"Kyiv Vocational College of Communications"

Cycle Commission of Computer Engineering

**REPORT ON THE IMPLEMENTATION OF**

**LABORATORY WORK №1**

in the discipline: "Operating systems"

Topic: "Introduction to the working environment

virtual machines and operating systems

of different families"

Performed by student

of the group BICS-13

Los Zlata Volodymyrivna

Checked by the teacher

Sushanova V.S.

Work by Zlata Volodymyrivna Los, a student of BICS-13 group

Kyiv 2022

**Objectives:**

1. Familiarity with hypervisors of various types, virtualisation when working with operating systems.

2. Acquaintance with the main types of modern operating systems, a brief overview of their capabilities.

**Material support of the classes**

1. IBM PC type computer.

2. OS of the Windows family (Windows 7).

3. Virtual machine - Virtual Box (Oracle).

4. GNU/Linux operating system - CentOS.

5. Cisco Network Academy website netacad.com and its online Linux courses.

**Tasks for preliminary preparation.**

1. Read the brief theoretical information for the lab and make a small glossary of basic English terms on the classification of virtual environments.

|  |  |
| --- | --- |
| Operating System | An operating system is a basic set of programs that manages the hardware of a computer or virtual machine; provides control over the computing process and organises interaction with the user. |
| Shared hosting | Shared hosting is a type of hosting where many websites are located on one web server. |
| Hypervisor | Hypervisor or Virtual Machine Monitor - a computer program or processor hardware that provides simultaneous and parallel execution of several virtual machines, each running its own operating system, on one physical computer |
| Guest operating system | A guest OS is an operating system installed on a virtual machine rather than on a physical ("host") machine. |
| JVM (Java Virtual Machine) | Java Virtual Machine - a virtual machine for executing Java bytecode. |
| Linux | Linux is a common name for Unix-like operating systems based on the kernel of the same name. |

2. After reading the brief theoretical information, answer the following questions:

2.1. Describe the concept of "hypervisor". What are their types?

A **hypervisor** is software that allows you to separate physical hardware from programs running in the computer's operating system.

It is customary to divide hypervisors into two types - "Type 1" and "Type 2". Despite this, there is a third type (hybrid) that combines the properties of both types.

The first type of hypervisor is characterised by a compact and specific operating system. It is installed directly on a real server or hard drive. Therefore, it has similar features to an OS:

* "Bottom view" - when the available set of resources is managed: memory, processor time, programs that want to use computer resources.
* "Top view". It uses an abstract amount of resources intended for the correct functioning of applications.

The second type of hypervisor has another name - host-based. This technology is installed as a "second layer" on top of the installed operating system. In fact, this type is an application of the main OS that is being executed. Linux is often chosen for stable operation. All physical resources and emulation are managed from the host operating system. The second type of hypervisor has fewer powers. They include KVM, Oracle VM VirtualBox, and others.

2.2. List the main components and capabilities of hypervisors according to your variant (serial number in the log), Table 1. (Variant-12, VMware)

VMware Workstation Pro is a hypervisor for Windows and Linux. It has advanced features and is fully integrated with vSphere. This allows you to move applications between desktop and cloud environments. For MacOS users, VMware has developed Fusion, which is similar to their Workstation product. It comes with slightly fewer features, but it is also priced lower.

VMWare ESXi and vSphere virtualisation software are available free of charge, but with limited features. Advanced features and support are available at paid levels.

VMware offers security support for HIPAA, CJIS, and PCI DSS 3.2 through its Compliance and Cyber Risk Solutions (CCRS) tools. They provide the infrastructure and guidance to ensure virtual workloads are secure and compliant with regulatory standards. Because they are supported by the VMware Enterprise environment, these tools may be preferred by businesses that need assurance of security compliance.

VMware runs directly on the ESXi architecture.

**Procedure.**

**1. Watch the introductory videos and demos.**

**2. After watching the videos, answer the following questions.**

**2.1. List the steps to deploy an operating system based on a VirtualBox virtual machine.**

1) Open the program and click the "Create" button.

2) Select the size of the virtual hard drive.

3) After that, a new virtual machine appears in the list.

4) Methods of starting a virtual machine:

- normal start;

- run in the background;

- run in the background with an interface.5)Двічі клікаємо на новоствореній віртуальній машині, після чого відкривається вікно вибору завантажувального образу системи.

6) If everything is done correctly, the installation screen appears in the virtual machine window. Select "Install Ubuntu".

7) Follow all the steps of the installer and wait for the process to complete.

8) It's done.

**2.2. Are there any hardware limitations when installing 32-bit and 64-bit OSes?**

Yes, here are some of them:

- 32-bit OSes can run on 32-bit and 64-bit processors;

64-bit OSes require a 64-bit processor

- 32-bit OSes can typically use up to 4 gigabytes of RAM;

64-bit OSes can manage a large amount of memory, usually more than 4 gigabytes (e.g. 8, 16, or even more than a terabyte).

- 32-bit OSes can only use 32-bit drivers and applications;

64-bit OSes can use both 32- and 64-bit drivers and applications.

- 64-bit addressing can lead to an increase in the amount of memory used by programs due to the larger size of pointers.

- The Basic Input/Output System (BIOS) or Unified Extensible Firmware Interface (UEFI) can also affect the ability to install 64-bit operating systems.

**2.3 What are the main steps in installing CentOS in text mode?**

1) Boot from the installation media:

- Start your computer and insert the media containing the CentOS installation image (usually a DVD or USB stick).

2) Select the installation type:

- You will be prompted to select an installation type. In text mode, select "Install CentOS" and press Enter.

3) Language and regional settings:

- Select the language and regional settings for your system.

4) Select local storage:

- Determine the location where CentOS will be installed. Select the hard drive or partition to install it on.

5) Network settings:

- Configure the network settings. This may include entering the IP address, subnet mask, gateway, and DNS servers.

6) Enter the host name and set the time:

- Enter the hostname for your server and select the time zone.

7) Setting the password for the root user:

- Enter a strong password for the "root" user (system administrator).

8) Select components to install:

- Select the groups of packages and components you want to install on your server.

9) Wait for the installation to complete:

- After selecting all the settings, confirm that you want to start the installation. Wait for the installation process to complete.

**2.4. How can I install the Gnome and KDE desktop environments on CentOS if it is already installed in text mode (specify the necessary commands and packages)?**

If you have installed CentOS in text mode and now want to add a graphical user interface such as Gnome or KDE, there are some steps you need to follow. Here's how to do it with commands and packages:

**Installing Gnome:**

1) Perform a package update: sudo yum update

2) Install the graphical package for Gnome: sudo yum groupinstall "Server with GUI"

3) Determine whether the system should use the graphical interface at boot: sudo systemctl set-default graphical.target

4) Reboot the system: sudo reboot

5) After the reboot, Gnome should start automatically.

**Installing KDE:**

1) Perform a package update: sudo yum update

2) Install the graphical package for KDE: sudo yum groupinstall "KDE Plasma Workspaces"

3) Determine whether the system should use the graphical user interface at boot: sudo systemctl set-default graphical.target

4) Reboot the system: sudo reboot

5) After the reboot, KDE should start automatically.

**2.5. Give a brief description of the graphical interfaces used in different Linux distributions according to your variant (serial number in the log), Table 2... (Variant-12, Xfce and Fvwm).**

**Xfce** is a lightweight desktop environment for Unix-like operating systems. The goal is to be fast and resource-efficient, while being attractive and easy to use.

Xfce embodies the traditional UNIX philosophy of modularity and reusability. Xfce consists of a number of interconnected components that can be used in other projects if desired. These components include:

- window manager;

- application launcher;

- Display manager;

- user session management and power management manager;

- file manager - Thunar;

- web browser - Midori

- a system for configuring environment settings. They are packaged separately and you can choose from existing packages to create your own working environment.

Another priority of Xfce is to comply with standards, especially those defined by freedesktop.org.

Xfce can be installed on almost all UNIX platforms: Linux, NetBSD, FreeBSD, Solaris, Cygwin, MacOS X, x86, PowerPC, Sparc, and Alpha.

**FVWM** - F Virtual Window Manager (F is currently not officially used) is a virtual window manager for the X Window System. Originally a derivative of twm, FVWM has evolved into a powerful and customisable environment for Unix-like systems.

FVWM provides a convenient view of the user's desktop and contains additional functional modules.

Fvwm is compatible with ICCCM and has extensive customisation options. Starting with the default configuration, Fvwm can be configured using both internal tools and third-party software to customise most aspects of the desktop.

**Checklist questions**

**1. Compare hypervisors of type 1 and type 2, what is the difference between them and their scope of application?**

**Hypervisor: type 1**

A native hypervisor is a layer of software that we install directly on top of the physical server and its underlying hardware. There is no software or operating system in between, hence the name native. A Type 1 hypervisor is proven to provide superior performance and stability because it does not run on Windows or any other operating system.

Type 1 hypervisors are a very simple OS in themselves, on top of which you can run virtual machines. The physical machine that runs the hypervisor is for virtualisation purposes only. You can't use it for anything else. Type 1 hypervisors are mostly used in enterprise environments.

Hypervisor: type 2

A hosted hypervisor runs inside the operating system of a physical host computer. Unlike type 1 hypervisors, which run directly on the hardware, hosted hypervisors have a single software layer.

Type 2 hypervisors are typically used in environments with a small number of servers.

**2. Explain the concept of "GNU GPL", what is its main concept?**

GNU GPL (GNU General Public Licence) is a licence agreement developed by the Free Software Foundation (FSF). It is one of the most popular licences for free software, which defines the conditions under which software can be used, copied, modified and distributed.

The basic concept of the GNU GPL stems from the ideology of free software, which recognises that users have the right to freely use, modify and distribute software.

**3. What is the essence of open source software?**

Open source software refers to software that is released and distributed with the source code open for modification by others. The copyright owner releases the source code under a licence that grants the right to study, use, distribute or modify the software.

**4. What is a distribution kit?**

A distribution is a form of software distribution.

**5. What system administration tasks can be implemented on the basis of Linux?**

Management of users and access rights:

- Create, delete, and manage users and groups.

- Setting up access rights to files and directories.

Resource monitoring and analysis:

- Track CPU, RAM, network, and other resource usage.

- Examine event logs to identify problems and analyse failures.

Package and update management:

- Install, uninstall, and update software using package managers (e.g., APT, YUM).

- Manage system updates and security patches.

Network settings:

- Configure IP addresses, subnet masks, gateways, and DNS servers.

- Manage network interfaces and network security settings.

Automate tasks:

- Create and manage automated tasks using cron, systemd, and other automation tools.

- Deploy maintenance scripts and scripts for routine tasks.

Ensure security:

- Setting up firewalls and restricting network access.

- Implementation of security policies and vulnerability monitoring.

Manage logs and logs:

- Monitor and analyse system logs to identify errors and issues.

- Configuration and rotation of logs to ensure efficient use of disk space.

Recovery and backup:

- Develop and implement backup plans.

- Restore the system in case of failure or data loss.

Problem resolution and technical support:

- Troubleshooting and resolving system issues.

- Provide technical support to users and developers.

**6. What is the relationship between Android and Linux?**

Android and Linux are interconnected through the use of the Linux kernel as part of the Android operating system. Here are some key aspects of this interaction:

1) Android uses the Linux kernel as the core part of its operating system. The kernel is responsible for interfacing hardware with software, managing resources, and performing basic operations.

2) The Linux kernel is open source, and this provides Android with openness and flexibility in development. Developers can modify the kernel to suit the needs of Android.

3) Android uses many tools and libraries from the Linux world, such as the GNU C Library (glibc), the kernel build system, and others.

4) Although Android uses the Linux kernel, Android itself is a separate operating system designed primarily for mobile devices. It includes specific components such as the Android Runtime (ART), application framework and user interface.

**7. What are the main features and applications of Embedded Linux?**

The wealth of open source code in Linux allows embedded system developers to easily adapt and modify the code to suit their needs.

Embedded Linux supports a variety of processor architectures, allowing it to be used in a wide range of embedded devices, from microcontrollers to high-performance processors.

Embedded Linux can be easily extended with modules and packages, making it suitable for a large number of different embedded applications.

Embedded Linux is widely used in the Internet of Things (IoT) industry, where embedded devices need to be able to connect, process and transmit data to a network.

Embedded Linux enjoys an active developer community, which contributes to the stability, security and support of the system.

Embedded Linux is used in a variety of embedded systems such as mobile phones, tablets, smart TVs, networking equipment, medical equipment, automotive systems, and many other devices.

**8. How can you change the Linux boot type: in text mode (level 3) or graphical mode (level 5)? What is the difference between CLI and GUI modes?**