Journal scientific and applied research, vol. 21, 2021
International Journal

Original Contribution

ISSN 1314-6289

VIRTUALIZATION OF THE OPERATING SYSTEM MICROSOFT WINDOWS 10 (64-BIT) VIA VMWARE VSPHERE HYPERVISOR ESXI 6.5.0 FOR EDUCATIONAL PURPOSES IN THE FACULTY OF TECHNICAL SCIENCES

Petar Kr. Boyanov

DEPARTMENT OF MANAGEMENT OF SECURITY SYSTEMS, FACULTY OF TECHNICAL SCIENCES, KONSTANTIN PRESLAVSKY UNIVERSITY OF SHUMEN, SHUMEN 9712,115, UNIVERSITETSKA STR,
E-MAIL: petar.boyanov@shu.bg

ABSTRACT: *In this paper virtualization of the operating system Microsoft Windows 10 (64-bit) via VMware vSphere Hypervisor ESXi 6.5.0 for educational purposes in well-equipped laboratories at the Faculty of Technical Sciences at the Konstantin Preslavsky University of Shumen is made.*

KEY WORDS: *Computer resources, Hypervisor, Implementation, LAN, Operating systems, Simulation, System administration, Virtualization, VMware, VSphere, Windows 10.*

1. Introduction

VMware is one of the first players in the recently launched virtualization platform and patented its virtualization software techniques. Along with this, it launches quite efficient and professional virtualization products of various sizes: from VMware Workstation, designed for the end user to VMware ESXi Server, designed for virtual infrastructures in large enterprises. VMware's extensive list includes many tools to increase efficiency in the virtualization process, managing virtual servers and tools for migrating the physical platform to a virtual one [4,5,7,10,11,12,14,15]. VMware products are especially popular all over the world, as this modern soil process is gaining more and more popularity compared to other programs that have less functionality. In addition to the various performance tests of virtualization tools, VMware almost always beats its competitors [1,2,3,4,5,6,8,9,12,13].

2. Experiment

In the last few years, server virtualization technology has moved rapidly into the IT mass market. Of the vendors offering hypervisor-based products, only VMware can be considered ready-made [3,5,7,9,10,12,14,16]:

VMware's architectural vision is based on years of experience that solves real-world problems in terms of performance, security, and compatibility, rather than unproven academic research [2,3,5,7,9,10,13,16].

The VMware hypervisor is enhanced by a wide range of technologies that allow its use in a variety of solutions for security [2,3,6,7,8,10,11,12].

VMware products have reached the level required of enterprise customers.

The scientific experiment in well-equipped laboratories at the Faculty of Technical Sciences at the Konstantin Preslavsky University of Shumen is made. The aim of the simulation is to illustrate the methods for virtualization of the operating system Microsoft Windows 10 (64-bit) via VMware vSphere Hypervisor ESXi 6.5.0.

The first computer configuration consists of the following computer components:

- Main Board: Gigabyte B75M-D3V socket 1155;
- CPU: Intel Core i3-3225 3,3 GHz socket 1155;
- RAM: 2 x 4 GB DDR3;
- HDD: 500 GB+ 128 SSD;
- Optical drive: LG DVD-RW;
- Monitor: Asus 19" LCD VW199TR with serial number: C6LMTF101835. The second monitor: Acer 19" LCD KA210HQ.

The second computer configuration consists of the following computer components:

- Main Board: Gigabyte A320M-S2H AM4;
- CPU: AMD Ryzen 5 3400 4.2 GHz;
- RAM: 2 x 8 GB DDR4;
- HDD: 1 TB SSD;
- Optical drive: LG DVD-RW;
- Monitor: Philips 23,8" LCD 243V7QDAB with serial number: UHBA2019009966.

3. Results

On fig. 1 the installation of ESXi 6.5.0 is shown.

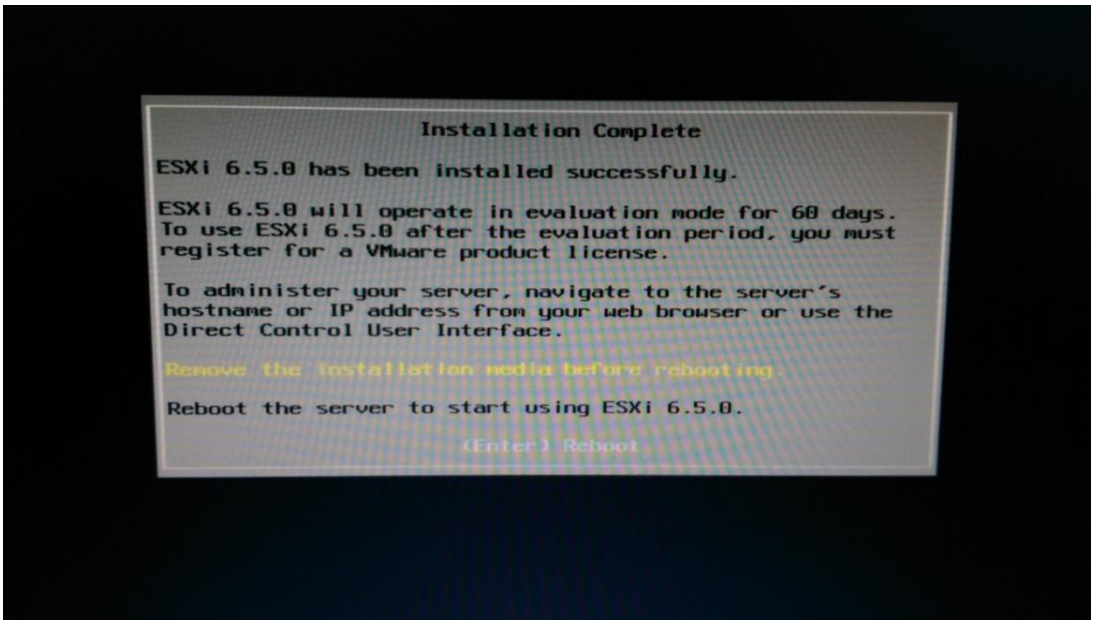

Fig. 1. The installation of ESXi 6.5.0

On fig. 2 the basic graphical user interface of VMware ESXi 6.5.0 and the IPv4 network access address for managing the VMware vSphere hypervisor is displayed.

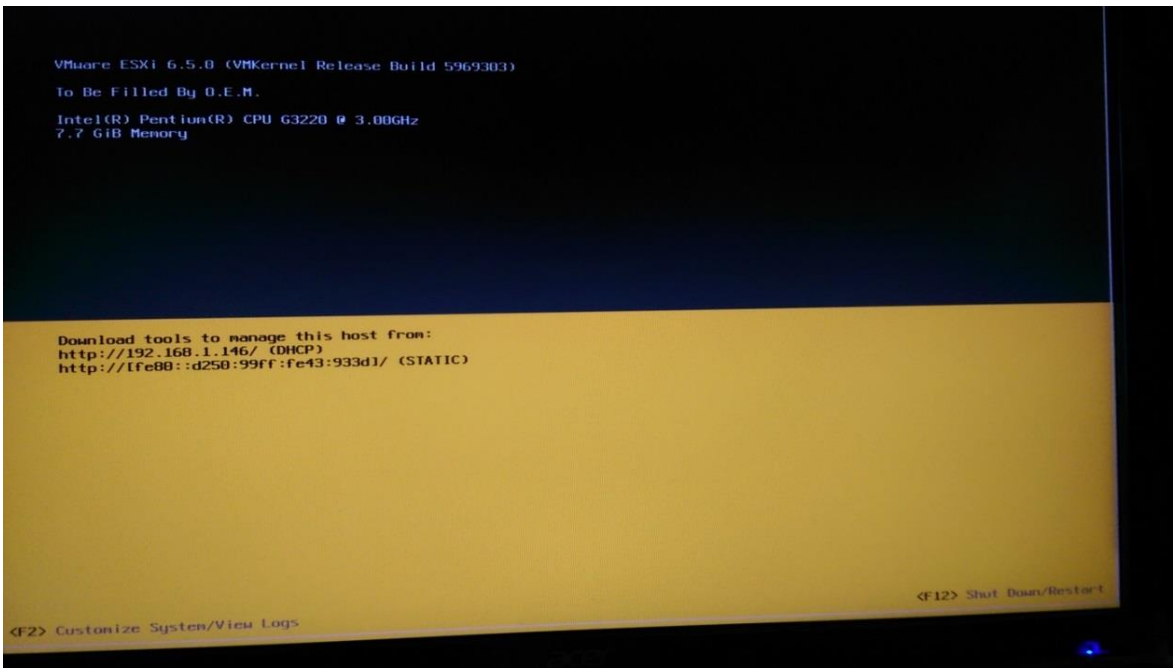

Fig. 2. The IPv4 network access address for managing the VMware vSphere hypervisor

On fig. 3 the IPv6 network configuration is shown.

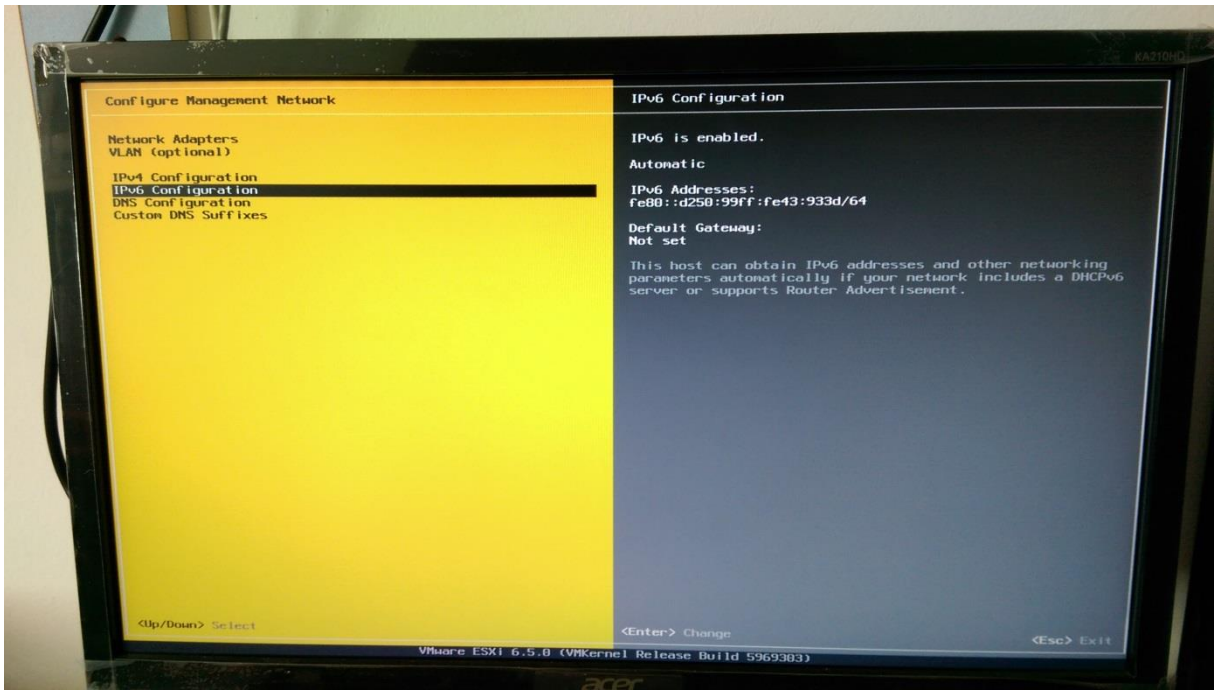

Fig. 3. IPv6 network configuration

On fig. 4 the web access address for VMware ESXi 6.5.0 is shown.

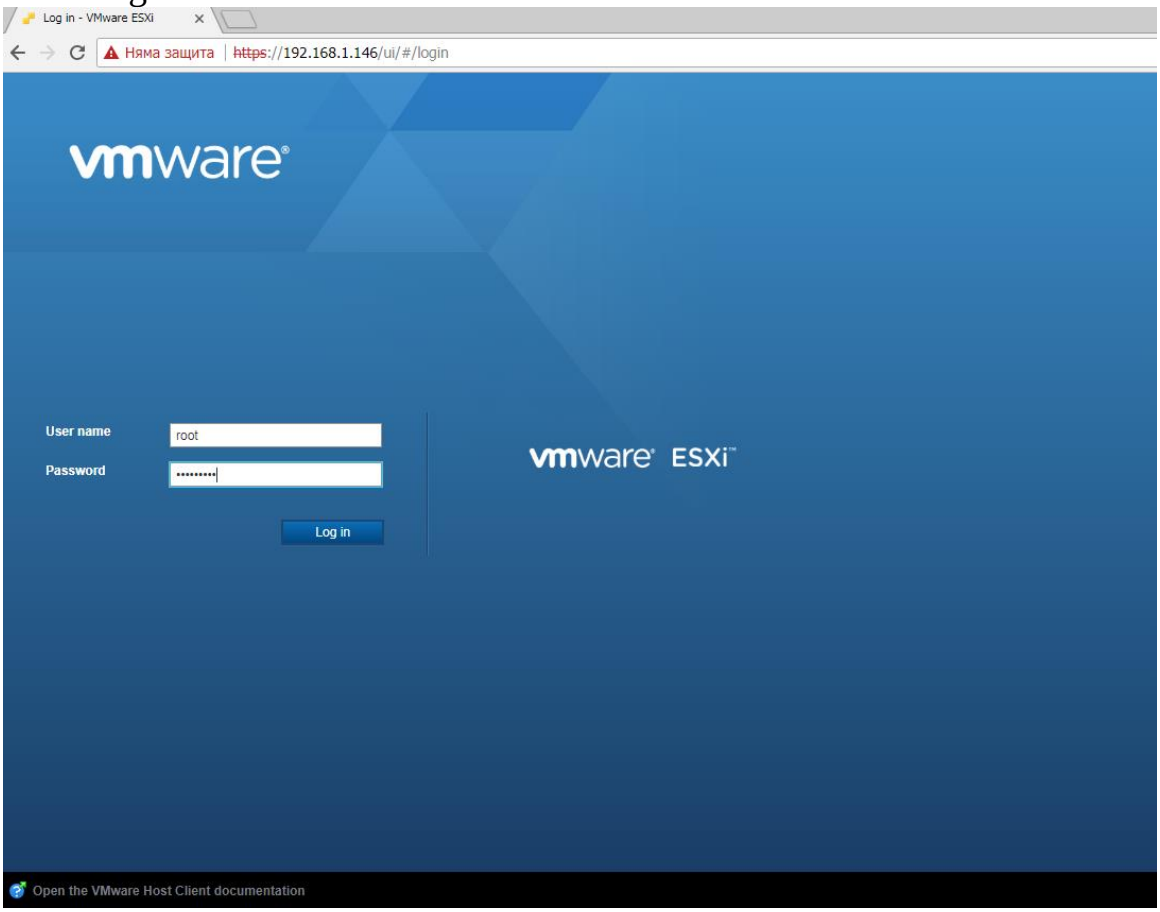

Fig. 4. The web access address for VMware ESXi 6.5.0

On fig. 5 the common characteristics of the operating system Microsoft Windows 10 (64-bit) is shown.

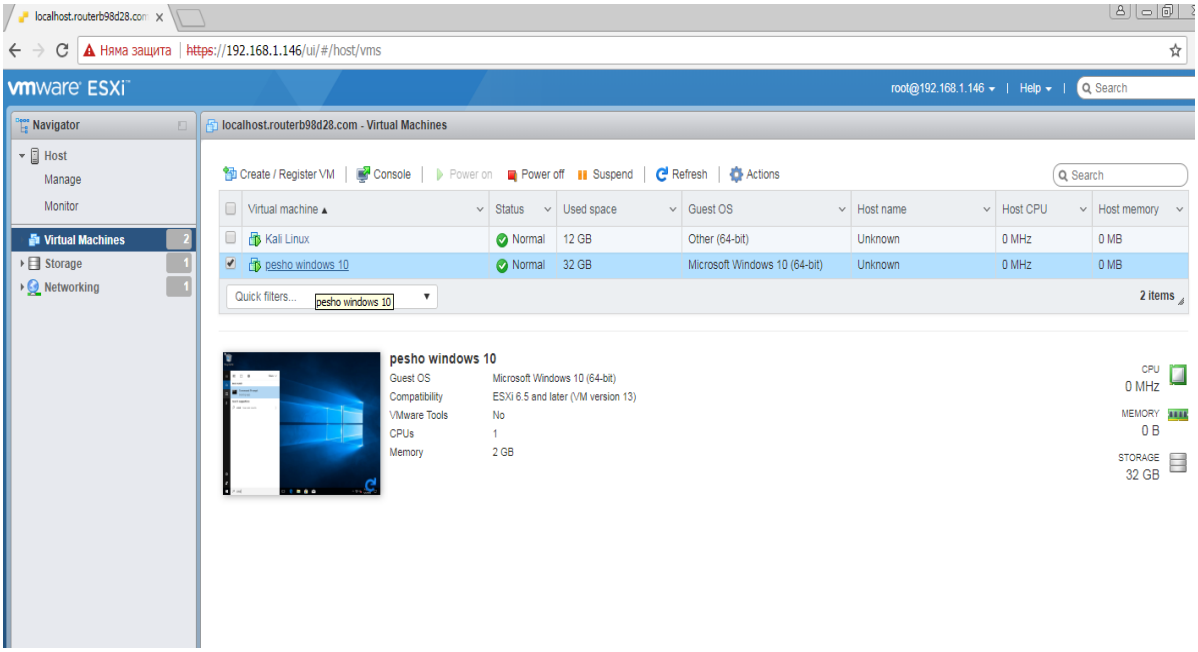

Fig. 5. Characteristics of the operating system Microsoft Windows 10 (64-bit)

On fig. 6 the virtualization of the operating system Microsoft Windows 10 (64-bit) is shown.

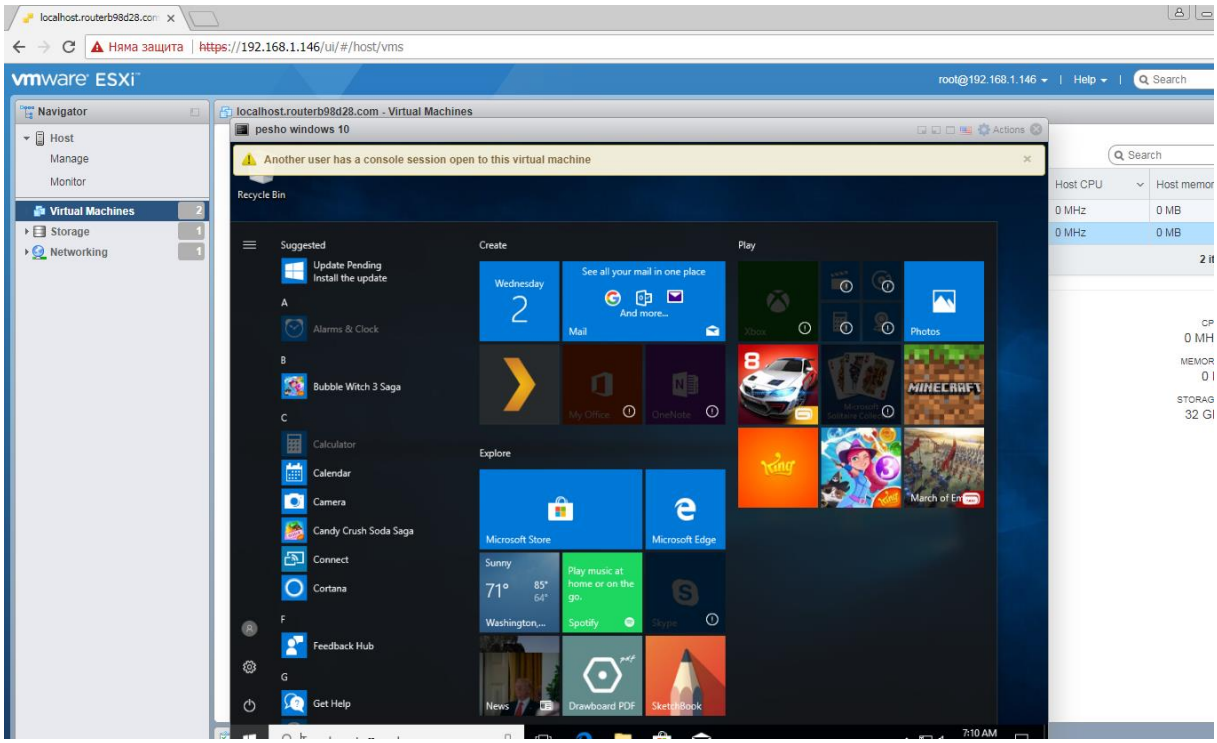

Fig. 6. Virtualization of the operating system Microsoft Windows 10 (64-bit)

On fig. 7 the technical information about the virtualization of the operating system Microsoft Windows 10 (64-bit) is illustrated.

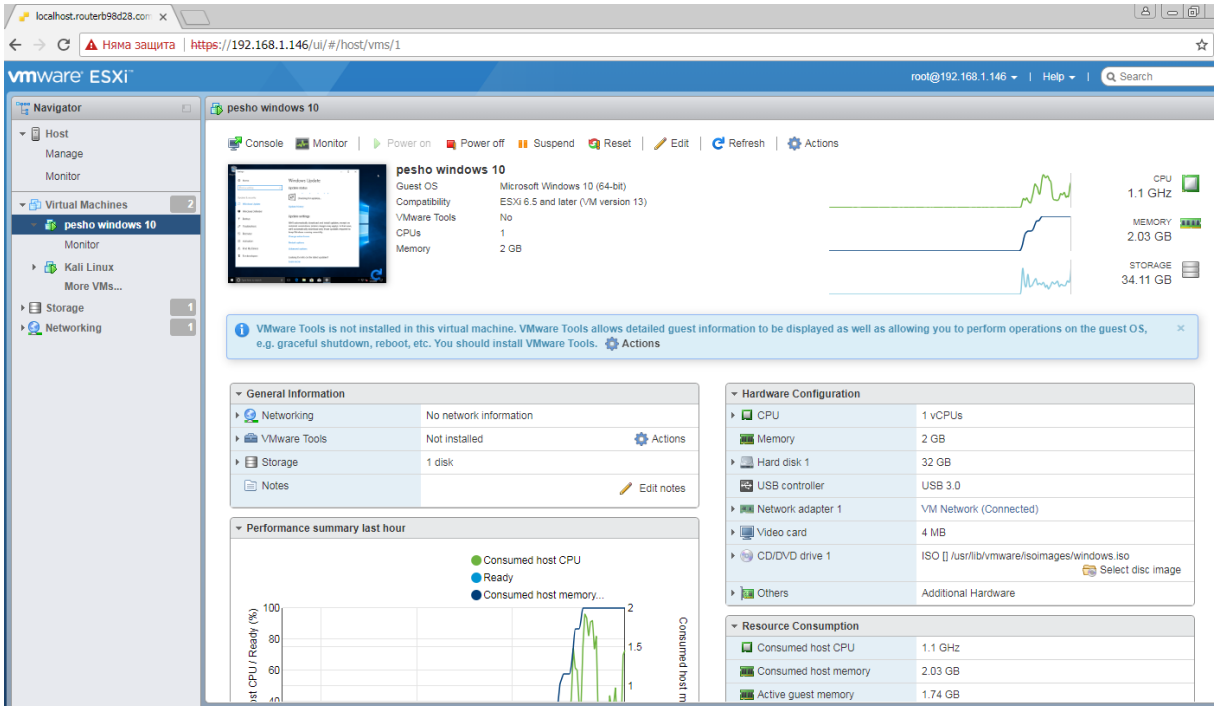

Fig. 7. Technical information about the virtualization of the operating system Microsoft Windows 10 (64-bit)

On fig. 8 the connection to the operating system Windows 10 via VMware Workstation is shown.

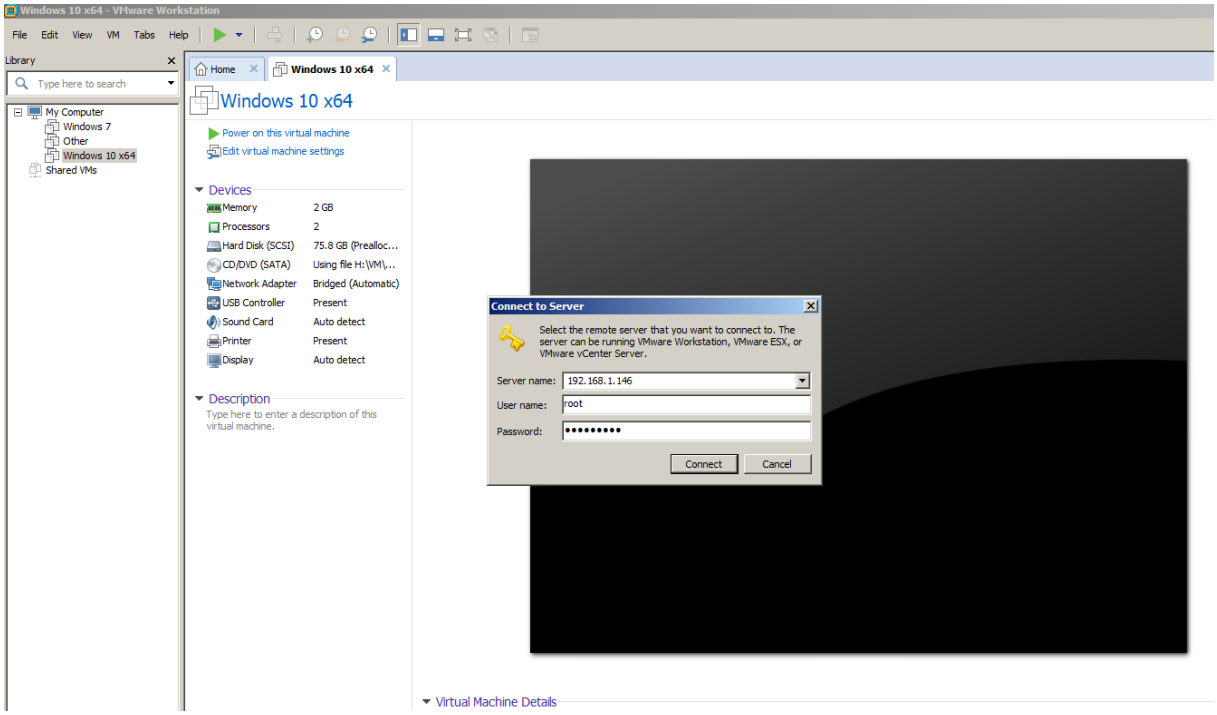

Fig. 8. Connection to the operating system Windows 10 via VMware Workstation

On fig. 9 the performance monitor for operating system Windows 10 is shown.

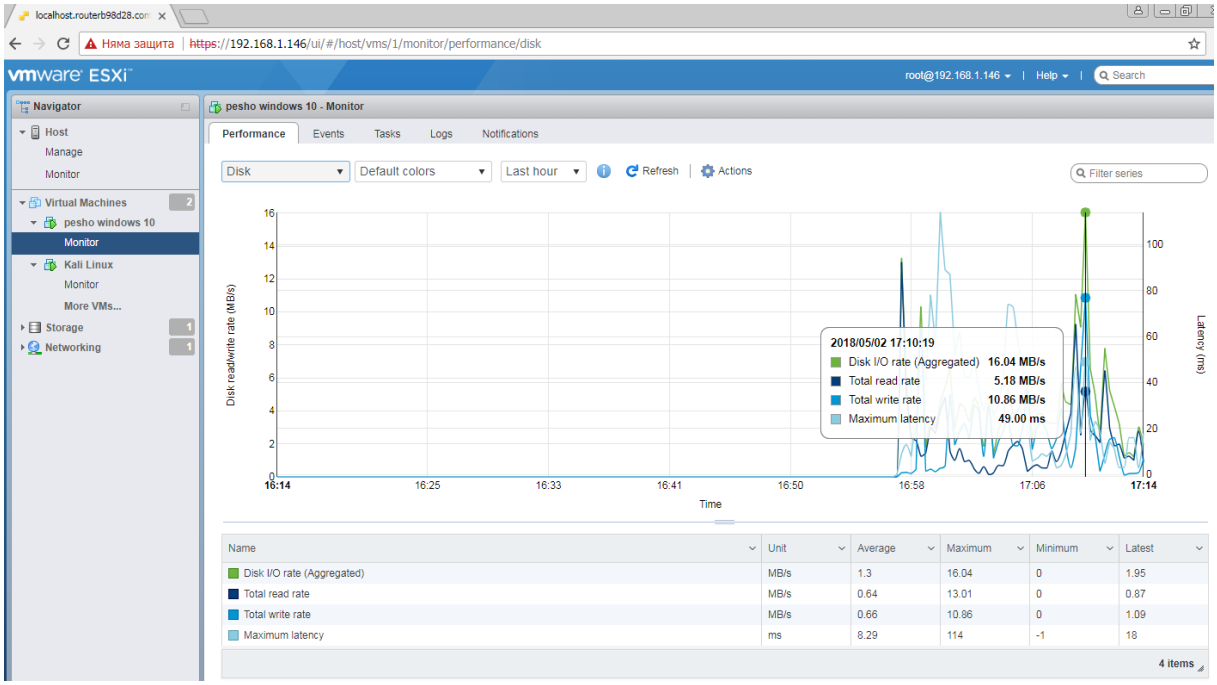

Fig. 9. Performance monitor for operating system Windows 10

On fig. 10 the VMware ESXi 6.5.0 (VMKernel release build 5969303) information is shown.

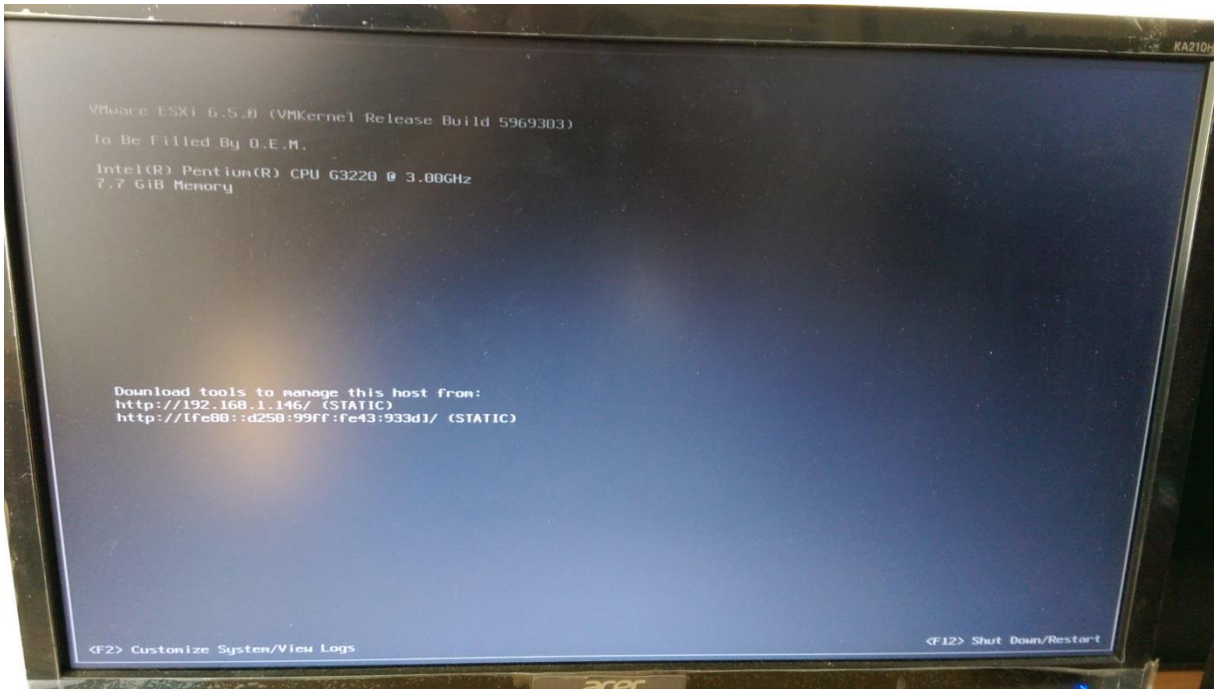

Fig. 10. VMware ESXi 6.5.0 (VMKernel release build 5969303)

ATTENTION: The scientific experiments and research works in this paper are made in a specialized computer laboratories at the Faculty of Technical Sciences of the Konstantin Preslavsky University of Shumen. Everything illustrated and explained in this paper is for research work and educational purposes and the authors are not responsible in cases of abuse.

3. Conclusion

The actual virtualization of the operating system Microsoft Windows 10 (64-bit) via VMware vSphere Hypervisor ESXi 6.5. is made in order to develop logical and correct thinking in the students when they have to virtualize different operating systems for a specific research purposes. The exceptionally well-equipped laboratories at the Faculty of Technical Sciences at the Konstantin Preslavsky University of Shumen give great opportunities to students majoring in "Communication and Information Systems" and "Computer Technologies for Production Automation" to gain extensive theoretical and practical experience in real virtualization with different operating systems.

References:

[1] A. Menon, J. R. Santos, Y. Turner, G. J. Janakiraman, and W. Zwaenepoel. Diagnosing performance overheads in the Xen virtual machine environment. In Proceedings of the 1st ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments, VEE'05, pages 13--23, Chicago, IL, USA, 2005.

[2] A. Burtsev, K. Srinivasan, P. Radhakrishnan, L. N. Bairavasundaram, K. Voruganti, and G. R. Goodson. Fido: fast inter-virtual-machine communication for enterprise appliances. In Proceedings of the 2009 USENIX Annual Technical Conference, ATC'09, pages 313--326, San Diego, CA, USA, 2009.

[3] C. A. Waldspurger, Memory resource management in vmware esx server, SIGOPS Oper. Syst. Rev. 36 (SI) (2002) 181–194. doi:http://doi.acm.org/10.1145/844128.844146.

[4] F. Bellard, QEMU, a fast and portable dynamic translator, in: USENIX Annual Technical Conference, FREENIX Track, USENIX, 2005, pp. 41–46.

[5] G. Heiser, V. Uhlig, and J. LeVasseur. Are virtual-machine monitors microkernels done right? SIGOPS Operating Systems Review, 40(1):95--99, Jan. 2006.

[6] H. Raj and K. Schwan. High performance and scalable I/O virtualization via self-virtualized devices. In Proceedings of the 16th International

Symposium on High Performance Distributed Computing, HPDC'07, pages 179--188, Monterey, CA, USA, 2007.

[7] J. LeVasseur, V. Uhlig, J. Stoess, and S. Götz. Unmodified device driver reuse and improved system dependability via virtual machines. In Proceedings of the 6th USENIX Symposium on Operating Systems Design & Implementation, OSDI'04, pages 17--30, San Francisco, CA, USA, 2004.

[8] J. R. Santos, Y. Turner, G. Janakiraman, and I. Pratt. Bridging the gap between software and hardware techniques for I/O virtualization. In Proceedings of the 2008 USENIX Annual Technical Conference, ATC'08, pages 29--42, Boston, Massachusetts, 2008.

[9] J. E. Smith, R. Nair, The architecture of virtual machines, Computer 38 (5) (2005) 32–38. doi:http://doi.ieeecomputersociety.org/10.1109/MC.2005.173.

[10] Linko G. Nikolov, Wireless network vulnerabilities estimation, International Scientific Journal "Security & Future", Vol. 2 (2018), Issue 2, pg(s) 80-82; WEB ISSN 2535-082X; PRINT ISSN 2535-0668.

[11] P. Barham, B. Dragovic, K. Fraser, and et al. Xen and the art of virtualization. In Proceedings of the 19th ACM Symposium on Operating Systems Principles, SOSP'03, pages 164--177, Bolton Landing, NY, USA, 2003.

[12] R. Nikolaev and G. Back. Perfctr-Xen: a framework for performance counter virtualization. In Proceedings of the 7th ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments, VEE'11, pages 15--26, Newport Beach, CA, USA, 2011.

[13] R. P. Goldberg, Architecture of virtual machines, in: Proceedings of the workshop on virtual computer systems, ACM Press, New York, NY, USA, 1973, pp. 74-112. doi:http://doi.acm.org/10.1145/800122.803950.

[14] S. Hand, A. Warfield, K. Fraser, E. Kotsovinos, and D. Magenheimer. Are virtual machine monitors microkernels done right? In Proceedings of the 10th Workshop on Hot Topics in Operating Systems, HOTOS'05, Santa Fe, NM, 2005. Google Scholar.

[15] VMWare, Performance Tuning Best Practices for ESX Server 3. Guide., http://www.vmware.com/pdf/vi_performance_tuning.pdf (2007).

[16] VMWare, ESX Performance Tips and Tricks. Whitepaper. Latest Revision: Feb 7, 2005, http://www.vmware.com/pdf/esx_performance_tips_tricks.pdf (2005).