Journal of Automation, Electronics and Electrical Engineering

APPLICATION OF VIRTUALISATION ENVIRONMENT FOR DATA SECURITY IN OPERATIONAL DATA PROCESSING SYSTEMS

Bartłomiej Ulatowski[1]
Marek Gróbarczyk[2]
Zbigniew Łukasik[3]

[1] Uniwersytet Technologiczno-Humanistyczny, Wydział Transportu, Elektrotechniki i Informatyki, Malczewskiego 29, 26-600 Radom, Polska, b.ulatowski@uthrad.pl
[2] Uniwersytet Technologiczno-Humanistyczny, Wydział Transportu, Elektrotechniki i Informatyki, Malczewskiego 29, 26-600 Radom, Polska, marek.grobarczyk@wp.pl
[3] Uniwersytet Technologiczno-Humanistyczny, Wydział Transportu, Elektrotechniki i Informatyki, Malczewskiego 29, 26-600 Radom, Polska, z.lukasik@uthrad.pl

DOI: https://doi.org/10.24136/jaeee.2021.004

Abstract – This paper presents a concept, developed and tested by the authors, of a virtualisation environment enabling the protection of aggregated data through the use of high availability (HA) of IT systems. The presented solution allows securing the central database system and virtualised server machines by using a scalable environment consisting of physical servers and disk arrays. The authors of this paper focus on ensuring the continuity of system operation and on minimising the risk of failures related to the availability of the operational data analysis system.

Keywords – data, exploitation, virtualization, IT systems, security

INTRODUCTION

The use of virtualisation technology is having a significant impact on the entire IT industry. Its use is particularly evident in data centres to reduce costs and increase efficiency. [7]

Virtualisation technology is developing rapidly and more and more developers are aiming to create cloud applications. All these advances can be used in the future to simplify data handling techniques and enhance IT security. [7]

Virtualisation is a technology used to share the capabilities of physical computers by sharing resources between operating systems. Currently, there are several virtualization techniques that can be used to support the creation of entire operating systems in a scalable environment. We classify virtualization techniques from an operating system point of view: operating system level virtualization and paravirtualization. [1,5,6]

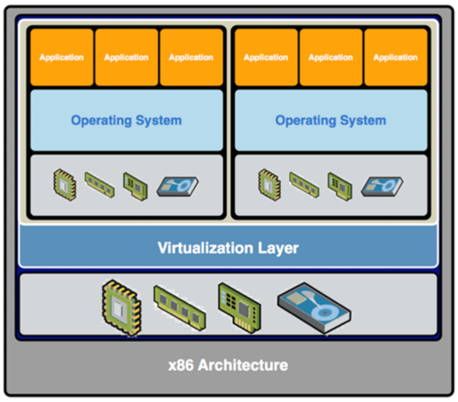


Fig. 1. Depiction of the virtualisation server architecture [1]

The figure above shows a diagram of the architecture of a basic virtualisation server, which works on the basis of a master server or hypervisor. The solution that is shown demonstrates the principle of sharing the resources of the master server for virtualised machines.

Virtualisation technology provides an alternative technical approach to delivering infrastructure, platforms and operating systems, servers, software and systems and applications. Most virtualised computing environments have much in common with conventional data centres, using highperformance hardware and specialised software that allows a single physical server to function as multiple instances running in parallel. The use of virtual environments allows organisations to utilise IT resources more efficiently by scaling up or down depending on business needs. The use of virtual environments utilizes many of the same procedures and criteria used in data centre audits, with additional emphasis on provisioning, deprovisioning, managing and maintaining multiple virtual servers that share compute, network and infrastructure resources. [6- 8]

I. Functional assumptions of the exploitation data processing system

The IT system, the protection of which is analysed in this study, is presented in Fig. 2. The presented architecture takes into account the use of a central database system, access to which is provided from devices located in places with access to the Internet by means of appropriately configured VPN network protocols. Thanks to the indicated solution, the system will be secured both in terms of hardware and software.

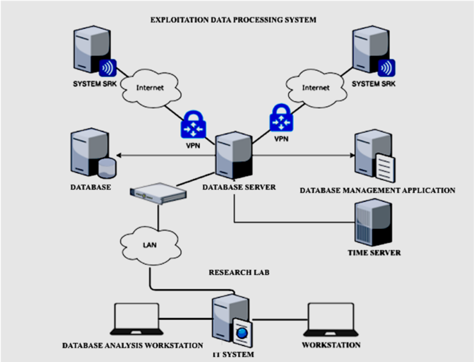


Fig. 2. Proposal of functioning of the exploitation data processing system (own elaboration)

The authors of the article, while carrying out research related to the subject of exploitation data analysis, have observed that the constantly developing railway market sector requires undertaking work related to computerisation of maintenance processes.

Therefore, the proposed database system architecture is based on a professional virtualised IT environment from VMware. These systems, when properly configured, can allow the availability of services in a high reliability mode. The use of multiple master servers called hosts and an extensive disk array can ensure the availability of the offered services and access to the database system with minimum failure times.

High Reliability [2] or HA systems are a solution that continuously monitors all servers in the resource pool and detects server failures. An agent located on each server maintains constant communication with other servers connected in the resource pool, and loss of communication initiates the process of restarting all affected virtual machines on other servers. This type of solution can allow to ensure the security of the exploitation data processing systems that are analysed in this paper. [3]

The HA solution ensures that sufficient resources are available in the resource pool at all times to restart VMs on different physical servers in the event of a server failure. VM restart is made possible through the use of a clustered Virtual Machine File System (VMFS), which provides multiple instances with simultaneous read and write access to the same virtual machine files. High availability systems can be easily configured with the appropriate virtual environment management software. [3]

The decision to consider a solution based on virtualisation systems is related to the necessity of its possible scalability. Dynamic load distribution, which is possible in the above mentioned systems, allows smooth scaling of the virtual environment along with the increase in demand for resources for the application responsible for storing and processing operational data.

The implementation of the solution proposed by the authors in a virtualisation environment may ensure a quick response during a possible system failure. The use of a virtual environment makes it possible to create snapshots of the entire virtualised machine. Thanks to this solution, while making frequent security copies on external carriers and NAS disks, it is possible to restore a fully functional system without having to install the entire environment from scratch.

The suggested solution presented in this article consists of three DELL PowerEdge M620 physical servers running VMware ESXi Server 6.7 installed in a blade enclosure chassis M1000e. The servers are located in a single data centre and form a private computing cloud based on a VMware cluster called "Cluster". The cluster provides the functionality of VMware HA increased availability and constitutes a platform for the virtual machine environment.

The servers were named esx01.pr.radom.pl, esx02.pr.radom.pl and esx03.pr.radom.pl respectively and use shared LAN and SAN resources provided on a Hitachi HUS 100 array.

For central management of the entire virtual infrastructure, VMware vCenter Server was used, which is installed as a virtual machine (appliance. vCenter Server uses the SUSE 11 operating system, a preinstalled vPostgreSQL database and Single Sign-On (SSO) management service. Figure 3 shows the logical architecture of the virtual environment developed by the authors.

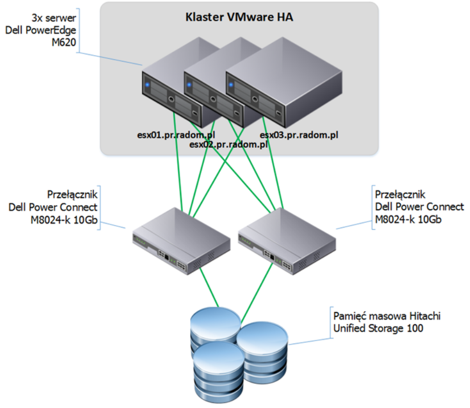


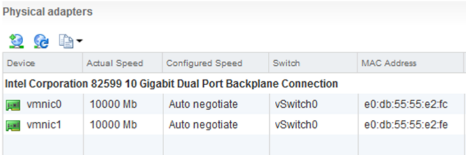
Fig. 3. Logical architecture of the virtualisation system (own elaboration)

II. Transmission Performance

In order to provide redundancy of the high performance LAN connection for the entire virtualisation environment, the authors applied the use of two physical interfaces with a capacity of 10 Gbps each. The high performance of the connection is necessary to maximise the efficiency of the operating data processing environment.

The cards indicated in Figure 4 in the proposed solution should be combined into the following functional pairs:

- vmnic0 (active) and vmnic1 (standby) cards for production traffic, MGMT and vMotion
- vmnic1 (active) and vmnic0 (standby) cards for iSCSI SAN support

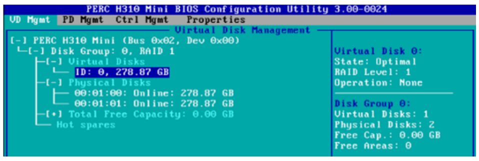


Physical adapters

Device	Actual Speed	Configured Speed	Switch	MAC Address
Intel Corporation 82599 10 Gigabit Dual Port Backplane Connection				
vmnic0	10000 Mb	Auto negotiate	vSwitch0	e0:db:55:55:e2:fc
vmnic1	10000 Mb	Auto negotiate	vSwitch0	e0:db:55:55:e2:fe

Fig. 4. Network interfaces required in a virtualisation environment (own elaboration)

Master servers, which perform the function of virtualisation HOSTs, should be equipped with two SAS disks and must be connected to the local RAID controller of PERC H310 Mini type in RAID1 arrangement (mirror). In such configuration it is possible to create a virtual disk volume of 278GB. These resources may be used for the needs of virtualisation platform and storage of low critical virtual machines. The RAID controller configuration is shown in Figure 5.



```
               PERC H310 Mini BIOS Configuration Utility 3.00-0024
VD Mgmt  PD Mgmt  Ctrl Mgmt   Properties
                   Virtual Disk Management
[-] PERC H310 Mini (Bus 0x02, Dev 0x00)
 └─[-] Disk Group: 0, RAID 1                      Virtual Disk 0:
    ├─[-] Virtual Disks                            State: Optimal
    │  └── ID: 0, 278.87 GB                        RAID Level: 1
    ├─[-] Physical Disks                           Operation: None
    │  ├── 00:01:00: Online: 278.87 GB
    │  └── 00:01:01: Online: 278.87 GB             Disk Group 0:
    ├─[+] Total Free Capacity: 0.00 GB             Virtual Disks: 1
    └── Hot spares                                 Physical Disks: 2
                                                   Free Cap.: 0.00 GB
                                                   Free Areas: 0
```

Fig. 5. RAID controller configuration in a virtual environment (own elaboration)

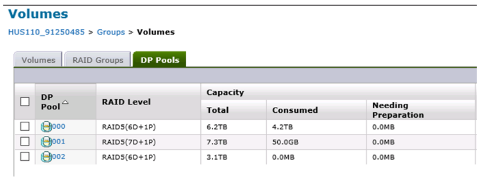
The basis of the production disk subsystem must be a disk array connected redundantly to each ESXi server via a single data network. The network in the proposed environment consists of two switches with a capacity of 10Gb each. The storage should be directly connected via two 10GbE Fibre Channel cables to the switches supporting the indicated 10Gb per second throughput.

It is necessary to create logical volumes on the disk array, which can then be configured by ESXi servers. [own elaboration].

Each server can include a software implemented iSCSI initiator. The iSCSI operations are in this case performed by the processor (and not by a separate PCI-X/PCI-Express card). Thanks to the high performance of currently available processors, this solution does not noticeably reduce server performance. Normal network cards are used to transmit SCSI commands. This way of connecting the disk subsystem allows access to disk resources using 1 data path, one path to each LUN. [own elaboration].

III. Disk Resources - Use of Arrays for the Security of Processed Data

A server in the storage network is referred to as an iSCSI target. One iSCSI target can provide one or more Logical Units (LUs). Logical Units are often abbreviated as LUNs (although this abbreviation stands for Logical Unit Number). [own elaboration].



Volumes

HUS110_91250485 > Groups > Volumes

☐	DP Pool	RAID Level	Capacity		
			Total	Consumed	Needing Preparation
☐	000	RAID5(6D+1P)	6.2TB	4.2TB	0.0MB
☐	001	RAID5(7D+1P)	7.3TB	50.0GB	0.0MB
☐	002	RAID5(6D+1P)	3.1TB	0.0MB	0.0MB

Fig. 6. Disk resources for the virtualization environment (own elaboration)

Within the array designated as 001 configured in RAID5 mode (Fig. 6) and using 7 disks for data and 1 disk for parity, 3 LUNs were created for the virtual environment with the following characteristics illustrated in Table 5.

Table 1 Disk resources used in a high reliability virtual environment (own elaboration)

Matrix	LUN ID	Size	Purpose
VOL0003	LUN 0	2000 GB	Virtual machines
VOL0004	LUN 1	2000 GB	Virtual machines
VOL0005	LUN 2	2000 GB	vSphere Data Protection

Since virtual machines running on individual servers can synchronise time with the ESXi server, it is necessary to configure appropriate synchronisation with the specified time server on all servers, as confirmed by the authors' research.

IV. Summary

After the study, it can be concluded that by using virtualisation technology operating in HA mode, i.e. high availability, in the case of a need to expand the server environment, the exploitation data analysis system in question or a failure of the master server responsible for virtualisation, we have ensured increased data security. The use of high reliability mode for systems responsible for safety is a priority, because an appropriate analysis of operational data can directly contribute to increased safety during all transport processes.

Zastosowanie środowiska wirtualizacyjego do zabezpieczenia danych w systemach przetwarzania danych eksploatacyjnych

Niniejszy artykuł przedstawia koncepcję środowiska wirtualizacyjnego umożliwiającego zabezpieczenie agregowanych danych poprzez zastosowanie wysokiej dostępności (HA) systemów informatycznych. Przedstawione rozwiązanie pozwala zabezpieczyć centralny system bazodanowy oraz zwirtualizowane maszyny serwerowe poprzez wykorzystanie skalowalnego środowiska składającego się z fizycznych serwerów oraz macierzy dyskowych. Autorzy pracy skupiają się na zapewnieniu ciągłości działania systemów oraz na minimalizacji ryzyka awarii związanych z dostępnością systemu analizy danych eksploatacyjnych.

Słowa kluczowe: dane, eksploatacja, wirtualizacja, systemy informatyczne, bezpieczeństwo

Bibliography

[1] Bobek Sz. Wirtualizacja pełna i parawirtualzacja, Institute of Applied Computer science AGH University of Science and Technology, AGH 2013 (https://ai.ia.agh.edu.pl/wiki/_media/pl:dydaktyka:sitw:2015:xen:l_full-para.pdf)

[2] Gray J.,"High-Availability Computer Systems" Digital Equipment Corp.Daniel P. Siewiorek, Carnegie Mellon University, 1991

[3] Vmware High Availability, VMWare Product datasheet, strona internetowa: https://www.vmware.com/pdf/ha_datasheet.pdf

[4] Nomnga P., Nyambi P. B., Scott M. S., A Technical Cost Effective Network-Domain Hosting through Virtualization: a VMware ESXi and vSphere Client Approach, International Journal of Computer Applications 91(10):39-47, 2014

[5] Ridriguez-Haro F., Freitag F., Navrro L., Hernanchez-sanchez E., Farias-Mendoza N., Guerrero-Ibanez J., Gonzales-Potes., A summary of virtualization techniques, Procedia Technology Volume 3, 2012, Pages 267-272, Elsevier (https://www.sciencedirect.com/science/article/pii/S2212017312002587)

[6] Sharma S., VIRTUALIZATION: A REVIEW AND FUTURE DIRECTIONS Executive Overview, American Journal of Information Technology, 2011

[7] Hassan N., Hijazi R., Chapter 8 - Future Trends, Data Hiding Techniques in Windows OS, A Practical Approach to Investigation and Defense, , Pages 291-298, 2017 (https://www.sciencedirect.com/science/article/pii/B9780128044490000087)

[8] Virtualization for Security - Including Sandboxing, Disaster Recovery, High Availability, Forensic Analysis, and Honeypotting, 2009, Pages 1-43 (https://www.sciencedirect.com/science/article/pii/B9781597493055000013)