UNIVERSITY OF Baguio

SCHOOL OF INFORMATION TECHNOLOGY

NAME: Sueno, Johnray K.	
SECTION: IDC2	COURSE AND YEAR: BSIT-3rd

(SYSADM1) PORTFOLIO

Table of Contents

Quizzes			
Assignment 1	Oct 08, 2024	31/40	12
Seatwork 1	Oct 10, 2024	33/40	13
Other Activities			
Laboratory Activity 1	Sept 26, 2024	/50	14-15
Laboratory Activity 2	Oct 10, 2024	/50	16
Laboratory Activity 3	Oct 17, 2024	/50	17-18
Midterm Exam: Lecture	Nov 07, 2024	40/60	19
Midterm Exam: Laboratory	Nov 07, 2024	48/80	19-20
Finals			
Quizzes			
Assignment 1	Nov 28, 2024	/50	21
Assignment 2	Dec 05, 2024	/50	22
Seatwork 1	Nov 05, 2024	/60	23-24
Quiz 1	Nov 21, 2024		24-25
Other Activities			
Laboratory Activity 1	Nov 14, 2024	/50	25-27
Laboratory Activity 2	Nov 21, 2024		28
Final Exam			
Course Reflection			29-30

First Grading Lecture:

Quiz 1:

Sueno, Johnray K. JDC2 17/20 8/20/24

How could a company ensure the availability of critical data in case of service disruptions?

A company should have backup that can work even in offline situations. And they should practice or have data recovery plans such as to be able to maintain and recovery data while to be able to reduce data loss. Another option is to ensure that data are distributed

Assignment 1:

UNIVERSITY OF Baguio
SCHOOL OF INFORMATION AND TECHNOLOGY

NAME: Sueno, Johnray K.	DATE PERFORMED: August 15, 2024	44/50
Section: IDC2	DATE SUBMITTED: August 15, 2024	

Evolution of Systems Administration: From Manual to Automated

SYSADM1

Case study

SysPro Corporation, a mid-sized manufacturing company, began operations in the 1980s. As the company grew, so did its reliance on technology. This case study explores the evolution of SysPro Corporation, from manual operations to a highly automated environment.

SysPro Corporation was primarily focused on hardware maintenance and software installation. The system administrators were responsible for tasks such as installing operating systems, configuring applications, and troubleshooting hardware issues. They experience frequent system downtime, slow response times, and limited scalability because of outdated computing equipment. The corporation used basic scripting for repetitive tasks, but most processes were manual. However, after two years, the corporation expanded rapidly, leading to increased IT infrastructure and complexity. The implementation of a company-wide network enabled better communication and data sharing. The basic automation tools progressed to advanced to manage user accounts and software installations. Managing the growing infrastructure, security threats increased thus demanding more user support.

At present, SysPro Corporation migrated a significant portion of its infrastructure to the cloud, reducing hardware and maintenance costs. The company embraced automation and DevOps practices to improve efficiency and reliability of their day to day operations. Configuration management tools were also used to define and manage infrastructure. The stockholders also invested a lot on automated pipelines to implement software development and deployment that later on ensured data security in the cloud, managing cloud costs, and developing new skills for cloud-based operations.

Based on the case study,

1.Describe the role of system administrators at SysPro Corporation in the early years. What were the primary challenges they faced?

- In the early years at SysPro Corporation, system administrators handled tasks like hardware maintenance, software installation, and configuring applications. They were also responsible for troubleshooting issues. Their main challenges included frequent system downtime, slow response times, and limited scalability due to outdated equipment.

2. Discuss the limitations of manual system management as experienced by SysPro Corporation. How did these challenges impact the business?

- Manual system management at SysPro Corporation was limited by inefficiencies such as constant system downtimes, slow responses to issues, and difficulty scaling operations. These limitations negatively impacted the business by reducing productivity and potentially affecting customer satisfaction.

3. Identify the automation tools mentioned in the case study and explain their role in improving efficiency.

- The case study mentions several automation tools, including basic scripting, advanced tools for managing user accounts and software installations, and automated pipelines for development and deployment.**Basic Scripting:** Used for repetitive tasks such as routine maintenance and backups.

  Advanced Automation Tools:Managed user accounts and software installations, helping to streamline processes.

  Configuration Management Tools: Defined and managed infrastructure, improving consistency and deployment efficiency.

  Automated Pipelines: Facilitated software development and deployment, ensuring faster and more reliable releases.

  These tools improved efficiency by automating repetitive tasks, reducing manual errors, and streamlining processes.

4. Analyze the impact of cloud adoption and DevOps practices on SysPro Corporation's IT operations.

- Migrating to the cloud and adopting DevOps practices significantly improved SysPro Corporation's IT operations. It reduced hardware and maintenance costs, enhanced scalability, and made software deployment more efficient. Additionally, it improved data security and cost management in the cloud.

5. Predict potential future trends in system administration and their implications for organizations like SysPro Corporation.

- Future trends might include more AI-driven automation, predictive maintenance using machine learning, and advancements in cloud technologies. These trends could further streamline IT operations, reduce costs, and require IT professionals to develop new skills to keep up with evolving technologies.

Page 2 of 2

Assignment 2:

UNIVERSITY OF Baguio

SCHOOL OF INFORMATION AND TECHNOLOGY

NAME: Sueno, Johnray K.	DATE PERFORMED: 08/29/2024	
Section: IDC2	DATE SUBMITTED: 08/29/2024	

SYSADM1 – Physical Infrastructure

Instructions:

Answer the following questions based on Week 3 Lecture notes.

1. Identify potential issues in physical infrastructure setups and propose solutions to optimize performance or reduce costs

Potential Issues	Solution
Outdated or Old equipment may fail or become inefficient over time.	Regularly update or replace outdated equipment. Implement a maintenance schedule and consider investing in newer, more energy-efficient technology.
Poorly designed physical layouts can lead to bottlenecks or wasted space.	Redesign the layout to optimize space usage. Use simulations or models to plan the most efficient arrangement of resources and equipment.
Managing multiple virtual machines and storage instances can become complex and time-consuming.	Use management tools provided by the cloud provider to streamline operations and automate routine tasks.
Lack of Redundancy, single points of failure can lead to major disruptions.	Introduce redundancy for critical components. For example, have backup power supplies and multiple network connections.
Inadequate Maintenance, neglecting maintenance can lead to unexpected breakdowns.	Establish a regular maintenance routine and use monitoring tools to detect potential issues before they become critical.
Virtual environments can be vulnerable to attacks if not properly secured.	Implement robust security measures, including firewalls, encryption, and regular security audits. Utilize the cloud provider's security features and best practices
FaaS functions are stateless, which can complicate tasks requiring persistent state.	Use external storage solutions like databases or object storage to manage state and maintain data consistency.

2. You are a project manager responsible for implementing a new infrastructure project, such as a smart city initiative or a digital transformation strategy.

A. What IT systems and technologies are necessary to support the project's objectives?

- **IoT Sensors and Devices**
  These devices collect real-time data on city operations, such as traffic, air quality, and waste management. By placing sensors throughout the city, we can monitor conditions and make informed decisions.
- **Connectivity Infrastructure**
  High-speed internet, 5G networks, and Wi-Fi hotspots are crucial for enabling communication between IoT devices and citizens. This connectivity allows for real-time data transmission and access to city services.
- **Data Management Platforms**
  These platforms store, process, and analyze the vast amounts of data collected from IoT devices. They help derive insights that can inform city planning and operations.
- **Artificial Intelligence and Machine Learning**
  AI and ML can analyze data to optimize city services, such as traffic management and energy use. They enable automated decision-making based on real-time information.
- **Citizen Engagement Platforms**
  Mobile apps and web portals facilitate communication between citizens and the city. They allow residents to report issues, access information, and engage in local governance.

B. How can the IT infrastructure be designed to be scalable and flexible?

- **Modular and Distributed Architecture**
  Breaking the infrastructure into smaller components allows for easy scaling. This means that as the city grows, additional resources can be added without overhauling the entire system.
- **Cloud-based Services**
  Using cloud computing provides on-demand resources and reduces the need for expensive on-premises infrastructure. This enables quick adjustments based on city needs.

- **Open Standards and APIs**
  Implementing open standards allows different systems to work together seamlessly. This flexibility supports integration and expansion without vendor lock-in.
- **Automated Network Management**
  Centralized management tools can monitor and optimize the network, improving efficiency and reducing manual oversight.

C. What are the potential security risks and vulnerabilities, and how can they be addressed?

- **Cyberattacks on IoT Devices**

  Potential Risks:

  - Insecure Default Settings: Many IoT devices come with default usernames and passwords that are widely known or easily guessable.
  - Lack of Encryption: If data transmitted by IoT devices is not encrypted, it can be intercepted and accessed by unauthorized parties.
  - Firmware Vulnerabilities: Outdated or unpatched firmware can be exploited by attackers.
  - Insecure Communication Protocols: Weak or outdated communication protocols can be exploited to gain unauthorized access or disrupt services.

  Mitigation Strategies:

  - Change Default Credentials: Always change default usernames and passwords to strong, unique credentials.
  - Implement Encryption: Use strong encryption methods for data both at rest and in transit. Ensure IoT devices support and use secure communication protocols like TLS/SSL.
  - Regular Firmware Updates: Implement a policy for regular updates and patches for device firmware to fix known vulnerabilities.
  - Network Segmentation: Isolate IoT devices on a separate network segment from critical systems to limit the potential impact of a compromise.

- **Data Privacy Concerns**

  Potential Risks:

  - Unauthorized Data Access: Sensitive data may be accessed by unauthorized users or entities due to inadequate access controls.

  - Data Breaches: Inadequate security measures can lead to data breaches, exposing personal or sensitive information.
  - Non-Compliance with Regulations: Failure to adhere to data protection laws such as GDPR or CCPA can result in legal and financial repercussions.

  Mitigation Strategies:

  - Data Encryption: Encrypt sensitive data both in storage and during transmission to protect it from unauthorized access.
  - Access Controls: Implement strict access controls and authentication mechanisms to ensure that only authorized personnel can access sensitive data.
  - Regular Audits and Compliance Checks: Regularly audit data protection practices and ensure compliance with relevant data protection regulations.
  - Data Minimization: Collect and retain only the minimum amount of data necessary for business operations to reduce the risk of exposure.

- **Network Vulnerabilities**

  Potential Risks:

  - Unpatched Systems: Systems and software with known vulnerabilities that are not patched can be exploited by attackers.
  - Open Ports and Unsecured Services: Open ports and services that are not properly secured can be targeted by attackers.
  - Man-in-the-Middle (MitM) Attacks: Attackers can intercept and alter communications between systems if communication channels are not secured.

  Mitigation Strategies:

  - Automated Threat Detection: Deploy automated threat detection systems to monitor network traffic for suspicious activity and potential threats.
  - Regular Security Audits: Conduct regular security audits and vulnerability assessments to identify and address security weaknesses.
  - Patch Management: Implement a robust patch management process to ensure that all systems and software are updated with the latest security patches.
  - Network Segmentation and Firewalls: Use network segmentation and configure firewalls to limit access to critical systems and reduce the attack surface.
  - Secure Communication Channels: Use encryption and secure communication protocols (e.g., VPNs, TLS) to protect data in transit and prevent MitM attacks.

D. How can the IT infrastructure be integrated with existing systems and processes to minimize disruption?

- **Conduct a Thorough Assessment**
  Identify existing systems and processes that need integration and create a detailed plan.
- **Adopt a Phased Approach**
  Implement the new infrastructure in stages to allow for testing and adjustments, reducing the risk of widespread disruption.
- **Utilize Middleware and APIs**
  Middleware can facilitate communication between new and existing systems, enabling smooth data exchange.
- **Provide Training and Support**
  Offer training for city employees on new systems and provide ongoing support to ensure a successful transition.

First Grading Laboratory:

Labwork 1:

UNIVERSITY OF Baguio

SCHOOL OF INFORMATION AND TECHNOLOGY

NAME: Sueno, Johnray K.	DATE PERFORMED: 08/22/24	
Section: IDC2	DATE SUBMITTED: 08/22/24	50/50

SYSADM1 – Introduction to File Systems in Windows and Linux

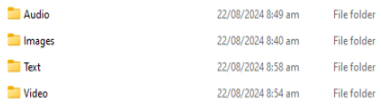
Requirement:

- A virtual machine running Linux and Windows OS

Instructions:

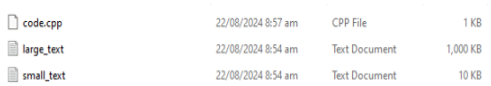
Part A: Windows File System

1. **Open File Explorer:** Click the File Explorer icon on your desktop or press the Windows key + E.
2. **Navigate to your Documents folder:** This is usually the default location for user files.
3. **Create a new folder:** Right-click in an empty space, select "New," then "Folder." Name it "Lab1_Windows."
4. **Create a text file:** Right-click in the "Lab1_Windows" folder, select "New," then "Text Document." Rename it to "info.txt."
5. **Open the text file:** Double-click the "info.txt" file to open it in Notepad.
6. **Type some text:** Write a short paragraph about yourself or the purpose of the file.
7. **Save the file:** Close the Notepad window and save the changes.
8. **Create a subfolder:** Create a new folder inside "Lab1_Windows" called "Data."
9. **Copy the text file:** Copy the "info.txt" file to the "Data" subfolder.
10. **Rename the copied file:** Rename the copied file to "data.txt.
11. Create a folder named "LabFiles" with subfolders for each file type. Use the internet for the resources of the files listed below.



LabFiles

1. **Text**
   1. large_text.txt
   2. small_text.txt
   3. code.cpp



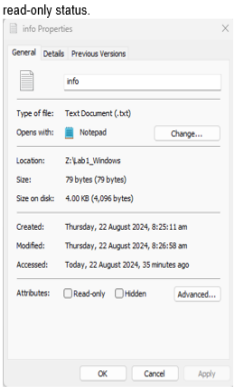
2. **Images**
   1. image1.jpg
   2. image2.png
   3. image3.bmp

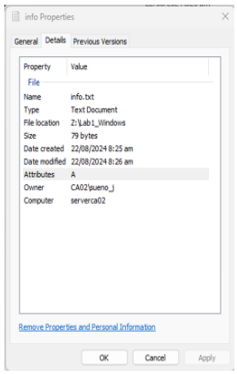
3. **Audio**
   1. song.mp3
   2. speech.wav

4. **Video**
   1. clip.mp4

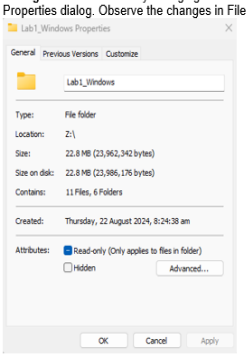
12. **Check file properties:** Right-click on the "info.txt" file and select "Properties." Explore the General, Details, and Security tabs to understand file attributes like creation date, size, and

read-only status.





13. **Change file attributes:** Try changing the file attributes (e.g., read-only, hidden) using the Properties dialog. Observe the changes in File Explorer.



14. **Share the folder:** Right-click on the "Lab1_Windows" folder, select "Properties," and then the "Sharing" tab. Share the folder with a specific user or group, setting appropriate permissions (e.g., Read, Write, Full control)
15. **Create an archive:** Use WinRAR or 7-Zip to create a compressed archive of the "Lab1_Windows" folder.
16. **Extract an archive:** Create a new folder, then extract the created archive into it.

Part B. Create a log report structure

Date And Time	Task	Description	Media Type	Status	Notes
Thursday, 22 August 2024, 8:22:18 am	1	Open File Explorer	-/-	Completed	Accessed via desktop icon or Windows key + E
Thursday, 22 August 2024, 8:23:23 am	2	Navigate to Documents Folder	-/-	Completed	Default user file location
Thursday, 22 August 2024, 8:24:38 am	3	Create Folder "Lab1_Windows"	-/-	Completed	Folder Created
Thursday, 22 August 2024, 8:25:11 am	4	Create Text File name "info.txt" in "Lab1_Windows"	txt	Completed	Text document created
Thursday, 22 August 2024, 8:27:20 am	5	Create subfolder named Data inside Lab1_Windows	-/-	Completed	Subfolder created
Thursday, 22 August 2024, 8:27:33 am	6	Copy "info.txt" to the subfolder Data and rename it to "data.txt"	-/-	Completed	File copied and renamed
Thursday, 22 August 2024, 8:29:15 am	7	Create new Folder named "LabFiles" inside of "Lab1_Windows" with subfolders Audio, Images, Text, and Video	-/-	Completed	Folder and subfolders created
Thursday, 22 August 2024, 8:40:45 am to Thursday, 22 August 2024, 8:58:06 am	8	Download files for "LabFiles" subfolders Audio, Images, Text, and Video	txt, cpp, jpg, png, bmp, mp3, wav, mp4	Completed	Files downloaded from the internet

Thursday, 22 August 2024, 9:05:06 am	9	Check file properties of "info.txt"	-/-	Completed	Explored General, Details, and Security tabs
Thursday, 22 August 2024, 9:06:26 am	10	Change file attributes of "info.txt"	-/-	Completed	Attributes changed (e.g., read-only)
Thursday, 22 August 2024	11	Share the "Lab1_Windows" folder	-/-	Not Completed	Folder shared with specific permissions
Thursday, 22 August 2024, 9:30:19 am	12	Create an archive of "Lab1_Windows"	Archive file	Completed	Archive created using WinRAR or 7-Zip
Thursday, 22 August 2024, 9:32:47 am	13	Extract the created archive into a new folder	-/-	Completed	Archive extracted successfully

Problems Encountered	Description	Task	Date
Cannot Share folder	Folder shared with specific permissions was not completed	11	Thursday, 22 August 2024

Labwork 3:

UNIVERSITY OF Baguio
SCHOOL OF INFORMATION AND TECHNOLOGY

NAME: Sueno, Johnray K.	DATE PERFORMED: 08/29/2024
Section: IDC2	DATE SUBMITTED: 08/292024

SYSADM1 – Managing Services in Windows

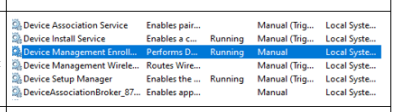
Requirement:

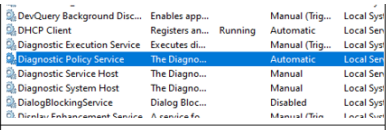
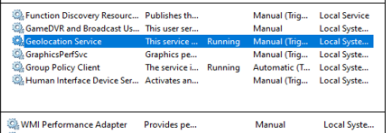
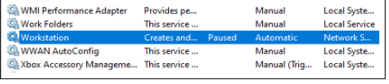
- A virtual machine running Linux and Windows OS

Services are background processes that run independently of user interactions in Windows. They provide essential system functions, such as network connectivity, printing, and time synchronization. This lab will guide you through the process of managing services using the Services app.

Instructions:

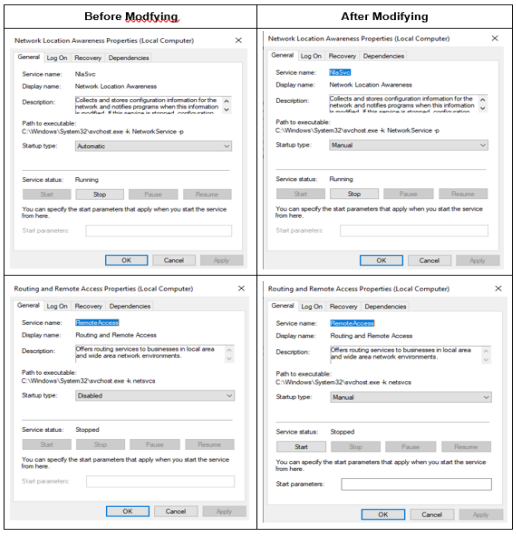
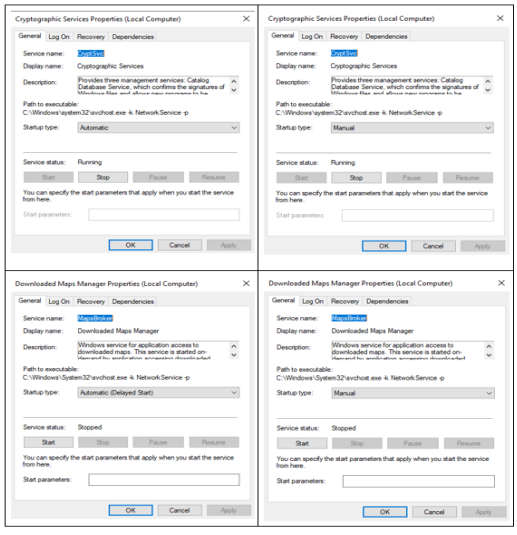
1. Open the Start menu and search for "Services"
2. Familiarize yourself with the columns, including Service Name, Display Name, Status, and Startup type.
3. Right-click on a service and select "Start", "Stop", or "Restart". Fill out the table below

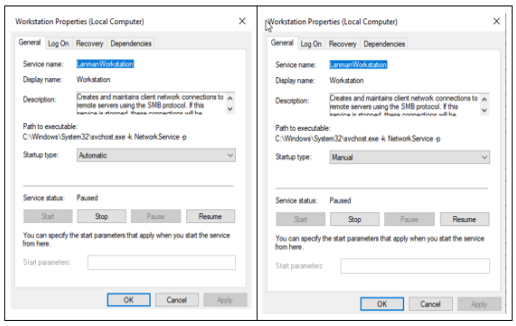
Status	Name of Service	Screenshot
Start	Device Management Enrollment Services	

Stop	Diagnostic Policy Service	
Restart	Geolocation Service	
Pause	Workstation	

4. Select five network services, right-click to view its properties. Modify the startup setting to Manual.

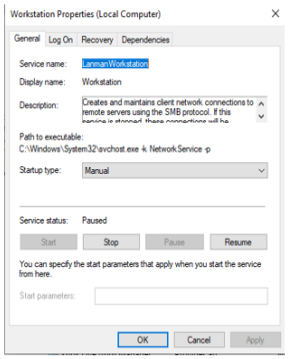
SS:

Before Modifying	After Modifying
	

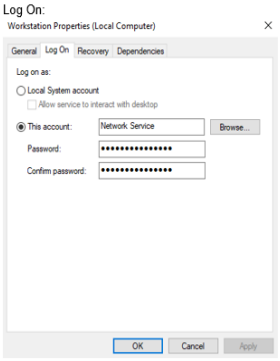


5. Explore the "General", "Recovery", and "Log On" tabs to understand additional service settings.

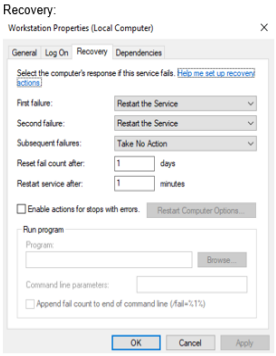
General:



Log On:



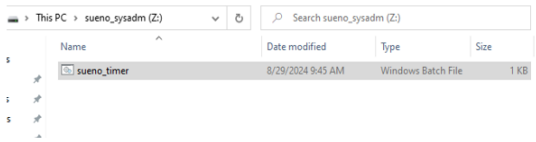
Recovery:



6. Create a batch file that will be added as a new service later on. Refer to the batch file code below.

```
@echo off
set /p seconds=Enter the countdown time in seconds:
:countdown
if %seconds% gtr 0 (
    echo Time remaining: %seconds% seconds
    timeout /t 1 >nul
    set /a seconds=%seconds%-1
    goto countdown
)
echo Timer finished!
```

7. Save the batch file in Z:\lastname_timer.bat



8. Use the sc command to add timer.bat service in the command line interface.

sc create BatchTimerService binPath= "path_to_your_batch_file.bat" start= auto

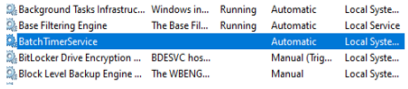
net start BatchTimerService

Replace path_to_your_batch_file.bat with the actual path to your batch file.

```
C:\Windows\system32>sc create BatchTimerService binPath="Z:\sueno_timer.bat" start=auto
[SC] CreateService SUCCESS
```

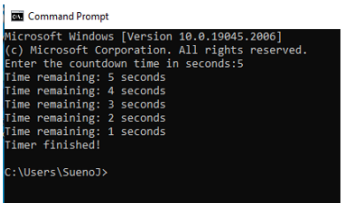
9. Verify that BatchTimerService has been added to the services.

SS:



10. **Testing the Service:** Now, if you open a new command prompt, you should see the timer countdown without requiring your interaction. Once the timer finishes, you'll see the "Timer finished!" message.

SS:



Rubric

Criteria	Excellent (10)	Good (7)	Needs Improvement (3)	Unsatisfactory (1)
Understanding of Services	Demonstrates a deep understanding of the concept of services, their roles, and their importance in Windows.	Shows a solid understanding of services, but may lack some depth in specific areas.	Has a basic understanding of services, but may struggle with specific concepts.	Shows little or no understanding of services.
Service Management Skills	Successfully starts, stops, restarts, and configures services using the Services app.	Demonstrates proficiency in managing services, but may encounter minor difficulties.	Can perform basic service management tasks, but may need assistance or guidance.	Struggles to perform even basic service management tasks.
Custom Service Creation	Successfully creates and manages a custom service using the appropriate tools and techniques.	Can create a custom service, but may encounter minor difficulties or require assistance.	Has limited experience with creating custom services.	Cannot create a custom service.
Problem-Solving	Demonstrates strong problem-solving skills when encountering challenges or errors.	Can effectively troubleshoot and resolve most issues related to service management.	May require assistance to troubleshoot some issues.	Struggles to troubleshoot and resolve issues.
Documentation and Reporting	Provides clear and concise documentation of the lab activities, including relevant screenshots and observations.	Documents the lab activities adequately, but may lack some detail or clarity.	Provides basic documentation, but may be disorganized or incomplete.	Does not provide any documentation or reporting.
Score:	**/50**			

Labwork 4:

UNIVERSITY OF Baguio
SCHOOL OF INFORMATION AND TECHNOLOGY

NAME: Sueno, Johnray K.	DATE PERFROMED: 09/12/24	
Section: IDC2	DATE SUBMITTED: 09/12/24	

SYSADM1 – Managing Services in Linux

Requirement:

- A virtual machine running Linux

Important Commands:

- `systemctl start <service_name.service>`
- `systemctl stop <service_name.service>`
- `systemctl restart <service_name.service>`
- `systemctl status <service_name.service>`

Complete this lab as follows:

1. Use the `service -status-all` command to list all active and inactive services.
   List down active and inactive services in the table below. Provide five (5) services for each column.

Active	Inactive
alsa-utils	anacron
sysstat	uuidd
procps	sssd
openvpn	rsync
kerneloops	saned

SS:
ACTIVE:

```
[ + ]  alsa-utils
[ + ]  sysstat
[ + ]  procps
[ + ]  openvpn
[ + ]  kerneloops
```

INACIVE:

```
[ - ]  anacron
[ - ]  uuidd
[ - ]  sssd
[ - ]  rsync
[ - ]  saned
```

2. Start the Bluetooth service using the systemctl command.
   Ex. `sudo systemctl start httpd`

> In this command:
> - `sudo` tells Linux you are running the command as the root user.
> - `systemctl` manages systemd services.
> - `start` tells the systemctl command to start the Apache service.
> - `httpd` is the name of the Apache web server service.

3. Check the status of the Bluetooth service. What is its status?
   SS:

```
ubuntu@ubuntu:~$ sudo systemctl start bluetooth
ubuntu@ubuntu:~$ systemctl status bluetooth.service
○ bluetooth.service - Bluetooth service
     Loaded: loaded (/usr/lib/systemd/system/bluetooth.service; enabled; preset>
     Active: inactive (dead)
       Docs: man:bluetoothd(8)

Sep 12 01:21:27 ubuntu systemd[1]: bluetooth.service - Bluetooth service was sk>
Sep 12 01:22:10 ubuntu systemd[1]: bluetooth.service - Bluetooth service was sk>
Sep 12 01:28:15 ubuntu systemd[1]: bluetooth.service - Bluetooth service was sk>
Sep 12 01:29:05 ubuntu systemd[1]: bluetooth.service - Bluetooth service was sk>
Sep 12 01:30:00 ubuntu systemd[1]: bluetooth.service - Bluetooth service was sk>

[7]+  Stopped                 systemctl status bluetooth.service
```

4. Check the status of the cups services. Since when was it running?
   SS:

```
ubuntu@ubuntu:~$ systemctl status cups.service
● cups.service - CUPS Scheduler
     Loaded: loaded (/usr/lib/systemd/system/cups.service; enabled; preset: ena>
     Active: active (running) since Thu 2024-09-12 01:06:11 UTC; 17min ago
TriggeredBy: ● cups.socket
             ● cups.path
       Docs: man:cupsd(8)
   Main PID: 1846 (cupsd)
     Status: "Scheduler is running..."
      Tasks: 1 (limit: 4557)
     Memory: 4.2M (peak: 4.4M)
        CPU: 67ms
     CGroup: /system.slice/cups.service
             └─1846 /usr/sbin/cupsd -l

Sep 12 01:06:10 ubuntu systemd[1]: Starting cups.service - CUPS Scheduler...
Sep 12 01:06:11 ubuntu systemd[1]: Started cups.service - CUPS Scheduler.
lines 1-16/16 (END)
```

5. Stop cups services.

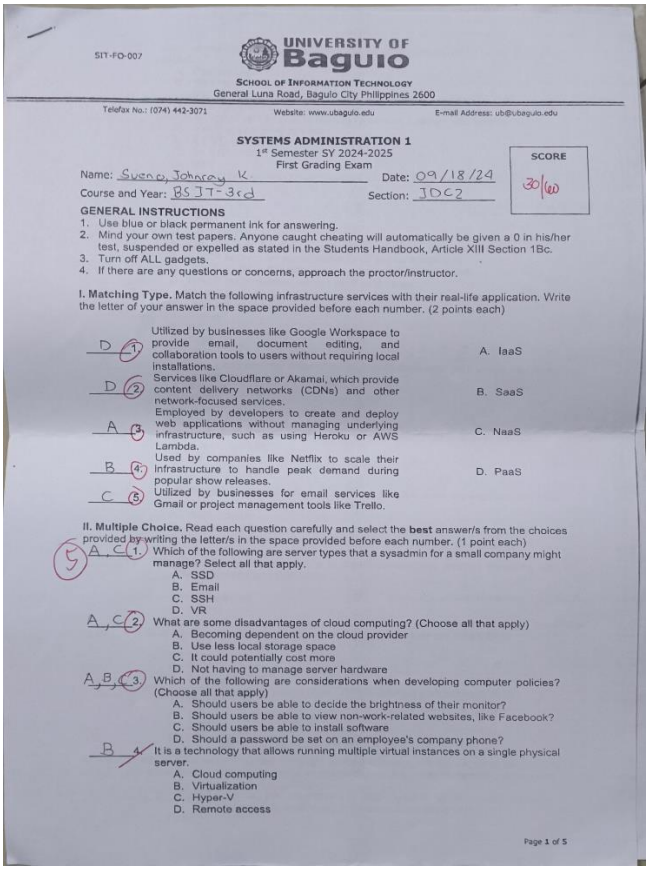
6. Verify if the service was stopped.
   SS:

```
ubuntu@ubuntu:~$ systemctl status cups.service
○ cups.service - CUPS Scheduler
     Loaded: loaded (/usr/lib/systemd/system/cups.service; enabled; preset: ena>
     Active: inactive (dead) since Thu 2024-09-12 01:25:40 UTC; 35s ago
   Duration: 19min 29.956s
TriggeredBy: ○ cups.socket
             ○ cups.path
       Docs: man:cupsd(8)
    Process: 1846 ExecStart=/usr/sbin/cupsd -l (code=exited, status=0/SUCCESS)
   Main PID: 1846 (code=exited, status=0/SUCCESS)
     Status: "Scheduler is running..."
        CPU: 69ms

Sep 12 01:06:10 ubuntu systemd[1]: Starting cups.service - CUPS Scheduler...
Sep 12 01:06:11 ubuntu systemd[1]: Started cups.service - CUPS Scheduler.
Sep 12 01:25:40 ubuntu systemd[1]: Stopping cups.service - CUPS Scheduler...
Sep 12 01:25:40 ubuntu systemd[1]: cups.service: Deactivated successfully.
Sep 12 01:25:40 ubuntu systemd[1]: Stopped cups.service - CUPS Scheduler.
lines 1-17/17 (END)
```

7. Restart the cups services

8. Verify if the service was restarted.
   SS:

```
ubuntu@ubuntu:~$ sudo systemctl restart cups.service
ubuntu@ubuntu:~$ systemctl status cups.service
● cups.service - CUPS Scheduler
     Loaded: loaded (/usr/lib/systemd/system/cups.service; enabled; preset: ena>
     Active: active (running) since Thu 2024-09-12 01:32:21 UTC; 14s ago
TriggeredBy: ● cups.socket
             ○ cups.path
       Docs: man:cupsd(8)
   Main PID: 5858 (cupsd)
     Status: "Scheduler is running..."
      Tasks: 1 (limit: 4557)
     Memory: 1.6M (peak: 1.9M)
        CPU: 5ms
     CGroup: /system.slice/cups.service
             └─5858 /usr/sbin/cupsd -l

Sep 12 01:32:21 ubuntu systemd[1]: Starting cups.service - CUPS Scheduler...
Sep 12 01:32:21 ubuntu systemd[1]: Started cups.service - CUPS Scheduler.
lines 1-16/16 (END)
```



SIT-FO-007

UNIVERSITY OF Baguio

SCHOOL OF INFORMATION TECHNOLOGY
General Luna Road, Baguio City Philippines 2600

Telefax No.: (074) 442-3071 Website: www.ubaguio.edu E-mail Address: ub@ubaguio.edu

SYSTEMS ADMINISTRATION 1
1st Semester SY 2024-2025
First Grading Exam

SCORE: 30/60

Name: Suson, Johnrey K. Date: 09/18/24
Course and Year: BSIT-3rd Section: IDC2

GENERAL INSTRUCTIONS
1. Use blue or black permanent ink for answering.
2. Mind your own test papers. Anyone caught cheating will automatically be given a 0 in his/her test, suspended or expelled as stated in the Students Handbook, Article XIII Section 1Bc.
3. Turn off ALL gadgets.
4. If there are any questions or concerns, approach the proctor/instructor.

I. Matching Type. Match the following infrastructure services with their real-life application. Write the letter of your answer in the space provided before each number. (2 points each)

D (1)	Utilized by businesses like Google Workspace to provide email, document editing, and collaboration tools to users without requiring local installations.	A. IaaS
D (2)	Services like Cloudflare or Akamai, which provide content delivery networks (CDNs) and other network-focused services.	B. SaaS
A (3)	Employed by developers to create and deploy web applications without managing underlying infrastructure, such as using Heroku or AWS Lambda.	C. NaaS
B (4)	Used by companies like Netflix to scale their infrastructure to handle peak demand during popular show releases.	D. PaaS
C (5)	Utilized by businesses for email services like Gmail or project management tools like Trello.	

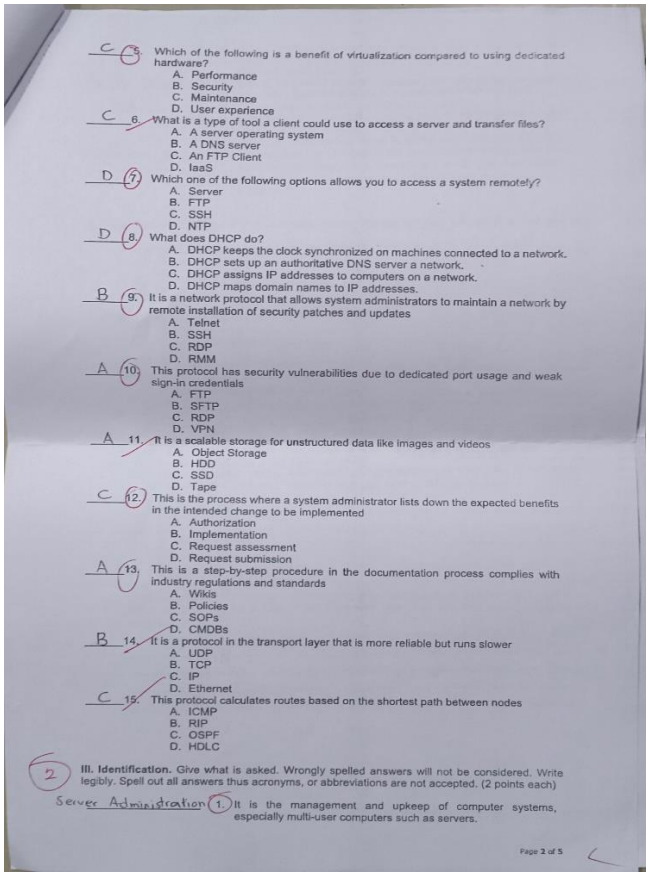
II. Multiple Choice. Read each question carefully and select the **best** answer/s from the choices provided by writing the letter/s in the space provided before each number. (1 point each)

5
A, C (1.) Which of the following are server types that a sysadmin for a small company might manage? Select all that apply.
A. SSD
B. Email
C. SSH
D. VR

A, C (2.) What are some disadvantages of cloud computing? (Choose all that apply)
A. Becoming dependent on the cloud provider
B. Use less local storage space
C. It could potentially cost more
D. Not having to manage server hardware

A, B, C (3.) Which of the following are considerations when developing computer policies? (Choose all that apply)
A. Should users be able to decide the brightness of their monitor?
B. Should users be able to view non-work-related websites, like Facebook?
C. Should users be able to install software
D. Should a password be set on an employee's company phone?

B (4.) It is a technology that allows running multiple virtual instances on a single physical server.
A. Cloud computing
B. Virtualization
C. Hyper-V
D. Remote access



C (5.) Which of the following is a benefit of virtualization compared to using dedicated hardware?
A. Performance
B. Security
C. Maintenance
D. User experience

C (6.) What is a type of tool a client could use to access a server and transfer files?
A. A server operating system
B. A DNS server
C. An FTP Client
D. IaaS

D (7.) Which one of the following options allows you to access a system remotely?
A. Server
B. FTP
C. SSH
D. NTP

D (8.) What does DHCP do?
A. DHCP keeps the clock synchronized on machines connected to a network.
B. DHCP sets up an authoritative DNS server a network.
C. DHCP assigns IP addresses to computers on a network.
D. DHCP maps domain names to IP addresses.

B (9.) It is a network protocol that allows system administrators to maintain a network by remote installation of security patches and updates
A. Telnet
B. SSH
C. RDP
D. RMM

A (10.) This protocol has security vulnerabilities due to dedicated port usage and weak sign-in credentials
A. FTP
B. SFTP
C. RDP
D. VPN

A (11.) It is a scalable storage for unstructured data like images and videos
A. Object Storage
B. HDD
C. SSD
D. Tape

C (12.) This is the process where a system administrator lists down the expected benefits in the intended change to be implemented
A. Authorization
B. Implementation
C. Request assessment
D. Request submission

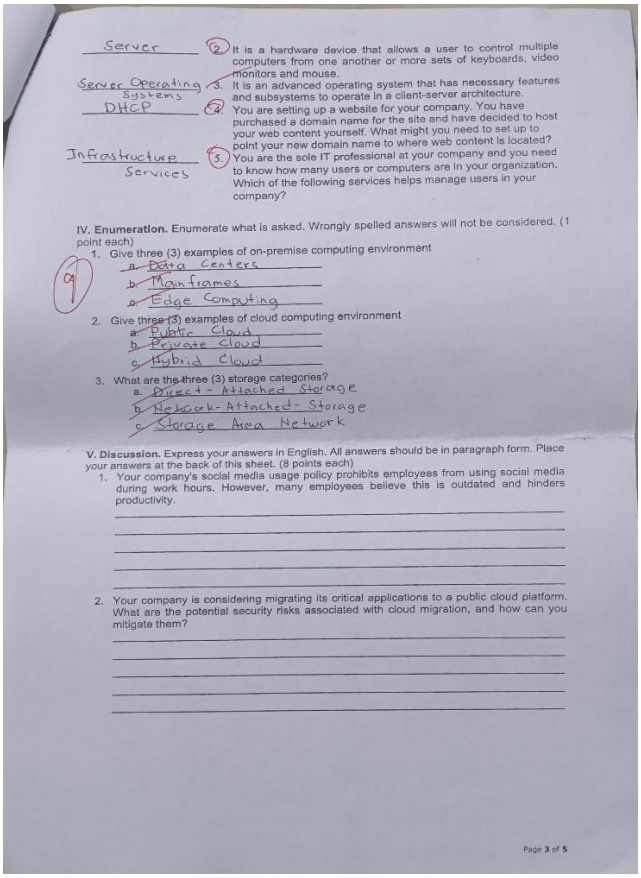
A (13.) This is a step-by-step procedure in the documentation process complies with industry regulations and standards
A. Wikis
B. Policies
C. SOPs
D. CMDBs

B (14.) It is a protocol in the transport layer that is more reliable but runs slower
A. UDP
B. TCP
C. IP
D. Ethernet

C (15.) This protocol calculates routes based on the shortest path between nodes
A. ICMP
B. RIP
C. OSPF
D. HDLC

2
III. Identification. Give what is asked. Wrongly spelled answers will not be considered. Write legibly. Spell out all answers thus acronyms, or abbreviations are not accepted. (2 points each)

Server Administration (1.) It is the management and upkeep of computer systems, especially multi-user computers such as servers.



Server (2.) It is a hardware device that allows a user to control multiple computers from one another or more sets of keyboards, video monitors and mouse.

Server Operating Systems (3.) It is an advanced operating system that has necessary features and subsystems to operate in a client-server architecture.

DHCP (4.) You are setting up a website for your company. You have purchased a domain name for the site and have decided to host your web content yourself. What might you need to set up to point your new domain name to where web content is located?

Infrastructure Services (5.) You are the sole IT professional at your company and you need to know how many users or computers are in your organization. Which of the following services helps manage users in your company?

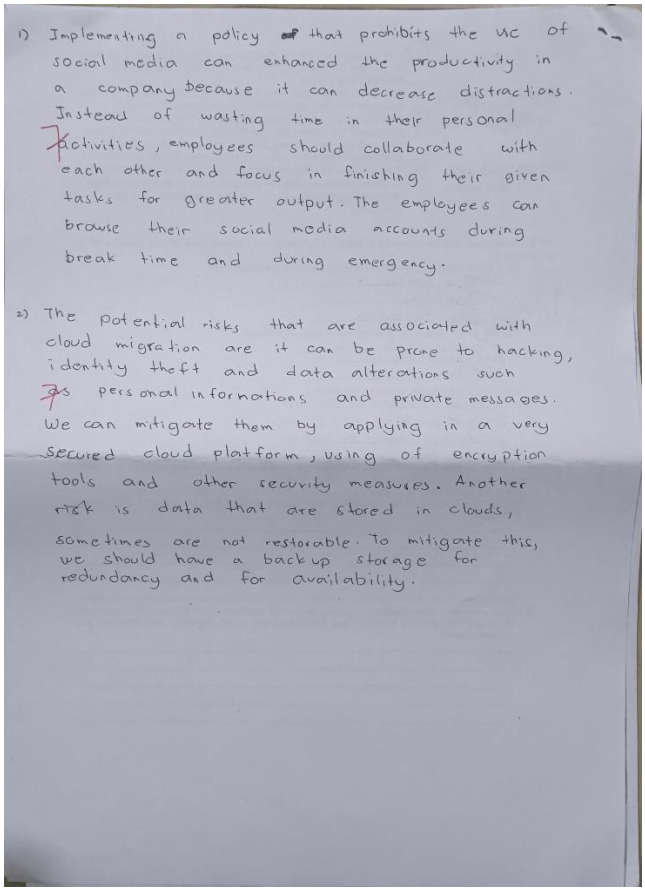
IV. Enumeration. Enumerate what is asked. Wrongly spelled answers will not be considered. (1 point each)

9
1. Give three (3) examples of on-premise computing environment
   a. Data Centers
   b. Mainframes
   c. Edge Computing
2. Give three (3) examples of cloud computing environment
   a. Public Cloud
   b. Private Cloud
   c. Hybrid Cloud
3. What are the three (3) storage categories?
   a. Direct-Attached Storage
   b. Network-Attached Storage
   c. Storage Area Network

V. Discussion. Express your answers in English. All answers should be in paragraph form. Place your answers at the back of this sheet. (8 points each)

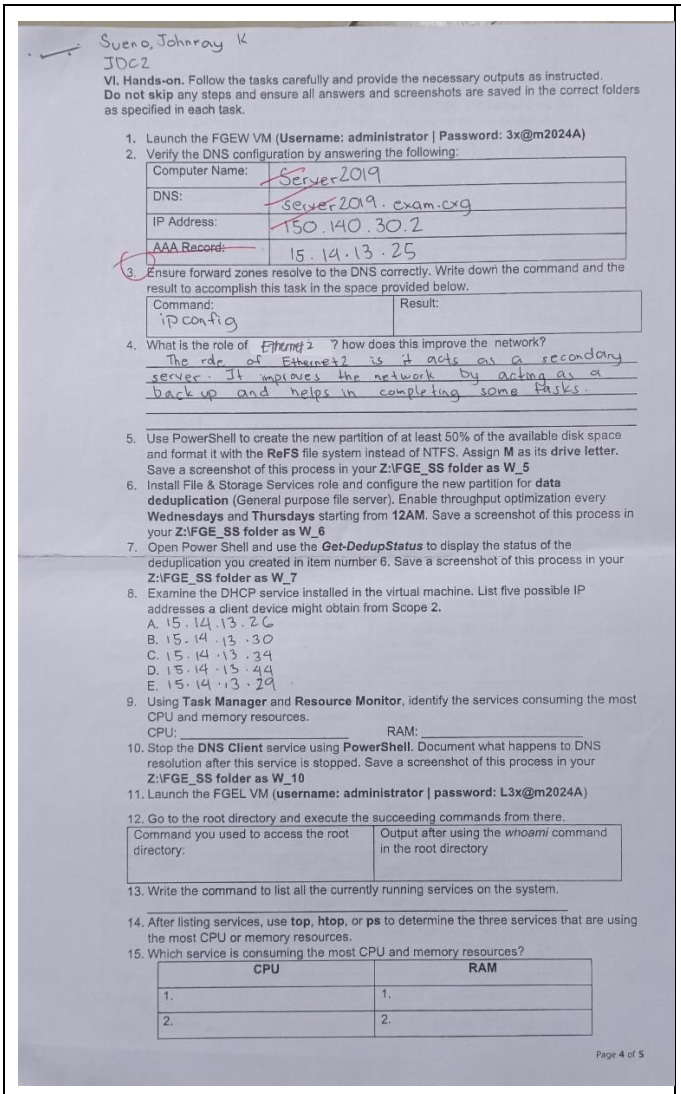
1. Your company's social media usage policy prohibits employees from using social media during work hours. However, many employees believe this is outdated and hinders productivity.

2. Your company is considering migrating its critical applications to a public cloud platform. What are the potential security risks associated with cloud migration, and how can you mitigate them?



1) Implementing a policy that prohibits the use of social media can enhanced the productivity in a company because it can decrease distractions. Instead of wasting time in their personal activities, employees should collaborate with each other and focus in finishing their given tasks for greater output. The employees can browse their social media accounts during break time and during emergency.

2) The potential risks that are associated with cloud migration are it can be prone to hacking, identity theft and data alterations such as personal informations and private messages. We can mitigate them by applying in a very secured cloud platform, using of encryption tools and other security measures. Another risk is data that are stored in clouds, sometimes are not restorable. To mitigate this, we should have a backup storage for redundancy and for availability.



Suero, Johnray K
JDC2

VI. Hands-on. Follow the tasks carefully and provide the necessary outputs as instructed. **Do not skip** any steps and ensure all answers and screenshots are saved in the correct folders as specified in each task.

1. Launch the FGEW VM (**Username: administrator | Password: 3x@m2024A**)
2. Verify the DNS configuration by answering the following:

Computer Name:	Server2019
DNS:	Server2019.exam.org
IP Address:	150.140.30.2
AAA Record:	15.14.13.25

3. Ensure forward zones resolve to the DNS correctly. Write down the command and the result to accomplish this task in the space provided below.

Command:	Result:
ipconfig	

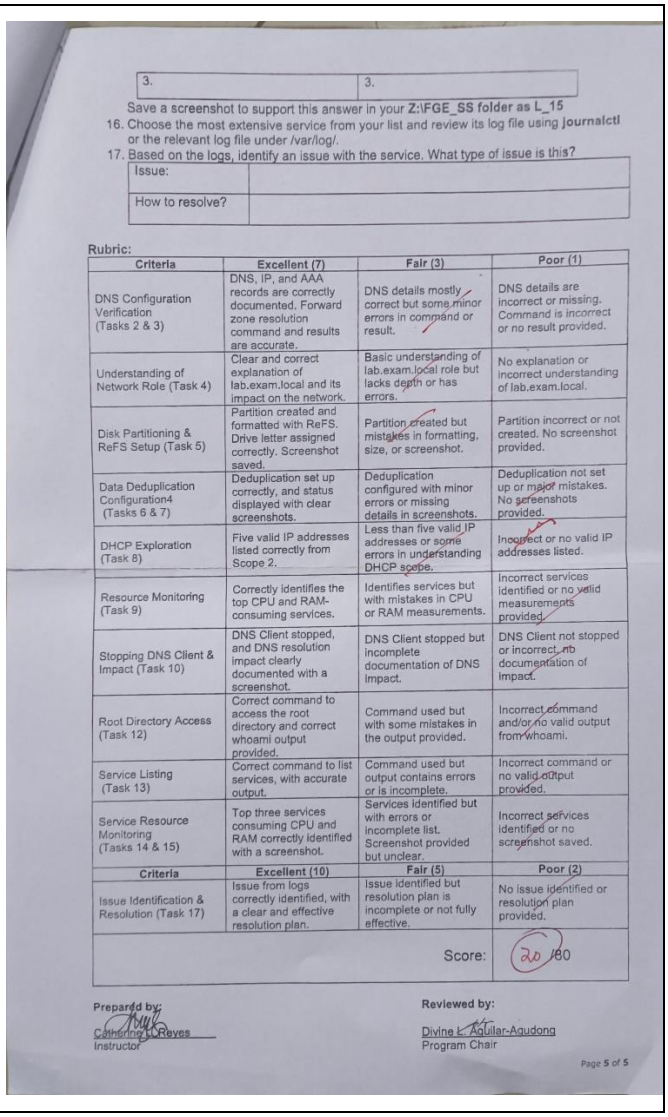
4. What is the role of Ethernet2 ? how does this improve the network?
   The role of Ethernet2 is it acts as a secondary server. It improves the network by acting as a back up and helps in completing some tasks.
5. Use PowerShell to create the new partition of at least 50% of the available disk space and format it with the **ReFS** file system instead of NTFS. Assign **M** as its **drive letter.** Save a screenshot of this process in your **Z:\FGE_SS folder as W_5**
6. Install File & Storage Services role and configure the new partition for **data deduplication** (General purpose file server). Enable throughput optimization every **Wednesdays** and **Thursdays** starting from **12AM**. Save a screenshot of this process in your **Z:\FGE_SS folder as W_6**
7. Open Power Shell and use the ***Get-DedupStatus*** to display the status of the deduplication you created in item number 6. Save a screenshot of this process in your **Z:\FGE_SS folder as W_7**
8. Examine the DHCP service installed in the virtual machine. List five possible IP addresses a client device might obtain from Scope 2.
   A. 15.14.13.26
   B. 15.14.13.30
   C. 15.14.13.34
   D. 15.14.13.44
   E. 15.14.13.29
9. Using **Task Manager** and **Resource Monitor**, identify the services consuming the most CPU and memory resources.
   CPU: _____ RAM: _____
10. Stop the **DNS Client** service using **PowerShell**. Document what happens to DNS resolution after this service is stopped. Save a screenshot of this process in your **Z:\FGE_SS folder as W_10**
11. Launch the FGEL VM (**username: administrator | password: L3x@m2024A**)
12. Go to the root directory and execute the succeeding commands from there.

Command you used to access the root directory:	Output after using the *whoami* command in the root directory

13. Write the command to list all the currently running services on the system.
14. After listing services, use **top**, **htop**, or **ps** to determine the three services that are using the most CPU or memory resources.
15. Which service is consuming the most CPU and memory resources?

CPU	RAM
1.	1.
2.	2.

Page 4 of 5



3.	3.

Save a screenshot to support this answer in your **Z:\FGE_SS folder as L_15**

16. Choose the most extensive service from your list and review its log file using **journalctl** or the relevant log file under /var/log/.
17. Based on the logs, identify an issue with the service. What type of issue is this?

Issue:	
How to resolve?	

Rubric:

Criteria	Excellent (7)	Fair (3)	Poor (1)
DNS Configuration Verification (Tasks 2 & 3)	DNS, IP, and AAA records are correctly documented. Forward zone resolution command and results are accurate.	DNS details mostly correct but some minor errors in command or result.	DNS details are incorrect or missing. Command is incorrect or no result provided.
Understanding of Network Role (Task 4)	Clear and correct explanation of lab.exam.local and its impact on the network.	Basic understanding of lab.exam.local role but lacks depth or has errors.	No explanation or incorrect understanding of lab.exam.local.
Disk Partitioning & ReFS Setup (Task 5)	Partition created and formatted with ReFS. Drive letter assigned correctly. Screenshot saved.	Partition created but mistakes in formatting, size, or screenshot.	Partition incorrect or not created. No screenshot provided.
Data Deduplication Configuration4 (Tasks 6 & 7)	Deduplication set up correctly, and status displayed with clear screenshots.	Deduplication configured with minor errors or missing details in screenshots.	Deduplication not set up or major mistakes. No screenshots provided.
DHCP Exploration (Task 8)	Five valid IP addresses listed correctly from Scope 2.	Less than five valid IP addresses or some errors in understanding DHCP scope.	Incorrect or no valid IP addresses listed.
Resource Monitoring (Task 9)	Correctly identifies the top CPU and RAM-consuming services.	Identifies services but with mistakes in CPU or RAM measurements.	Incorrect services identified or no valid measurements provided.
Stopping DNS Client & Impact (Task 10)	DNS Client stopped, and DNS resolution impact clearly documented with a screenshot.	DNS Client stopped but incomplete documentation of DNS impact.	DNS Client not stopped or incorrect, no documentation of impact.
Root Directory Access (Task 12)	Correct command to access the root directory and correct whoami output provided.	Command used but with some mistakes in the output provided.	Incorrect command and/or no valid output from whoami.
Service Listing (Task 13)	Correct command to list services, with accurate output.	Command used but output contains errors or is incomplete.	Incorrect command or no valid output provided.
Service Resource Monitoring (Tasks 14 & 15)	Top three services consuming CPU and RAM correctly identified with a screenshot.	Services identified but with errors or incomplete list. Screenshot provided but unclear.	Incorrect services identified or no screenshot saved.
Criteria	**Excellent (10)**	**Fair (5)**	**Poor (2)**
Issue Identification & Resolution (Task 17)	Issue from logs correctly identified, with a clear and effective resolution plan.	Issue identified but resolution plan is incomplete or not fully effective.	No issue identified or resolution plan provided.
		Score:	20 /80

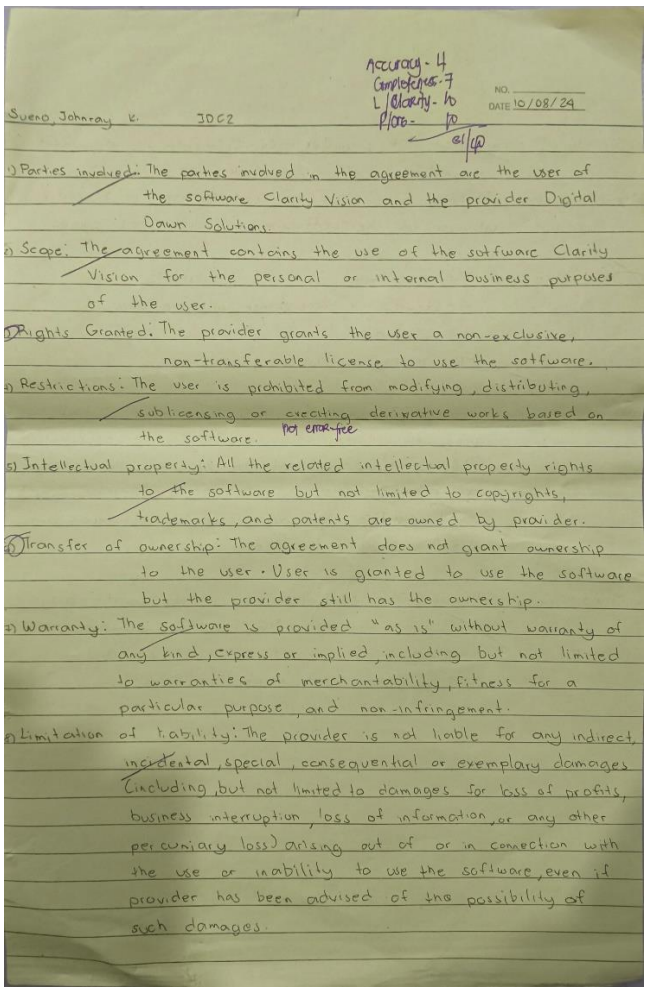
Prepared by:
Catherine C. Reyes
Instructor

Reviewed by:
Divine K. Aguilar-Agudong
Program Chair

Page 5 of 5

Midterm Lecture:

Assignment 1:



Sueno, Johnray K. IDC2

NO.
DATE 10/08/24

Accuracy - 4
Completeness - 7
Clarity - 10
Flow - 10
/31

1) Parties involved: The parties involved in the agreement are the user of the software Clarity Vision and the provider Digital Dawn Solutions.

2) Scope: The agreement contains the use of the software Clarity Vision for the personal or internal business purposes of the user.

3) Rights Granted: The provider grants the user a non-exclusive, non-transferable license to use the software.

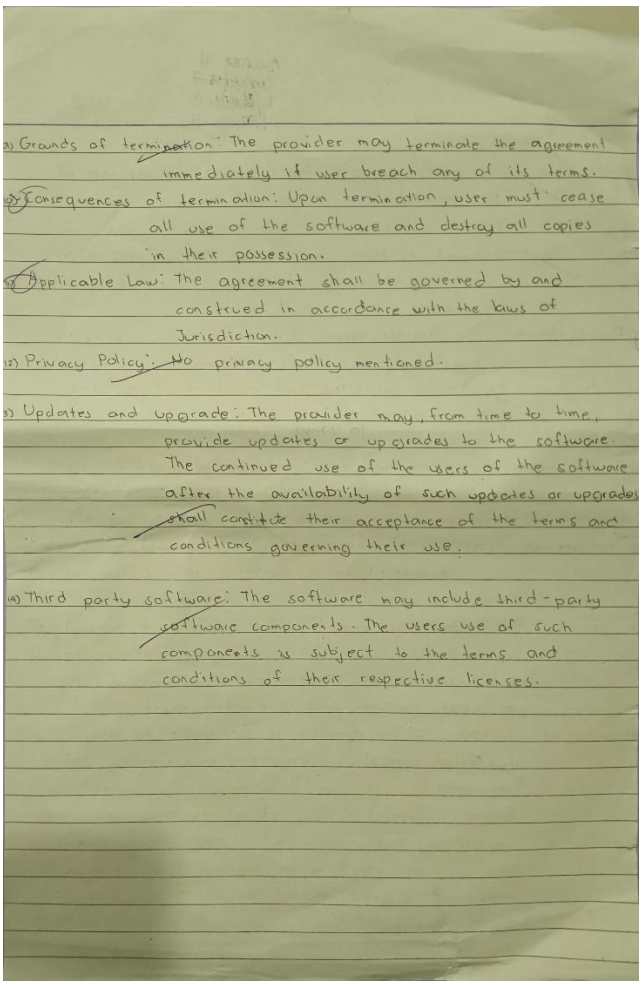
4) Restrictions: The user is prohibited from modifying, distributing, sublicensing or creating derivative works based on the software. not enforce

5) Intellectual property: All the related intellectual property rights to the software but not limited to copyrights, trademarks, and patents are owned by provider.

6) Transfer of ownership: The agreement does not grant ownership to the user. User is granted to use the software but the provider still has the ownership.

7) Warranty: The software is provided "as is" without warranty of any kind, express or implied, including but not limited to warranties of merchantability, fitness for a particular purpose, and non-infringement.

8) Limitation of liability: The provider is not liable for any indirect, incidental, special, consequential or exemplary damages (including, but not limited to damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or in connection with the use or inability to use the software, even if provider has been advised of the possibility of such damages.



9) Grounds of termination: The provider may terminate the agreement immediately if user breach any of its terms.

10) Consequences of termination: Upon termination, user must cease all use of the software and destroy all copies in their possession.

11) Applicable Law: The agreement shall be governed by and construed in accordance with the laws of Jurisdiction.

12) Privacy Policy: No privacy policy mentioned.

13) Updates and upgrade: The provider may, from time to time, provide updates or upgrades to the software. The continued use of the users of the software after the availability of such updates or upgrades shall constitute their acceptance of the terms and conditions governing their use.

14) Third party software: The software may include third-party software components. The users use of such components is subject to the terms and conditions of their respective licenses.

Seatwork 1:

Sueno, Johnray K. JDC2 10/10/24

SYSADM1 -Web Server Monitoring 32/40

1) How do you monitor web server statistics?

▶ In monitoring web server statistics, we can use tools such as Performance Monitor for real-time data and logging. Task Manager can be used also, it can provide an overview of running applications, processes, system resource usage, including CPU, memory, disk and network activity

2) What are the key metrics that you need to monitor in a web server?

- Memory Usage: Assesses available resources.
- CPU usage: Indicates processing capacity.
- Response Time: Measures how quickly the server responds to requests.
- Error Rates: Tracks failed request to identify issues.
- Active Connections: Number of current connections being handled.

3. Analyze the provided web server statistics

A. Average response time: 738.88 ms
B. Request per second: 1 Request per second
C. Memory Usage: 97.78 mb (average memory usage)
D. Error Rate: 22.22 %
E. Common Error Types: 404 Not Found and 500 Internal Server Error.

- What are the possible issues in the web server statistics above?

▶ The possible issues are ithe average response time is too high that can lead to poor user experience. The error rate is above 20% which should indicate that one in five requests fails.
▶ The /images/error.png cant be found, it may be deleted or moved
▶ URL /contact took high response time, can be cause by high cpu usage or high traffic load or overload.
▶ It can just handle 1 request per second.

Midterm Laboratory:

Labwork 1:

UNIVERSITY OF Baguio

SCHOOL OF INFORMATION AND TECHNOLOGY

NAME: Sueno, Johnray K.	DATE PERFORMED: 09/26/2024	
Section: IDC2	DATE SUBMITTED: 09/26/2024	/50

SYSADM1 – Monitoring Print Services in Windows Server 2019

Requirement:

- A virtual machine running Linux and Windows OS

Part 1: Setting Up Print Services

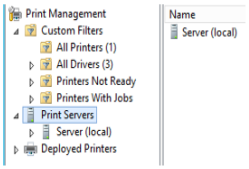
1. Install and configure print.srv domain

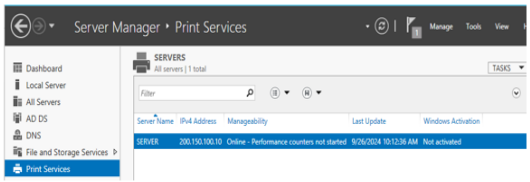
```
C:\Users\Admin>nslookup
Default Server:  print.srv
Address:  200.150.100.10
```

2. Connect one client to the recently created domain

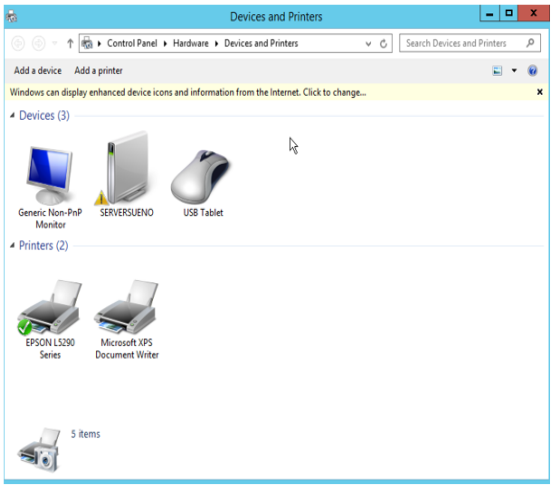
```
C:\Users\User1>nslookup
Default Server:  print.srv
Address:  200.150.100.10
```

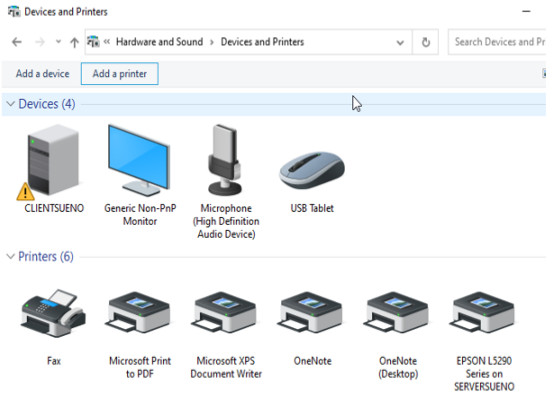
3. Install Print Services Role:





4. Search the internet for any printer installer and convert it to iso
5. Install and deploy it as network printer

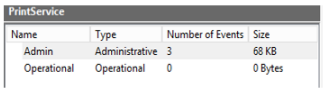




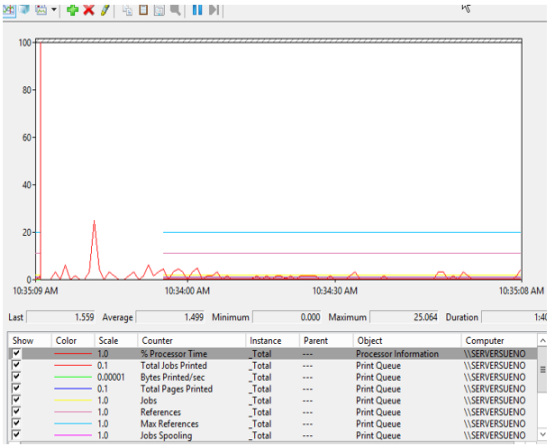
Part 2: Monitoring Print Services

Objective: Familiarize yourself with monitoring tools available in Windows Server 2019.

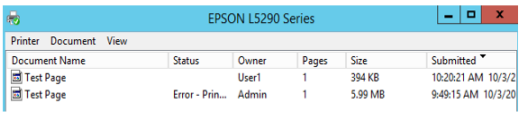
1. Event Viewer:
   - Open Event Viewer (run eventvwr.msc).
   - Navigate to Applications and Services Logs > Microsoft > Windows > PrintService.
   - Review logs for print jobs, errors, and warnings.



2. Performance Monitor:
   - Open Performance Monitor (run perfmon).
   - In the left pane, expand Data Collector Sets > System.
   - Right-click System Performance and select Start.
   - Monitor performance metrics related to print services.



3. Using Print Management Console:
   - Open Print Management from Server Manager.
   - View active print jobs and their status.
   - Use the Printers node to check the status of all printers.



Part 3: Exploring Third-Party Monitoring Tools

1. Research at least two third-party print monitoring tools
   - Consider factors such as features, pricing, and compatibility with Windows Server 2019.

1. PaperCut

- Features:

Print tracking and reporting.

User authentication and access control.

Cost recovery features.

Web-based interface for management.

- Pricing: Pricing is based on the number of users or printers, with a free trial available. Contact for specific quotes.

- Compatibility: Compatible with Windows Server 2019 and various other operating systems.

2. PrinterLogic

- Features:

Centralized print management.

Print driver management without the need for print servers.

User self-service portal for managing printers.

Detailed reporting and analytics.

- Pricing: Pricing typically requires a quote based on the number of users or devices.

- Compatibility: Works well with Windows Server 2019 and supports various environments.

2. Install and Configure:
   - Choose one of the tools to install in your environment.
   - Follow the installation instructions provided by the tool's documentation.
   - Configure it to monitor your print services.
3. Test and Report Findings:
   - Generate a report or dashboard from the tool.
   - Analyze the collected data (e.g., print volume, errors, user activity).

Rubric

Criteria	1 (Unsatisfactory)	2 (Needs Improvement)	3 (Satisfactory)	4 (Good)	5 (Excellent)	Score
Part 1: Setting Up Print Services						
Domain Installation	No domain created	Domain created with errors	Domain created correctly	Domain configured well	Domain configured and documented thoroughly	
Client Connection	Client not connected	Connection attempt failed	Client connected but with issues	Client connected correctly	Client connected and documented well	
Print Services Role Installation	Role not installed	Role installed with issues	Role installed correctly	Role installed and configured	Role installed, configured, and documented thoroughly	
Printer Installer Conversion	No installer found	Installer conversion attempted but failed	Installer converted but not used	Installer converted and used	Installer converted, used, and documented well	
Network Printer Deployment	Printer not deployed	Deployment failed	Printer deployed but not functional	Printer deployed correctly	Printer deployed, tested, and documented well	
Part 2: Monitoring Print Services						
Event Viewer Usage	Event Viewer not opened	Opened but no logs reviewed	Logs reviewed but superficial	Logs reviewed with some analysis	Logs reviewed with thorough analysis and documentation	
Performance Monitor Usage	Performance Monitor not opened	Opened but no metrics monitored	Metrics monitored but not analyzed	Metrics monitored with some analysis	Metrics monitored, analyzed, and documented thoroughly	
Print Management Console Usage	Console not opened	Opened but functionality not used	Active jobs viewed superficially	Active jobs viewed with some detail	Active jobs viewed and documented thoroughly	
Part 3: Exploring Third-Party Tools						
Research on Tools	No tools researched	Research incomplete	Research on one tool completed	Research on two tools with some analysis	Research on two tools, detailed analysis, and comparison	
Installation and Configuration	Tool not installed	Installation failed	Tool installed but not configured	Tool installed and configured with issues	Tool installed, configured, and documented thoroughly	
Reporting Findings	No report generated	Report lacks detail	Report generated but lacks analysis	Report generated with some analysis	Comprehensive report with thorough analysis and documentation	

Labwork 2:

UNIVERSITY OF BAGUIO
SCHOOL OF INFORMATION AND TECHNOLOGY

NAME: Sueno, Johnray K.	DATE PERFORMED: 10/10/2024	
Section: IDC2	DATE SUBMITTED: 10/10/2024	/50

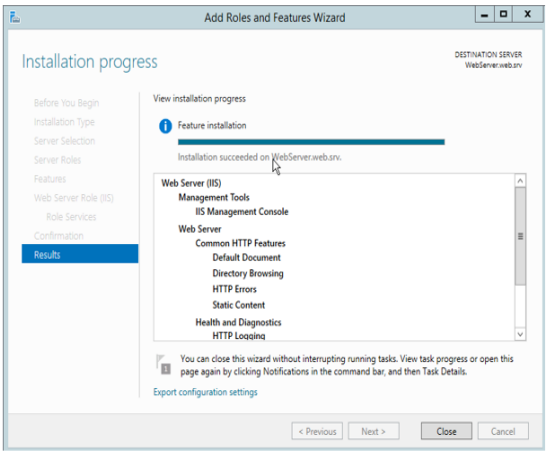
SYSADM1 – Setting Up Webserver

Requirement:

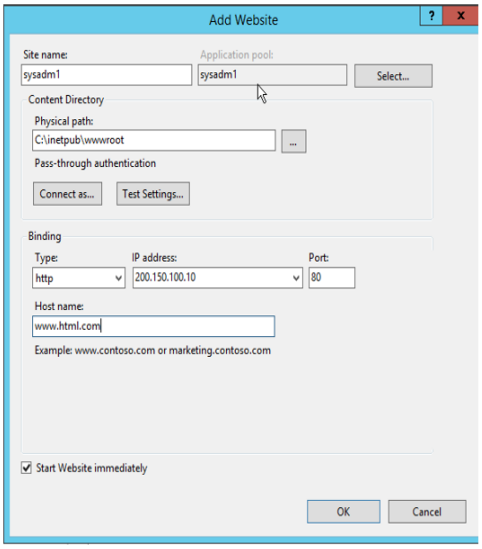
- A virtual machine running Linux and Windows OS

Task Instructions:

1. Install IIS by adding it as a role, select necessary features, include monitoring tools



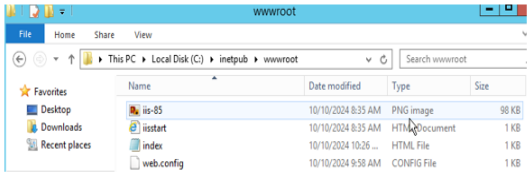
2. Create a website by opening IIS Manager
   - Right-click on the server's name and select Internet Information Services Manager.
   - Right-click on Sites and select Add Website.
   - Enter a name, description, physical path (where your website files will reside), IP address, port, and host name.



3. Configure the Website:
   - Right-click on your website and select Edit.
   - Set the Default Document to the name of your main HTML file >default.html
   - Configure other settings as needed (e.g., SSL certificates, authentication)
4. Create a Web Page:
   - Create an HTML file in the physical path you specified.

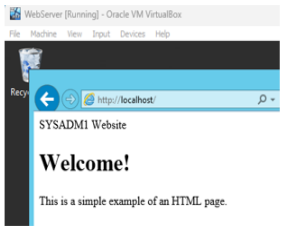
```
<!DOCTYPE html>
<html>
<head>
    <title>SYSADM1 Website</title>
</head>
<body>
    <h1>Welcome!</h1>
    <p>This is a simple example of an HTML page.</p>
</body>
</html>
```


   - Save it as default.html or your preferred name. (name : index.html)

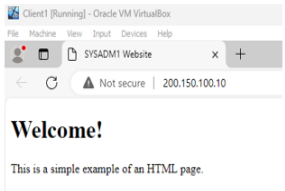


5. Test the Web Server:
   - Open a web browser and enter the URL of your website (e.g., http://localhost).
   - You should see your web page displayed.

SERVER:



CLIENT:



Grading Rubric

Criteria	Points	Description
Web Server Installation	15	Correctly installs IIS or another web server on the virtual machine.
Website Configuration	15	Successfully configures the website with the correct physical path, IP address, port, and default document.
Successful Access	15	Successfully accesses the web page from the client computer using the correct URL.
Troubleshooting	15	Demonstrates ability to troubleshoot common issues, such as network connectivity problems or configuration errors.
Documentation	10	Provides clear and concise documentation of the installation, configuration, and testing process.
Total	/70	

Labwork 3:

UNIVERSITY OF Baguio
SCHOOL OF INFORMATION AND TECHNOLOGY

NAME: Sueno, Johnray K.	DATE PERFORMED: 10/17/2024	
Section: IDC2	DATE SUBMITTED:10/17/2024	/50

SYSADM1 – Platform Services

Requirement:

- A virtual machine running Windows Server

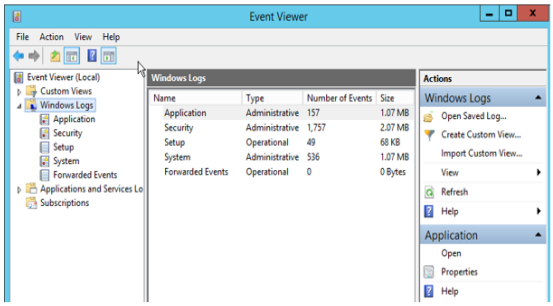
Objective/s:

To analyze IIS logs in the Event Viewer to identify critical web service metrics, understand common error codes, and learn how to monitor the health of web applications.

Instructions

Part 1: Opening Event Viewer and Loading Logs

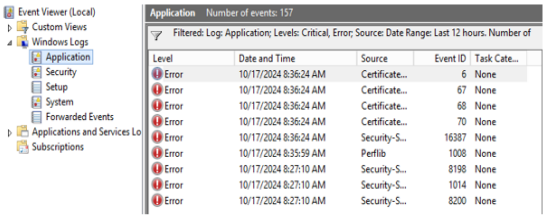
1. Access the event viewer in the server.
2. From the event viewer, explore the windows log and list down its major categories

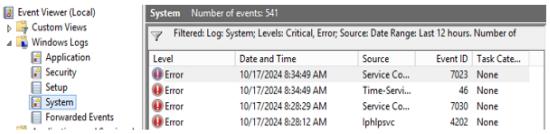


➢ The major categories are Application, Security, Setup, System and Forwarded Events.

Part 2: Filtering and Analyzing IIS Events

1. Apply filter to the windows log categories to display errors for the past 12 hours.





2. **Identify Critical Events** or recurring events.

➢ The critical or recurring events are the Source CertificateServicesClient-CertEnroll, Security-SPP and Service Control Manager.

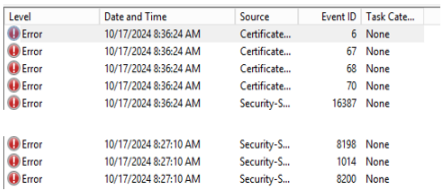
3. **Analyze the Events**:
   - For each critical or recurring event, **record the following details**:

EVENTS	SOURCE	TIMESTAMP	DESCRIPTION
67	CertificateServicesClient-CertEnroll	10/17/2024 8:36:24 AM	Certificate enrollment for Local System failed to load policy from policy servers. The specified domain either does not exist or could not be contacted.
68	CertificateServicesClient-CertEnroll	10/17/2024 8:36:24 AM	Certificate enrollment for Local System failed in authentication to policy servers.
70	CertificateServicesClient-CertEnroll	10/17/2024 8:36:24 AM	Certificate enrollment for Local System failed because no valid

			policy can be obtained from policy servers.
16387	Security-SPP	10/17/2024 8:36:24 AM	Failed to run task\Microsoft\Windows\WS\License Validation.
8198	Security-SPP	10/17/2024 8:27:10 AM	License Activation failed.
1014	Security-SPP	10/17/2024 8:27:10 AM	Acquisition of End User License failed.
8200	Security-SPP	10/17/2024 8:27:10 AM	License Acquisition failed.
7023	Service Control Manager	10/17/2024 8:34:49 AM	The Windows Time service terminated with the error an attempt was made to logon, but the network logon service was not started.
7030	Service Control Manager	10/17/2024 8:28:29 AM	The Printer Extensions and Notifications service is marked as an interactive service but the system is configured to not allow interactive services causing it to not function properly.

Part 3: Troubleshooting and Solution Development

1. Review the logs and check for recurring errors.
2. Is there a specific time or pattern to these errors?



➢ Yes there is, the errors have occurred at the same time as 10/17/2024 8:36:24 AM and 10/17/2024 8:27:10 AM.

3. Draft a Troubleshooting Report:
   - Based on the events found, create a short report with the following sections:

Report Structure

1. Overview

- A brief summary of the issue and scope of your analysis.

➢ This report summarizes the analysis of errors found in the Server Event Viewer, specifically focusing on critical events and errors that occurred in the last 12 hours such as Certificate Services Client Cert-Enroll, Security-SPP and Service Control Manager. The report aimed to identify recurring issues and their potential impact on system operations. Some errors also occurred at the same time.

2. Key Findings

- List the critical events you found.
  - **Event ID 67**: Certificate enrollment for Local System failed to load policy from policy servers at 10/17/2024 8:36:24 AM.
  - **Event ID 68**: Certificate enrollment for Local System failed in authentication to policy servers at 10/17/2024 8:36:24 AM.
  - **Event ID 70**: Certificate enrollment for Local System failed because no valid policy can be obtained from policy servers at 10/17/2024 8:36:24 AM.
  - **Event ID 16387**: Failed to run task\Microsoft\Windows\WS\License Validation at 10/17/2024 8:36:24 AM.
  - **Event ID 8198**: License Activation failed at 10/17/2024 8:27:10 AM.
  - **Event ID 1014**: Acquisition of End User License failed at 10/17/2024 8:27:10 AM.
  - **Event ID 8200**: License Acquisition failed at 10/17/2024 8:27:10 AM.
  - **Event ID 7023**: The Windows Time service terminated with an error at 10/17/2024 8:34:49 AM.

- **Event ID 7030**: The Printer Extensions and Notifications service is marked as an interactive service but is not functioning properly at 10/17/2024 8:28:29 AM.

3. Root Causes and Solutions

- Describe the likely cause of each error and how you would fix it.

1. CertificateServicesClient-CertEnroll **Errors**:

Likely Causes: Network issues or misconfigured permissions such as the specified domain either does not exist or could not be contacted leading to failure in certificate enrollment.

Solutions:

- Check network connectivity to the Certificate Authority.
- Verify permissions for the Local System account and ensure Group Policy settings are correctly configured.

2. **Security-SPP Errors**:

Likely Causes: Issues with license validation, license acquisition and activation processes.

Solutions:

- Ensure that the Windows licensing services are running properly.
- Check the system's internet connection for reaching Microsoft's activation servers.

3. **Service Control Manager Errors**:

Likely Causes: Services not starting due to configuration issues like an attempt was made to logon, but the network logon service was not started and the system is configured to not allow interactive services causing it to not function properly.

Solutions:

- For the Windows Time service, ensure the Network Logon service is running.
- Review service configuration settings for the Printer Extensions service.

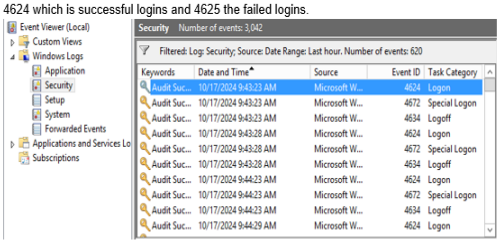
Part 4: Reflection Questions

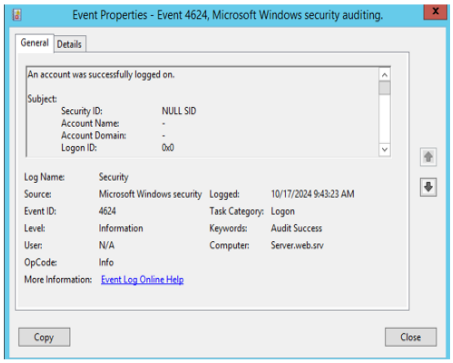
1. What are the most common causes of a CertificateServicesClient-CertEnroll and **Security-SPP** error?

➢ The most common causes of CertificateServicesClient-CertEnroll and Security-SPP errors include network issues, permissions problems, and misconfigurations. For CertificateServicesClient-CertEnroll errors, if the network is down, doesn't exist and cannot be found the system/server can't connect to the Certificate Authority to get certificates. If the account doesn't have the right permissions or policies it can't enroll and expired or missing certificates can cause problems too. For Security-SPP errors, issues with license validation or a bad internet connection can prevent license activation and incorrect Group Policy settings can also lead to these errors.

2. How would you **monitor login attempts** to detect potential security threats?

➢ To monitor login attempts, regularly checking the Security log in Event Viewer for Event IDs 4624 which is successful logins and 4625 the failed logins.





3. Why is **monitoring logs** in Event Viewer important for administrators?

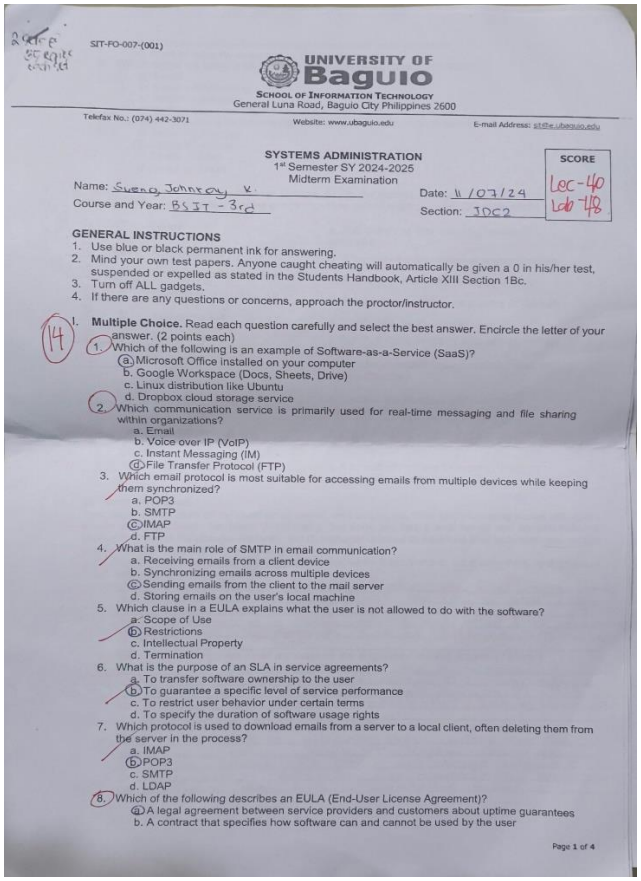
➢ Monitoring logs in Event Viewer is very important because it helps in identifying an issue and guide us what or how to troubleshoot this system issues, it can also help in detecting login, failed and unauthorized access and potential security threats to ensure compliance with regulations and improving overall system performance and reliability.

Grading Rubric

Criteria	Excellent	Good	Needs Improvement	Poor	Points
Log Analysis	Identifies all key events (503, 404, 500, etc.) with accurate event details.	Identifies most key events with minor errors in details.	Identifies some events, but with incomplete or incorrect details.	Fails to identify key events or provides incorrect details.	/10
Troubleshooting Solutions	Proposes logical, effective solutions to all identified issues.	Solutions are mostly correct but miss some key points.	Solutions are somewhat vague or incomplete.	Solutions are unclear or incorrect.	/10
Report Structure & Clarity	Well-organized report with all sections clearly completed.	Report is mostly organized with minor formatting issues.	Report is disorganized or missing sections.	Report is unclear or incomplete.	/10

Recommendations for Monitoring	Provides thoughtful, proactive recommendations to prevent future issues.	Recommendations are relevant but lack depth.	Recommendations are vague or incomplete.	Fails to provide relevant recommendations.	/10
Participation & Effort	Actively engaged in the activity, followed instructions thoroughly.	Participated but required some guidance.	Minimal participation, needed significant help.	Did not participate meaningfully.	/10
				Score	**/50**

Midterm Exam: Lecture



SIT-FO-007-(001)

UNIVERSITY OF Baguio
SCHOOL OF INFORMATION TECHNOLOGY
General Luna Road, Baguio City Philippines 2600
Telefax No.: (074) 442-3071 Website: www.ubaguio.edu E-mail Address: sit@e.ubaguio.edu

SYSTEMS ADMINISTRATION
1st Semester SY 2024-2025
Midterm Examination

SCORE: Loc-40, Lab-48

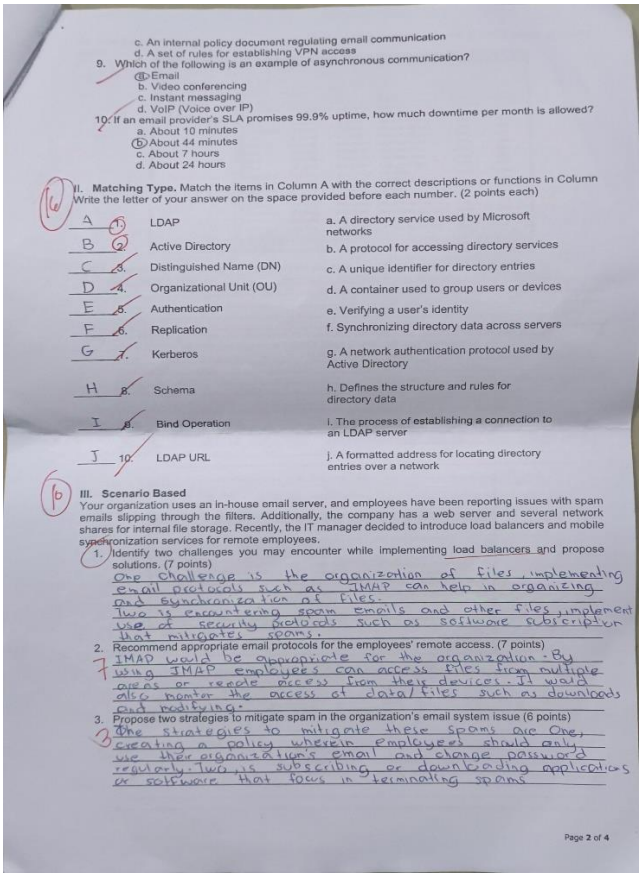
Name: Sueno, Johnroy V.
Course and Year: BSIT - 3rd
Date: 11/07/24
Section: IDC2

GENERAL INSTRUCTIONS
1. Use blue or black permanent ink for answering.
2. Mind your own test papers. Anyone caught cheating will automatically be given a 0 in his/her test, suspended or expelled as stated in the Students Handbook, Article XIII Section 1Bc.
3. Turn off ALL gadgets.
4. If there are any questions or concerns, approach the proctor/instructor.

I. Multiple Choice. Read each question carefully and select the best answer. Encircle the letter of your answer. (2 points each) — 14

1. Which of the following is an example of Software-as-a-Service (SaaS)?
   a. Microsoft Office installed on your computer
   b. Google Workspace (Docs, Sheets, Drive)
   c. Linux distribution like Ubuntu
   d. Dropbox cloud storage service
2. Which communication service is primarily used for real-time messaging and file sharing within organizations?
   a. Email
   b. Voice over IP (VoIP)
   c. Instant Messaging (IM)
   d. File Transfer Protocol (FTP)
3. Which email protocol is most suitable for accessing emails from multiple devices while keeping them synchronized?
   a. POP3
   b. SMTP
   c. IMAP
   d. FTP
4. What is the main role of SMTP in email communication?
   a. Receiving emails from a client device
   b. Synchronizing emails across multiple devices
   c. Sending emails from the client to the mail server
   d. Storing emails on the user's local machine
5. Which clause in a EULA explains what the user is not allowed to do with the software?
   a. Scope of Use
   b. Restrictions
   c. Intellectual Property
   d. Termination
6. What is the purpose of an SLA in service agreements?
   a. To transfer software ownership to the user
   b. To guarantee a specific level of service performance
   c. To restrict user behavior under certain terms
   d. To specify the duration of software usage rights
7. Which protocol is used to download emails from a server to a local client, often deleting them from the server in the process?
   a. IMAP
   b. POP3
   c. SMTP
   d. LDAP
8. Which of the following describes an EULA (End-User License Agreement)?
   a. A legal agreement between service providers and customers about uptime guarantees
   b. A contract that specifies how software can and cannot be used by the user

Page 1 of 4



   c. An internal policy document regulating email communication
   d. A set of rules for establishing VPN access
9. Which of the following is an example of asynchronous communication?
   a. Email
   b. Video conferencing
   c. Instant messaging
   d. VoIP (Voice over IP)
10. If an email provider's SLA promises 99.9% uptime, how much downtime per month is allowed?
   a. About 10 minutes
   b. About 44 minutes
   c. About 7 hours
   d. About 24 hours

II. Matching Type. Match the items in Column A with the correct descriptions or functions in Column B. Write the letter of your answer on the space provided before each number. (2 points each) — 16

A	1.	LDAP	a. A directory service used by Microsoft networks
B	2.	Active Directory	b. A protocol for accessing directory services
C	3.	Distinguished Name (DN)	c. A unique identifier for directory entries
D	4.	Organizational Unit (OU)	d. A container used to group users or devices
E	5.	Authentication	e. Verifying a user's identity
F	6.	Replication	f. Synchronizing directory data across servers
G	7.	Kerberos	g. A network authentication protocol used by Active Directory
H	8.	Schema	h. Defines the structure and rules for directory data
I	9.	Bind Operation	i. The process of establishing a connection to an LDAP server
J	10.	LDAP URL	j. A formatted address for locating directory entries over a network

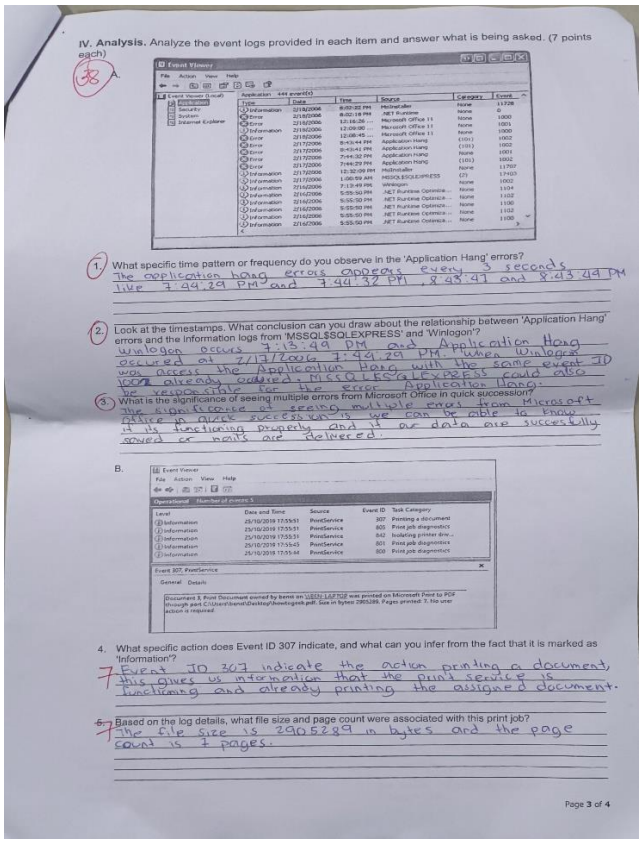
III. Scenario Based — 10

Your organization uses an in-house email server, and employees have been reporting issues with spam emails slipping through the filters. Additionally, the company has a web server and several network shares for internal file storage. Recently, the IT manager decided to introduce load balancers and mobile synchronization services for remote employees.

1. Identify two challenges you may encounter while implementing load balancers and propose solutions. (7 points) — 7
   One challenge is the organization of files, implementing email protocols such as IMAP can help in organizing and synchronization of files.
   Two is encountering spam emails and other files, implement use of security protocols such as software subscription that mitigates spams.
2. Recommend appropriate email protocols for the employees' remote access. (7 points) — 7
   IMAP would be appropriate for the organization. By using IMAP employees can access files from multiple areas or people access from these devices. It would also monitor the access of data/files such as downloads and modifying.
3. Propose two strategies to mitigate spam in the organization's email system issue (6 points) — 3
   The strategies to mitigate these spams are One, creating a policy wherein employees should only use their organization's email and change password regularly. Two, is subscribing or downloading applications or software that focus in terminating spams.

Page 2 of 4

Midterm Exam: Laboratory



IV. Analysis. Analyze the event logs provided in each item and answer what is being asked. (7 points each) — 28

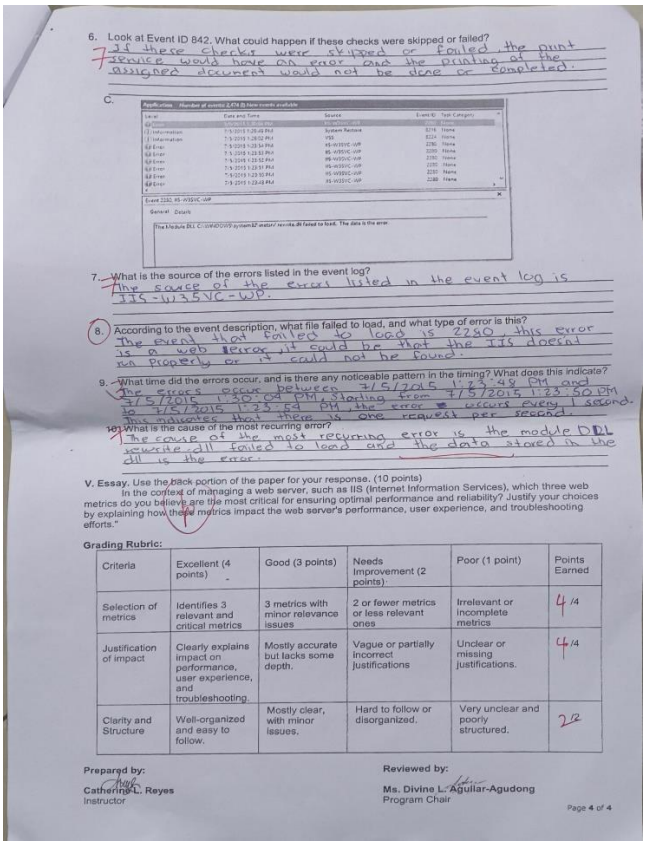
A.

1. What specific time pattern or frequency do you observe in the 'Application Hang' errors?
   The application hang errors appears every 3 seconds like 7:44:29 PM and 7:44:32 PM, 8:43:41 and 8:43:44 PM
2. Look at the timestamps. What conclusion can you draw about the relationship between 'Application Hang' errors and the information logs from 'MSSQL$SQLEXPRESS' and 'Winlogon'?
   Winlogon occurs 7:13:49 PM and Application Hang occured at 7/13/2006 7:44:29 PM when Winlogon was access the Application Hang with the same event ID 1002 already caused MSSQL$SQLEXPRESS could also be responsible for the error Application Hang.
3. What is the significance of seeing multiple errors from Microsoft Office in quick succession?
   The significance of seeing multiple errors from Microsoft Office in quick succession is we can be able to know if its functioning properly and if or data are successfully saved or mails are delivered.

B.

4. What specific action does Event ID 307 indicate, and what can you infer from the fact that it is marked as 'Information'?
   Event ID 307 indicate the action printing a document, this gives us information that the print service is functioning and already printing the assigned document.
5. Based on the log details, what file size and page count were associated with this print job?
   The file size is 2905289 in bytes and the page count is 1 pages.

Page 3 of 4



6. Look at Event ID 842. What could happen if these checks were skipped or failed?
   If these checks were skipped or failed, the print service would have an error and the printing of the assigned document would not be done or completed.

C.

7. What is the source of the errors listed in the event log?
   The source of the errors listed in the event log is IIS-W3SVC-WP.
8. According to the event description, what file failed to load, and what type of error is this?
   The event that failed to load is 2250, this error is a web error, it could be that the IIS doesn't run Properly or it could not be found.
9. What time did the errors occur, and is there any noticeable pattern in the timing? What does this indicate?
   The errors occur between 7/5/2015 1:23:49 PM and 7/5/2015 1:50:04 PM, starting from 7/5/2015 1:23:50 PM to 7/5/2015 1:23:54 PM, the error occurs every 1 second. This indicates that there is one request per seconds.
10. What is the cause of the most recurring error?
    The cause of the most recurring error is the module DDL source call failed to load and the data stored in the dll is the error.

V. Essay. Use the back portion of the paper for your response. (10 points)
In the context of managing a web server, such as IIS (Internet Information Services), which three web metrics do you believe are the most critical for ensuring optimal performance and reliability? Justify your choices by explaining how these metrics impact the web server's performance, user experience, and troubleshooting efforts."

Grading Rubric:

Criteria	Excellent (4 points)	Good (3 points)	Needs Improvement (2 points)	Poor (1 point)	Points Earned
Selection of metrics	Identifies 3 relevant and critical metrics	3 metrics with minor relevance issues	2 or fewer metrics or less relevant ones	Irrelevant or incomplete metrics	4/4
Justification of impact	Clearly explains impact on performance, user experience, and troubleshooting.	Mostly accurate but lacks some depth.	Vague or partially incorrect justifications	Unclear or missing justifications.	4/4
Clarity and Structure	Well-organized and easy to follow.	Mostly clear, with minor issues.	Hard to follow or disorganized.	Very unclear and poorly structured.	2/2

Prepared by:
Catherine L. Reyes
Instructor

Reviewed by:
Ms. Divine L. Aguilar-Agudong
Program Chair

Page 4 of 4

1. The three web metrics that would be critical for ensuring optima performance and reliability would be Average Response Time, Memory Usage and Error Rate. Average response time because we must consider to monitor if the web server is running smoothly, slow or fast response and how long does it take for each event to be completed. Memory usage because we must monitor if the memory usage is too high or low to ensure smooth performance, reduce errors and traffics. Error rate because if the error rate exceeds 15%, I would be considered as above average and it would affect other events and reduce the server performance.

Finals Lecture:

Assignment 1:

UNIVERSITY OF Baguio
SCHOOL OF INFORMATION AND TECHNOLOGY

NAME: Magno, Ronnie L. Sueno, Johnray K.	DATE PERFORMED: 11/28/2024	
Section: IDC2	DATE SUBMITTED: 11/28/2024	/50

SYSADM1 – Capacity Management & Planning

Part 1. A Simulated Dataset for Capacity Planning Exercise

Scenario: A mid-sized e-commerce website is expecting a significant surge in traffic due to an upcoming holiday sale.

Date	Time	CPU Utilization (%)	Memory Utilization (%)	Network In (Mbps)	Network Out (Mbps)	Response Time (ms)
2023-11-20	09:00 AM	25	50	100	50	200
2023-11-20	12:00 PM	40	60	150	75	250
2023-11-20	03:00 PM	60	70	200	100	300
2023-11-20	06:00 PM	35	55	125	60	225

Projected Traffic Increase

- **Expected Peak Traffic:** 5x the normal peak traffic
- **Peak Time:** 12:00 PM - 3:00 PM on the sale day

System Specifications

- **Server Count:** 5
- **CPU Cores per Server:** 8
- **RAM per Server:** 32GB
- **Network Bandwidth per Server:** 1Gbps

Additional Considerations

- **New Product Launch:** A highly anticipated product will be released during the sale.
- **Marketing Campaign:** A major marketing campaign will be launched to promote the sale.

- **Potential Cyber Threats:** Increased traffic can attract malicious actors.

Tasks:

1. Review the provided server performance data and identify potential bottlenecks.

CPU Usage: At 9:00 AM, the CPU is only 25% used, but by 3:00 PM, it's already at 70%. If traffic increases by 5x, the CPU usage will likely exceed 100%, causing servers to slow down or crash.

Memory Usage: Memory usage also rises from 50% at 9:00 AM to 70% at 3:00 PM. A huge increase in users will likely push memory usage to its limit, making the system unstable or unresponsive.

Bandwidth Usage: At 3:00 PM, the servers are handling 200 Mbps in and 100 Mbps out, which is still within the 1 Gbps limit. However, with 5x traffic, this will easily exceed the limit, leading to slow loading times or failed connections.

Response Time: The response time starts at 200 ms in the morning but increases to 300 ms by 3:00 PM. This shows the servers are already struggling with higher traffic. During the sale, the response time could increase even more, frustrating customers and causing them to leave the site.

Cybersecurity Risks: High traffic can attract hackers or malicious attacks like DDoS. If we don't prepare for this, the website could go offline during the most critical hours.

Key Bottlenecks:

1. CPU Usage: The servers may not handle the processing demands of 5x traffic.
2. Memory Limits: Insufficient RAM could cause crashes or slow performance.
3. Bandwidth Saturation: Increased data transfer during peak hours could overwhelm the network.
4. Response Time: Longer delays could hurt user experience and sales.
5. Cyber Threats: High traffic may attract DDoS attacks or other malicious activities, leading to system instability.

Proposed Solutions

1. **Add More Servers**
   - To handle the extra traffic, we could add more servers to increase the total CPU, RAM, and bandwidth available. For example, adding two extra servers would boost our overall capacity by 40%. This will ensure that the website doesn't crash under heavy traffic.
2. **Upgrade Current Servers**
   - If adding servers is too expensive, we could upgrade the existing ones. For instance, we could replace the CPUs with higher-performance models or add more RAM to each server. This is a cheaper option than adding servers but may not handle traffic as effectively as scaling horizontally.
3. **Use a Content Delivery Network (CDN)**
   - A CDN stores copies of static content (like images, CSS, and JavaScript) on multiple servers across different locations. When users visit the website, they'll download these files from the nearest CDN server, which reduces the load on our main servers and speeds up the site for users.

4. **Implement Load Balancers**
   - Load balancers distribute incoming traffic evenly across all servers. This prevents any single server from becoming overwhelmed. It also improves response times because user requests are directed to the least busy server.
5. **Strengthen Cybersecurity**
   - We should install firewalls, set up DDoS protection, and monitor traffic in real-time. This will help block malicious traffic and protect the website during the sale.
6. **Perform Stress Testing**
   - Before the sale, we should simulate a 5x traffic surge to test how well the system handles it. This will help us identify and fix any weak points in advance.

2. Discuss the pros and cons of each proposed solution by filling out the table below.

Evaluation of Solutions

Proposed Solution	Pros	Cons	Cost	Complexity	Impact on Performance
Adding More Servers	- Increases capacity for traffic. - Reduces risk of system crashes.	- Expensive to buy and maintain. - Time-consuming to set up.	High	Medium	High: Ensures system stability under heavy load.
Upgrading Existing Servers	- Cheaper than adding new servers. - Faster to implement.	- Limited scalability. - May not be sufficient for extreme traffic.	Medium	Low	Medium: Improves capacity but not ideal for 5x surge.
Using a CDN	- Reduces load on main servers. - Improves website loading speed for users worldwide.	- Requires setup and configuration. - Ongoing costs based on usage.	Medium	Medium	High: Speeds up content delivery for global users.
Implementing Load Balancers	- Ensures even distribution of traffic. - Improves system stability and response time.	- Requires careful setup and maintenance. - Adds complexity to system architecture.	Medium	Medium	High: Prevents bottlenecks and improves response time.
Strengthening Cybersecurity	- Protects system from attacks (e.g., DDoS). - Ensures website remains secure during high-traffic	- Additional tools and expertise are required. - Increases setup and monitoring costs.	High	High	High: Prevents downtime and maintains customer trust.
Performing Stress Testing	- Identifies weak points before the actual sale. - Ensures the system is prepared for high traffic.	- Time-consuming and requires team effort.	Low	Medium	High: Helps prevent unexpected issues on sale day.

Grading Rubric:

Criteria	Excellent | 10pts	Good | 7pts	Needs Improvement | 4pts
Problem Identification	Accurately identifies the primary problem and provides a detailed explanation.	Identifies the main problem and provides a basic explanation.	Identifies a problem but lacks clarity or accuracy.
Solution Proposal	Proposes multiple relevant solutions and provides detailed explanations, including potential drawbacks and benefits.	Proposes one or two relevant solutions but lacks detailed explanation.	Proposes a solution but lacks feasibility or relevance.
Evaluation of Solutions	Provides a thorough evaluation of the proposed solutions, considering factors like cost, complexity, and potential impact.	Provides a basic evaluation of the proposed solutions, but lacks depth.	Does not evaluate the proposed solutions or provides a superficial evaluation.
		Score:	/30

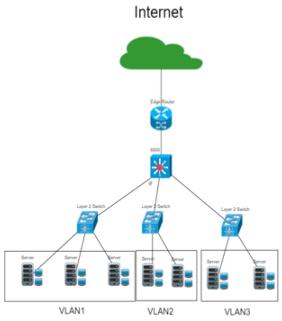
Assignment 2:

UNIVERSITY OF BAGUIO
SCHOOL OF INFORMATION AND TECHNOLOGY

NAME: Magno, Ronnie L. Sueno, Johnray K.	DATE PERFORMED: 12/05/24	
Section: IDC2	DATE SUBMITTED: 12/05/24	/50

Part 2. Network Scalability Analysis

Recall the e-commerce website scenario we discussed earlier. Given the expected surge in traffic, analyze the provided network topology diagram. Identify potential bottlenecks and areas where scalability might be a concern. Propose specific strategies to improve the network's scalability and performance to ensure a seamless user experience during the peak traffic period. Consider factors such as increased user demand, new applications, and security threats.



Potential Bottlenecks:

- **Bandwidth Constraints on Uplinks:** The uplinks connecting Layer 2 switches to the Core Switch or the Core Switch to the Edge Router might not have sufficient bandwidth, especially if they are using older technologies like 1 Gbps Ethernet, limiting the overall throughput and causing delays during peak traffic.
- **Lack of Redundancy:** The network lacks redundant links between critical components such as routers, switches, and servers. A single point of failure, such as a broken link or hardware malfunction, could lead to significant downtime and service disruption.
- **Scalability Limits:** As user demand grows, the current architecture may not support adding more devices or servers without significant reconfiguration. Limited capacity in the current switch model could also restrict the ability to scale VLANs or handle additional traffic efficiently.
- **Inter-VLAN Traffic Congestion:** High inter-VLAN traffic would rely heavily on the Core Switch for routing, increasing its load and reducing performance. This issue can become particularly problematic if applications or services in different VLANs communicate frequently.
- **Security Vulnerabilities (No Firewalls)**:
  Without firewalls, the network is directly exposed to external threats through edge routers. The lack of traffic filtering or inspection creates the following risks:
  1. **External Attacks**: Vulnerability to unauthorized access, malware, and DDoS attacks.
  2. **Internal Threats**: Devices within one VLAN can potentially compromise devices in other VLANs if ACLs and VLAN isolation are not effectively configured.
  3. **Unrestricted Traffic**: Inbound and outbound traffic are not thoroughly inspected, allowing malicious packets to traverse the network undetected.

- **Security Processing Delays:** Increased security processing for monitoring and filtering traffic in a high-demand environment can slow down packet forwarding and response times if security measures like intrusion detection/prevention systems are not scaled appropriately. The absence of firewalls places a greater burden on edge routers to handle basic security tasks like ACLs and intrusion detection. If these systems are not scaled appropriately, they can slow down packet forwarding and response times.

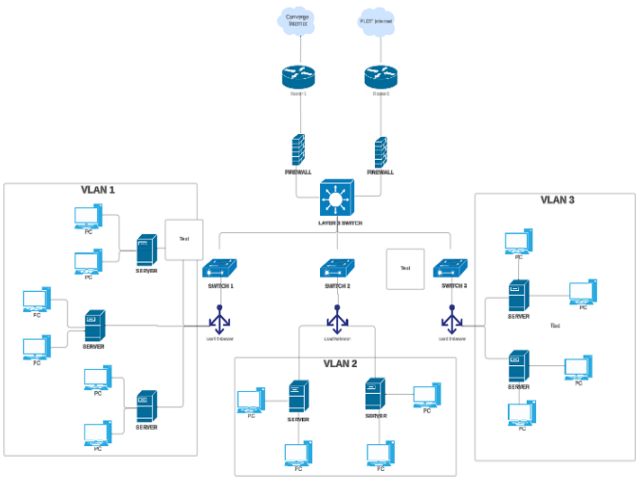
SOLUTION:

To improve the scalability and performance of the network, several strategies are recommended, focusing on both hardware enhancements and software configurations. First, the deployment of dual edge routers connected to Converge and PLDT ISPs with failover capabilities ensures reliable internet connectivity. This setup minimizes the risk of downtime by providing load balancing and redundancy, effectively addressing potential failures. The existing Layer 3 core switch will remain central to the network, handling inter-VLAN routing efficiently without the need for upgrading the Layer 2 access switches. To further enhance network performance, high-speed 10Gbps uplinks should be implemented between the core switch and both the edge routers and the Layer 2 access switches. These uplinks will accommodate increased traffic volumes, reducing congestion and ensuring faster data transfers, especially during peak periods.

Load balancing is crucial for VLAN 1, where multiple servers handle user requests. Installing load balancers will distribute traffic evenly among the servers, preventing overload and improving response times. Security is also a priority, and the addition of redundant firewalls between the edge routers and the core switch will protect the network from external threats. Also, VLAN isolation and the implementation of Access Control Lists (ACLs) on the Layer 3 core switch will safeguard sensitive resources and restrict unauthorized access. To proactively monitor and manage network performance, integrating tools like SNMP will enable real-time tracking, allowing IT personnel to identify and address potential bottlenecks promptly.

While these strategies significantly improve scalability, reliability, and performance, they also present challenges. Upgrades such as 10Gbps uplinks, load balancers, and firewalls involve considerable costs, which may affect limited budgets. Additionally, the increased complexity of managing redundant systems, load balancers, and monitoring tools requires skilled IT staff to ensure smooth operations. Despite these challenges, this proposed design effectively prepares the network for future growth and peak traffic demands while maintaining a secure and reliable infrastructure.

Proposed Network Design



Criteria	Excellent | 10pts	Good | 7pts	Needs Improvement | 4pts
Network Analysis	Accurately identifies potential bottlenecks, security risks, and capacity limitations.	Identifies key network components and some potential bottlenecks.	Identifies some basic network components but lacks a comprehensive analysis.
Scalability Planning	Proposes multiple relevant solutions and provides detailed explanations, including potential drawbacks and benefits.	Proposes some relevant scalability strategies but lacks detail.	Proposes limited scalability strategies.
Evaluation of Solutions	Proposes comprehensive scalability strategies, including specific recommendations for hardware upgrades, software configurations, and network optimizations.	Provides a basic evaluation of the proposed solutions, but lacks depth.	Does not evaluate the proposed solutions or provides a superficial evaluation.
Proposed Design	Provides a detailed and well-justified design, including network diagrams, configuration details, and implementation plans.	Provides a basic design but lacks specific details and justifications.	Does not provide a clear and detailed design.
Evaluation and Justification	Provides a thorough evaluation of the proposed solutions, considering factors like cost, complexity, and potential impact.	Provides a basic evaluation of the proposed solutions, but lacks depth.	Does not evaluate the proposed solutions or provides a superficial evaluation
		Score:	/50

Seatwork 1:

UNIVERSITY OF Baguio

SCHOOL OF INFORMATION AND TECHNOLOGY

NAME: Sueno, Johnray K.	DATE PERFORMED: 11/05/2024	
Section: IDC2	DATE SUBMITTED: 11/05/2024	

SYSADM1 – Acceptable Use Policy

1. Revisit the policy you drafted for TechLease
2. Based on comments, edit the Acceptable Use Policy (AUP) that aligns with the company's profile and addresses its unique requirements by providing details to the following sections.

Acceptable Use Policy (AUP)	1. Purpose and Scope (Explain the intent of the policy, emphasizing that the policy supports TechLease's mission to provide accessible, reliable technology for students and educators.) Specify who this policy applies to (all TechLease users, including students and teaching staff renting devices and accessories).
	2. General Usage Guidelines 2.1 Permitted Uses 2.2 Prohibited Uses
	3. Device Care and Maintenance 3.1 User Responsibilities 3.2 Prohibited Actions 3.3 Consequences of Neglect
	4. Data Security and Privacy 4.1 User Data 4.2 Privacy Compliance
	5. Penalties for Policy Violations 5.1 Consequences
	6. Appeal Process (Offer a way to appeal penalties if users believe they were unfairly penalized)

*** Attach the commented or checked Organizational Policy draft

Grading Rubric

Criteria	Exemplary (10 pts)	Proficient (7 points)	Developing (4 points)	Incomplete (2 points)
Purpose and Scope	Clearly defines the policy's purpose and scope, fully aligning with TechLease's mission and goals.	Defines the purpose and scope with minor misalignments to TechLease's mission or goals.	Partially defines the purpose and scope, with vague or limited connection to TechLease's mission or goals.	Missing or fails to address purpose and scope.
General Usage Guidelines	Provides detailed permitted and prohibited uses, aligned with educational and acceptable use standards for TechLease devices.	Lists general permitted and prohibited uses but lacks specific examples or full alignment with TechLease's educational focus.	Mentions permitted and prohibited uses but lacks depth or relevance to TechLease's mission.	Missing or lacks clear usage guidelines.
Device Care and Maintenance	Clearly outlines user responsibilities, prohibited actions, and consequences for device misuse, with specific and practical guidance.	Outlines basic responsibilities and prohibited actions but lacks some detail or specificity.	Lists some responsibilities or consequences but lacks thoroughness and clarity.	Missing or unclear expectations for device care.
Data Security and Privacy	Comprehensively addresses data security, privacy, and TechLease's compliance with laws, emphasizing user data responsibility.	Includes guidelines on data security, privacy, and TechLease's compliance with laws, emphasizing user data responsibility.	Mentions data security or privacy but provides limited information on data security and privacy but lacks comprehensive guidelines.	Mentions data security or privacy, but guidelines are incomplete or vague.	Missing or lacks information on data security.
Penalties for Policy Violations	Clearly specifies consequences for violations and outlines an appeal process, with penalties that align with the severity of misuse.	Clearly specifies consequences for violations and outlines an appeal process, with penalties that align with the severity of misuse.	Lists general penalties but lacks an appeal process or detailed consequence guidelines.	Mentions penalties for violations but lacks detail or clarity on the appeals process.	Missing or lacks penalties for violations.
Appeal Process	Provides a clear, fair, and accessible appeal process for users to contest penalties, with well-defined steps for submitting appeals.	Includes a basic appeal process but lacks some detail or fairness considerations.	Includes a basic appeal process but lacks some detail or fairness considerations.	Mentions an appeal process but lacks clarity or specific steps.	Missing or lacks an appeal process.
Score:	/60			

1. Purpose and Scope

The TechLease Acceptable Use Policy is the set of rules and guidelines to be followed for responsible use of technology provided by TechLease. Dedicated to offering accessible, reliable, and high-quality technology solutions, our mission is to empower students and educators by providing affordable devices that enhance their academic success. This policy ensures that all users employ responsible and ethical practices in using rented devices and accessories in promoting a secure, productive, and educational environment.

Scope:
The renting devices, accessories, or other technologies from TechLease are subject to the policy and include students, teachers, school administrators, and other users who are given access or use their services.

2. General Usage Guidelines

2.1 Permitted Uses

TechLease devices and accessories are intended for educational purposes and activities. The following uses are permitted:

- **Educational Use:** Devices may be used to access learning materials, conduct research, complete assignments, and collaborate on academic projects.
- **Communication:** Devices can be used to communicate with educators, peers, and academic groups through approved platforms (e.g., email, educational apps).
- **Academic Support:** Devices may be used for additional learning tools, such as online tutoring, practice exercises, or educational games that aid academic growth.
- **Limited Personal Use:** Personal use is permitted as long as it does not interfere with the educational purpose or violate other parts of this policy.

2.2 Prohibited Uses

The following activities are prohibited when using TechLease devices and services:

- **Illegal Activities:** Engaging in illegal activities such as accessing pirated content, hacking, or distributing malware.
- **Inappropriate Content:** Accessing or distributing explicit, offensive, or discriminatory material, including pornography, hate speech, and harmful content.
- **Non-Educational Use:** Using the devices for non-academic purposes such as excessive gaming, personal business, or entertainment not related to educational activities.
- **Device Misuse:** Modifying or tampering with the devices' software or hardware, including installing unauthorized applications, attempting to bypass security protocols, or altering configurations.
- **Disruption of Services:** Using the devices or network in a manner that disrupts or degrades the service for others (e.g., launching denial-of-service attacks, spreading viruses).

3. Device Care and Maintenance

3.1 User Responsibilities

Users must handle TechLease devices with care and take the following steps to maintain the devices in good working condition:

- **Physical Care:** Keep devices free from physical damage by avoiding exposure to extreme conditions (e.g., moisture, high heat, direct sunlight). Use protective covers or cases when necessary.
- **Software and Security:** Ensure that devices are regularly updated with the latest software updates and security patches provided by TechLease. Do not install unauthorized software or apps.
- **Proper Charging:** Users should ensure devices are charged and ready for use and return devices with sufficient battery life when applicable.

3.2 Prohibited Actions

Users must avoid the following actions to prevent damage or misuse of the devices:

- **Physical Damage:** Avoid dropping, spilling liquids, or exposing devices to harsh environments.
- **Tampering with Device Settings:** Do not alter device configurations, bypass security measures, or install unauthorized software or applications that could harm the device or compromise its functionality.
- **Unauthorized Repair:** Users should not attempt to repair or modify devices themselves. All technical issues should be reported to TechLease for proper handling.

3.3 Consequences of Neglect

Failure to maintain the device properly or misuse of the device will result in penalties, including but not limited to:

- **Repair Fees:** Users may be charged for repairs or replacement costs due to device damage caused by negligence.
- **Suspension of Device Access:** Repeated or severe misuse may result in temporary or permanent suspension of rental privileges.
- **Financial Penalties:** In cases of excessive damage or loss, users may be required to pay full replacement costs for devices.

4. Data Security and Privacy

4.1 User Data

TechLease is committed to protecting user privacy and maintaining the security of personal and

- **Protect Login Information:** Users should not share their login credentials or personal information with others.
- **Use Secure Networks:** Devices should be used on trusted and secure networks to avoid data breaches.
- **Data Storage:** Users should avoid storing personal or sensitive data on rented devices unless required for academic use.

4.2 Privacy Compliance

TechLease adheres to all relevant privacy laws, including the **Data Privacy Act of 2012** in the Philippines. We are committed to protecting the privacy of our users by ensuring:

- **No Unauthorized Sharing:** Personal data, including academic or financial information, will not be shared with third parties without the user's consent, except as required by law.
- **Confidentiality:** TechLease will implement safeguards to ensure the confidentiality and security of all data accessed or processed through rented devices.

5. Penalties for Policy Violations

5.1 Consequences

Violations of this Acceptable Use Policy may lead to penalties that vary depending on the severity of the infraction:

- **Warnings:** Minor infractions may result in a written warning.
- **Suspension of Service:** Users who repeatedly violate the AUP may face temporary or permanent suspension of their rental privileges.
- **Fines and Restitution:** Users may be held financially accountable for damages or losses resulting from misuse or neglect of rented devices.
- **Legal Action:** In cases of illegal activities, TechLease reserves the right to report the incident to appropriate authorities, which could lead to legal action.

5.2 Late Return Penalty

A late fee of ₱500 per week will be charged for each week the device is returned past the due date. For example, a 2-week late return will incur a ₱1,000 fee.

5.3 Damage or Loss of Device

Customers are responsible for any damage, loss, or theft of rented devices. Fees range from ₱1,000 - ₱5,000 for damage and ₱10,000 - ₱50,000 for full replacement costs in cases of severe damage or loss.

5.4 Failure to Remove Personal Data

Before returning a device, customers must delete all personal files and log out of accounts. Failure to do so will result in a cleaning fee of ₱1,000 - ₱3,000.

6. Appeal Process

Users who believe that they have been unfairly penalized may file an appeal through the following process:

1. **Submit a Written Appeal:** Users must submit a written appeal within 10 business days of receiving a penalty. The appeal should include a detailed explanation of why the penalty should be reconsidered.
2. **Review of Appeal:** A TechLease representative will review the appeal and the circumstances

3. **Decision:** After reviewing the appeal, the user will be informed of the final decision. If the appeal is accepted, the penalty will be adjusted or removed. If the appeal is denied, the original penalty will stand.

POLICIES:

1. The rental period of each technology device is one month. If the technology device is not returned on or before the end, an additional late fee is applied. For every week that exceeds the rental period, a late fee of ₱500 per week is applied. For example, if a student rents a laptop for 1 month but returns it 2 weeks late from the date, there would be a late fee of ₱1,000 because those extra weeks cost ₱500 a week. If an educator rents a tablet for 1 month but returns it 3 weeks late, he or she would be charged an extra ₱1,500 because there is an additional fee of ₱500 per week for 3 weeks.

2. All rented devices must be well cared for by the clients and maintained in good condition and only utilized for educational purposes. Damaged, lost, or stolen device costs additional fees. Cuts or dents, minor damages will be charged ₱1,000 - ₱3,000 while moderate damage which is screen broken or other hardware malfunction, fees range from ₱3,000 - ₱5,000. In cases wherein the damage is not recoverable, for example in cases of water damages or unrecoverable damage, replacement cost is justified in order to pay for it; depending on the device it ranges between ₱10,000 to ₱50,000. In case that a lost or stolen phone occurred, the customer will be shouldered the full replacement cost. However, if preventive measures like using protective case and preventing the devices to come close to liquids as well as being exposed to extreme conditions were done, customers won't have to suffer those additional charges. All damages must be reported immediately to TechLease so as not to exacerbate any problem. Any damage, loss, or theft will be returned and paid by the customer for any repairs or replacements during their lease period.

3. Customers are allowed to rent a maximum of three devices at a time. This policy is in place to ensure that all customers have access to the technology they need, while maintaining fair availability of devices across our rental pool. If a customer wishes to rent additional devices, they must return one or more of their current rentals before renting new ones.

4. Downloading and installing applications that may harm the rented technology, such as those that contain malware, corrupt files, or harmful viruses, is strictly prohibited. Customers should only install apps that are necessary for academic use and must ensure that these applications come from trusted sources, such as official app stores (Google Play Store, Apple App Store, or approved educational platforms). Unauthorized or third-party apps that may compromise device security, such as file-sharing programs, unverified game downloads, or apps that interfere with the device's functionality, are not allowed. TechLease recommends using only essential, educational apps to ensure the safety and proper functioning of the rented devices.

5. Before returning any rented devices, customers are required to delete all personal files, including documents, images, PowerPoint presentations, videos, and any other stored data. Additionally, all social media accounts and personal profiles must be logged out, and no personal credentials (such as social media accounts or email login information) should be saved on the device. Customers must ensure that all downloaded files, applications, and browser history are completely removed to protect their privacy and security. Failure to follow these guidelines may result in an additional cleaning fee of ₱1,000 to ₱3,000, depending on the extent of the data removal required, or other penalties as deemed necessary by TechLease.

Quiz 1:

UNIVERSITY OF BAGUIO
SCHOOL OF INFORMATION AND TECHNOLOGY

NAME: Sueno, Johnray K.	DATE PERFORMED: 11/21/2024	
Section: IDC2	DATE SUBMITTED: 11/21/2024	

WINDOWS ADMINISTRATIVE TOOLS

Read the case study presented below and answer the questions after reading the case study.

Cybersecurity Resilience: TechGuard Solutions' Recovery Disk Strategy in Action

TechGuard Solutions, a medium-sized cybersecurity firm, recently encountered a malware attack that put its systems and sensitive client information at risk. This case study explores how TechGuard Solutions solved this crisis, highlighting the pivotal role of their comprehensive recovery disk strategy.

TechGuard Solutions discovered signs of a malware attack during a routine cybersecurity audit. The malware, equipped with ransomware capabilities, posed a significant threat to the confidentiality and integrity of client data. The incident prompted a reevaluation of the company's preparedness and response mechanisms.

Prior to the incident, TechGuard Solutions had implemented a series of proactive measures. Robust cybersecurity protocols, routine system audits, and employee training programs formed the foundation of the company's preemptive approach. The incident emphasized the importance of foreseeing and preparing for potential threats in an industry where the stakes are high. A linchpin of TechGuard Solutions' preparedness was its comprehensive recovery disk strategy.

Crafted meticulously, these recovery disks went beyond standard restoration tools. They included offline backup copies of critical client databases and proprietary threat intelligence. The recovery disk strategy aimed to provide a swift and effective response in the face of a cybersecurity crisis. When the malware attack unfolded, the IT security team at TechGuard Solutions swiftly used the recovery disks.

Booting the infected workstations in an isolated environment prevented the malware from spreading further within the company's network. The recovery disks, equipped with decryption tools specific to the ransomware, played a critical role in decrypting and restoring files from offline backups. The inclusion of offline backups on the recovery disks proved pivotal in ensuring data protection during the ransomware attack. With redundant copies of critical client data stored offline, TechGuard Solutions efficiently restored files without being pressured into letting the attackers' get critical information in their own system.

This not only minimized data loss but also emphasized the strategic importance of data backup in cybersecurity resilience. Following the resolution of the cybersecurity incident, TechGuard Solutions conducted a thorough post-incident analysis. The insights gleaned from this analysis informed the implementation of enhanced security measures. This included regular updates to threat intelligence on the recovery disks and targeted employee training programs to prevent future phishing attempts. The company's commitment to continuous improvement in its cybersecurity protocols shone through. The rapid and effective response to the cybersecurity crisis had a positive impact on client services. By minimizing downtime and swiftly restoring operations, TechGuard Solutions bolstered client confidence and demonstrated a steadfast commitment to safeguarding sensitive information.

Questions to answer:

1. Can you provide a brief overview of the cybersecurity incident that TechGuard Solutions encountered? What were the key challenges and risks posed by the malware attack?
   - The TechGuard Solutions encountered a malware attack that can affect their internal systems and make their sensitive information at risk, posing a significant threat to the confidentiality and integrity of client data.
   - Key Challenges:
     - Data loss can occur.
     - Damage to client's trust and company's reputation.
     - Possible hardware/ Software damaged.
     - Hacked Information.
2. What preventive measures did TechGuard Solutions have in place before the cybersecurity incident occurred? How did the company anticipate and prepare for potential threats?
   - Prior to the attack, TechGuard Solutions implemented several preventive measures to protect against cybersecurity threats. They developed robust cybersecurity protocols to establish secure practices and conducted regular system audits to identify and address vulnerabilities. The company also prioritized employee training programs to ensure staff could recognize and mitigate potential threats like phishing. A key aspect of their preparedness was the creation of a recovery disk strategy designed to respond effectively to worst-case scenarios.
3. Could you elaborate on TechGuard Solutions' recovery disk strategy? What specific components and tools were included in the recovery disks, and how did they contribute to the recovery process?
   - The recovery disks strategy tools:
     - Offline Backup Copies: Redundant copies of critical client databases to ensure data recovery without relying on compromised systems.
     - Decryption Tools specific for Ransomware: Enabled the IT team to decrypt files encrypted by the attack.
     - Proprietary Threat Intelligence: Contained detailed data on potential threats to aid swift action.
4. How was the recovery disk strategy implemented during the cybersecurity crisis? What steps did the IT security team take to isolate infected systems and restore encrypted files?
   - When the attack occurred, the IT security team acted quickly to mitigate and recover compromised systems. They booted infected workstations in an isolated environment to prevent the malware from spreading across the network. The recovery disks were then used to decrypt the ransomware-encrypted files and restore them from secure offline backups.

This approach allowed the company to minimize the impact of the attack while ensuring that operations could resume efficiently.

5. How did the inclusion of offline backups on the recovery disks contribute to data protection during the ransomware attack? Were there any specific challenges or considerations in the file decryption and restoration process?

   ➢ The inclusion of offline backups in the recovery disks played a pivotal role in protecting TechGuard Solutions data during the ransomware attack. Because these backups were stored offline it ensured that the critical client data remained inaccessible to the attackers to ensure data integrity. This allowed the IT team of TechGuard Solutions to recover files without being pressured by the attackers. The decryption and restoration processes must be done requiring careful execution to ensure a minimal data loss and system disruption.

6. Following the resolution of the cybersecurity incident, what steps did TechGuard Solutions take in the post-incident analysis? Were there specific findings that influenced the company's cybersecurity protocols?

   ➢ Following the resolution of the attack, TechGuard Solutions conducted a detailed post-incident analysis to identify vulnerabilities and opportunities for improvement. The analysis revealed gaps in employee awareness such as phishing attempts, and implemented the need for regular updates to recovery disk tools and threat intelligence on the recovery disks. These insights provided a foundation for implementing targeted security enhancements such as employee training programs and refining the company's overall cybersecurity protocols.

7. Can you outline the enhanced security measures implemented by TechGuard Solutions based on the post-incident analysis? How do these measures strengthen the company's cybersecurity posture against future threats?

   ➢ Based on the findings from the post-incident analysis, TechGuard Solutions strengthened its cybersecurity defenses. The company updated its recovery disks to include the latest decryption tools and threat intelligence to address evolving threats. Additional measures such as improving phishing detection through simulated attacks and employee training programs, also enhancing network monitoring systems to detect and isolate threats early. These updates enhanced their ability to respond to future incidents effectively.

8. How did the rapid and effective response to the cybersecurity crisis impact client services and relationships? Did TechGuard Solutions experience any long-term consequences or benefits?

   ➢ The rapid and effective response to the attack had a positive impact on client services and relationships. The company demonstrated its commitment to protecting sensitive client data by minimizing downtime and quickly restoring operations. This proactive approach not only maintain and strengthen client confidence but also enhanced the company's reputation as a reliable and resilient cybersecurity partner. For long-term, these efforts would help in maintaining/bolstering client trust and attracted new business opportunities.

9. Were there specific employee training programs or awareness initiatives implemented to prevent future cybersecurity threats, such as phishing attempts? How is the company ensuring that employees are well-informed and vigilant?

   ➢ To prevent future cybersecurity incidents, TechGuard Solutions introduced enhanced employee training programs focusing on teaching staff how to identify and report phishing attempts and other cyber threats. The company aimed to make its workforce a critical line of defense against future cyber threats by prioritizing employee awareness in this kind of situations.

10. What key lessons did TechGuard Solutions learn from this cybersecurity incident? How has the experience influenced the company's approach to cybersecurity and recovery strategies moving forward?

    ➢ The cybersecurity incident provided TechGuard Solutions with valuable lessons on the importance of preparedness and continuous improvement. It emphasized the need for a robust recovery strategy such as their recovery disks to mitigate risks during attacks. This experience also emphasized the value of updating security protocols regularly and ensuring employees are well-trained in recognizing and responding to threats. This also helped the company committed to maintaining a proactive and adaptive approach to cybersecurity to strengthen its resilience against future challenges.

Finals Laboratory:

Labwork 1:

UNIVERSITY OF BAGUIO SCHOOL OF INFORMATION AND TECHNOLOGY		
NAME: Sueno, Johnray K.	DATE PERFORMED: 11/14/2024	
Section: IDC2	DATE SUBMITTED: 11/14/2024	/50

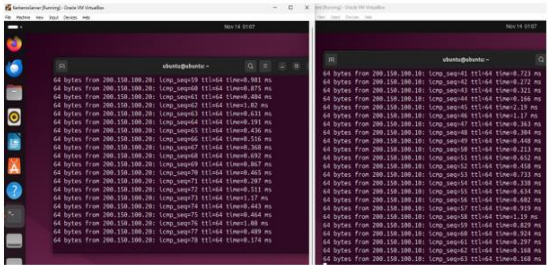
SYSADM1 – Kerberos Lab Activity: A step-by-step Guide

Objective:

Set up a basic Kerberos authentication system to understand how Kerberos manages secure logins through ticket-based access.

Setup Requirements:

- Two VMs in Oracle VM, both running a Linux distribution like Ubuntu or CentOS.
- VM1: Kerberos Server
- VM2: Kerberos Client

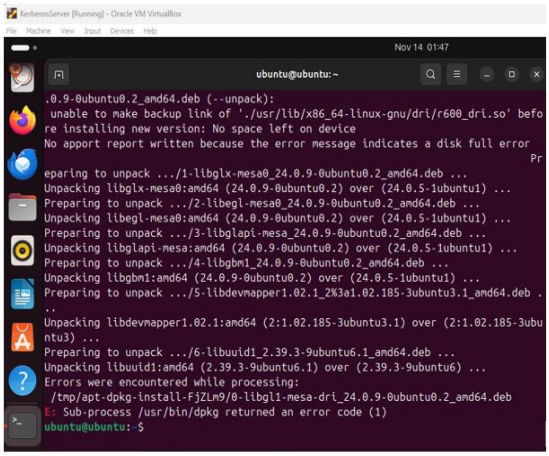


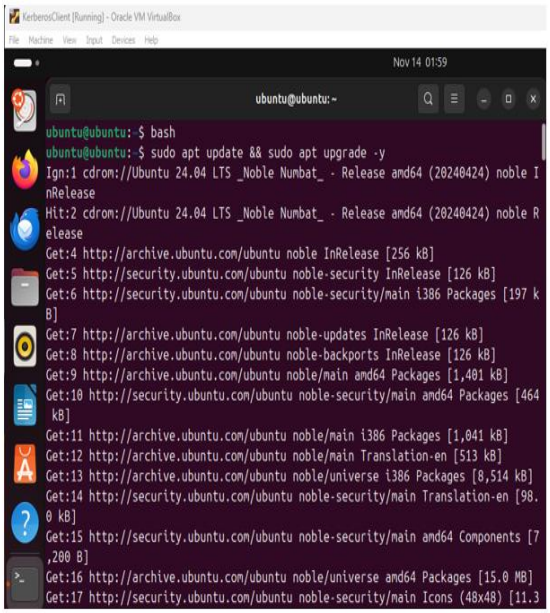
Step 1: Initial Setup and Package Installation

1. **Update Packages on Both VMs:**
   - Open a terminal on each VM and run:

bash

sudo apt update && sudo apt upgrade –y

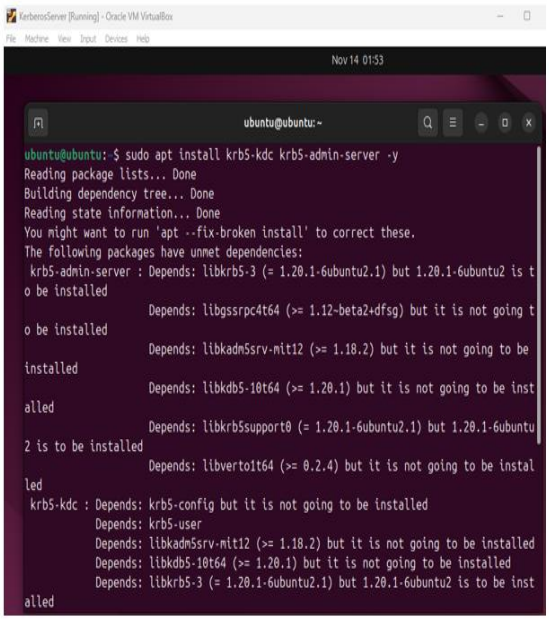




2. **Install Kerberos Server Packages on VM1 (Kerberos Server):**
   - In VM1, install the Kerberos Key Distribution Center (KDC) and admin server:

bash

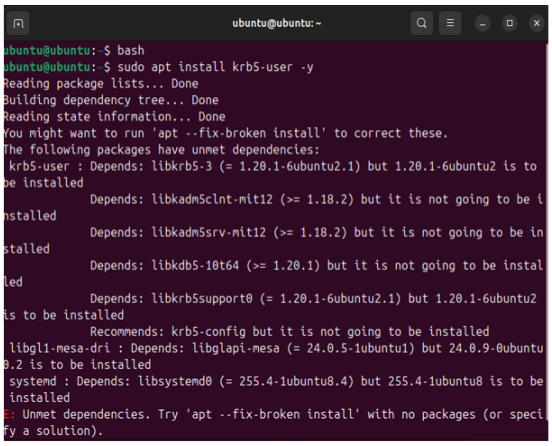
sudo apt install krb5-kdc krb5-admin-server –y



3. **Install Kerberos Client Package on VM2 (Kerberos Client):**
   - In VM2, install the Kerberos client software:

bash

sudo apt install krb5-user –y



   - During installation, when prompted, enter the Kerberos realm you plan to set up, e.g., MYLAB.LOCAL.

Step 2: Configure the Kerberos Server (VM1)

1. **Edit the Kerberos Configuration File:**
   - Open /etc/krb5.conf for editing:

bash

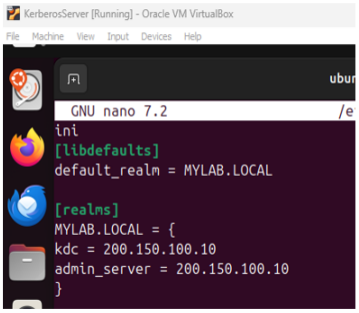
sudo nano /etc/krb5.conf

   - Set the realm as MYLAB.LOCAL. You should also specify the KDC and admin server as VM1's hostname or IP address:

ini

```
[libdefaults]
    default_realm = MYLAB.LOCAL

[realms]
    MYLAB.LOCAL = {
        kdc = <VM1_IP_or_hostname>
        admin_server = <VM1_IP_or_hostname>
    }
```

   - Save and close the file (Ctrl+X, then Y, and Enter to confirm).



2. **Initialize the Kerberos Database:**
   - Create the database for the Kerberos realm:

bash

sudo krb5_newrealm

```
ubuntu@ubuntu:~$ sudo krb5_newrealm
sudo: krb5_newrealm: command not found
```

   - You will be prompted to set a password for the Kerberos database.

3. **Start and Enable the Kerberos Services:**
   - Start the KDC and admin server, and ensure they start automatically on boot:

bash

sudo systemctl start krb5-kdc

sudo systemctl start krb5-admin-server

sudo systemctl enable krb5-kdc

sudo systemctl enable krb5-admin-server

```
ubuntu@ubuntu:~$ sudo systemctl start krb5-kdc
Failed to start krb5-kdc.service: Unit krb5-kdc.service not found.
ubuntu@ubuntu:~$ sudo systemctl start krb5-admin-server
Failed to start krb5-admin-server.service: Unit krb5-admin-server.service not fo
und.
ubuntu@ubuntu:~$ sudo nano /etc/krb5.conf
ubuntu@ubuntu:~$ sudo systemctl start krb5-kdc
Failed to start krb5-kdc.service: Unit krb5-kdc.service not found.
ubuntu@ubuntu:~$ sudo systemctl start krb5-admin-server
Failed to start krb5-admin-server.service: Unit krb5-admin-server.service not fo
und.
ubuntu@ubuntu:~$ enable krb5-kdc
bash: enable: krb5-kdc: not a shell builtin
ubuntu@ubuntu:~$ enable krb5-admin-server
bash: enable: krb5-admin-server: not a shell builtin
```

Step 3: Set Up a Kerberos User Principal

1. **Create a New User Principal:**
   - Run the following command to create a test user in the Kerberos realm:

bash

sudo kadmin.local -q "addprinc testuser@MYLAB.LOCAL"

   - Set a password for testuser.

```
ubuntu@ubuntu:~$ sudo kadmin.local -q "addprinc testuser@MYLAB.LOCAL"
sudo: kadmin.local: command not found
ubuntu@ubuntu:~$
```

2. **Verify the User Principal:**
   - To confirm the principal is created, list all principals:

bash

sudo kadmin.local -q "listprincs"

```
ubuntu@ubuntu:~$ sudo kadmin.local -q "listprincs"
sudo: kadmin.local: command not found
```

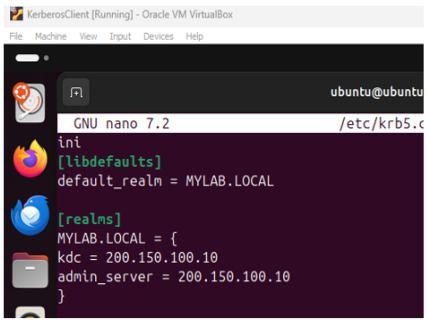
Step 4: Configure the Kerberos Client (VM2)

1. **Edit the Kerberos Configuration File on VM2:**
   - Open /etc/krb5.conf for editing on VM2:

bash

sudo nano /etc/krb5.conf

   - Set the default realm to MYLAB.LOCAL and point to the KDC and admin server on VM1. The configuration should match what you set on VM1.



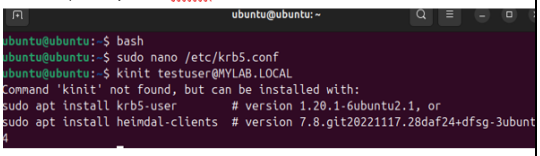
Step 5: Test Kerberos Authentication

1. **Request a Kerberos Ticket for the User on VM2:**
   - In the terminal on VM2, request a ticket for testuser:

bash

kinit testuser@MYLAB.LOCAL

   - Enter the password you set for testuser.



2. **Verify the Ticket:**
   - Check if the ticket was issued by listing active Kerberos tickets:

bash

klist


```
ubuntu@ubuntu:~$ bash
ubuntu@ubuntu:~$ klist
Command 'klist' not found, but can be installed with:
sudo apt install krb5-user        # version 1.20.1-6ubuntu2.1, or
sudo apt install heimdal-clients  # version 7.8.git20221117.28daf24+dfsg-3ubuntu
4
```

   - You should see details about the ticket, such as the principal and expiration time, confirming successful Kerberos authentication.

Labwork 2:

SCHOOL OF INFORMATION AND TECHNOLOGY

NAME: Sueno, Johnray K.	DATE PERFORMED: 11/21/2024	
Section: IDC2	DATE SUBMITTED: 11/21/2024	

SYSADM1 – Git Basics

Answer the following research questions about Git, GitLab desktop and GitHub.

1. What is Git, and why is it important in software development?
   - ➢ Git is a version control system that helps track changes in code, enabling teams to collaborate on projects efficiently. It is important because it allows developers to work on the same project without overwriting each other's changes and makes it easy to track, manage, and revert changes if needed.
2. How does Git track changes in a project?
   - ➢ Git tracks changes using a system of snapshots. Each time you "commit," Git saves the current state of your project. It compares the changes with the previous snapshot and stores only the differences. This allows for efficient tracking and reverting if necessary.
3. What is the difference between a local repository and a remote repository in Git?
   - ➢ **Local Repository:** This is stored on local machines such as your computer and contains your project files and history.
   - ➢ **Remote Repository:** This is stored on a server (like GitHub or GitLab) and can be accessed by others for collaboration.
4. What are the basic Git commands?
   - **git init:** Initialize a new repository.
   - **git add:** Stage changes to be committed.
   - **git commit:** Save changes to the repository.
   - **git status:** Check the status of changes.
   - **git push:** Send changes to a remote repository.
   - **git pull:** Update your local repository with changes from the remote repository.
5. How do you check the status of a Git repository?
   - ➢ To check the status of Git repository use the command 'git status'.
6. What is the purpose of branches in Git, and how do you create and switch between them?
   - ➢ Branches purpose is to allow developers to work on testing features or bug fixes without affecting the main codebase.

   To create a branch: git branch branch-name

   To switch to a branch: git checkout branch-name

   Command 'git checkout –b branch-name' can also be used for creating and switching.
7. What are GitLab Desktop and GitHub, and how are they different from Git?
   - ➢ GitLab Desktop and GitHub are platforms for hosting remote repositories and facilitating team collaboration. Git is the version control tool used locally to manage code changes, while GitLab and GitHub provide social coding, open-source and web-based features like issue tracking, pull requests, and CI/CD integration.
8. How do you connect a local Git repository to a GitLab or GitHub repository?

   Step 1: Copy the repository URL from GitLab or GitHub.

   Step 2: Run this command in your local repository: git remote add origin repository-URL

   Step 3: Push your changes: git push -u origin main
9. What are the steps to collaborate with others using GitLab or GitHub?

   Step 1: Clone the remote repository: git clone repository-URL

   Step 2: Create a new branch for your changes.

   Step 3: Commit and push your changes.

   Step 4: Open a pull request (GitHub) or merge request (GitLab) to get your changes reviewed and merged.

   Step 5: Pull updates regularly to keep your branch updated: git pull
10. How do you resolve merge conflicts in Git?

    Step 1: Identify the conflict by running git status.

    Step 2: Open the conflicting file and manually fix the conflicting code.

    Step 3: Mark the conflict as resolved: git add file-name

    Step 4: Commit the resolution: git commit
11. What is a pull request, and why is it used in GitHub?
    - ➢ A pull request is a request is a proposal to merge a set of changes from one branch to another in GitHub. It is used to review, discuss, and approve changes before merging them into the main branch/codebase.
12. What are some best practices for writing commit messages?
    - ➢ Keep the subject line concise.
    - ➢ Use the imperative mood.
    - ➢ Regular commits.
    - ➢ Commit related changes.
    - ➢ Separate subject and body.
    - ➢ Include tests in commits.
    - ➢ Use branches.
    - ➢ Fix a workflow.
    - ➢ Capitalize the subject line.
    - ➢ Write good commit messages or names.
    - ➢ Include a brief description of why the change was made if needed.
    - ➢ Keep the subject line under 72 characters.
    - ➢ Reference issues.

Course Reflection

What were your initial expectations for the course? Did the course meet, exceed, or fall short of these expectations?

Before starting SYSADM1, I expected the course to introduce me to the foundational principles of system administration, focusing on topics like user management, network configuration, and troubleshooting techniques. I hoped it would help me to prepare and gain some knowledge that I could use and apply for my future studies. The course met my expectations by providing detailed lectures, assignments, laboratory activities and quizzes that clearly explained the responsibilities of a system administrator. Although it lacked hands-on activities, the theoretical approach was sufficient to help me grasp the key concepts.

What were the main topics or concepts covered in the course? How did these topics contribute to your understanding of the subject matter?

The course covered key topics like operating system installation, user and group management, file permissions, network configuration, and system backups. These concepts helped me understand the critical and important role of a system administrator in maintaining secure and efficient IT infrastructure. Learning these topics gave me a step-by-step approach to managing systems and solving problems effectively. Each lesson built upon the previous one, making it easier to grasp the subject matter as a whole.

Reflecting on your learning process, what were the most effective strategies or techniques that helped you grasp and retain the course material?

The most effective strategies that worked for me is during lab activities and reviewing it after every session. The laboratory works approach allowed me to practice real-world scenarios, which helped me understand the subject better. I also found that studying with classmates and discussing problems helped me learn different perspectives and approaches. Consistently revisiting my notes, activities and assignments ensured I gained some knowledge throughout the course.

Were there any particular assignments, projects, or activities that significantly enhanced your learning experience? Why were they effective?

The laboratory activities, especially setting up and troubleshooting systems, were some of the most effective parts of the course. These activities were effective because they made me apply theoretical knowledge in a controlled environment, preparing me for real-world situations. Assignments that required scripting or configuring systems helped me learn step-by-step processes and improve my attention to detail. These tasks boosted my confidence in handling system administration tasks independently.

Did you encounter any challenges or difficulties during the course? How did you overcome these obstacles, and what did you learn from them?

One of the biggest challenges I faced was understanding some of the more complex configurations during lab activities such as the Kerberos and use of Linux. I overcame these difficulties by asking questions and collaborating with my peers, and researching additional materials online. By doing this, I not only understood the tasks better but also developed problem-solving and time-management skills. These challenges taught me to stay persistent and resourceful, which are essential traits in system administration.

Did the course encourage critical thinking and analysis? How did it promote higher-order thinking skills, such as problem-solving or decision-making?

The course encouraged critical thinking by requiring us to analyze system errors and find the best solutions. Tasks like troubleshooting networks or managing permissions forced me to think simple answers and consider the broader impact of my decisions. This approach promoted higher-order thinking skills, such as evaluating multiple solutions and determining the most efficient one. It helped me see system administration as a problem-solving role, not just a technical one.

Reflecting on your personal growth, what new knowledge, skills, or perspectives did you gain from this course?

Through this course, I gained a deeper understanding of system management and the responsibilities of a system administrator. I also learned technical skills like configuring operating systems, managing file permissions, and setting up secure networks. Beyond technical knowledge, I developed better critical thinking, collaboration, and problem-solving skills. These experiences have made me more confident in tackling challenges related to IT infrastructure.

How do you plan to apply what you have learned in this course to your future studies, career, or personal life?

I plan to use the knowledge and skills I gained in this course for future studies and internships. In particular, I aim to apply these skills in roles related to IT support or system administration, where problem-solving and technical expertise are critical. This course has also inspired me to explore more advanced IT topics, such as cybersecurity and cloud computing. Additionally, I can see myself applying these skills in personal projects, such as setting up networks or managing systems for small businesses.