical infrastructure of data centers

¹ http://en.wikipedia.org/wiki/Infrastructure_as_a_service#Infrastructure_as_a_service_.28IaaS.29

² <http://arxiv.org/pdf/1302.6267v1.pdf>

Private Cloud is essentially composed of all the elements that make up each regulated data center with a few differences. This also means that the elements of private Cloud are physical servers, physical network cards, physical routers, switches, storage, surveillance cameras and other physical equipment. However, besides these physical (real) elements, there are virtual elements and their representations in the virtual environment.

In other words, virtual machines that can be placed directly on hosts or remote storages operate on existing physical (real) hosts. Also, these virtual machines have virtual network cards that are connected to virtual network switches. Virtual network switches can be isolated, connected to a host or connected via host to another host and virtual computers.

As in physical environments, virtual environments consist both of physical and logical components. The following figures show the connection between physical and logical infrastructure of hypothetical environment of a company.

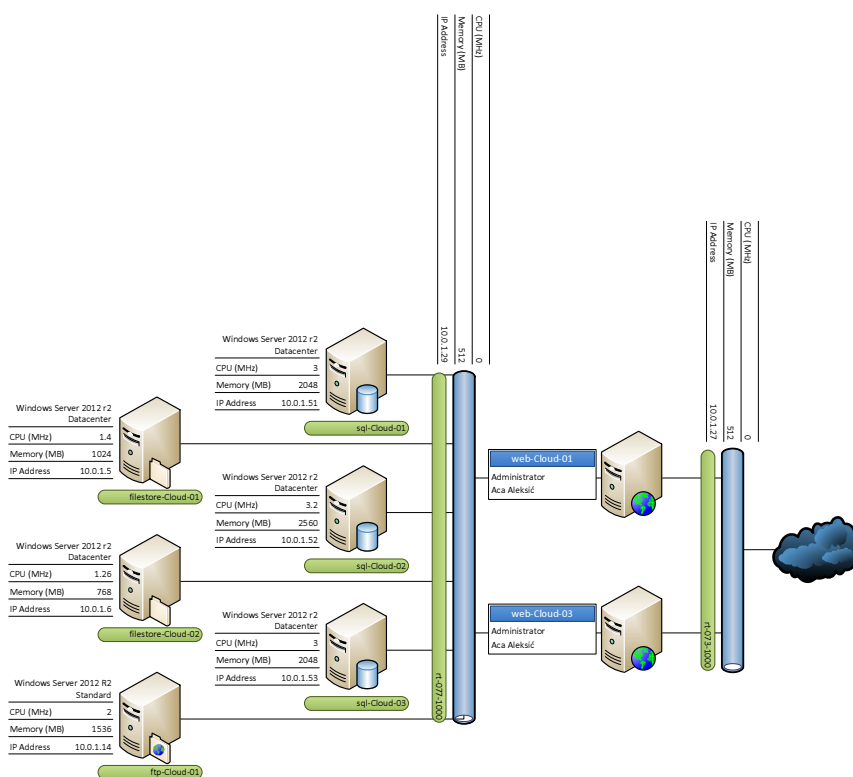


Fig. 2 – Example of logical server and network infrastructure

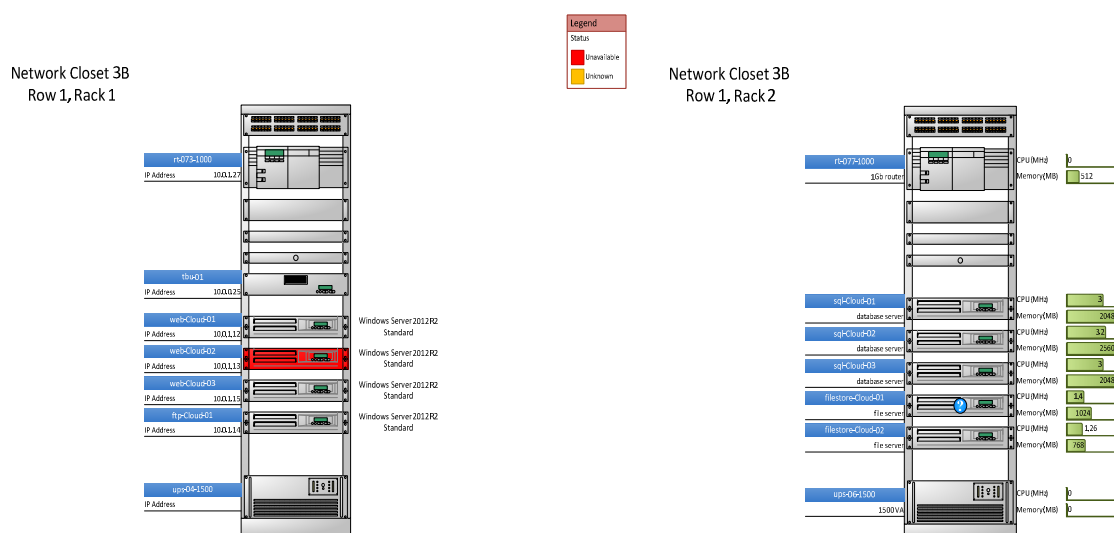


Fig. 3 – Example of physical server and network infrastructure

Before the advent of Cloud computing, virtual solutions were very similar to physical solutions. What's more, they even overlapped with them in logical infrastructure. It was almost impossible to distinguish the difference between physical and virtual machines in logical infrastructure. With the advent of Cloud computing, situation had somewhat changed, both in physical and logical parts. In this way much more complex models could be created using the same (existing) physical infrastructure.

However, there is the question of what does Cloud actually represent? Cloud is a set of physical resources of a data center that are designed for that role. In other words, Cloud represents a number of hosts, network devices and accessories that are treated as a single resource called Cloud. This also means that, when a virtual environment is created, resources that are set aside for Cloud are treated as a single item, i.e. as an available resource. In this way, control and utilization of resources within data center are simplified.

Due to this, there can be more than one Cloud resource within a single data center. Environments created within these Clouds may or may not be interconnected.

This thesis describes how it is possible to organize infrastructure monitoring from the standpoint of service providers, i.e. company that has created private Cloud.

Private Cloud offers the ability to virtualize an environment using software and hardware. In other words, it offers a way to take an existing physical environment and transfer it to a virtual one. This means that physical computer can be transferred to virtual environment and into virtual machines. Networks that are created on physical routers can be virtualized and moved into virtual network. Physical storages can be transferred into virtual, or shared virtual disks can be created which can be used for clusters or file servers. In this way it is possible to create solutions that are counterparts of physical, i.e. real environments.

Taking into account all these elements, it can be concluded that monitoring of such systems can be very serious task because the whole system consists of large number of components.

Each of these components can have its own system for monitoring events and collecting logs. However, these systems do not always have advanced monitoring options, or the ability to collect information in one central point. Processing information obtained in such a way is problematic since there is no automatic integration of these information into a logical sequence of events.

In addition, it should be taken into account that, besides virtual environment, physical (real) environment should be monitored, since it is the basis for setting private Cloud environments.

Moving a company to a virtual or private Cloud environment represents a big step. The decision to create private Cloud environment depends on multiple components and offers a variety of environment customizations to suit the needs of the company. In case of IaaS services, company receives high level of automation of virtual solutions.

Proactive forensic monitoring of such services is quite complicated. This is supported by the fact that service provider offers hardware on which users can install their virtual desktops. In this case, service provider's monitoring is reduced to monitoring physical hosts and networks, while monitoring operating systems and virtual machines depends solely on the user. It can be concluded that, if users have operating systems with no active monitoring, some piece of information will be missing during the forensic investigation.

Creating private Cloud environment depends on multiple components and offers a variety of environment customizations to suit the needs of the company. Therefore, it is necessary to explain what are all the other options available to companies that opt for Cloud technologies.

2.2. Software as a service (SaaS)

*"In the business model using software as a service (SaaS), users are provided access to application software and databases. Cloud providers manage the infrastructure and platforms that run the applications. SaaS is sometimes referred to as "on-demand software" and is usually priced on a pay-per-use basis. SaaS providers generally price applications using a subscription fee."*³

SaaS is used for publishing software solutions offered within existing pre-created application platform. In other words, users can use applications by remote access or through web interface.

This system allows users to use applications that are installed on physical and virtual computers that can be located within private Cloud environments, or within public Clouds. This can best be compared with some services that are publicly available, such as Office 365, which allows the use of the Office package over the Internet and is based on Remote Desktop service (formerly known as Terminal Services).

³ http://en.wikipedia.org/wiki/Infrastructure_as_a_service#Infrastructure_as_a_service_.28IaaS.29

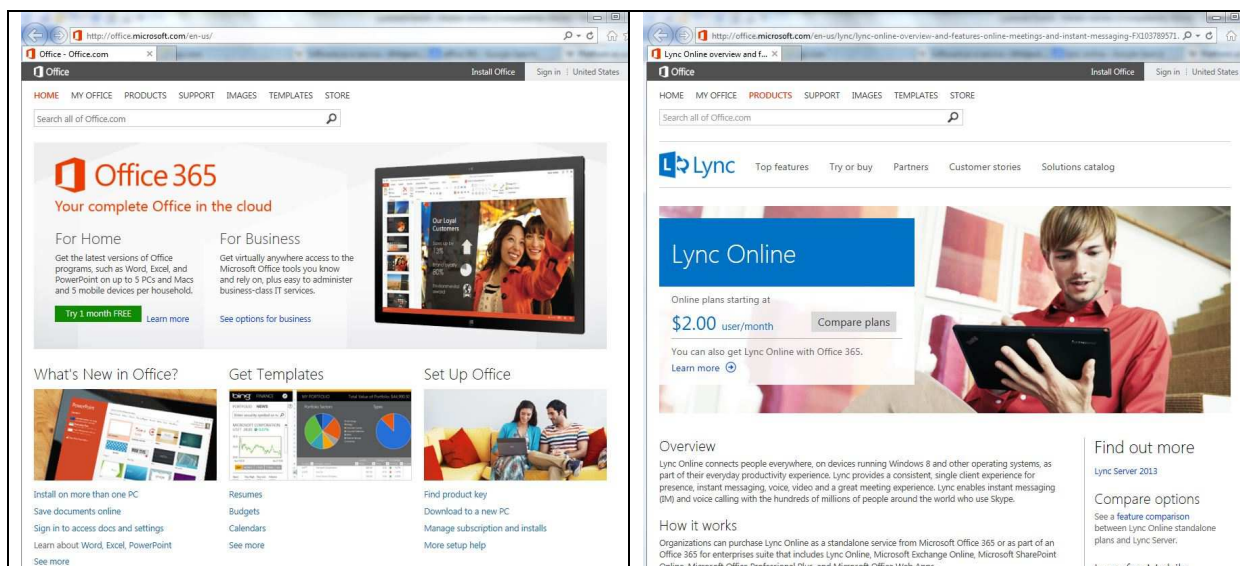


Fig. 4 – Examples of two SaaS services, Office 365⁴ and Lync online⁵

In addition to this approach, there are services such as SQL Server, Exchange Server and Lync Server online. Those services are installed and preconfigured by Cloud provider and are published in such a way that clients can use them in their own environment, whether they are installed on provider's infrastructure, either physical or virtual.

In this way, clients are offered complete software solution that requires specific software and hardware resources within their companies. This reduces the implementation costs of expensive software and hardware solutions. The good side of these solutions is that they allow users to access applications as if they were installed on their computers or in their own environment.

Since the service provider possesses almost complete software and hardware segment, he carries out monitoring and log collecting at the same time. However, in this case, monitoring of events is additionally complicated by the fact that one part of monitoring depends on the user. Part of the components related to solution access are installed at user side. If it is assumed that the user did not activate any monitoring on their side, that part of information may remain uncovered by monitoring systems.

⁴ Snapshot of Office 365 service home page

⁵ Snapshot of Lync Online service home page

2.3. Platform as a service (PaaS)

*"In the PaaS model, cloud providers deliver a computing platform, typically including operating system, programming language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers."*⁶

This method of Cloud service enables the use of offered software platforms and tools for creating applications. Applications that are created can be immediately placed at already predefined slots that actually represent operating systems running either on virtual or real hardware. Also, those applications can and usually are virtualized so they could be deployed on different OS platforms. In this way, developers can customize offered solutions to their specific needs.

Thanks to this way of publishing applications, anyone can develop different software for their specific needs.

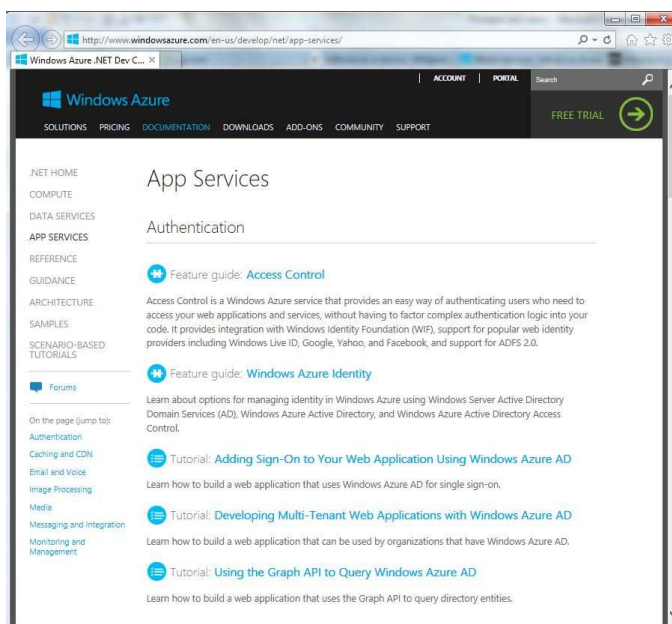


Fig. 5 – Example of IaaS Azure⁷ App service

However, applications developed in such way may not necessarily be tailored to safety standards which, in this case, makes monitoring events very difficult.

Since the complete hardware and software infrastructure is located with the service provider, most of the information can be gathered from there. However, monitoring events within the application depends on the application's ability to execute monitoring. This can pose a problem in case that, while developing the application, creating modalities for monitoring were not taken into account.

⁶ http://en.wikipedia.org/wiki/Infrastructure_as_a_service#Infrastructure_as_a_service_.28IaaS.29

⁷ Windows Azure APP service web page

As an example of a PaaS solution, IIS web service (web server) can be taken as the basis for PaaS platform for which users create applications. While using web service as a platform for developing software solutions within IIS service, there are systems for collecting logs and monitoring services that are embedded in the operating system within which IIS runs as a service. However, it is impossible to predict which applications will be used on it, as well as the ways in which they will be created.

Functionality, safety and traceability of applications that run on a web server, depend exclusively on the skills of developers who wrote those apps. Also, levels of security settings for these applications depend on developers and their ability to allow monitoring. Hindering factor in collecting information is the likelihood that it might not be possible to set up monitoring for the application created in such a way. The reason may lie in the fact that monitoring was not planned or configured when creating custom application.

Looking at this kind of resource publishing, it can be concluded that monitoring, for the most part, depends solely on the developer of the application.

2.4. Network as a service (NaaS)

*"A category of cloud services where the capability provided to the cloud service user is to use network/transport connectivity services and/or inter-cloud network connectivity services. NaaS involves the optimization of resource allocations by considering network and computing resources as a unified whole."*⁸

The idea behind NaaS service is to optimize communications. In addition, NaaS establishes some types of traffic that were not possible to create in the past. In this way it is possible to create networks that are spread across multiple hosts, allowing communication between virtual machines regardless of the type of traffic. Of course, network traffic is not restricted solely to Cloud framework. In other words, traffic can be established through private and public Clouds.

The role of NaaS is not only network traffic optimization; it also performs the role of controlling the flow of information. The reason for this is its ability to offer different groups of traffic flows to users, and different modes of access to resources within Cloud. In this way, rules that allow or prevent access to resources within Cloud solutions can be created. Also, using NaaS it is possible to create isolated networks for communication between virtual machines within a single Cloud resource, regardless of how many physical hosts that Cloud resource is spread across.

NaaS service and its infrastructure are described in a scientific paper published by Microsoft Research titled: *"Naas: Network-as-a-Service in the Cloud."*⁹

⁸ http://en.wikipedia.org/wiki/Infrastructure_as_a_service#Infrastructure_as_a_service_.28IaaS.29

⁹ <http://research.microsoft.com/pubs/198841/costa12naas.pdf>

3. Description of components and their functionality within Cloud solution

Environment that was used for this thesis represents a simulation of a private company. Therefore, one should start from the assumption that a particular company requires very high level of automation and functionality of virtual solutions. This is demonstrated through the use of large number of virtual machines, virtual and physical applications. In addition, it is necessary to define the manner of publishing certain segments or entire virtual environment to users. To achieve this, the company can completely implement all of the above services that Cloud technologies offer.

Of course, when creating such solutions within the company, the most important fact is to define the company needs for them. This solution is very complex and requires both hardware and software resources for this to be accomplished. Besides this, the company needs IT personnel with experience in wide variety of technologies. All this amounts to relatively big expenses for the company. So to validate those expenses there have to be some benefits.

Accordingly, the first step may be to simplify hardware infrastructure. This can most easily be achieved using virtualization services.

Using virtual machines is no more novelty in the world or in our country. There are different platforms for hardware and software virtualization. Some of these are Hyper-V, VMware, Citrix, VirtualBox and others.

The difference between most of these solutions is reflected in different user interfaces and options that vary in different versions of the software, both among different manufacturers and among different versions within one of them. In addition, further confusion may be brought in a situation when, in some cases, different names are used for the same thing. Example of different naming could be seen when recording the current state of a virtual computer. When it comes to Microsoft Hyper-V, such recording is called Snapshot, whereas with VMware it is called Checkpoint. Also interesting is the fact that Microsoft used this name until the appearance of Windows Server 2012 R2, when Snapshot was renamed to Checkpoint, as can be seen in the figure below.



Fig. 6 – Example of one manufacturer's different naming of the same thing

In addition to these cosmetic, there are also some functional differences. These differences are reflected in the types of supported operating systems and hardware support. Examples could be seen through increased support for different operating systems with each new version of virtualization software. Also, with the improvement of physical hardware, which is reflected in faster and better processors and support for larger amounts of memory, virtual solutions keep pace and follow the development through their own versions.

Regardless of all these differences, the essence remains the same, which is to create virtual instead of using physical computers, and that those virtual computers are almost in no way different from real computers. Virtualization gives company better utilization of existing hardware resources. This also means that it is possible to run not one, but multiple operating systems on existing computer. These operating systems can share hardware of real computer they are executing on.

The example in the thesis represents an environment that is completely built using virtual machines. The only real components are hosts and a network switch which connects them. This is the most realistic representation of conditions that can be expected in a company that has decided to use virtualization.

For purposes of the thesis, virtual Cloud environment is created. The bases of virtualization is Microsoft Hyper-V platform. The base of the platform and the entire solution is Windows Server 2012 R2. This operating system was chosen because of the expanded support for operating systems and hardware resources. An additional feature that influenced this decision is support for virtual machines Generation 1 and 2. Both versions of these virtual machines were used in the thesis.

Generation 2 virtual machines offer a number of advantages compared to Generation 1. They are reflected in the following:

- Secure Boot (enabled by default)
- Boot from a SCSI virtual hard disk
- Boot from a SCSI virtual DVD
- PXE boot by using a standard network adapter
- UEFI firmware support

Main differences between Generation 1 and Generation 2 machines are shown in the fact that Generation 2 virtual machines are better optimized for work through reducing the amount of emulated hardware. They also come with installed PXE boot which allows these virtual machines to boot from network drives. In this way, it is possible to create diskless machines. Apart from these new formats for virtual disks, they have also noticeably increased the size of virtual disk files. Also, now it is possible to assign up to 64 virtual processors to virtual machine, as well as many other improvements.

Figure below shows differences in configuration between virtual machines Generation 1 and Generation 2.

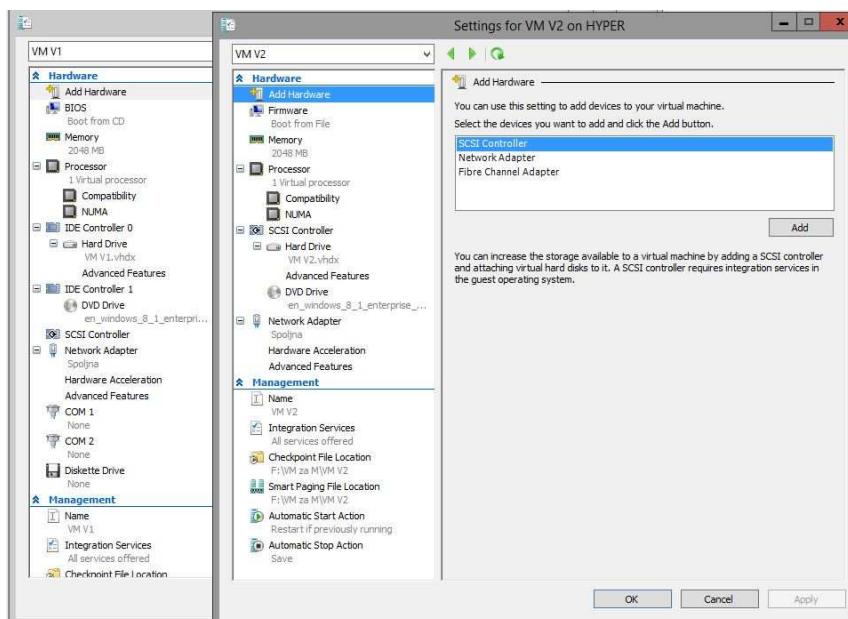


Fig. 7 – Differences in configuration between virtual machines Generation 1 and 2

Generation 2 virtual machines bring a number of advantages over the Generation 1. However, they also bring a certain number of limitations. The biggest limitation is currently reflected in operating systems that can be installed on virtual machines Generation 2. Those are only Windows Server 2012 and 2012 R2, and client operating systems Windows 8 and 8.1. These and other information are described on Microsoft TechNet¹⁰ website in detail. All in all, virtual machines Generation 2 may be a critical factor that can prompt companies to use this operating system as a foundation for virtualization.

¹⁰ <http://technet.microsoft.com/en-us/library/dn282285.aspx>

3.1. Virtualization using Hyper-V hosts

To better understand all processes required for creating and using Cloud virtual environments, one should start from the beginning. First step is creating initial virtual environment.

Creating a single virtual machine is a relatively simple process. This process consists of only a few elements, such as defining the amount of RAM memory, selecting new or existing virtual disk and network selection. However, adding additional processors, disk drives, and advanced configurations are carried out afterward. Therefore, with increasing number of virtual machines that a company needs, grows the increasing number of operations which are necessary for its creation. This also means that creation of large number of virtual machines with same features is quite limited and complicated. Also, controlling multiple host computers is hard because it is necessary to use separate console connections to each individual host.

Creating multiple virtual machines in this case is based on the creation of BASE image for each type of virtual machine to be multiplied. BASE images represent virtual disk of an operating system with pre-installed and configured applications. Creating BASE image is very hard work because it is necessary to install and configure each such virtual computer. Then it is necessary to remove SIDs from that image and save it to disk. This procedure is very time consuming and requires large amounts of free space on disks to store all BASE images. Also, these images have to be copied to all hosts on which virtual machines that are using them as their basis. This complicates and slows the administration of virtual machines and hosts with the increasing the number of hosts.

Therefore, there is a need for centralized administration of hosts and virtual machines. For the purposes of centralized administration, there are different solutions from different manufacturers. Examples include Microsoft System Center Virtual Machine Manager, VMware vCenter, IBM SmartCloud Orchestrator and others.

Besides all the differences between these solutions, which are reflected in whether or not there is the possibility of creating a Cloud environment, however, as in the previous case, there is one common aspect. This aspect is reflected in the fact that they are used to create and maintain a large number of virtual machines and hosts. This approach enables centralized control and monitoring of part or the entire virtual environment.

In this thesis, some segments of System Center 2012 R2 products have been used. More specifically, it uses System Center Virtual Machine Manager 2012 R2 as the basis of system for hosts monitoring and management. In addition to these basic roles it has the ability to create private Cloud environments. It also has the ability to connect private Cloud solutions with public Cloud environments, thus creating hybrid Cloud environment.

3.2. Virtualization using VMM

As a major advantage of increasing automation, this offers the possibility of creating virtual machine templates and service templates. With this option it is possible to quickly create large numbers of same or different virtual machines. In addition, there is the ability to create self-service portals that allow users to automatically create virtual machines according to predefined templates or adapted to user needs.

Figure below shows part of VMM console with focus on configuration of virtual service templates.

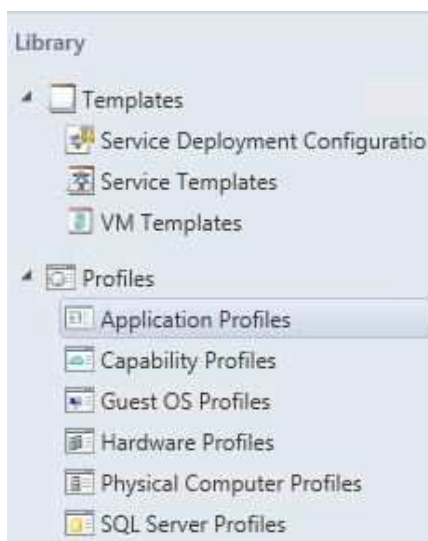


Fig. 8 – Example of profiles and templates in VMM

Virtual Machine template allows creating virtual machines that have unique hardware settings. In addition to these settings, it is possible to reconfigure operating system of each new virtual computer. It is also possible to install necessary roles on desired computers and reconfigure some services. Examples of these configurations are seen in already predefined templates, for example, like in SQL server. With this kind of template it is possible to install SQL server on a virtual machine during its creation. In addition to SQL template, it is possible to create a template for any other application using Application Profiles. In this way, virtual machines can be very well adapted to user needs.

The advantage of using templates is reflected in the fact that there is no longer a need for large numbers of BASE images for a number of different virtual machines. In fact, it is possible to use only one initial virtual image and different profiles to create a number of different virtual machines.

It is also possible to create service template, but to better understand what that represents, it must be taken into account that modern applications often consist of many components, i.e. they are modular. This can be illustrated through an example of a bank's web site where the bank's customers check their account balance and make payments. In this case the web site is only the front of the whole system, since it represents portal for accessing information. The

information are displayed in the applications running within a web service. Information themselves are located in the database, which is usually located on another server. Taking a look at this situation it can be seen that this solution consists of several components, such as web server, database server and the application. In other words, for this solution it is not sufficient to create single virtual computer or to use single templates, since it is also necessary to create links between existing components. Creating several such component solutions is achieved using service templates that can be created using System Center Virtual Machine Manager 2012 R2.

Hereinafter, System Center Virtual Machine Manager 2012 R2 will be called VMM.

The thesis uses VMM as the basis for private Cloud environment and manages the virtual environment with its help. Using this method of infrastructure virtualization, IaaS Cloud role was simulated.

The thesis uses different versions of templates and service templates for the simulations. It also uses VMM as the basis for private Cloud environment. In addition to these uses, VMM was used for managing virtual environment.

3.3. Virtualization of presentation

In addition to creating virtual machines, in this case, the company may opt for virtualization of presentation and publishing applications installed on the servers. This is achieved by using terminal server-client service.

Very important components in the functioning of a company, in addition to computers and operating systems, are applications that are used in day to day operations. Applications can be installed within client operating systems or on servers. Installation and maintenance of these applications is complex process that is no different when it comes to physical or virtual computers. Also, applications progress and advance over time, which entails implementing patches and upgrades. With each newer version of a specific application, hardware requirements for its execution also grow. Increasing hardware requirements for new versions of the application causes the need to purchase new hardware. This also increases costs of deployment of new applications. Because of these ever growing requirements it is necessary to have very demanding applications run on clients with older hardware who would not be able to run them anyway. Therefore, the solution is to buy or utilize servers in a way that the applications will be published from them and allowed to be used by clients. This is achieved by using terminal server client service.

Publishing applications in this manner allows the company to distribute once installed and configured application to its customers or users from one central point. In addition, this approach of publishing applications allows the use of hardware demanding applications from any client. It also offers more possibilities like the use of old and incompatible clients, which

reduces the cost of constant investments in new hardware. Also, in this way it is possible to use applications with mobile devices.

In addition to publishing applications, it is possible to publish virtual desktops. Virtual desktops are virtual machines with client operating system. Their role is to enable users to have their own desktops regardless from what computer or device they access them. Also, Virtual Desktop Infrastructure (hereinafter referred to as VDI) offers the ability to use different versions of client operating systems. There are several solutions that allow this type of VDI solutions publishing such as Microsoft Remote Desktop Services (hereafter RDS), Horizon VMware View, XenDesktop Virtual Desktop and others.

The figure shows a web portal created using RDS services within Windows Server 2012 R2.



Fig. 9 – Example of a web site with published applications and virtual desktops

The thesis uses applications published using RDP service and Session host role. The bases of the solution is Windows Server 2012 R2 virtual machine with installed RDP role. On that machine application software has been installed that is published to users for remote access.

Using this method of virtualization of presentation SaaS Cloud role was simulated.

3.4. Application virtualization

The next option that a company can use is the use of virtual applications. Instead of using physical applications, they can be virtualized and thus increase their compatibility with operating systems and hardware environments in which they are executed.

Therefore, an equally important option that companies can take advantage of is publishing virtual applications. Virtual applications are applications that are independently virtualized and not dependant on single operating system. Very important fact is that users will not notice that they are using a virtual application. "Look and feel is the same" as users can access both local and network resources using that application. Microsoft's representation of this solution is called Application Virtualization (hereafter App-V).

Using App-V it is possible to create virtual application using software called Sequencer. Sequencer software monitors installation of the application which needs to be virtualized. It records changes that the application creates in the registry, folders it creates on the hard drive and services it runs or uses. This allows creation of a virtual application package using the Sequencer. By creating virtual applications it is possible to simultaneously run multiple, mutually incompatible, applications on the same computer.

An example may represent the use of two different versions of a financial application. For example, a company is currently using the application version 1.0 that is written for Windows XP. However, after switching to Windows 7 this financial application had to be changed to version 2.0. At that moment there was a problem presented in accessing the data from the old database, which only works with application version 1.0. However, version 1.0 cannot be executed within Windows 7. The solution is to virtualize one, another or both versions of the application. In this way, user can simultaneously use both versions on Windows 7 and on Windows XP.

Such App-V package can also be installed on terminal RDS server and then be published to clients. Another option is to distribute it to each client computer locally, from which this application will be running.

Using this method of application virtualization it is possible to simulate PaaS Cloud role.

3.5. Network virtualization on Hyper-V hosts

Taking into account the fact that today's applications are modular and all their components are not stored on a single computer, either physical or virtual, there is the necessity of establishing network communications between virtual machines, as well as between applications running on these operating systems.

The basic idea of a computer network is communication between resources. Network equipment is used for communication between computers. That equipment can be hubs, switches, routers, firewalls and other devices. Each of these devices has its own role and function; each uses certain methods of communication and has good and bad qualities. Their common feature is that they allow connection between multiple computers and information sharing between them.

With the advent of virtualization, virtual network devices appeared. These devices have the same or similar functionality as physical network devices. For example, each virtual computer may have one or more virtual network adapters. Each of these network adapters can be connected to a virtual switch. As in previous cases, each of these components carries a different name depending on the application with which it has been created, as well as the virtualization version of the company that made it. The following example describes virtual switches that can be created under Microsoft Hyper-V platform.

Basic division of virtual switches are these three types:

- Private network
- Internal network
- External network

Private network virtual switches can be used for isolated communication between virtual machines within the host. In this way, virtual machines that are connected to this switch are isolated and can only communicate with each other.

Internal network is virtual switch that enables communication to virtual computers that are connected to it, as in previous case, but with the added option to communicate with host computer from which it runs. Besides this option, internal network switches have the ability to create virtual LANs, i.e. create VLAN IDs. This feature allows defining and separating which computers can be connected to each other.

External network is special kind of virtual switch that is using physical NIC (Network Interface Card) and that allows virtual machines to communicate with other hosts on physical network, and with other virtual machines that are on other physical hosts.

3.6. Network virtualization using VMM

Virtual machines that run on hosts also need to communicate with other virtual and physical computers. This communication takes place through physical and virtual components.

However, within the Cloud, and as a result of previously mentioned need for communication between applications that run in the Cloud, there is a need to create isolated virtual networks that span multiple physical hosts. That was not possible to achieve with previous three virtual switches which do not allow spanning across multiple hosts.

*"In VMM, the networking infrastructure is a group of configurable network resources that can be used to create, model, organize, and manage virtualized server network connectivity. The following sections describe the configurable components and their subcomponents."*¹¹

With the advent of System Center VMM 2012 and Cloud technology within it, the situation has changed. Virtual networks and switches that can be created using VMM are:

- Logical Networks
- Network Sites
- MAC Address Pools
- Virtual IP Templates
- Load Balancer Integration
- Logical Switches
- Port Profiles
- Port Classifications
- Network Service



Fig. 10 – SCVMM virtual networks

The thesis uses virtual switches and networks created using VMM service. In this way, the role of NaaS service is simulated.

¹¹ Knjiga "Implementing an Advanced Server Infrastructure," Microsoft Press, 2012.

3.7. Description of hardware and software configuration of master's thesis

Case study that is the subject of this thesis deals with the principles of monitoring and collecting information (logs) in private Cloud environment of a company.

Environment that is used as an example is based on Microsoft System Center platform.

The following text describes the components of Microsoft System Center 2012R2 solution that are the basis of private Cloud environment.

System Center 2012R2 package is composed of following components:

- Virtual Machine Manager - is the basis of Cloud environment, it is used to create the Cloud resources, for creation and management of virtual machines, installation and management of virtualization hosts.
- App Controller - offers the ability to deploy services based on pre-configured templates, and provides the ability to connect to public Clouds and therefore manage hybrid environments.
- Configuration Manager - its basic role is improved settings management with remediation, antivirus service, deployment of clients, servers and applications.
- Operations Manager - tool for monitoring process activities and service functioning, monitoring applications and performance.
- Orchestrator service - used to automate processes using predefined tasks.
- Service Manager - the hub for process management in the System Center portfolio, through which business processes within the Cloud can be monitored.
- Data Protection Manager - it is designed to protect and recover data from such key business applications as: Windows file shares, client data, and system state; Hyper-V technology; SQL Server; SharePoint products and technologies; Microsoft Exchange Server.

Each of these components is an individual unit and requires installation on separate server, whether it is physical or virtual computer. Also, with the use of some or all of the components in an appropriate manner it is possible to create highly safe and highly automated solution. This level of automation is present in solutions such as Windows Azure: Microsoft's Cloud Platform.¹²

In order to understand all the necessary different components, it is best to describe the environment in which the simulation was performed. It consists of two physical computers with installed Windows Server 2012 R2 operating system. Hyper-V roll was installed on these computers, as support to virtualization. Computers are connected to a network switch that allows communication between them and a link to the internet router. On one of the computers there is a virtual machine with installed Windows Server 2012 R2 that hosts specific roles. One of those virtual machines plays the role of a domain controller, and on the other SQL 2012 database while another separate one is System Center Virtual Machine Manager. All the roles are installed as add-ons to host OS. In addition to these computers, several additional virtual machines with different roles were created. These computers are used for various simulations. These components represent an environment that is complex

¹² Windows Azure, link: <http://www.windowsazure.com/en-us/>

enough to simulate one private Cloud environment that comes very close to a real world example.

Considering the fact that this is Microsoft solution and that it uses centralized authentication system, it is necessary to have Active Directory Domain service. In addition, it is necessary to have certain number of computers that will serve as virtualization hosts and at least one computer that will have Virtual Machine Manager Server. That presents the minimum necessary resources for private Cloud.

Initial installation and configuration of Active Directory Domain service, as well as the basics of security solutions, are explained in author's graduate paper.¹³ Subject of further text will be monitoring principles within Active Directory Domain service, creation of monitoring policies and log checking. Also, special attention was paid to the installation and configuration of VMM service, creation of virtual machines, networks and the Cloud.

¹³ [Implementacija bezbednosnog rešenja u okviru školskog centra kompanije CPU d.o.o.], Lj. Ivaniš

4. Basic principles of digital forensics

Basic principles of digital forensics are to find out what happened, when something happened, how it was done, whether that event was repeated, who was the perpetrator, the manner and the place from where it was done. In addition, digital forensics must provide evidence of such events, which must be valid before judicial authorities. Besides, the immutability of information is also the basis for conducting high-quality digital forensics. To achieve this, different forensic tools for event detection process can be used.

First of all, it is important to define processes and principles of digital forensics.

Computer forensics or digital forensics is a process that consists of following segments:¹⁴

- Identification of digital evidence and their sources,
- Presentation of evidence,
- The analysis of digital evidence,
- Authentication of digital evidence,
- Presentation of evidence in proper and legally acceptable manner.

Each of these segments is part of forensic case research. At the same time, each segment also consists of additional subcomponents. Each of these components is equally important for successful execution of digital forensics.

It is also necessary to draw attention to the principles of digital forensics, which are also the basis of proper execution of digital forensics. Those are the following:

1. Actions taken by the investigators should in no way lead to change of data on a computer or media for storing information and thus jeopardize the evidence that should be used in court.
2. When there is a need for the investigator to access original data on computers or storage media, they must possess high level of expertise, as well as permission to do so. In addition, they must provide an explanation of the reason why that is necessary and what are the consequences of those actions.
3. All the actions over the evidence taken by the investigator must be documented. This is necessary for reasons of verifiability of expertise. In other words, it is necessary to enable verifiability of presented evidence by a third party.
4. The person in charge of the case (the investigator) is fully responsible for compliance and enforcement of legislation. In other words, the investigator is responsible for complying with the law and legal procedures.

¹⁴ Digital forensics, Wikipedia

4.1. Problems faced by digital forensics

Given the complexity of Cloud computing environments, the execution of forensic investigation almost seems impossible. Therefore it is necessary to devise a way to facilitate collecting forensic information. One possible solution is proactive log collecting and event tracking, since preliminary data collecting can facilitate digital forensics in Cloud environments. Examples of log collecting and tools used for this purpose, aimed to facilitate forensic investigations, have been described in this master's thesis.

However, in order to better explain these processes and to facilitate the investigation for forensic teams, it is possible to set up preventive monitoring and log collecting. Generally speaking, when it comes to preventive monitoring or surveillance in modern information society, it is possible to monitor everything or almost everything.

The greatest problem in this case is the legality of monitoring, i.e. invasion of privacy of individuals. This is also defined in Data and personality protection act¹⁵ of Republic of Serbia, which was published in "Službeni glasnik RS," no. 97/2008.

Therefore, it is necessary to strike a balance between what is monitored and the right to privacy of individuals. This is extremely difficult, especially if it is taken into consideration that the information necessary for well-designed digital forensic investigation falls exactly in the category that affects privacy of the individual.

To counteract or bypass this, companies use different types of ways to inform users (notifications) that their digital communications are monitored. Also, they often use different types of contracts where service users and staff are forced to abide by the policy of information collecting including some personal information. With these contracts, the ownership of the data usually changes, so the company becomes the owner of all of the information, which gives it the right to monitor the information.

It must be taken into account the fact that a company that offers Cloud services needs not be located in the same state or country as the client. Also, global Cloud services providers often have data centers located in many states and countries around the world. Taking into account the structure of Cloud environment and the fact that virtual machines can be located on any segment of Cloud resources, it may happen that virtual machines of one client are scattered all over the world. In this case, the company may not want to grant access to its resources as they are located in different countries that are subject to various laws and thus prevent digital forensics. These facts can almost completely prevent digital forensics in public Cloud.¹⁶

In addition, large number of service providers have different types of contracts that provide or disallow various things. However, most contracts generally raise a number of obstacles that are put in front of the person who needs to do forensic investigation.

Examples can be shown through a number of different SLAs (Service Level Agreements) or through Privacy Statement. All public Cloud services providers have these contracts.

¹⁵ <http://www.minrzs.gov.rs/doc/porodica/ostali/Zakon%20o%20zastiti%20podataka%20o%20licnosti.pdf>

¹⁶ [Technical Challenges of Forensic Investigations in Cloud Computing Environments], Burk D.

Relatively interesting and a very good example of such a contract can be a contract related to Microsoft Public Cloud Solution Windows Azure Privacy Statement.¹⁷ For example, this contract, in segment relating to information privacy, *"Sharing Your Information,"* reads as follows:

"We will not disclose Customer Data, Administrator Data, Payment Data or Support Data ("your information") outside of Microsoft or its controlled subsidiaries and affiliates except as you direct, or as described in your agreement(s) or this privacy statement."

This also means that Microsoft has complete information about all events that are taking place in relation to a virtual environment, as well as the option to dispose of them at will within their own company.

In addition, the following is also stated:

"We will not disclose Customer Data to a third party (including law enforcement, other government entity, or civil litigant; excluding our subcontractors) except as you direct or unless required by law. Should a third party contact us with a demand for Customer Data, we will attempt to redirect the third party to request it directly from you. As part of that, we may provide your basic contact information to the third party. If compelled to disclose Customer Data to a third party, we will use commercially reasonable efforts to notify you in advance of a disclosure unless legally prohibited."

Microsoft may share Administrator Data or Payment Data with third parties for purposes of fraud prevention or to process payment transactions."

The text specified in the example indicates the option to access user data but not Cloud provider's. This also represents a huge problem, even in case that a warrant to obtain information from the provider is issued. Although this document may be completely valid and issued in the country of user of Cloud service, it may happen that it has no executive value in the country of Cloud service provider. In this way the forensic investigation can be blocked.

In addition, companies often change their contracts which can be read on the same page in *"Changes to this Privacy Statement,"* which states the following:

"We will occasionally update our privacy statements to reflect customer feedback and changes in our Services. When we post changes to a statement, we will revise the "last updated" date at the top of the statement. If there are material changes to the statement or in how Microsoft will use your information, we will notify you either by posting a notice of such changes before they take effect or by directly sending you a notification. We encourage you to periodically review the privacy statements for the products and services you use to learn how Microsoft is protecting your information."

In other words, even if there was the possibility of executing a warrant in the beginning, Cloud provider can change the SLA and thus prevent the work of the investigators. Also, in this case, they don't have to notify the customer directly. Therefore, it is explicitly stated that the customer is obliged to constantly check whether there has been a change in the contract.

¹⁷ <http://www.windowsazure.com/en-us/support/legal/privacy-statement/>

A very important fact may represent a situation in which Cloud providers automatically delete the contents of personal user information when the contract expires. For example, Cloud service user has paid to use a virtual computer on public Cloud service for a period of 30 days. During this time, the virtual computer could have been used for different purposes and have different software installed on it. However, after 30 days have passed, Cloud provider automatically deletes the computer along with all the information and content that were on it. Therefore, in case that the computer was used to commit a crime, all the information about that were deleted along with the data.

All these situations make digital forensics in public Clouds almost impossible. However, there are two possible scenarios for collecting forensic information when it comes to IaaS Cloud. The first is remote investigation and information gathering, and the other is to obtain information directly from service providers. Each of these scenarios uses a variety of approaches and tools for collecting forensic evidence.

This means it is still possible to perform digital forensics on client's side. In other words, it is possible to set up a so-called proactive forensics. This refers to the collecting of available information using monitoring systems that come with operating systems or devices.

One example could be detection of viruses or network attacks. These attacks can be detected in different ways, or by using variety of tools. In this case, investigator's goal is to find the source of infection, as well as to recognize (detect) all the other resources that could be infected. Mitigating circumstance is that the events of this type are relatively easy to recognize as they are "very noisy," in other words, they leave a large footprint. In addition, it is also necessary to examine the credibility of the threat, as well as its severity. This is achieved by collecting information about the incident, which is represented by monitoring behavior of the threat. These actions must be carried out so as to remain within legal limits regarding the privacy of information, and in such a way that they do not change their content.

When it comes to network attacks, it is necessary to narrow down (filter) the scope of the investigation in order to obtain more reliable information. This can be achieved in following ways:

- linking information to existing cases,
- directing investigator in the right direction,
- taking advantage of information about the level of knowledge required to commit a criminal offense,
- facilitating a structured approach to information to investigators for the sake of network abuse research.

However, the ability to detect offenses that use network is a challenge, both for the company and the investigator. Also the complexity of IaaS network environment is another challenge. This challenge is even greater if it is taken into account that most companies do not have or did not set up any system for monitoring events, regardless of whether they are systems for real-time monitoring or systems for collecting information into logs. In addition to these cases, there is a problem in the very tools used to collect information, because it can happen that some of the tools that are used to collect information may not be recognized in court.

Another problem may represent a situation in which a company collects information, but the sheer amount and storing of these information can make it difficult to investigate because of the large amount of data that was collected.

All these situations must be overcome, so it would be possible to do high-quality digital forensics.

It can be concluded that digital forensics in its essence is series of methods and techniques used to gather information. These information can be used in court proceedings. Therefore, it is necessary to draw attention to possible scenarios when that is not possible or almost impossible to achieve. In the next few lines several situations are described that pose the biggest problem for the execution of digital forensics in Cloud environments.

Given that the theme of this master's thesis is Cloud system and its subsystems, it starts from a situation where, for example, someone launches Distributed Denial of Service (hereinafter DDoS) attack from rented virtual machines of some public Cloud provider. Upon completion of the attack it is enough to delete or shutdown these virtual machines. Also, those machines can be automatically deleted by the Cloud provider. The investigation of digital forensics in this case, and when it comes to public Cloud, has a serious problem, since it depends solely on Cloud service provider (hereinafter referred to as CSP) and their willingness to provide access to the information. Assuming that resources that were used in the attack are deleted accidentally or intentionally by the CSP or user, the only way to connect the perpetrator to the event was to prove that they were logged in a Cloud service or had access to a service at that time. In most cases, it is almost impossible to prove that the perpetrator had accessed certain Cloud resource at a given time.

Another example may constitute storing of illegal information in the Cloud. In this way, offenders have no illegal information on their computers but keep them stored in the Cloud and have grounds to deny any involvement in the crime.

Additional example may represent the fact that a single Cloud resource holds virtual computers of different users. This incredibly complicates forensic investigation because the information in the log files are intertwined. In other words, log files that monitor events related to virtual machines contain information about all virtual machines within a Cloud resource. This also means that the perpetrator may claim that the information contained in these log files do not explicitly refer to events related to perpetrator's virtual machines. This is a huge problem for the investigator, given that the logs contain information from other users as well. In this way, investigation of a perpetrator may question the right to privacy of other users, which can also prevent the CSP to provide requested information.

Given that the problems that are put in front of digital forensics are quite complex, this master's thesis attempts to examine how can these situations be adequately mitigated. It starts from the fact that the entire Cloud environment is in the possession of a company, to ensure that all the information are completely reachable, as well as they are owned by the company. In this way, the thesis tries to define what information are possible to claim from CSP in case there is a need for forensic investigation.

4.2. Description of the environment used in master's thesis

Below, some of the basic policies that are necessary for collecting information will be explained. These systems can be used both in private and public Clouds.

Given that the theme of master's thesis is proactive preparation for digital forensics in private Cloud environment, this holds most of the focus. In other words, the focus of the paper relates to methods and tools for collecting information from servers or virtual computers that are owned by one company.

For the purposes of the thesis Microsoft System Center 2012 R2 solution and its components were used. The main component that is used to simulate private Cloud environment is System Center Virtual Machine Manager 2012 R2 (hereinafter VMM).

Another big advantage is the modularity of the system. This modularity enables the use of each service as an individual or as a group of products. Modularity of IaaS solution can be also a big problem when it comes to the execution of digital forensics within public Cloud infrastructure. However, taking into account that private IaaS infrastructure was used for master's thesis, the situation is somewhat made easier.

Starting from the statement that the entire System Center 2012 R2 package doesn't have to be used, it can be said that this facilitates collecting of information necessary for digital forensics.

Since the subject of the paper is to enable proactive digital forensics in private Cloud environment, the focus lies in this segment. To achieve this goal, it is necessary to determine places and manner of collecting necessary information. That is why it starts from computer's operating systems. Taking into account that the thesis uses Windows Server 2012 R2 as the main operating system for collecting information, tools that are built into it can be used.

Tools used for collecting information within this operating system can be divided into two groups.

The first group includes tools for collecting information in real time. Some examples of these tools can be:

- Task Manager, a tool that provides a quick overview of active services and applications. In addition, it can also be used to check the system load.

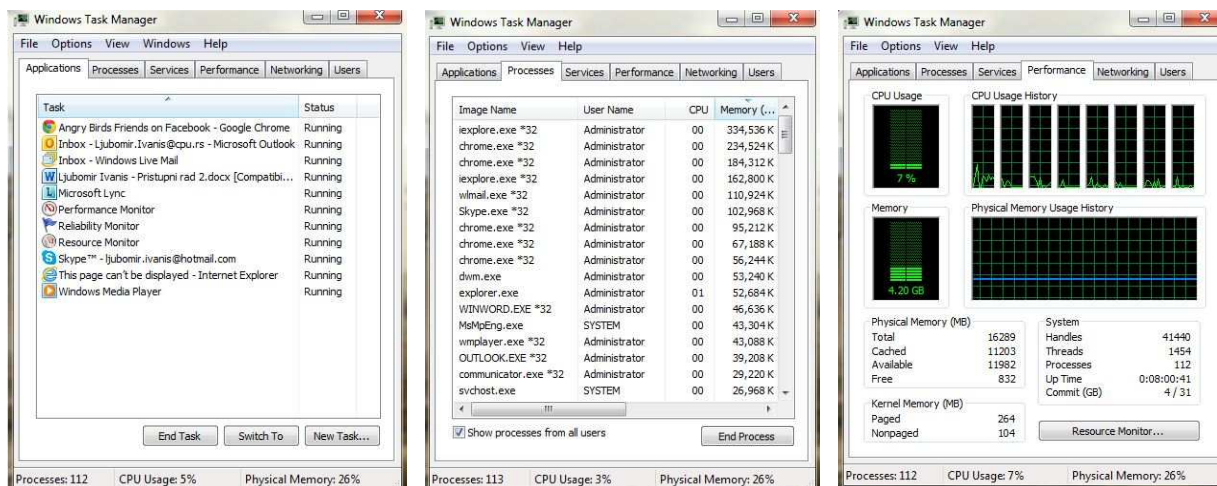


Fig. 11 - Task Manager

- Windows Resource Monitor, a tool that gives more information about events within the operating system than Task Manager, as well as processes that are running. It represents more complex tool and provides much more information.

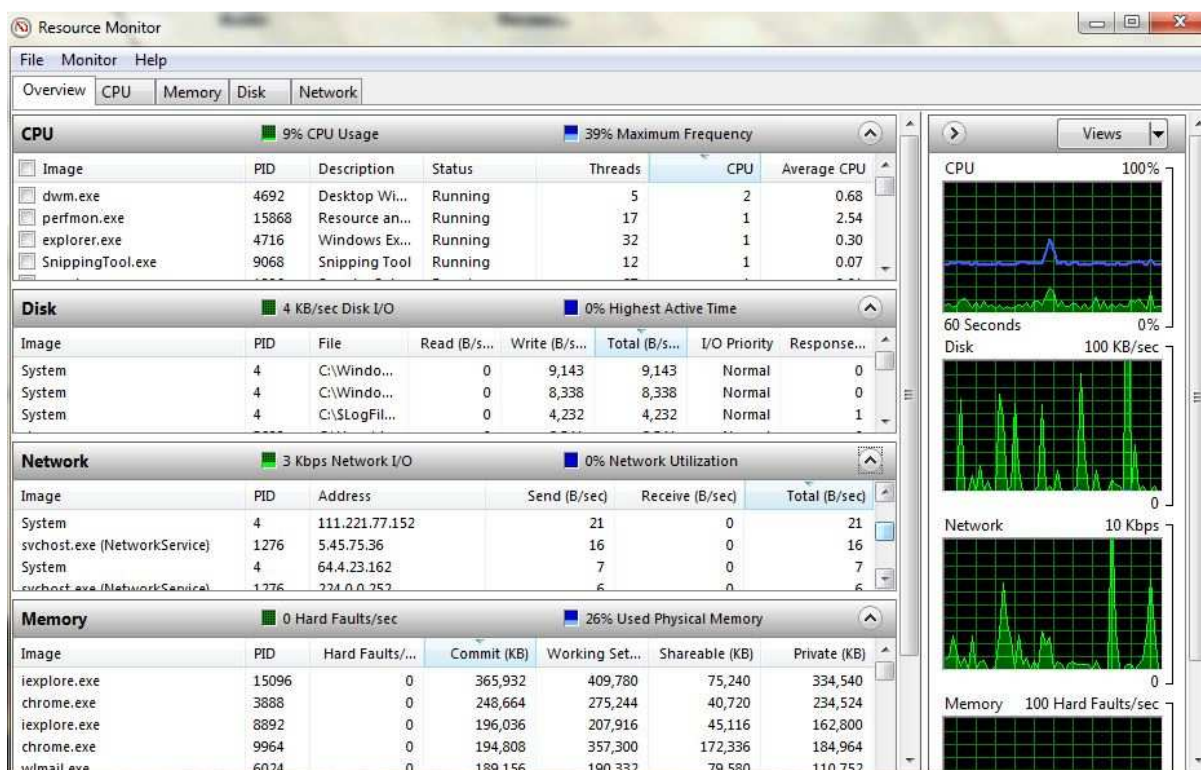


Fig. 12 - Windows Resource Monitor

- Windows Performance Monitor, a tool for monitoring current system performance. This tool has the ability to show reports on system behavior in a given period of time. In other words, using this tool it is possible to collect information in a given period of time. Therefore, Windows Performance Monitor can also be used to show performance reports in a given time segment, which can also be used in forensic investigations.

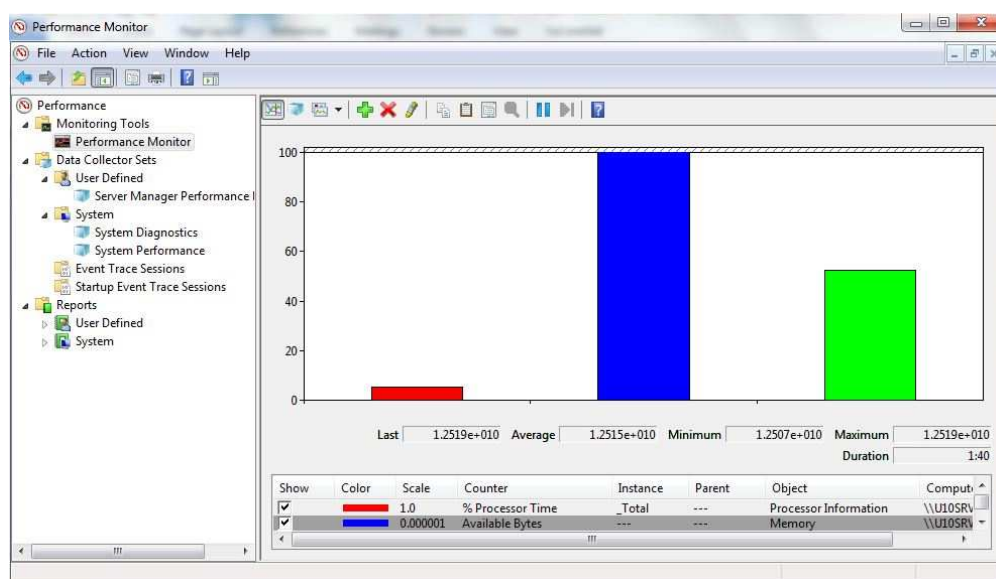


Fig. 13 - Windows Performance Monitor

The second group includes tools that collect information over a long period of time and place them in log files. Examples of some of these tools are:

- Reliability Monitor (Reliability History), a tool that allows system stability monitoring over some time period. Using it, it is possible to determine when the instability in the system occurred. In addition, it is possible to use it to check the number of times some event was repeated.

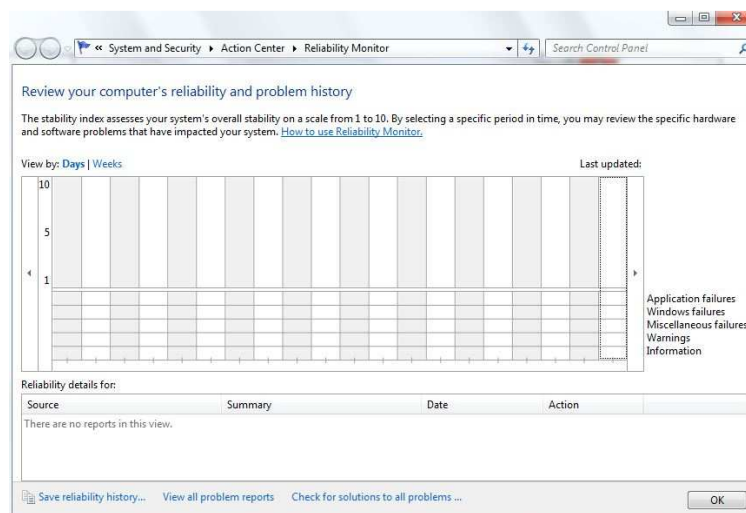


Fig. 14 - Reliability History

- Event Viewer, the most comprehensive tool for event monitoring within Microsoft operating systems. It consists of many components and can be used to monitor and collect information from local and remote computers.

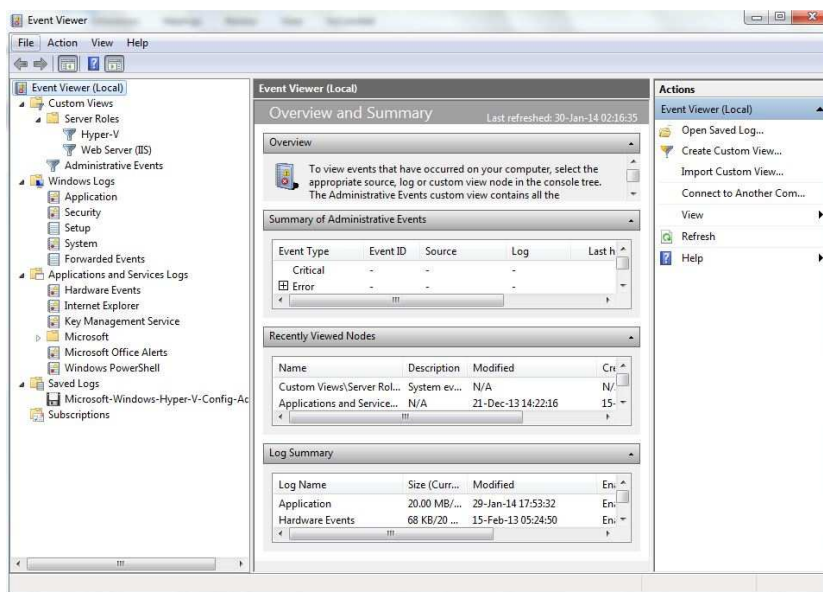


Fig. 15 – Event Viewer

In addition to these tools, there are tools that are not directly built into operating systems and can be downloaded for free from Microsoft web site¹⁸ and then used to monitor network traffic. An example of one such a tool is Network Monitor.

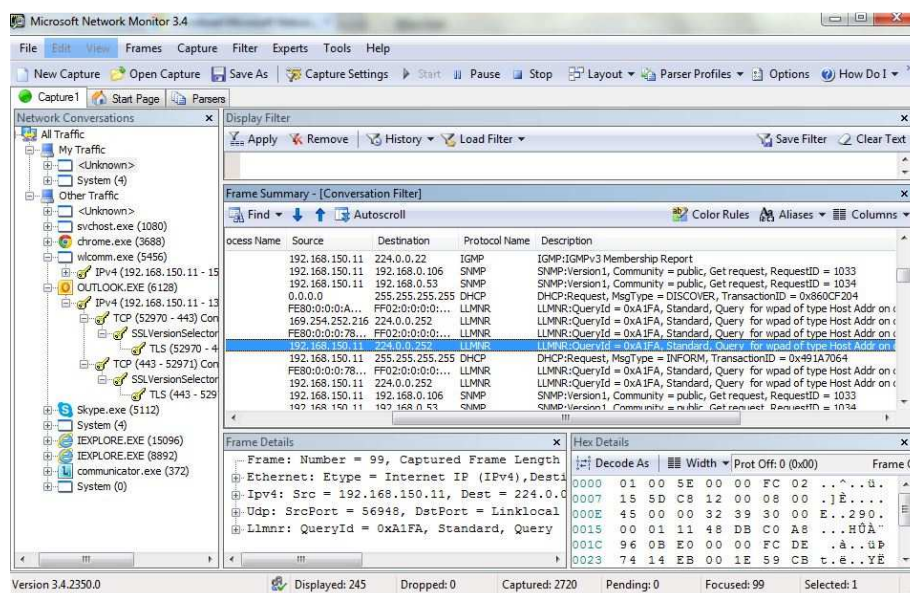


Fig. 16 – Network Monitor

Network Monitor is just one of the tools that can be used for this purpose, since there are large numbers of tools from other manufacturers that serve the same purpose. One thing common for all these tools is that they do packet inspection and provide access to their contents. This also affects data privacy, so tools for monitoring network traffic may only be used with company's consent.

¹⁸ <http://www.microsoft.com/en-us/download/details.aspx?id=4865>

In addition to these, there are specific tools for each segment of System Center 2012 R2 solutions that are embedded in these products.

Since the master's thesis uses VMM, it is the center piece. It is also important to note that VMM is an application (service) that is executed on top of server operating system. This also means that all the above tools can be used when VMM is concerned. However, within VMM there is a separate console that monitors execution of current tasks. This information is stored in a database that is located on Microsoft SQL server. As a result, using this console, it is possible to view tasks that have occurred up to 90 days in the past.

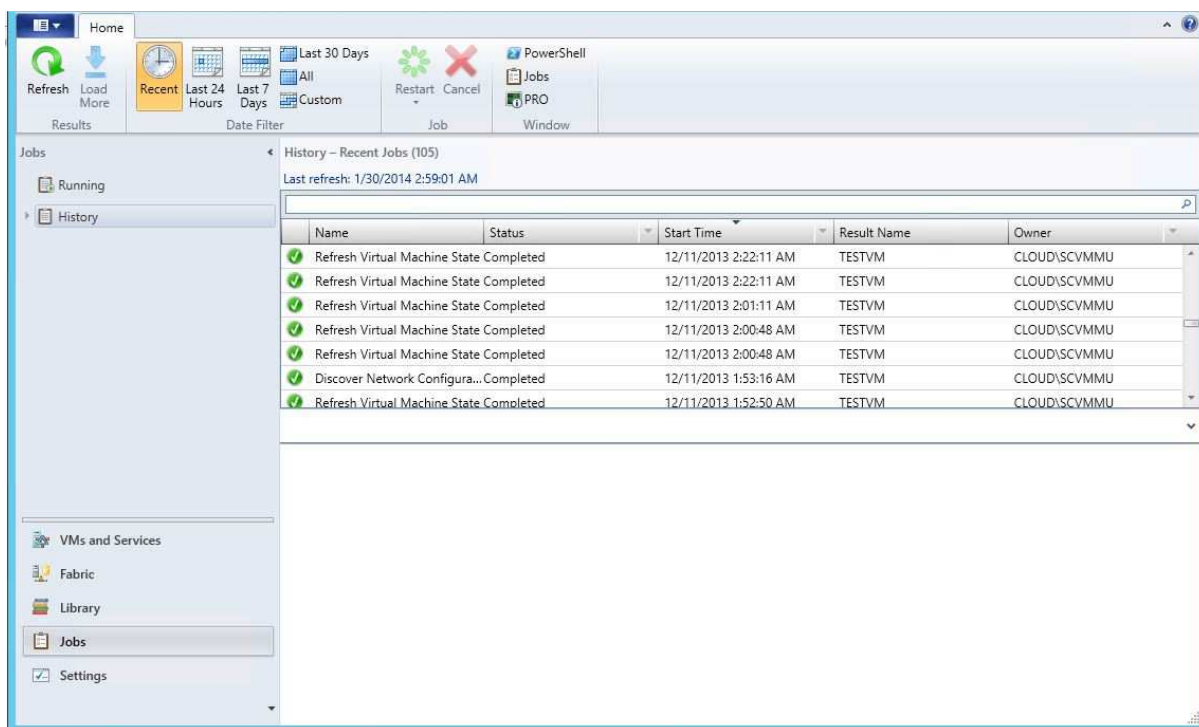


Fig. 17 – VMM job history

Each of these individual tools or reports generated using some of them, may allow the investigator to position themselves more easily or define time and place of the incident more precisely. In this way the forensic investigation can be facilitated.

However, all event information should be saved for later viewing or event checking. Review of saved information may help in understanding some of the more complex attacks consisting of many segments. Therefore, special attention should be paid to monitoring and collecting logs. Within Windows operating systems, there are tools that are used exclusively for this purpose and are used in the audit processes.

5. Log configuration for event monitoring within virtual and physical computers

Log files are documents in digital format which describe events. Log files can have different types and they may contain different information. More specifically, log file contains information about time, type and success of an event. Log files can be created and read using special software. Sometimes this software is part of the computer operating system and equipment.

Operating systems are the starting point. They have a large number of tools or system services that serve this purpose. These tools (services) allow users to create log bases that can be searched afterwards. Using this data it is possible to detect attempts of attacks that have been taking place over a longer time period. Logs that are collected in this way are accessed directly through the operating system or sent to another computer for storage and checking. This is called *subscription*. Using the method of subscription, the logs collected from multiple sources can be centralized on a single computer.

To better understand monitoring systems, it is important to make a distinction between monitoring and auditing processes. An example of such a log file is shown in Figure 18.

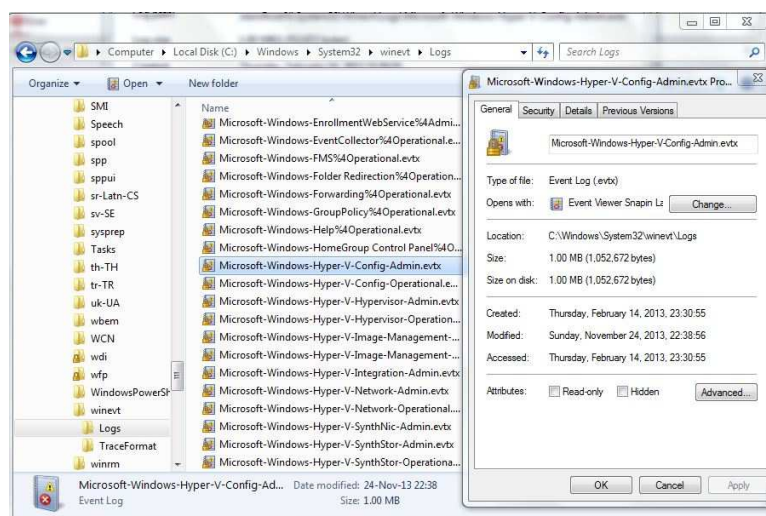


Fig. 18 – Example of log file

Monitoring is the monitoring of system or application functionality through tracking of resources or their successful execution. This is most visible through performance monitoring.

Auditing is the monitoring of collecting information on security events. It monitors success or failure of the event.

Contents of these files can be viewed using special software tools such as Event Viewer (Figure 19).

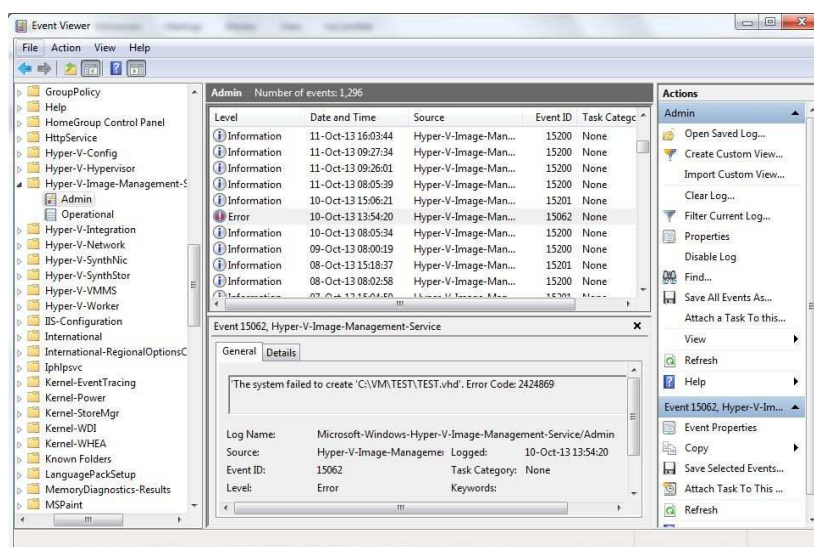


Fig. 19 –Example of Event Viewer log file

The sheer size of log file must also be taken into account, since it directly affects the amount of information that can be stored in it. Also, the way of entering information into log file is another factor that affects the amount of information (Figure 20).

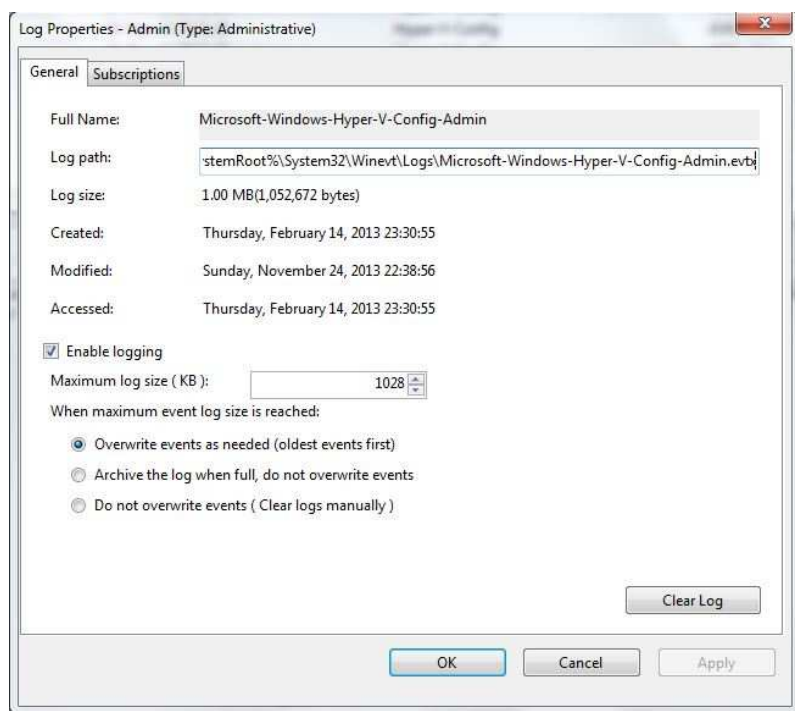


Fig. 20 – Log file properties

According to the figure above it can be seen that there are several ways to write into log files.

- Overwrite events as needed
- Do not overwrite events (clear log manually)
- Archive the Logs When Full, Do Not Overwrite Events

In the first case, new data is written in the log file as long as there is space. The moment it runs out of space for entering new information, more space is made by deleting oldest events within the same log file. The advantage of this method of collecting information is the small space they occupy. The downside is that it can happen that key events are overwritten by newly arrived information.

The second case solves the problem that may arise in the first. In other words, when a log file is completely full, there is no possibility of entering new information in that file. This is also a positive feature of this solution. But great attention must be paid to defining the size of the file which stores information. The negative features are reflected in the size of files that can be very large. Another negative aspect of this solution lies in the fact that when the file is full, because of the system's inability to enter new data, the operating system shuts down. This is a security feature that is built into the operating system and prevents its execution because the log file is unavailable for new entries. This behavior of operating systems can be abused, which may lead to denial of service attack types.

The third system for log collecting relies on lessons learned from previous types of log collecting. To collect logs it uses a log file that has a fixed size. When it is full, it renames itself automatically and creates a new initial log file where it continues to enter information. The downside of this type of collecting information is the amount of space that log files occupy on disk. In addition to this, there is no option to view all the information from all the log files, but they must be sought in each log file individually.

The conclusion that can be drawn from this is that the best system for log collecting is *Archive Logs When Full, Do Not Overwrite Events*. To use it, it is necessary to create log files that are very large in order to reduce their number and facilitate searching.

However, as can be seen from previous examples and the text above, the number of log files as well as the amount of information stored in them can be a problem in trying to find the necessary information.

One of the ways of processing and collecting information is to store them in a database. However, it is very complicated to search the database. The solution that deals with these problems is Reporting Services. These services have become an integral part of every information database.

The next, very important, information is the fact that logs are, by default, stored in different locations. This means that logs of physical or virtual computers are stored on them. Logs from network equipment, if any, are stored in those devices, and so on. That is a big problem when it comes to unification of necessary information in one central place, as well as their logical processing.

Every action over some log file causes information entry in that or some other log file. In this way, it is possible to find out whether a log file has been modified, because the information about that was entered in that log file and in a log file that monitors log file changes. These situations can be avoided by allowing log files to be collected in several places, and therefore prevent malicious persons to delete all the information stored in logs.

In addition to these monitoring systems that are embedded in the operating system, there are specialized systems for collecting information. An example of such a system for centralized

log and services collecting is System Center Operation Manager. This server system has the option of collecting logs from both operating systems and network devices.

The information collected in this way can be stored in SQL database and also provide a copy of logs from remote systems. Using this solution can proactively affect and reduce the possibility that some logs get accidentally or intentionally deleted, and possibly prove that attempts to change the information content have been made.

6. Log files

According to previous text, it can be concluded that there has been an increase in the number of places where unwanted events may occur, as well as many ways the information about them can be obtained. Therefore, this master's thesis tries to define what should be undertaken to enable successful monitoring, and what are all potential sites that could be used for collecting forensic material.

As mentioned before, Cloud systems consist of different solutions and various components. Staring from this fact, it can be assumed that gathering forensic data greatly differs between different types of Cloud environments.

Existing Cloud solutions such as IaaS, SaaS, PaaS and Naas offer a variety of benefits to users. They are more or less limited in terms of user interaction with them and have more or less the ability to adapt to user needs. In addition, these solutions can be personal property or property of third parties.

For example, they can be compared to SaaS, PaaS and IaaS models of Cloud environment. Monitoring and collecting logs in this case depends on whether it comes to private or public Cloud environments. When it comes to public SaaS and PaaS models, monitoring is very limited and mainly confined to monitoring network traffic, because usually there is no option to set up monitoring tools.

In case of IaaS Cloud solutions, some additional monitoring tools can still be used or set up. This means that in the first two cases (PaaS and SaaS models), CSP logs can be searched, which can be a problem according to previous statements and problems that investigators may encounter. The possibility that exists in case of IaaS Cloud solution is that, in case of need, the whole image can be pulled from virtual computer for the purposes of the investigation. However, the situation completely changes when it comes to private Cloud environments. This is supported by the fact that all the information are in the possession of the investigator and that presents the easiest way to access forensic investigation.

For the sake of this thesis and the need to define possible sites for collecting information more precisely, the thesis describes private Cloud environment. The reason for that is greater control of the environment and each of its individual segments. In this way it is possible to more accurately define what types of monitoring could be used in proactive digital forensics.

6.1. Description of a solution for collecting log files

In order to begin collecting logs, it is necessary to start that process. It is important to emphasize this since, by default, only certain types of information are collected and logged. In other words, not all the necessary information are collected, but only the information about operating system, and not about applications and virtual desktops.

This also means that if monitoring (audit) is not started by default, therefore it is very easy to lose information that an event has occurred.

The case study that is the subject of this thesis deals with postulates for monitoring and collecting information (logs) in private Cloud environment of a company. An environment that is used as an example is based on Microsoft System Center platform.

Initial installation and configuration of Active Directory Domain Services, and the basics of security solutions, have been explained in part in author's graduate paper¹⁹. Further text deals with the postulates of monitoring within Active Directory Domain Service, by creating policies for monitoring and log checking. It also deals with installation and configuration of VMM service, creating virtual machines, networks and Cloud.

Collecting information about events, both in operating system as well as in applications, is the most important step in proactive digital forensics. This also prepares the ground for successful execution of digital forensics.

As stated above, it is necessary to start information collecting in the log files. Since the example uses Active Directory environment, this is most easily achieved by creating appropriate group policies which will define audit policies.

Figure below shows Group Policy console in which the policy for event monitoring is attached to a domain environment.



Fig. 21 – Group Policy console

Collecting information by simply collecting them is easily achieved by turning it on. There are two options for collecting information about events, which are: Success and Failure.

¹⁹[Implementacija bezbednosnog rešenja u okviru školskog centra kompanije CPU d.o.o.], Lj. Ivaniš

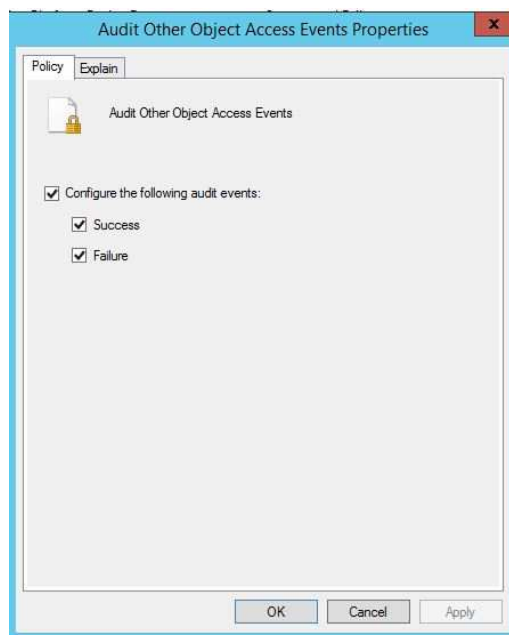


Fig. 22 – Group Policy console enabling audit

Success audit represents successful monitoring of a successful event. For example, user has successfully accessed a resource.

Failure audit represents successful monitoring of a failed event. An example might be user's failed attempt to delete a file or unsuccessful login attempt.

For example, if case of monitoring access to a shared folder in a company where both types of monitoring are active, it is possible that large number of events will be created. The reason for this is large number of successful events, so finding the required event in this case can be difficult. However, in the event that a decision has been made to monitor only successful or only unsuccessful events, then the user gets limited results.

In another example, if monitoring only unsuccessful attempts to access a resource, log file can show that someone has tried to access a resource, but it doesn't show if they were successful. In other words, to get more complete information, it is necessary to activate monitoring of both Success and Failure events. In this way the amount of information collected and space for log files increases, but it gives more concrete picture of an event.

Collecting information about events is called *audit* and is defined as a separate entity within Group Policy. Policies which define monitoring are called *auditing policies*.

It is also important to note that within Group Policy settings, there are two separate segments for monitoring configuration, depending on the support in different versions of operating systems.

The first part are policies for collection basic information that are compatible with all versions of Windows operating systems. The following policies are general and are used to collect large number of events. An example is shown in the figure below.



Fig. 23 – Audit policies

Thanks to these policies user logins can be traced, their access to resources, rights evaluation, system events and changes in policies themselves.

However, as already noted, these policies are quite general and thus collect large amount of information and create large log files. This also increases the need for free space to store all the information. In addition, this creates a new problem of finding required information in the sea of logs. Having seen these problems, Microsoft has created new audit policies that are specifically positioned and more precisely defined.

The second segment of monitoring setup using Group Policies can be seen in the figure below.

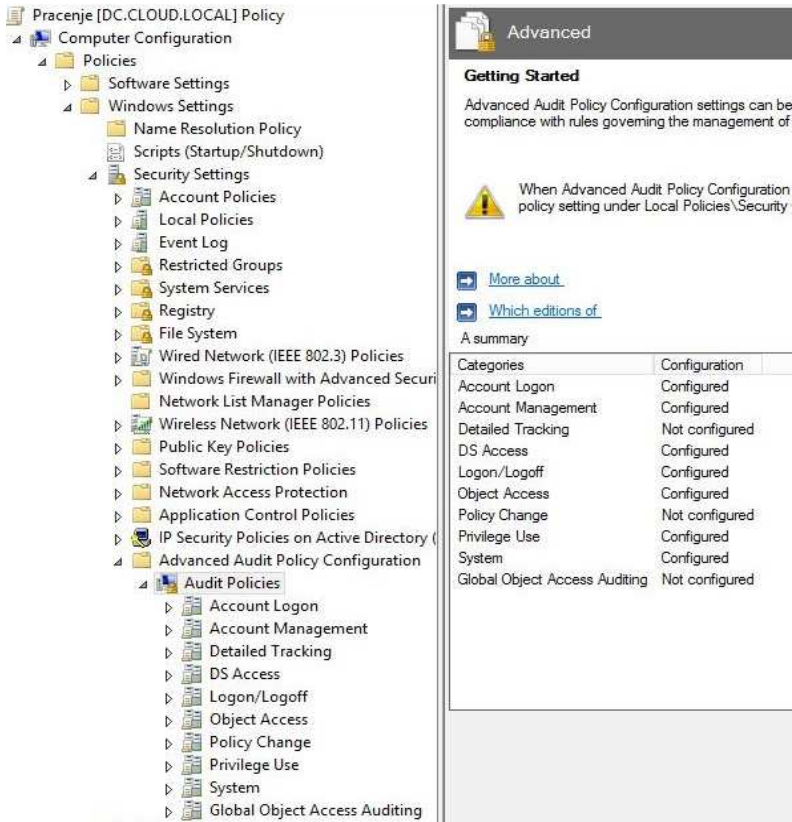


Fig. 24 – Advanced audit policies

The advantage of this setup is that it is possible to more accurately define what the user really wants to monitor. An example is seen in the figure below.

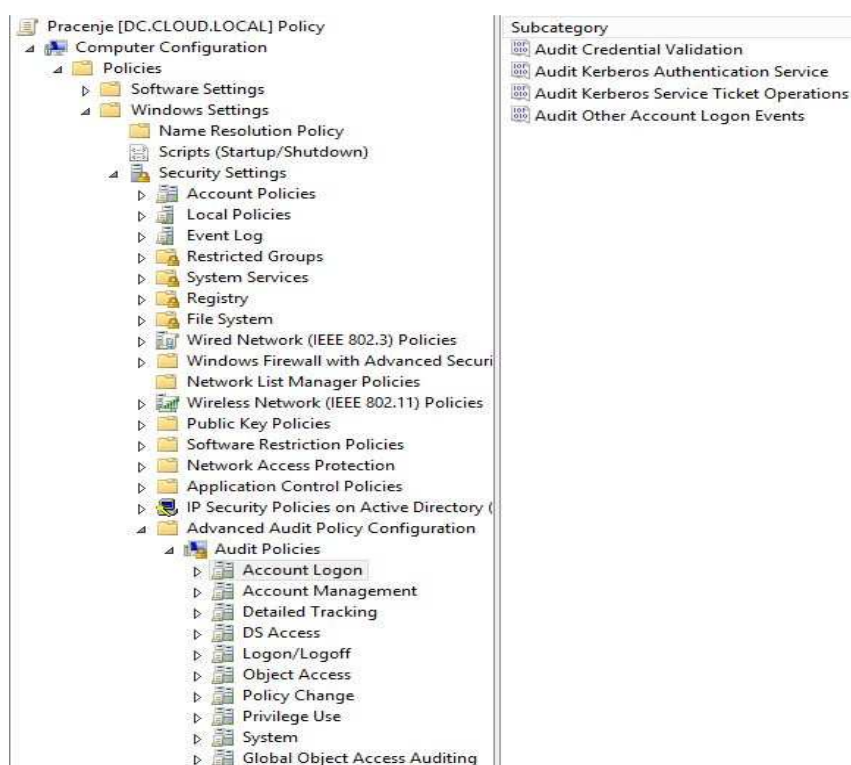


Fig. 25 – Advanced audit Account Logon

As can be seen in previous figures, it is now possible to more precisely define what should be monitored, as the policies for monitoring are divided into individual components. For example, monitoring of access to objects is divided into fourteen (14) subcategories. Each of these subcategories may be selected individually or independently of the need for monitoring.

Subcategory	Audit Events
Audit Application Generated	Success and Failure
Audit Certification Services	Success and Failure
Audit Detailed File Share	Success and Failure
Audit File Share	Success and Failure
Audit File System	Success and Failure
Audit Filtering Platform Connection	Success and Failure
Audit Filtering Platform Packet Drop	Success and Failure
Audit Handle Manipulation	Success and Failure
Audit Kernel Object	Success and Failure
Audit Other Object Access Events	Success and Failure
Audit Registry	Success and Failure
Audit Removable Storage	Success and Failure
Audit SAM	Success and Failure
Audit Central Access Policy Staging	Success and Failure

Fig. 26 – Advance audit Object Access

Taking into consideration this monitoring division, there is now the option to position monitoring very accurately. Another advantage of this policy is that, thanks to better positioning, the information that are entered in log files are automatically filtered. In this way the amount of information search area is smaller, as well as size of log files themselves.

However, to make these policies usable, it is necessary that operating systems recognize these fine (grain) settings. Operating systems that are compatible with this monitoring system are Windows and Vista client systems, Windows Server 2008 and later operating systems.

By creating these policies monitoring may be initiated, both on hosts and on virtual machines. The only problem that may arise is the inability to implement these settings on computers that are in workgroup environments. In other words, when there are such hosts or virtual machines, it is necessary to individually activate event monitoring.

6.2. Description of solution for centralized collecting of log files

Information about event monitoring are, by default, collected at client computers and local disks. This is relatively big problem when it comes to finding the information that is needed, as the search must be done on each individual client. Also, the situation may arise in which the logs are deleted accidentally or intentionally, which further complicates the investigation. To facilitate the search of information, as well as to avoid unpleasant situations with deleted log files, one of the solutions that can be used is *logs subscription*.

Subscription is a feature that exists within Event Viewer tool and it appeared with Windows Server 2008. Due to Subscription, it is possible to centrally collect logs from multiple computers on a single server in an environment, whether it comes to computers that are members of the domain or a workgroup.

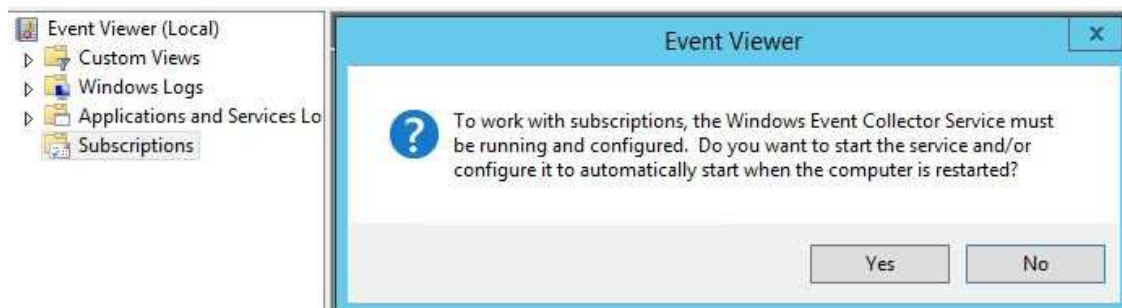


Fig. 27 – Starting Subscription service

When the service starts, user gets the option to collect log files and events from other computers in the network.

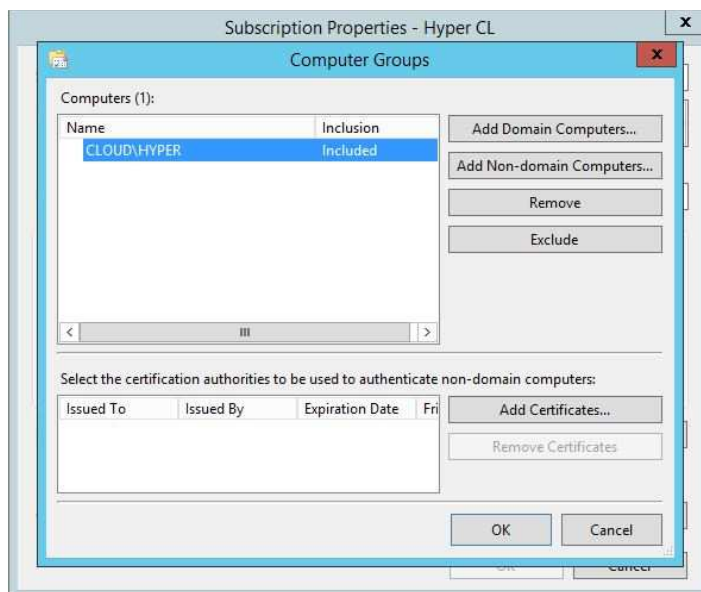


Fig. 28 –Choosing a client with from which the information are collected

As it can be seen in the figure, when choosing a client from which the information are collected, user is not limited to computers that are members of the domain. This also makes it easier to collect a lot of information from various sources.

Also, the information collected in this way can be very precisely positioned at the collection point and defined within which log file they will be stored. The figure below shows the possibility of defining log file for collecting information.

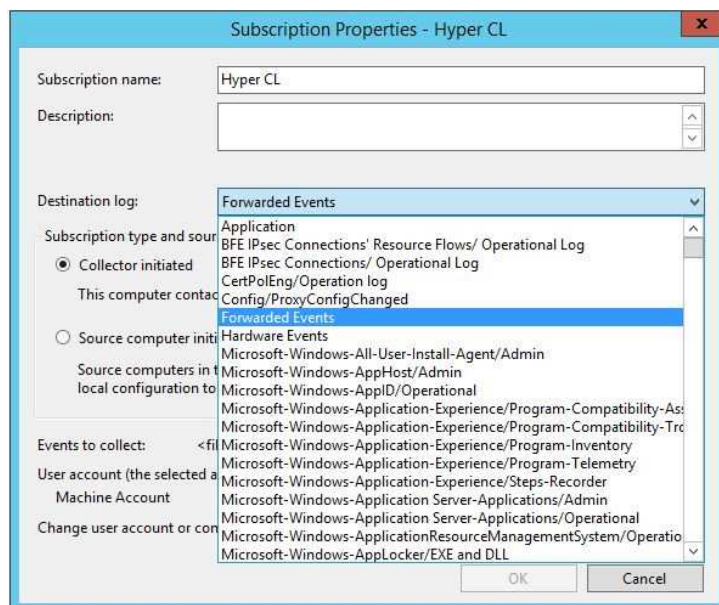


Fig. 29 – Choosing a log file which will store events

Since it is possible to collect all the information that are happening on a remote computer, there are problems related to the amount of information. Therefore, it is necessary to filter which events are forwarded to the collector, so that it can be chosen from which log file the information are submitted and which types of events should be collected, as shown in the figure below.

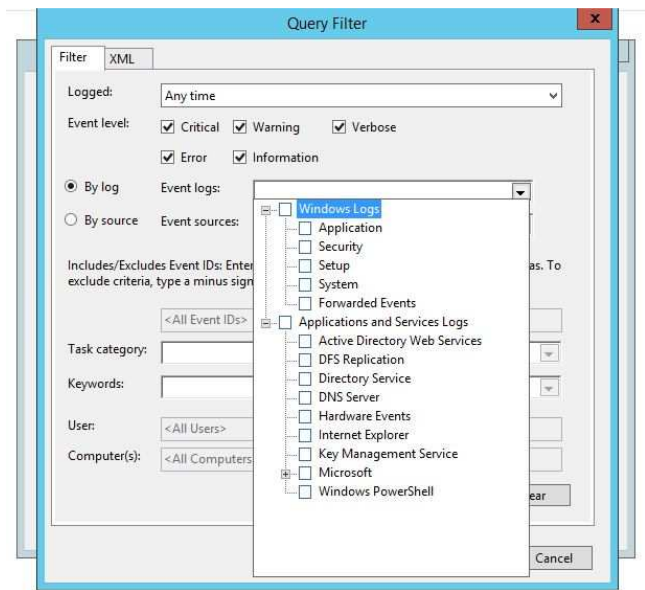


Fig. 30 – Choosing log file

In this way, enough information from a remote computer can be collected. At the same time the user can ensure that even in case of deletion of original logs at the source, the information will still be stored on the collector. An example of collected information is shown in Figure 31.

Event Viewer (Local)

- Custom Views
- Windows Logs
 - Application
 - Security
 - Setup
 - System
 - Forwarded Events
- Applications and Services Logs
- Subscriptions

Forwarded Events		Number of events: 261					
Level	Date and Time	Source	Event ID	Task Category	Log	Computer	
Information	3/24/2014 1:29:13 AM	Office Softw...	900	None	Application	Hyper.Cloud.local	
Warning	3/24/2014 1:27:10 AM	LSA (LsaSrv)	6037	None	System	Hyper.Cloud.local	
Information	3/24/2014 1:27:05 AM	Service Cont...	7036	None	System	Hyper.Cloud.local	
Information	3/24/2014 1:24:37 AM	Service Cont...	7036	None	System	Hyper.Cloud.local	
Information	3/24/2014 1:24:37 AM	Service Cont...	7036	None	System	Hyper.Cloud.local	
Information	3/24/2014 1:24:37 AM	Service Cont...	7036	None	System	Hyper.Cloud.local	
Information	3/24/2014 1:24:37 AM	Service Cont...	7036	None	System	Hyper.Cloud.local	
Information	3/24/2014 1:24:34 AM	Service Cont...	7036	None	System	Hyper.Cloud.local	
Information	3/24/2014 1:24:27 AM	Service Cont...	7036	None	System	Hyper.Cloud.local	
Information	3/24/2014 1:24:19 AM	Service Cont...	7036	None	System	Hyper.Cloud.local	

Fig. 31 – Display of collected information

Using these methods of centralized collecting of information, there is a possibility that a situation that covers several computers, either physical or virtual, can be observed from one central place.

However, it is important to note that information are collected from remote computers in a central place which also entails the use of network resources. With the increasing number of subscriptions and the amount of information that are collected, the load on existing network equipment is automatically increased.

Also important is the fact that data sent from a remote computer passes through network, at which point these data are vulnerable or susceptible to change by a third party. Fortunately, these communications can be protected by encrypting traffic using digital certificates.

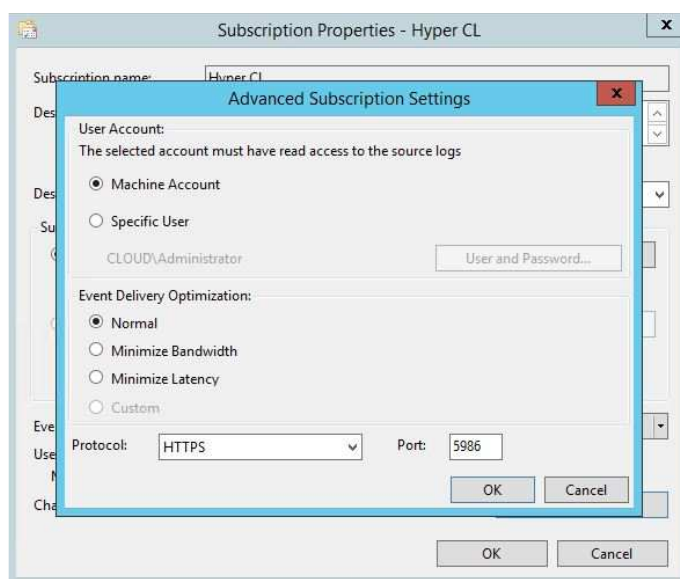


Fig. 32 –Authentication methods for collecting log information

This is just one of many possible ways of centralized collecting of information. For this purpose there are various specialized software from different companies such as SAP, IBM and Microsoft. Regarding Microsoft's solution, there is a software called System Center Operation Manager (hereinafter SCOM) which is included in System Center 2012 R2. SCOM is software which has the primary purpose of monitoring and alerting about events that took place on network or within software solutions. Information collected using SCOM are stored in SQL database, from which they can be displayed, if necessary, using Reporting service.

7. Case Study: Examples of proactive digital forensics in the Cloud

This unit holds some practical examples of collected information gathered through the audit process. The information that are collected in this way can be viewed later using different tools. For specific display of information from log files Event Viewer was used.

Since the entire master's thesis is based on the premise of private Cloud environment, the information presented mainly relate to virtual machines and events related to them. For example, one can start from the most basic information, such as starting and stopping virtual machine hosts. This is very important information because the hosts are the basis of virtual environment.

Starting Hyper-V host can be documented through following Event IDs.

Information	12/11/2013 11:48:21 AM	Hyper-V-VMMS	19500	None
Information	12/11/2013 11:48:20 AM	Hyper-V-VMMS	19020	None
Information	12/11/2013 11:48:20 AM	Hyper-V-VMMS	19020	None
Information	12/11/2013 11:48:20 AM	Hyper-V-VMMS	14094	None
Information	12/11/2013 11:48:15 AM	Hyper-V-VMMS	20410	None
Information	12/11/2013 11:48:15 AM	Hyper-V-VMMS	12514	None
Information	12/11/2013 11:48:01 AM	Hyper-V-Hypervisor	1	None

Fig. 33 – Events created when starting Hyper-V host

Previous figure suggests that all essential services that are needed to run virtual machines are successfully started. It also defines the time when these services were started. The most important event was recorded in Hyper-V hypervisor log under Event ID 1. This event indicates that support for virtualization was successfully started.

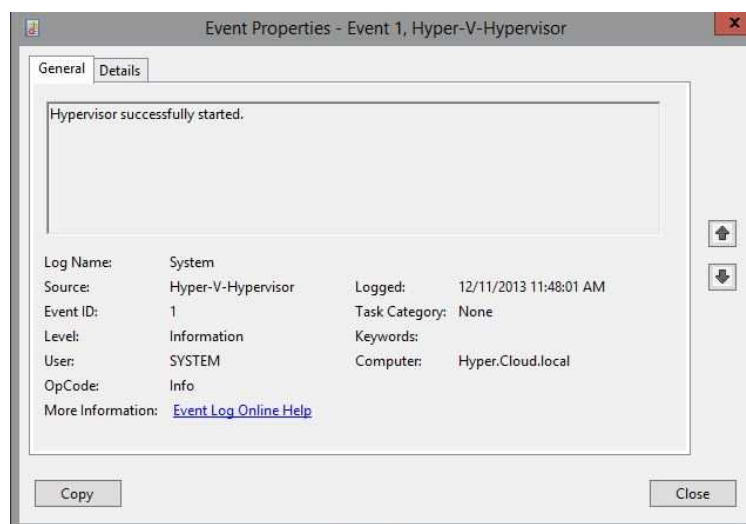


Fig. 34 – Starting Hyper-V host

In case that host is connected to VMM (controlled by VMM), then a service that enables VMM control over host is started. These events can be found in Hyper-V-VMMS log. This procedure is shown in the next few events.

The procedure begins by finding and validating certificate that authenticates the computer to VMM. Then it connects with VMM service, after which VMM management service on the host is started. The last event shows that the state of information between VMM and the host is updated.

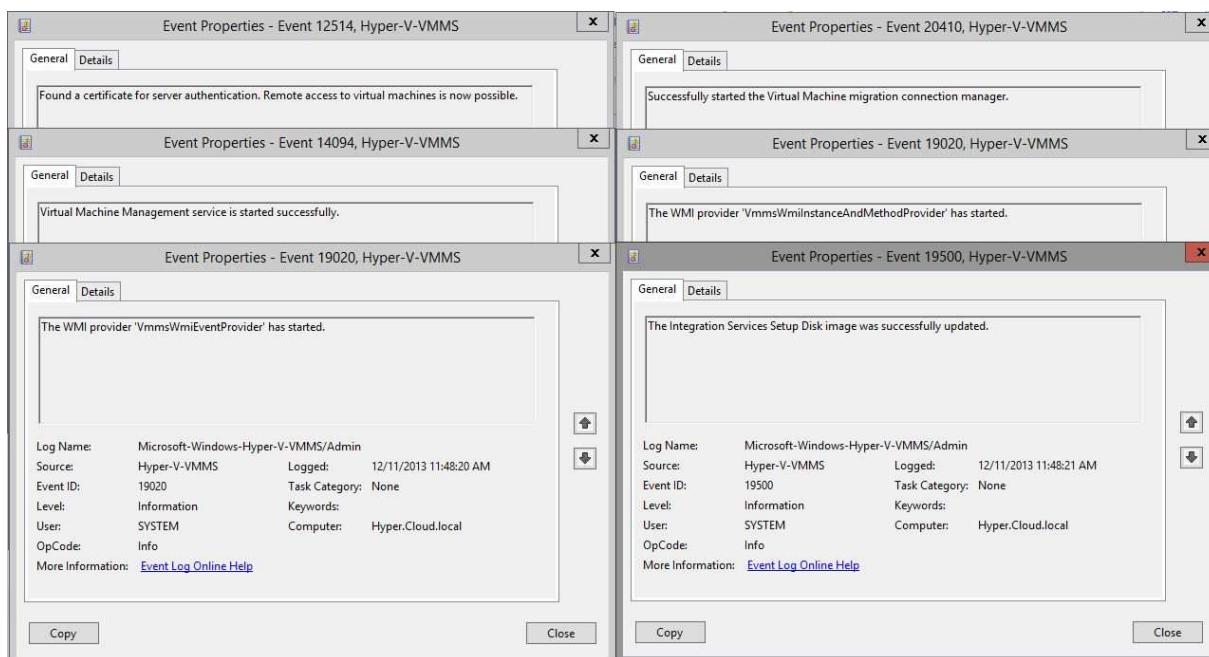


Fig. 35 – Connecting the host to VMM server

Each of these events is recorded in a log file with special ID number and time instance when it occurred. These logs can indicate when the communication between host and VMM was realized.

Given that this is virtualization, in addition to starting physical computers and their connection to VMM, it is necessary to pay attention to virtual desktops as well.

First important information may constitute the creation of virtual machine within Hyper-V service on the local host. It should be noted that, when creating virtual machine called TestVM, an event was created. That event is located in logs on Hyper-V VMMS. Log file is, by default, entered in a file at the following location:

%SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-Hyper-V-VMMS-Admin.evtx

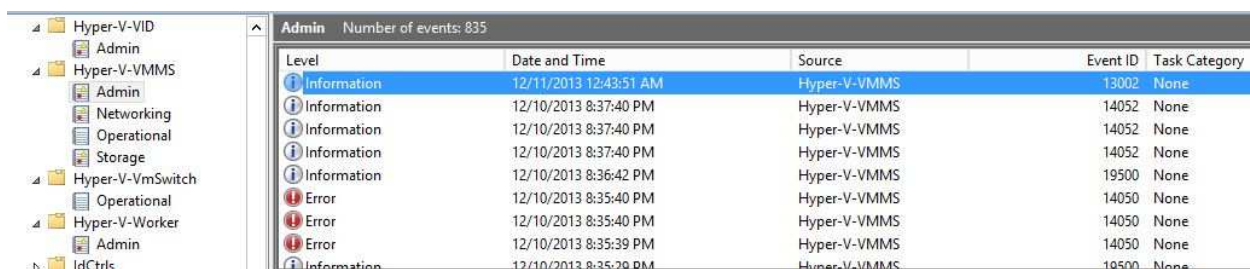


Fig. 36 – Information concerning creation of a virtual computer

The most important event that is recorded is the creation of virtual machine, which is shown in EventID 13002.

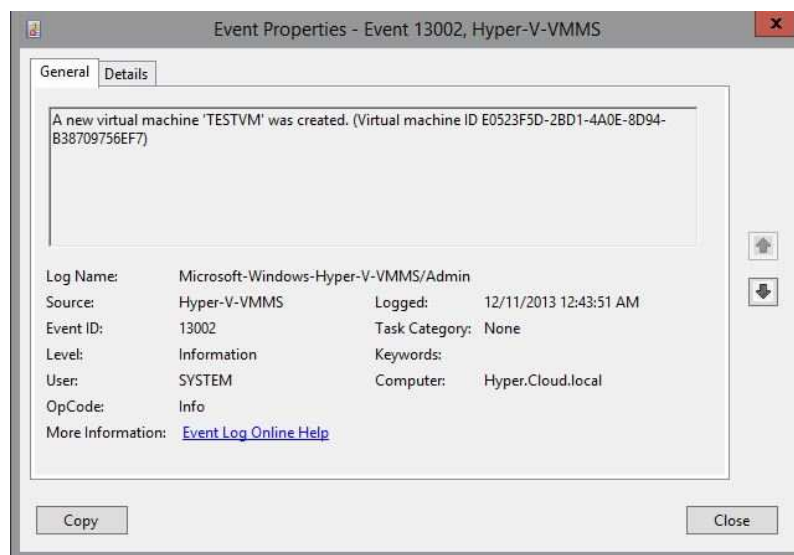


Fig. 37 – Creation of virtual computer event

The next step is to start the created virtual computer. This event has multiple records. When starting a virtual machine, a number of log events were created in two different log files.

Level	Date and Time	Source	Event ID	Task Category
Information	12/11/2013 12:55:38 AM	Hyper-V-Worker	23020	None
Information	12/11/2013 12:55:38 AM	Hyper-V-Worker	18500	None
Information	12/11/2013 12:55:38 AM	Hyper-V-SynthNic	12582	None
Information	12/11/2013 12:55:38 AM	Hyper-V-SynthNic	12597	None
Information	12/11/2013 12:43:51 AM	Hyper-V-VMMS	13002	None

Fig. 38 – Log files that record starting of a virtual computer

Event is recorded in different log files which also represent individual phases of the initialization of the virtual computer. Thus, first two log events are related to the network, i.e. initialization of the network card and the connection of the virtual machine to a network switch.

Hyper-V-SynthFC	Admin
Hyper-V-SynthNic	Admin
Hyper-V-SynthStor	Admin
Operational	

Level	Date and Time	Source	Event ID	Task Category
Information	12/11/2013 12:55:38 AM	Hyper-V-SynthNic	12582	None
Information	12/11/2013 12:55:38 AM	Hyper-V-SynthNic	12597	None
Information	12/10/2013 8:35:43 PM	Hyper-V-SynthNic	12582	None
Information	12/10/2013 8:35:43 PM	Hyper-V-SynthNic	12597	None

Fig. 39 – Log file used to record activities related to network

The events that are labeled by Event IDs are:

- 12597 which indicates that the virtual machine is connected to the virtual switch,
- 12582 which indicates that the network adapter has successfully started.

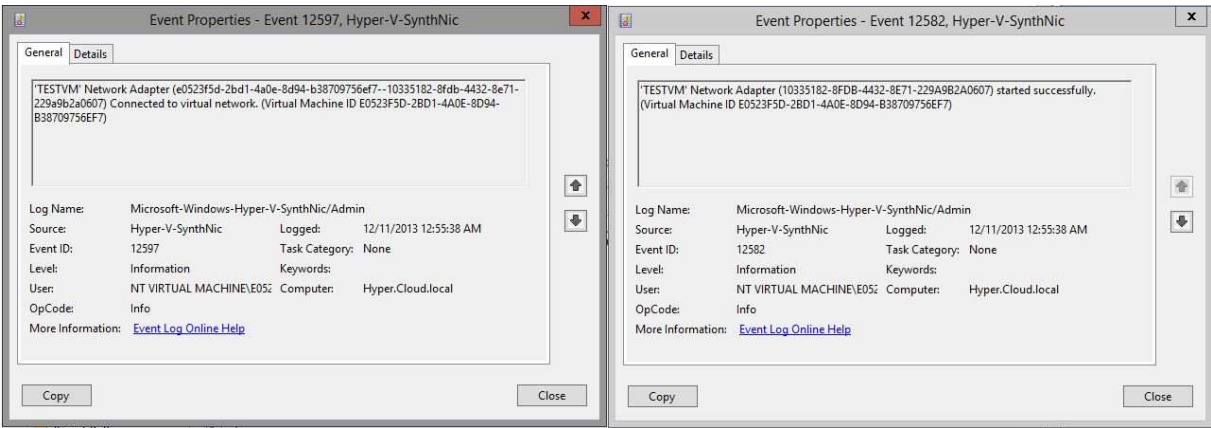


Fig. 40 – Events 12597 and 12582

After that follows the initialization of the virtual computer. Information on that are recorded in the events which are written within Hyper-V-Worker log and are shown in two events.

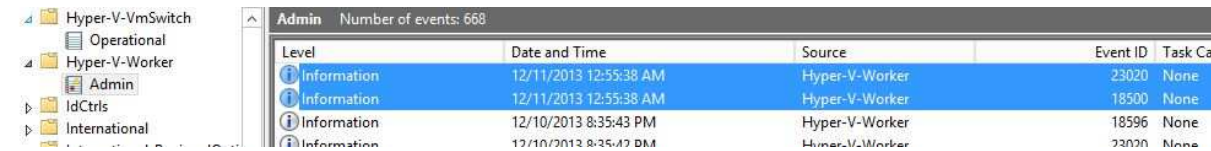


Fig. 41 – Hyper-V-Worker log

These two events show that virtual machine has successfully started and launched the possibility of graphic information display.

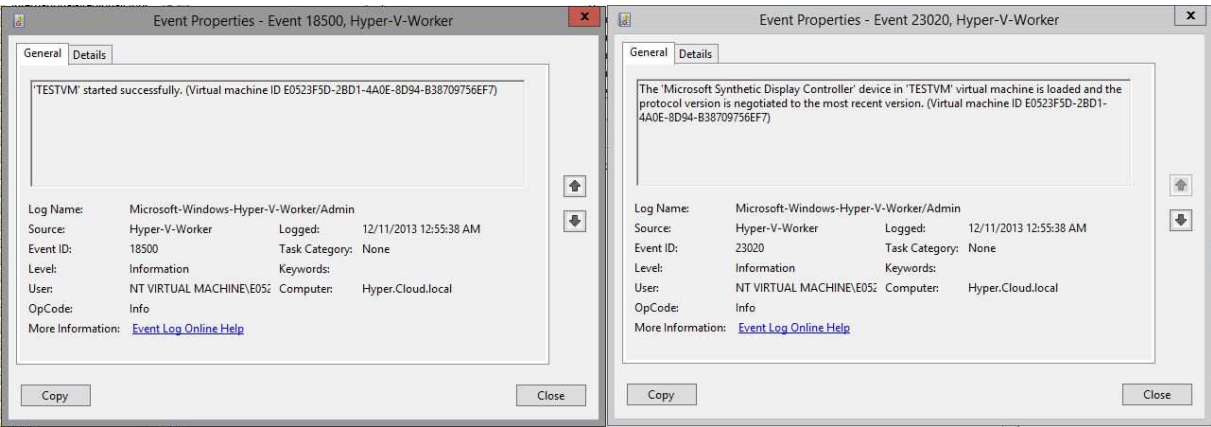


Fig. 42 –Events created when starting a virtual computer

Event ID 18500 is particularly important as it shows the initialization of virtual computer. Using these events it is possible to prove that a virtual computer was running at a certain time. It is important to note that these events are created whether a virtual computer was started locally from a console or remotely using VMM service. Also, other important event may be of a virtual computer shutdown, either regular or forced. For example, forced shutdown of a virtual computer creates following two event logs. These

events are recorded in two different log files, as well as when starting a virtual computer. They were divided into two groups: self-termination and network communication termination.

Information	12/11/2013 1:13:52 AM	Hyper-V-Worker	18502	None
Information	12/11/2013 1:13:52 AM	Hyper-V-SynthNic	12598	None

Fig. 43 – Information about virtual computer's unplanned shutdown

These information can also be seen within Event IDs.

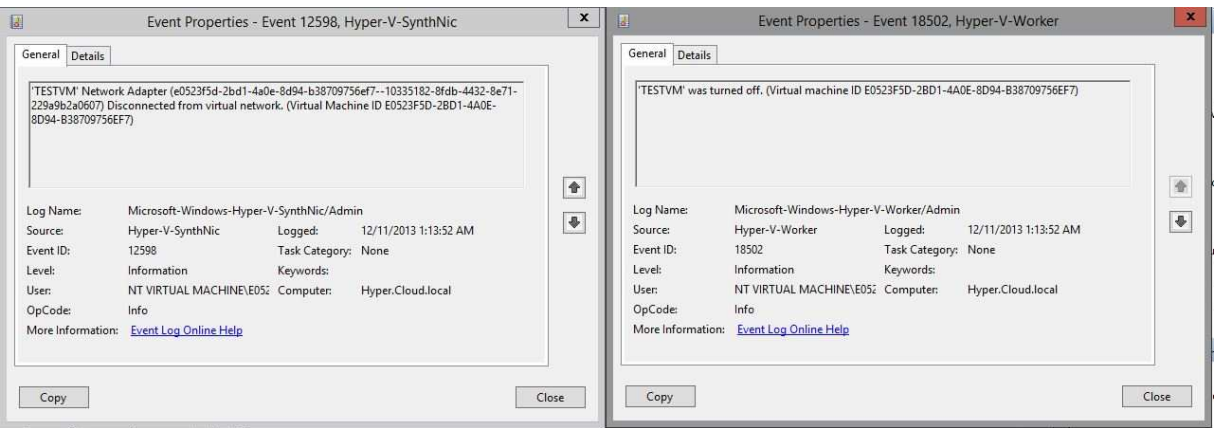


Fig. 44 – Events created during forced shutdown of a virtual computer

Very important event in this case is the event ID 18502 which indicates that a virtual machine was turned off. This event is different from events that are created during regular shutdown of a virtual computer.

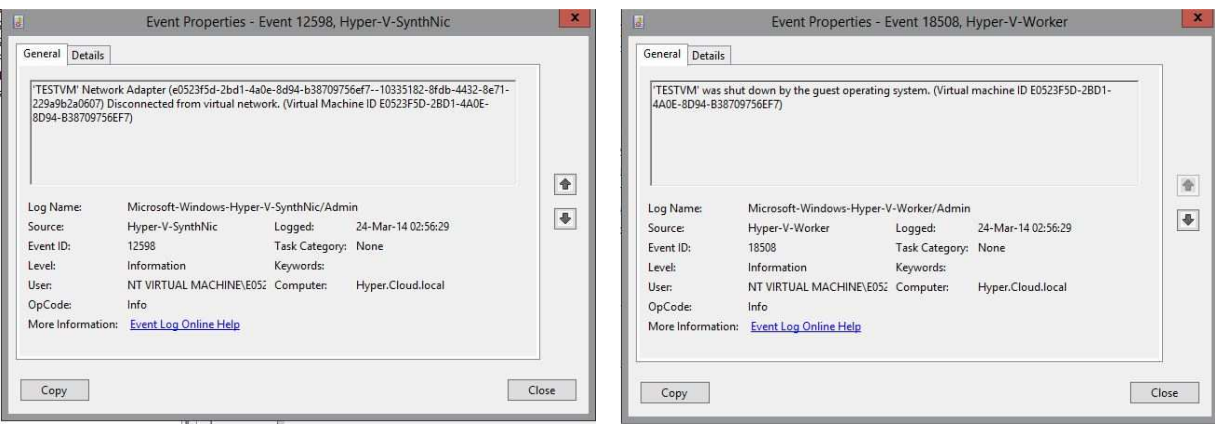


Fig. 45 – Events created during regular shutdown of a virtual computer

In addition to these events, which are related to startup and shutdown of virtual computers, one must pay attention to the actions taken on virtual machines. One of these actions can be addition or removal of hardware components.

Changes in hardware to virtual machines can be monitored in several log files.

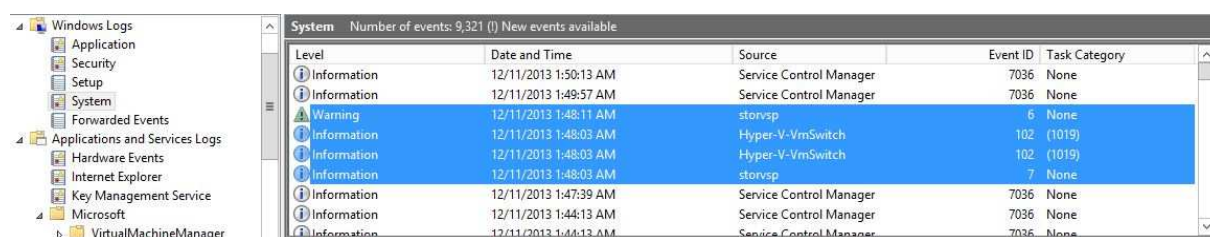


Fig. 46 – Adding hardware to a virtual computer

For example, adding a virtual DVD drive to a virtual computer and its launching is shown through following events which are recorded in two log files.

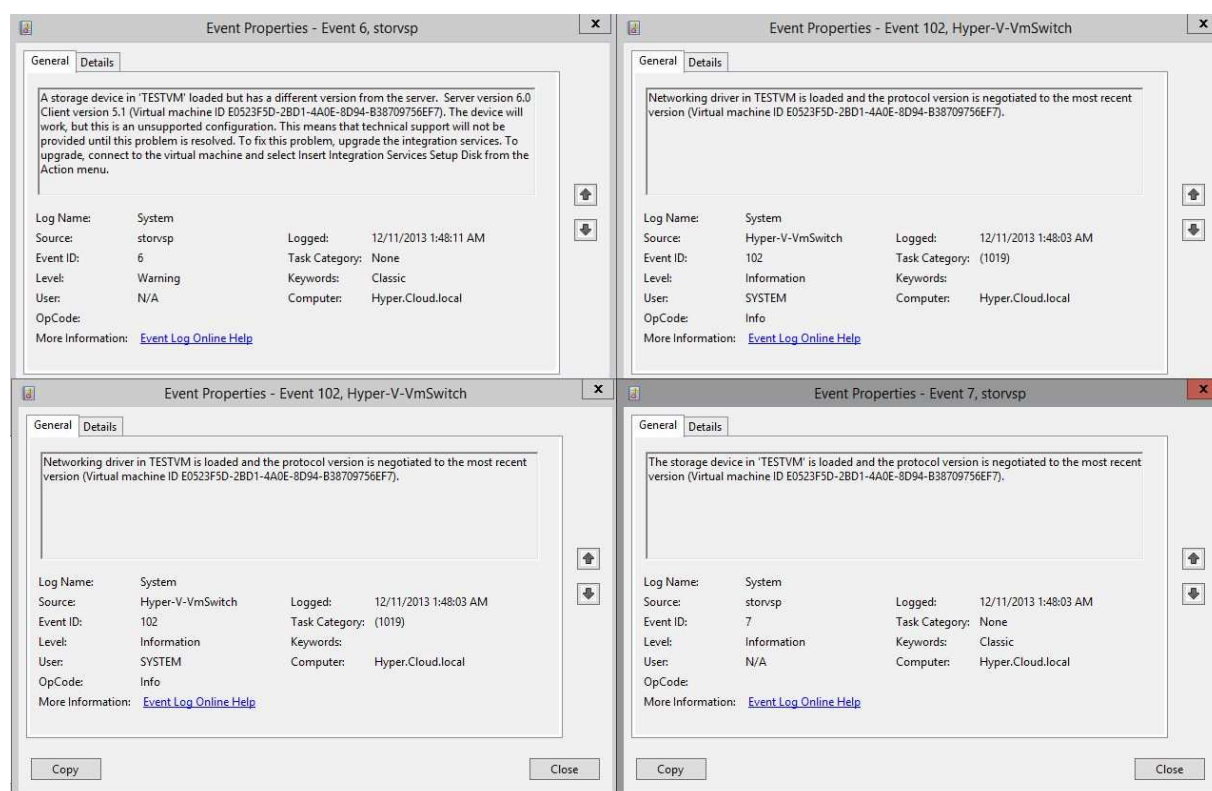


Fig. 47 – Events related to adding hardware to a virtual computer

Hyper-V service offers the option to start virtual machines that have complete support, as well as computers that can run in the so-called compatibility mode. Virtual machines that have full compatibility have better support when it comes to hardware, as opposed to operating systems that run in compatibility mode.

For example, when starting virtual machine that is compatible with Hyper-V services, the following events are created that are recorded in several log files. In this case the events can be divided into two groups.

Level	Date and Time	Source	Event ID	Task Category
Information	12/11/2013 2:01:06 AM	Hyper-V-Integration-Data-Exchange	4020	None
Information	12/11/2013 2:01:03 AM	Hyper-V-Integration-VSS	4020	None
Information	12/11/2013 2:01:02 AM	Hyper-V-Integration-TimeSync	4020	None
Information	12/11/2013 2:01:02 AM	Hyper-V-Integration-Rdp	4020	None
Information	12/11/2013 2:01:02 AM	Hyper-V-Integration-Shutdown	4020	None
Information	12/11/2013 2:01:02 AM	Hyper-V-Integration	4020	None
Information	12/11/2013 2:00:55 AM	Hyper-V-Worker	23020	None
Information	12/11/2013 2:00:53 AM	Hyper-V-Worker	23020	None
Information	12/11/2013 2:00:47 AM	Hyper-V-Worker	23020	None
Information	12/11/2013 2:00:47 AM	Hyper-V-Worker	18514	None
Information	12/11/2013 2:00:47 AM	Hyper-V-SynthNir	12582	None

Fig. 48 –Events created when starting a VM with support for Hyper-V

The first group of events is related to Hyper-V-Worker Event, while the other is related to integration components of Hyper-V service.

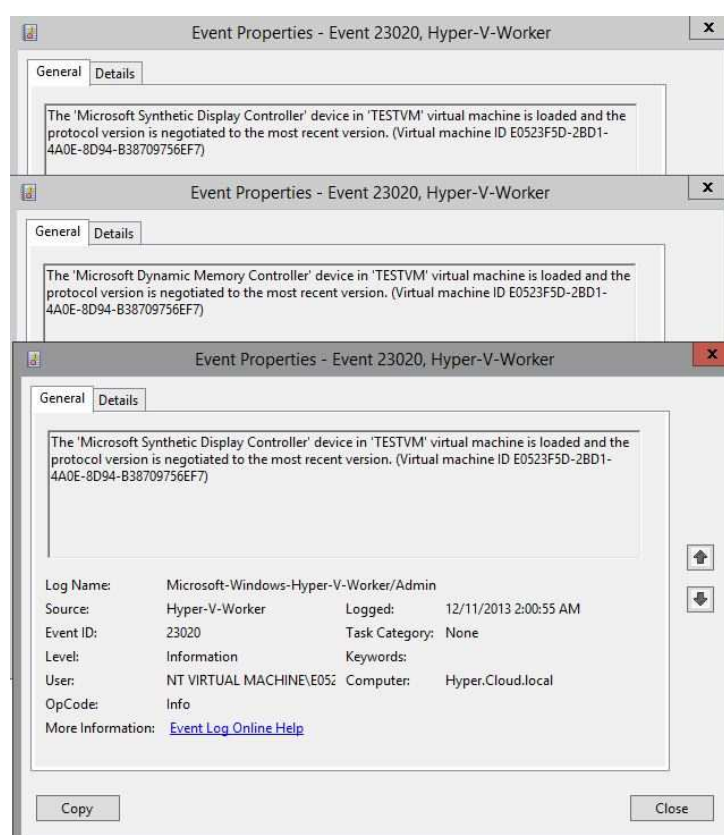


Fig. 49 – Hyper-V-Worker process events

It is interesting that all these events are related to the same event ID 23020, and services that are started as support for Hyper-V service are also incorporated under Event ID 4020.

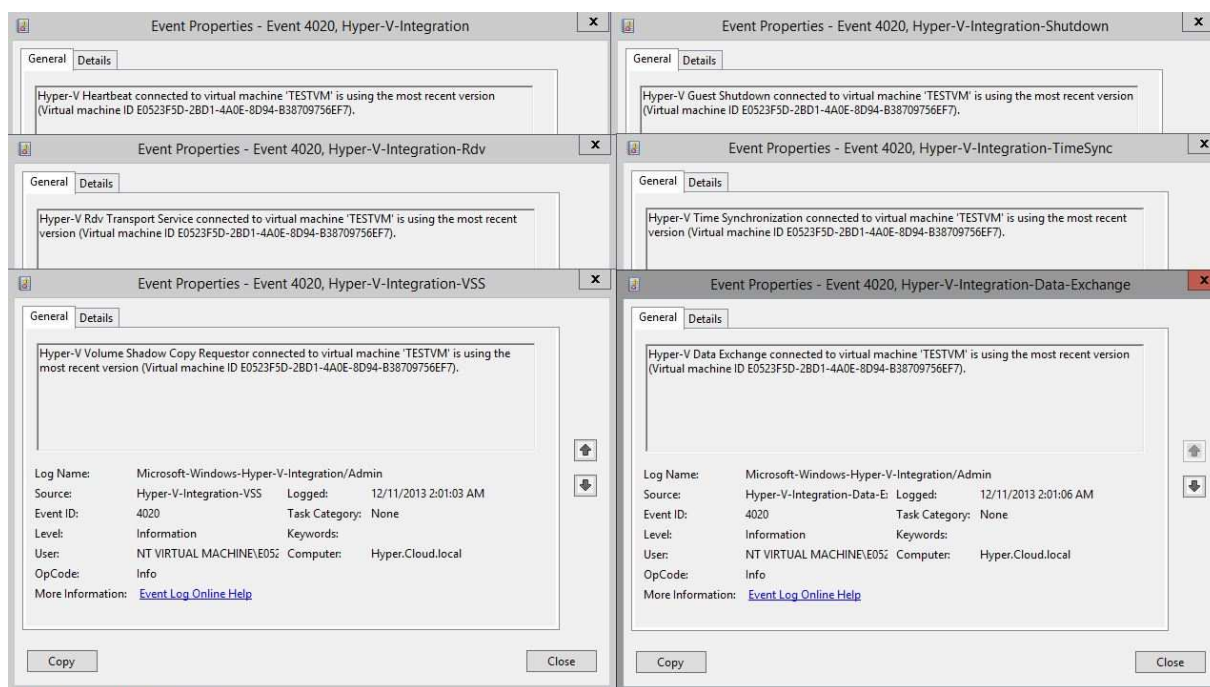


Fig. 50 – Hyper-V Integration service events

Although the mutual event ID number is used for group events, each of these events is separately defined and shows each specific step when starting a virtual computer.

7.1. Types of virtual networks and physical network infrastructure

In addition to creating virtual machines, it is necessary to enable them to communicate with each other, either between virtual machines within the host or between other hosts and their virtual machines. In order to achieve this, it is necessary to create physical and virtual networks. However, types of virtual networks that can be created should first be explained.

In addition to physical network devices, there are virtual network devices. The bases of virtual network devices are virtual network switches. Switches act as network hubs, with the difference that they have an additional layer of software. Thanks to the additional software, network switches have the ability to inspect packages, which allows them to determine the source and destination of the package, as well as to forward that package directly to its destination. Hyper-V virtual switches offer similar functionality as physical network switches. These virtual switches are software implementation of Layer 2 network switches that are available through Hyper-V role. They can be used to connect virtual machines to virtual and physical networks. They also have advanced features such as application of policies, isolation of computers, option to configure bandwidth (traffic shaping) as well as protection against malicious attacks on virtual machines. All these features are an integral part of Windows Server 2012 R2 with installed Hyper-V role.

Management of physical and virtual network equipment requires the use of multiple applications, consoles and command-line interfaces.

In addition to physical network devices and networks that can be created using them, different types of virtual networks can also be created. Examples are networks that are created using Hyper-V service. They are created using virtual switches.



Fig. 51 – Physical and virtual network switches

- **External** is network that enables virtual machines to communicate with one another within a single host, but also with other physical and virtual computers on a network. When creating this virtual switch, new network adapter on Hyper-V host was created.
- **Internal** is network that is used for communication between virtual machines that run on a single host computer. This network enables the exchange of information between the host and virtual machines that are on it. As in the previous case, new separate network adapter is created.
- **Private network** is used for virtual machine communication in an isolated environment within a single host. These virtual switches do not create new virtual adapters.

The figure shows the console for creating virtual networks using Hyper management console.

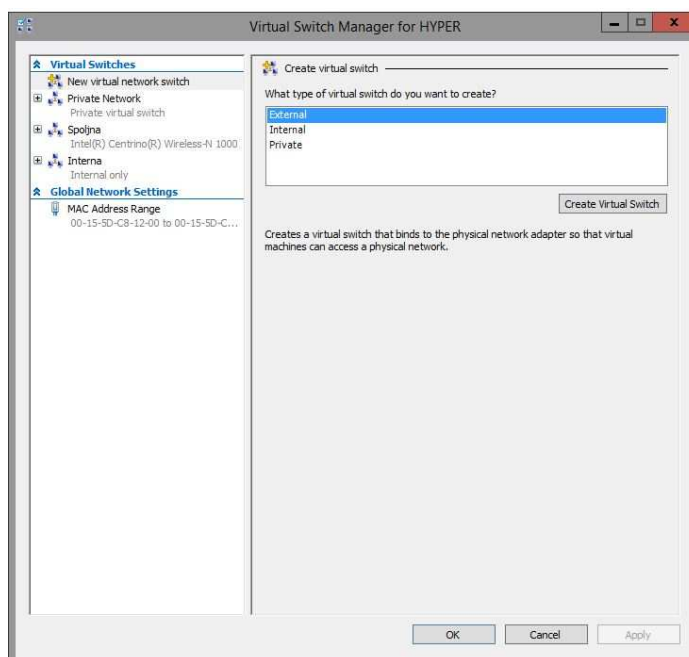


Fig. 52 – Hyper-V virtual networks

It is also important to emphasize that, when it comes to virtual switches, such as External and Internal, it is possible to create virtual LANs (VLAN). It should be noted that the term virtual LAN is not related to virtualization using Hyper-V service, as that standard has been in use for over thirty years.

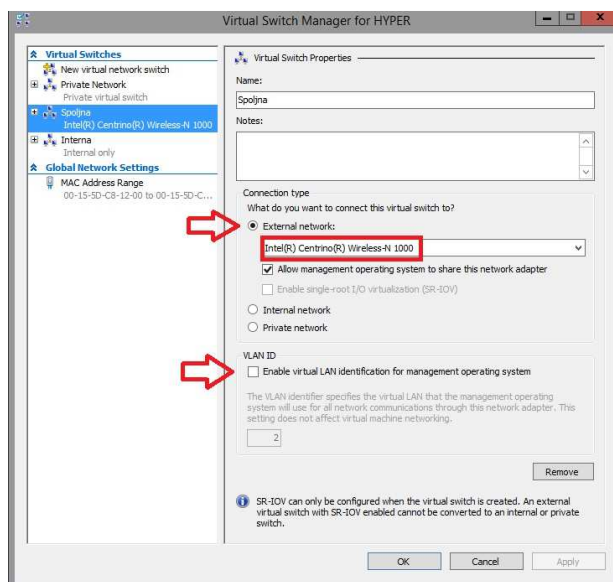


Fig. 53 – VLAN ID Hyper-V configuration of a virtual switch

In addition to this, there is an option to create separate VLAN IDs on individual virtual machines.

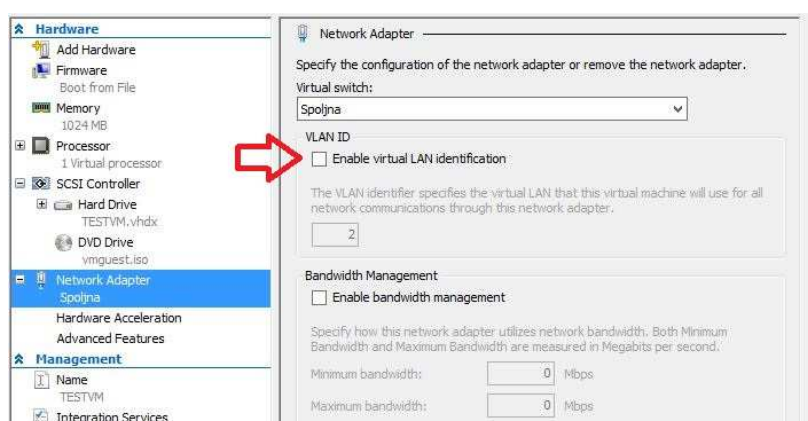


Fig. 54 – VLAN ID configuration on a single virtual computer

In addition, the configuration is further complicated by the presence of networks that can be created using SCVMM service.

When it comes to SCVMM, network infrastructure is a group of adjustable network resources that can be used for creating, organizing and management of virtual machines and their connection. The figure shows the options related to creation of virtual networks in SCVMM.



Fig. 55 – SCVMM virtual networks

Virtual network resources that can be created using SCVMM are:

- *Logical Networks*
Logical networks are network objects that can be used to create a network environment. These networks are available for the allocation to virtual computers in their creation, whether they are system administrators or end users.
- *Network sites*
It is possible to create network sites and join them to network subnets and VLANs. Their role is to enable the user to associate network facilities to host groups or departments within the company.

- *MAC Address Pools*

Since virtual network adapter is usually created when creating each virtual machine, there is a need to assign MAC address to the adapter. Thanks to SCVMM, it is possible to create MAC pool (group of MAC addresses) that can be assigned to virtual computers, whether these virtual computers are on Hyper-V, VMware ESX, or Citrix XenServer hosts. Within SCVMM there are two default static MAC address pools that are primarily related to Hyper-V and Citrix XenServer, as well as special MAC pool that is related to VMware virtual desktops and VMware ESX hosts. Static MAC pools are also used in situations when static MAC addresses have to be configured and assigned to clients. If this is not needed, then Hyper-V hosts can be allowed to assign dynamic MAC addresses to clients. However, using SCVMM, it is possible to define groups of MAC addresses that will be available to hosts for allocation to virtual machines.

- *Load Balancers*

They unload and distribute the load in hosts and virtual machines. It is possible to create virtual load balancers NLB using SCVMM or physical devices. When it comes to software load balancers that are created using SCVMM, they operate on Round Robin principle. Round Robin is a function that sends information to all clients in order, from first to last, and when it comes to the last one, the information is sent again to the first client, and so on. In case that physical equipment is used, it is necessary to add support for each of these devices in SCVMM.

- *VIP Templates (Virtual IP Templates)*

Essentially, VIP templates allow the creation of load balancer for specific type of network traffic. For example, it is possible to create VIP template for HTTPS and then assign it to specific group of computers or service templates.

- *Logical Switches*

Logical switches allow users to create unique configurations on multiple Hyper-V hosts. It is possible to assign them port profiles, uplink profiles, port classification and virtual switch extensions. Thanks to them, it is possible to create uniform network environment that spans over entire Cloud resource.

- *Port Profiles*

There are two basic Hyper-V port profiles that can be created using SCVMM:

- Virtual network adapter port profiles - these profiles enable the creation of adjustment rules related to offload, security, and bandwidth.
- Uplink port profiles - profiles of this type are used to create uplink ports and connect with other physical networks. They can also be assigned load balancing algorithms, as well as teaming mode of network cards.

- *Port Classifications*

They are used to define and configure multiple network switches, as well as for identifying and settings grouping.

- *Network Service*

It represents SCVMM console within which it is possible to configure services and devices such as gateways, virtual switch extensions, top-of-rack (TOR) switches, and network manager. To make this possible, it is necessary to add support for these devices in SCVMM.

- Gateway - will enable virtual computers to access the internet and communicate with other computers. In addition, gateway service can be used to create VPN connections to virtual PCs or create site-to-site VPN connection.
- Virtual switch extensions - they are used to allow non-Microsoft products to collect information about network events. For example, Cisco created Cisco Nexus 1000V for Hyper-V services. As a result, Cisco administrators can configure network devices and set information collecting using Cisco commands such as, for example, sFlow protocol.
- TOR switches - they offer the possibility of creating VLAN hosts within SCVMM and then implement these VLANs on physical switches from SCVMM console.
- Network manager - it allows users to initiate monitoring of logical networks, sites and virtual machine networks, regardless of which tools are used.

Considering that virtual machines that run on hosts also need to communicate with other virtual and physical computers, this communication has to take place over physical and virtual components. For each of these components it is necessary to define how they can collect information about their traffic flow and the methods to use when they get those information.

Having seen all this information, it can be concluded that monitoring of network events within private Cloud an extremely complex process.

7.2. Methods and tools for collecting information from physical network equipment

In addition to collecting information about virtual computers, it is necessary to collect information about network communication. For this purpose, a number of tools from various manufacturers that collect information can be used.

This is very common situation in which security teams within companies need to conduct their own investigations concerning events within a computer network. When such investigations are concerned, especially when the possibility of using Cloud is taken into account, the situation can change significantly.

When it comes to collecting information from Cloud computing, it depends on the model and its configuration. Depending on the platform, when it comes to SaaS and PaaS Cloud solutions, monitoring of network events is rather limited given that there is very little control over resources from which these solutions are executed. When it comes to IaaS Cloud solution, there is the possibility to implement variety of tools to monitor communications between computers. Also, when it comes to SaaS and PaaS solutions, collecting information also differs. For example, within SaaS service, there is complete dependence on the ISP and their ability to monitor and collect information related to the performance of a Web application that runs on their resources, and whether the ISP is willing to deliver the logs. When IaaS is concerned, the situation is somewhat different, though again it largely depends on the service provider, since it is possible to obtain complete image of a virtual computer and subsequently run detailed forensic processing.

However, when Public IaaS is concerned, the situation is different, since there is no access to hardware, but it is possible to monitor network events to some extent. However, when it comes to IaaS solutions, especially private Cloud solution, there is the possibility of physical access to network resources. This also means that it is possible to set up network monitoring tools to monitor traffic.

The necessity of network traffic monitoring is due to the need of noticing and detecting intrusions, both within Cloud system and the attacks that originate from it, or attacks on Cloud system itself. In addition, it is possible to detect spread of viruses, malware, or other undesirable types of communication.

Examples of different types of abuse may vary. For example, there are cases when the attacker rents or takes possession of machines within the Cloud, and uses them carry out the attack, and then turns off the machines or deletes them. Another example may represent a situation in which a person is hiding information that may constitute an element of criminal persecution on one of Cloud resources instead on their computer. So far, in these situations it is very difficult to prove that the perpetrator has committed a crime, because their computers were "clean," i.e. no information on the committed crimes were present on them. Using tools for network traffic monitoring, it is as possible to try to prove that offenders have accessed Cloud resources.

A particular problem, when it comes to Cloud, is the possibility of the presence of virtual computers of different companies on a single host within the Cloud. This situation can cause a problem when collecting log information, because the information from different users can be located in the same log file. It is also necessary to preserve the confidentiality of information of other users that are not the concern of the investigation. The offender may claim that the

information contained in the log files are not theirs, which can pose a major problem in proving the offenses. Monitoring is also complicated by the possibility that virtual computers "slide" between different host computers. This is possible thanks to the infrastructure of Cloud system which is different from classical virtualization infrastructure. This situation may result in additional set of problems, since the information about the events can now be found scattered on several resources, which complicates the investigation.

Because of all this, there is a need to mitigate these problems and find an appropriate solution that can facilitate monitoring of the events within Cloud system. Since it is necessary to use different information collected using different tools and from different sources, they should be combined into one whole.

To make this possible, or at least made easier, it is necessary to monitor network communications. Some of them will be mentioned in further text.

Starting from the option to monitor network communication that exists in Hyper-V service, the option to monitor traffic through port monitoring is extremely important. This enables the option to monitor and forward network events on each individual virtual machine. The figure below shows the configuration of port monitoring options within an individual virtual computer.

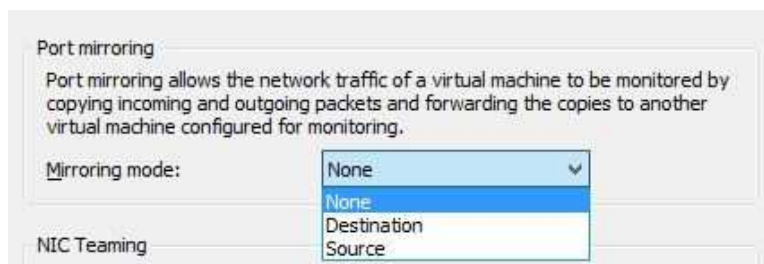


Fig. 56 – Port monitoring

However, in order to obtain a more concrete picture of events, it is necessary to use additional tools for monitoring communications.

In practice, frequently, for the purpose of monitoring network configuration, a tool called Snort is used. This tool has the ability to monitor all segments of network traffic as well as to inspect packages themselves. Information collected in this way are placed in log files. This tool is often used in forensic investigations.

```

C:\Snort\bin\snort.exe
Running in packet dump mode

--- Initializing Snort ---
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{F9C3FEB1-BEF8-4A56-97EB-AE53P00699}
37".
Decoding Ethernet

--- Initialization Complete ---

--> Snort! <--
Version 2.9.5.6-UM32 GRE (Build 208)
By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-
ean
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.3

Commencing packet processing (pid=5360)
03/26-07:17:11.456769 192.168.150.35:36354 -> 157.55.235.172:40005
UDP TTL:128 TOS:0x0 ID:11853 IpLen:20 DgnLen:61
Len: 33
=====
03/26-07:17:11.456197 192.168.150.35:36354 -> 157.55.130.176:40002
UDP TTL:128 TOS:0x0 ID:404 IpLen:20 DgnLen:62
Len: 34
=====
03/26-07:17:11.528753 157.55.235.172:40005 -> 192.168.150.35:36354
UDP TTL:52 TOS:0x0 ID:0 IpLen:20 DgnLen:910 DF
Len: 882
=====
03/26-07:17:11.526135 192.168.150.35:36354 -> 213.199.179.176:40020
UDP TTL:128 TOS:0x0 ID:29003 IpLen:20 DgnLen:174
Len: 146
=====
03/26-07:17:11.574942 157.55.130.176:40002 -> 192.168.150.35:36354
UDP TTL:51 TOS:0x0 ID:0 IpLen:20 DgnLen:480 DF
Len: 452
=====
03/26-07:17:11.578628 192.168.150.35:36354 -> 157.55.130.141:40003
UDP TTL:128 TOS:0x0 ID:7253 IpLen:20 DgnLen:178
Len: 150
=====
03/26-07:17:11.699509 157.55.130.141:40003 -> 192.168.150.35:36354
UDP TTL:51 TOS:0x0 ID:0 IpLen:20 DgnLen:49 DF
Len: 21
=====
03/26-07:17:11.869495 213.199.179.176:40020 -> 192.168.150.35:36354
UDP TTL:54 TOS:0x0 ID:0 IpLen:20 DgnLen:65 DF
Len: 37
=====

Administrator: Command Prompt
2F 02 78 66 1D 36 C1 D3 50 72 C8 00 74 06 B3 72 /..xf.6...Pr..t..r
C0 C1 8B 65 32 80 8B 99 .....e2...

*** Caught Int-Signal
03/28-12:48:15.011531 192.168.150.35:54695 -> 173.194.1.142:80
TCP TTL:128 TOS:0x0 ID:23152 IpLen:20 DgnLen:40 DF
**** Seq: 0xC1BE14AE Ack: 0x622BBE8F Win: 0x400 TcpLen: 20
*****

Run time for packet processing was 20.954000 seconds
Snort processed 1755 packets.
Snort ran for 0 days 0 hours 0 minutes 20 seconds
Pkts/sec:
87

Packet I/O Totals:
Received: 3688
Analyzed: 1755 (47.58%)
Dropped: 1651 (44.92%)
Filtered: 0 (0.00%)
Outstanding: 1933 (52.41%)
Injected: 0

Breakdown by protocol (includes rebuilt packets):
Ech: 1755 (100.00%)
GRE: 0 (0.00%)
IP4: 1755 (100.00%)
Prag: 0 (0.00%)
ICMP: 0 (0.00%)
UDP: 0 (0.00%)
TCP: 1755 (100.00%)
IP6: 0 (0.00%)
IP6 Ext: 0 (0.00%)
IP6 Opts: 0 (0.00%)
Pcap6: 0 (0.00%)
ICMP6: 0 (0.00%)
UDP6: 0 (0.00%)
TCP6: 0 (0.00%)
Teredo: 0 (0.00%)
ICMP-IP: 0 (0.00%)
ENPUL: 0 (0.00%)
IP4/IP4: 0 (0.00%)
IP4/IP6: 0 (0.00%)
IP6/IP4: 0 (0.00%)
IP6/IP6: 0 (0.00%)
GRE: 0 (0.00%)
GRE Ech: 0 (0.00%)
GRE ULAN: 0 (0.00%)
GRE IP4: 0 (0.00%)
GRE IP6: 0 (0.00%)
GRE IP6 Ext: 0 (0.00%)
GRE PPP: 0 (0.00%)
GRE ARP: 0 (0.00%)
GRE IPX: 0 (0.00%)
GRE Loop: 0 (0.00%)
MPLS: 0 (0.00%)
ARP: 0 (0.00%)
IPX: 0 (0.00%)
Eth Loop: 0 (0.00%)
Eth Disc: 0 (0.00%)
IP4 Disc: 0 (0.00%)
IP6 Disc: 0 (0.00%)
TCP Disc: 0 (0.00%)
UDP Disc: 0 (0.00%)
ICMP Disc: 0 (0.00%)
all Discard: 0 (0.00%)
Other: 0 (0.00%)
Bad Chk Sum: 0 (0.00%)
Bad TTL: 0 (0.00%)
SS G 1: 0 (0.00%)
SS G 2: 0 (0.00%)
Total: 1755

Snort exiting
C:\Snort\bin>

```

Fig. 57 – Overview of information obtained using SNORT tool

In addition to this tool, one of the products used to monitor network events comes from Microsoft Company, and is called Network Monitor.

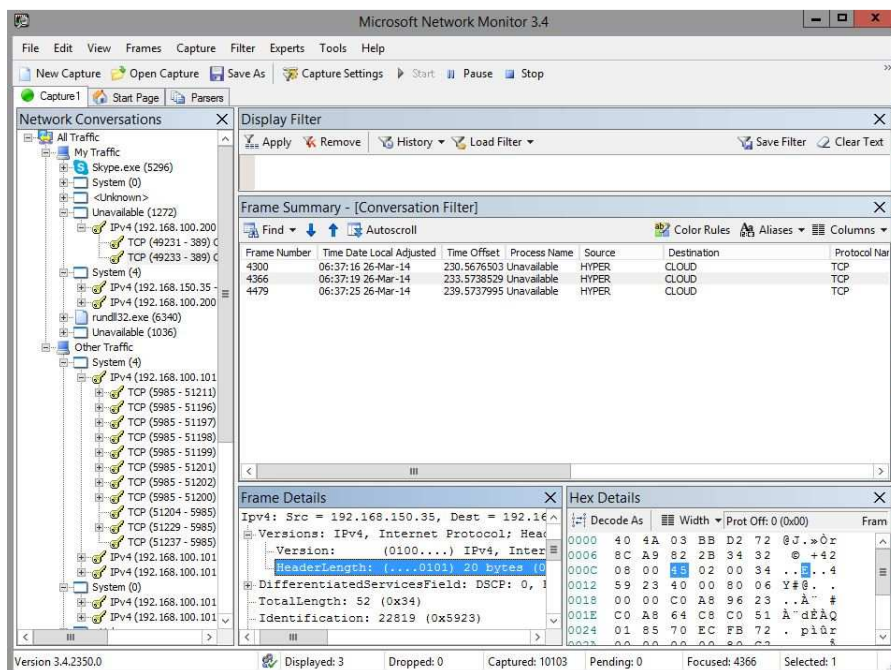


Fig. 58 – Microsoft Network Monitor

Although free, this product does not come pre-installed as part of operating systems from Microsoft. The reason for this can be possible invasion in privacy of users. Since it is a free tool, it can be downloaded from the internet.

With this tool it is possible to collect complete information regarding network communication, with detailed insight into events that take place within the host. Also, an additional benefit comes from the fact that using this tool it is possible to monitor physical and virtual network adapters, as well as traffic that goes through them.

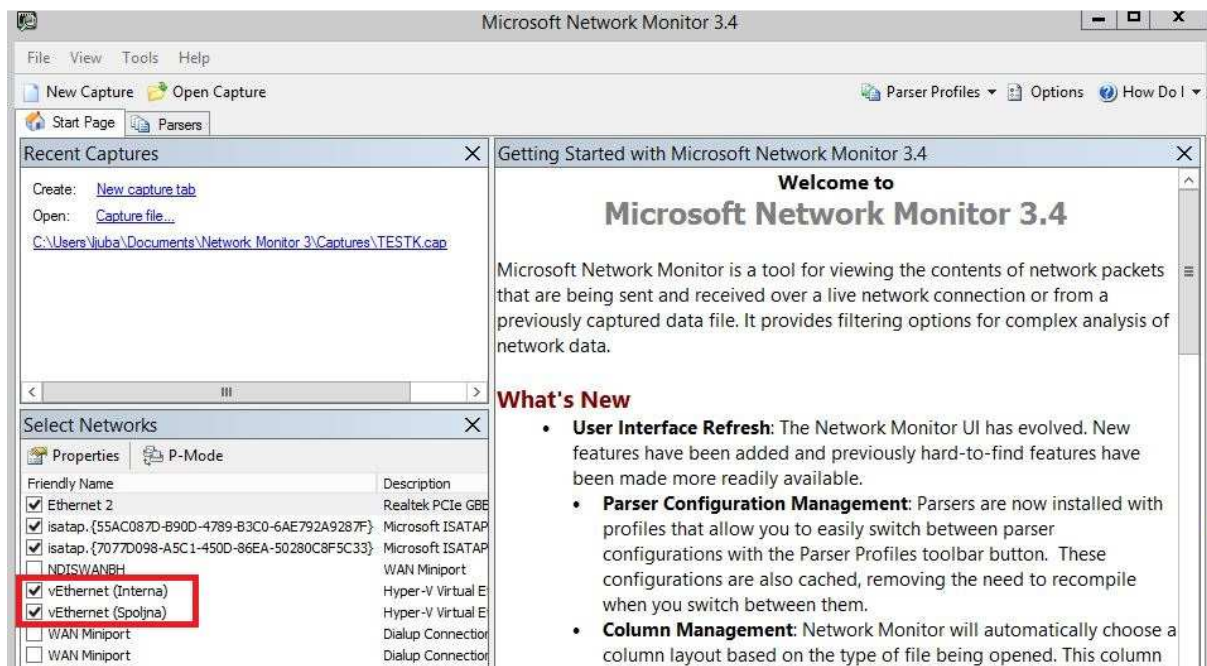


Fig. 59 – Monitoring Hyper-V virtual switches

The information that are collected using this tool can be stored in capture files for later examination.

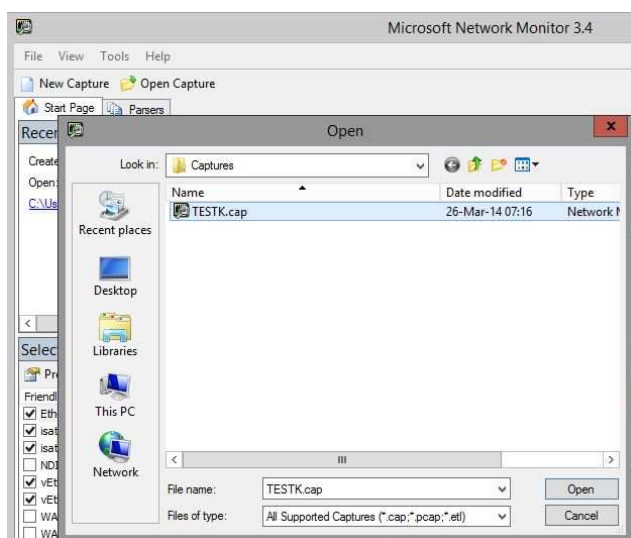


Fig. 60 –Opening of previously collected information gathered by monitoring network communication

However, these tools are mostly limited to monitoring a specific computer, whether it is physical or virtual. Since it is necessary to perform monitoring network communications within the Cloud, it should be noted that such tools also exist.

Company ManageEngine²⁰ offers a solution for monitoring Cloud system. This solution, called OpManager, allows monitoring of Cloud infrastructure, and its individual components.

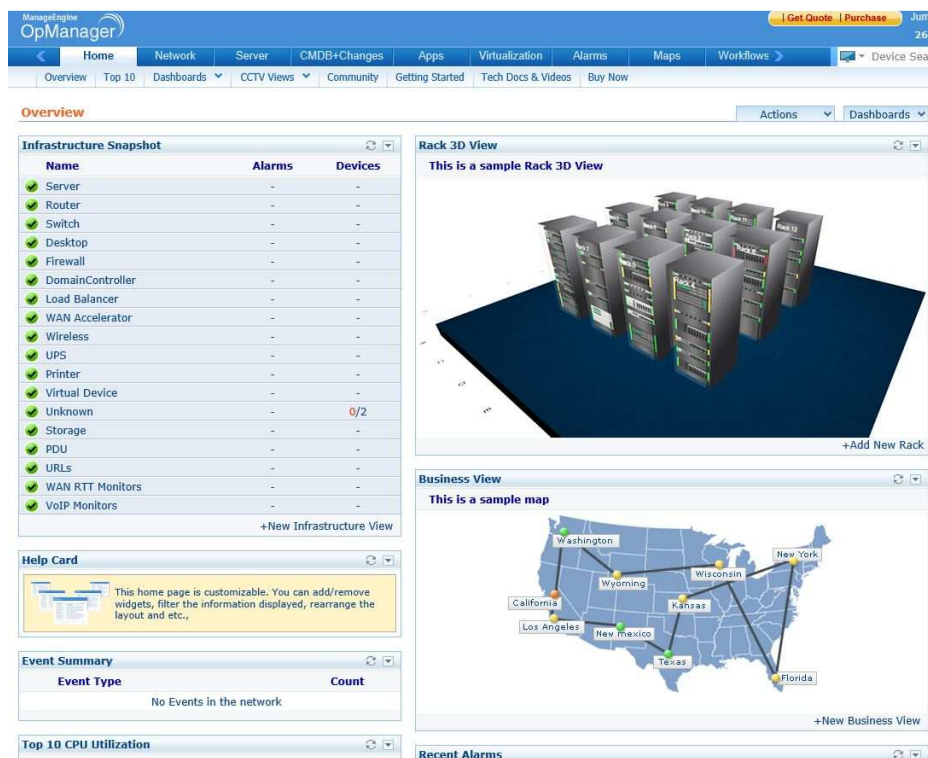


Fig. 61 – OpManager system for monitoring Cloud environment

Besides these solutions, there is one solution from RSA called “RSA Security Analytics Investigation”²¹ which is tailored specifically for these tasks. Initial role of this application is monitoring and performance base line creation. This allows the user to better optimize managed services. Also, this application is equipped with engine for real-time and log monitoring of events with specific targeting to threats as seen in the figure below.

²⁰ <http://www.manageengine.com/network-monitoring/?gclid=CNmuw-iPt0CFcuWtAodTDwAFw&gclidsrc=aw.ds>

²¹ <http://www.emc.com/security/rsa-security-analytics/applications/rsa-security-analytics-investigation.htm>

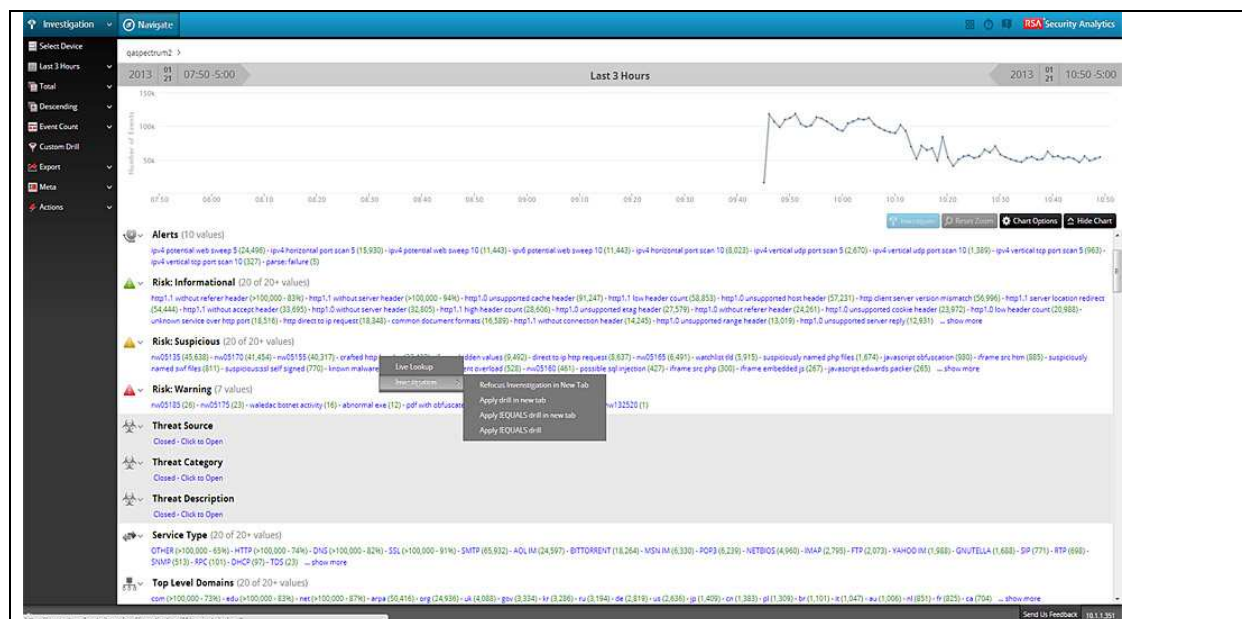


Fig. 62 – RSA management console with displayed threats

Current threats are displayed and easily visible. Also, the threats are linked together thus allowing the user to better pinpoint the source of event that is happening or has previously occurred.

8. Conclusion

The necessity of having virtual environments that have very high level of automation instigates the use of Cloud environment. In addition, the modularity of Cloud system is a great advantage. This modularity allows that each service can be used as an individual or as a group of products. From this fact it can be said that, when creating Cloud environments, it is not necessary to use all of the components mentioned above.

Direct selection of components is indirectly related to specific needs of the company. It depends solely on the level of functionality that is required in each case. The conclusion is that two different companies can create Cloud solutions, one using only a few elements, while the other may use all the elements of a Cloud environment.

Since collecting information about events within Cloud Computing solution depends on its components, it can be concluded that Cloud monitoring system is modular process of collecting information. This also complicates the whole process, and makes the creation of universal solution for monitoring events almost impossible. Although it seems that it is an unattainable task, there is a great need to find an appropriate solution for monitoring events. Consequently, it is necessary to create process of collecting information that would take into account the modularity of the solution. To explain this process, it is necessary to define the connection of the events between independent segments of Cloud environment.

From above it can be concluded that the execution of digital forensics in Cloud environments is very complex process that is almost impossible to do without proper preparation and complete knowledge of current infrastructure, both virtual and physical. That is why it is necessary to primarily define methods and procedures for collecting information in private Clouds, and thus set the guidelines for collecting necessary information, both in private and public Clouds. This is best achieved using logging and auditing processes. Collected information can then be viewed and searched.

The point is that the logs contain information about events, regardless of how they are collected, what software is used and where they will be located. These information are evidence that some event has occurred and what the result of that event is. In this thesis there are several suggested methods that might help achieve that goal.

Also, perhaps the most important fact is: in order to start collecting logs, that process should first be started or a tool for that should be installed and properly configured. This action is usually not automatically launched when the operating system is installed, but must be run manually or set up to run automatically. When it comes to manually launching a log tool, some of the tools mentioned in the text can be used, or group policies within Active Directory service can be used, as described in author's graduate paper,²² while some of the tools mentioned need to be bought separately.

Collecting information is the first step in forensic investigation. Quality procedures and information about the ways in which they can be collected present a basis that can be used to create the postulates of digital forensics in the Cloud.

²² [Implementacija bezbednosnog rešenja u okviru školskog centra kompanije CPU d.o.o.], Ivaniš Lj.

Because of this, digital forensics is best viewed from private Cloud standpoint and thus draws conclusions and make parallels with public Clouds. In other words, the information about the information collecting in the private Cloud should be used, and in that way create the basis (baseline), where all the information can be used in forensic investigations. These information can serve as a basis for investigators in case they have to obtain information from public CSP's so that investigators would have a better position to request the information from them.

9. LITERATURE

- [1] Ivaniš Lj., *Implementacija bezbednosnog rešenja u okviru školskog centra kompanije CPU d.o.o.*, graduate paper, Beograd 2013.
- [2] Birk D., *Technical Challenges of Forensic Investigations in Cloud Computing Environments*, IBM Zurich Research Laboratory, january 2012.
- [3] Dutta Amit K., Hasan R., Zawoad S., *SecLaaS Secure Logging-as-a-Service for Cloud*, University of Alabama at Birmingham, february 2013.
- [4] Dizdarević D., Reimer S., Thomas O., *Implementing an Advanced Server Infrastructure*, Microsoft Press, 2012.
- [5] Forrester Research company, *Enabling The Secure And Rapid Adoption of Cloud Services*, at Microsoft's request, october 2013.
- [6] Costa P., Migliavacca M., Pietzuch P., Wolf Alexander L., *NaaS: Network-as-a-Service in the Cloud*, Imperial College London, University of Kent, 2012.

Internet sources

- [7] *Cloud billing: The missing link for cloud providers*, CGI Group Inc,
<http://www.cgi.com/files/white-papers/cloud-billing-white-paper.pdf>,
[accessed: 20.12.2013]
- [8] *Cloud computing*,
http://en.wikipedia.org/wiki/Infrastructure_as_a_service#Infrastructure_as_a_service_.28IaaS.29,
[accessed: 20.12.2013]
- [9] *Generation 2 Virtual Machine Overview*,
<http://technet.microsoft.com/en-us/library/dn282285.aspx>,
[accessed: 20.12.2013]
- [10] *Windows Azure*
<http://www.windowsazure.com/en-us/>
[accessed: 10.12.2013]
- [11] *Windows Azure Privacy Statement*
<http://www.windowsazure.com/en-us/support/legal/privacy-statement/>
[accessed: 20.01.2014]
- [12] *Data and personality protection act, "Službeni glasnik RS", br. 97/2008*
<http://www.minrzs.gov.rs/doc/podrobnosti/Zakon%20o%20zastiti%20podataka%20o%20licnosti.pdf>
[accessed: 20.01.2014]
- [13] *Wikipedia*
http://en.wikipedia.org/wiki/Digital_forensics
[accessed: 20.01.2014]
- [14] *Microsoft Download Center*
<http://www.microsoft.com/en-us/download/details.aspx?id=4865>
[accessed: 20.01.2014]