

Introduction to System Administration and Maintenance

CTSYSADL – SYSTEMS ADMINISTRATION AND MAINTENANCE

LESSON 1 – WEEK 2

TERM 1, AY 2025-2026



INTRODUCTION TO SYSTEM ADMINISTRATION AND MAINTENANCE

- Principles of System Administration
- Windows Administration Tools
- Virtual Laboratory Environment



TOPIC OUTCOMES

At the end of the lesson students must be able to:

- Identify the role and responsibilities of a system administrator.
- Identify the challenges of system administrator.
- Identify the different Windows Administration tools.
- Setup and configure a virtualized laboratory environment using Oracle VirtualBox.



What is System Administration and Maintenance?

- System administration and maintenance refer to the management and upkeep of computer systems and networks, including hardware, software, and data storage systems. This includes tasks such as installing and configuring software, monitoring system performance, and ensuring the security of data and networks.
- In today's digital world, the importance of system administration and maintenance cannot be overstated. As organizations rely increasingly on technology to conduct business and store sensitive information, it is critical that these systems are secure, reliable, and always available.

What is System Administration and Maintenance?

- Effective system administration and maintenance help ensure that systems run smoothly and efficiently, prevent data loss or theft, and minimize downtime.
- System administration and maintenance are responsible for a range of tasks, including installing, configuring, and maintaining computer systems, networks, and software. They also monitor performance and troubleshoot any technical issues that may arise.
- In addition, they play a key role in ensuring the security of sensitive information and preventing cyberattacks by regularly updating software and implementing security measures.



WHAT DOES A SYSTEM ADMINISTRATOR DO?



System Administrator

- Also referred to as SysAdmin or SysOps, this is an IT professional responsible for setting up, maintaining, and troubleshooting an organization's servers, networks, and systems.
- Sysadmins are responsible for ensuring the uptime of their companies' computers, servers, and internet, essentially "keeping the lights on" to minimize work disruptions. This includes system maintenance and configuration, such as installing and troubleshooting hardware and software, as well as assessing new technologies for their clients' companies.



System Administrator

- For smaller IT departments typically assign a broader scope of responsibilities to the system administrator position. In some organizations, a sysadmin may need to support a wide range of systems, including end-user desktop computer systems, the organization's local area network, wireless LAN, voice over Internet Protocol phone system, and hybrid cloud storage.

What does a System Administrator do?

- **Monitoring system performance, logs, backups, and security updates** - overseeing system health, logs, patches, and backup integrity tasks.
- **Installing/configuring hardware, OS, software** - setting up new equipment, operating systems, applications.
- **Managing user accounts and permissions** - creating, modifying, and removing user access rights and roles
- **Provides technical support and troubleshooting** - resolving user issues, and assisting staff with system problems.



What does a System Administrator do?

- **Creating and managing system permissions and user accounts** - resolving user issues, assisting staff with system problems.
- **Performing regular security tests and security monitoring** - conducting audits, patching vulnerabilities, and enforcing policies.
- **Maintaining networks and network file systems** - managing LAN/WAN components and shared resources

Common Challenges of a System Administrator

- **Ensuring uptime and high availability** - keeping critical systems functional without interruption.
- **Keeping ahead of security threats** - responding proactively to vulnerabilities and attacks.
- **Managing budget constraints and the patching cycles** - applying updates and infrastructure changes within limited resources and scheduling windows.



Windows Administration Tools

- Windows Admin tools help manage servers, performance, automation, and monitoring.
- Core Tools and Functionality:
 - Windows Admin Center
 - Remote Server Administration Tools (RSAT)
 - Event Viewer, Services, Disk Management, PowerShell

Core Tools and Functionality of Windows Administration Tools

- Windows Admin Center
 - Includes browser GUI for servers, VMs, and clusters
- Remote Server Administration Tools (RSAT)
 - Includes Server Manager, MMC snap-ins for remote administration
- Event Viewer, Services, Disk Management, PowerShell (script automation)
 - Logs analysis and incident tracking
 - Control Windows services and drive partitions
 - Scriptable environment for automation, user accounts, backups, and admin tasks

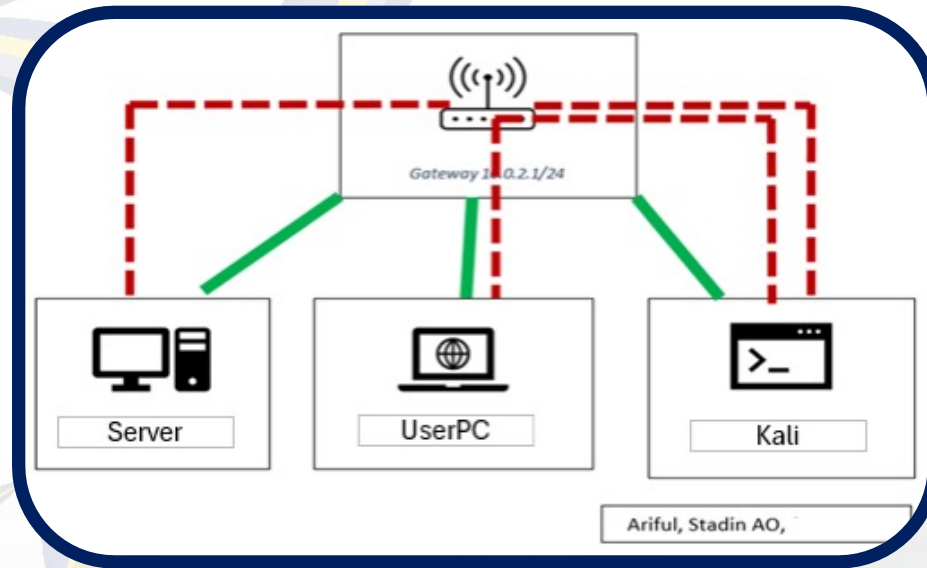
Virtual Laboratory Environment

What is VirtualBox?

- It is a virtualization tool that allows you to run multiple guest operating systems on a single host. The VirtualBox Extension Pack enhances functionality by adding support for USB 2.0/3.0 devices, RDP, disk encryption, and more.
- Oracle VirtualBox is a free, cross-platform x86 virtualization tool for running multiple guest OSes on a host.

Step-by-Step Setup

1. Install VirtualBox
2. Configure networks
3. Create VMs
4. Networking
5. Install tools
6. Snapshots and backups



Step-by-Step Guide in Creating a Virtual Lab Using VirtualBox

1. Install VirtualBox + Extension Pack for USB/RDP/shared folders

- To get started, download and install VirtualBox from the official website: <https://www.virtualbox.org>
- Next, download the VirtualBox Extension Pack, which adds additional features like USB support and RDP (Remote Desktop Protocol). Follow these steps:
 - Go to **File > Preferences** in VirtualBox.
 - Navigate to the **Extensions** tab and click the “+” button to add the extension pack.

2. Configure networks: NAT for the internet, Host-only for isolation

- In order to allow communication between your virtual machines, you need to create a virtual network:
 - Go to **File > Preferences**, then select the **Network** tab.
 - Under **Host-only Networks**, click the **Add** button to create a new virtual network.
 - Configure the network using **CIDR (Classless Inter-Domain Routing)**, which improves routing efficiency. For example, you can use a network like 192.168.56.0/24.
- This network will act as a virtual switch, enabling the virtual machines to communicate as if connected to a physical network.

Step-by-Step Guide in Creating a Virtual Lab Using VirtualBox

3. Create VMs: allocate resources, attach ISO images

Here's how to set up the first virtual machine, using Windows 10

- **Step 1: Create a New Virtual Machine**
 - Click the **New** button in VirtualBox.
 - Enter the **name** of your VM (e.g., “Windows 10”).
 - Select the **type** of OS (Microsoft Windows) and the **version** (Windows 10 64-bit).
- **Step 2: Configure Machine Settings**
 - Set the desired amount of **RAM** (at least 2 GB for Windows 10).
 - Allocate **CPU cores** according to your system's capacity.
- **Step 3: Attach a Bootable Disk**
 - In the **Storage** settings, click **Add** to attach an **ISO** file of the OS.
 - Select the **Windows 10 ISO** file that you've downloaded.
- **Step 4: Install the Operating System**
 - Start the virtual machine and follow the on-screen instructions to install Windows 10.
 - Repeat these steps to install other operating systems such as **Ubuntu, Kali Linux, and Windows Server 2016**, using their respective ISO files.

Step-by-Step Guide in Creating a Virtual Lab Using VirtualBox

4. Networking: assign static IPs, ensure host–guest and VM–VM connectivity

Once the operating systems are set up, install the necessary applications on each VM:

- **Windows 10 (VirtualBox)**

- Download and install **Chrome** for web browsing.
- Install **Wireshark** for network monitoring.
- Install **FileZilla** client for FTP file transfers.

- **Ubuntu (VirtualBox)**

- Install **Apache2** web server: `bashCopy codesudo apt update sudo apt install apache2`
- Install **WordPress** for web development: `bashCopy codesudo apt install wordpress`

- **Kali Linux (VirtualBox)**

- Use the built-in **Nmap** for network scanning.
- Install **Bettercap** for advanced network attacks: `bashCopy codesudo apt-get install bettercap`
- Retrieve **Seth's tool** from GitHub: `bashCopy codegit clone https://github.com/Seth-tool-repository.git`

- **Windows Server 2016 (VirtualBox)**

- Set up **FTP Server/FileZilla Server** for file sharing.
- Enable **RDP** for remote access.
- Install and configure **ADDS (Active Directory Domain Services)** and **DHCP**.

Step-by-Step Guide in Creating a Virtual Lab Using VirtualBox

5. Install tools: Guest Additions, RDP/SSH, AD, DHCP, NAT

- To allow communication between virtual machines:
 - Go to each VM's settings in VirtualBox.
 - Navigate to the **Network** tab and connect each VM to the **Host-only Adapter** you created earlier.
 - Ensure that the **IP address** range is assigned appropriately for each virtual machine.
- Example:
 - Windows 10: 192.168.56.10
 - Ubuntu: 192.168.56.11
 - Kali Linux: 192.168.56.12
 - Windows Server 2016: 192.168.56.13
 - Now, all machines will be connected to the same lab network and can communicate with each other, simulating a real-world network environment.



Step-by-Step Guide in Creating a Virtual Lab Using VirtualBox

6. Snapshots & backups: restore VM states for lab resets

- With your lab environment set up, you can now:
 - Test networking and communication between different operating systems.
 - Simulate attacks and defenses using tools like Nmap and Wireshark.
 - Practice setting up web servers, FTP servers, and more.
- This lab environment provides a safe way to experiment with networking, security tools, and server configurations without affecting your main system.