UNIVERSITY OF Baguio

SCHOOL OF INFORMATION TECHNOLOGY

NAME: Magno, Ronnie L.	
SECTION: IDC2	DATE SUBMITTED: 12/08/24

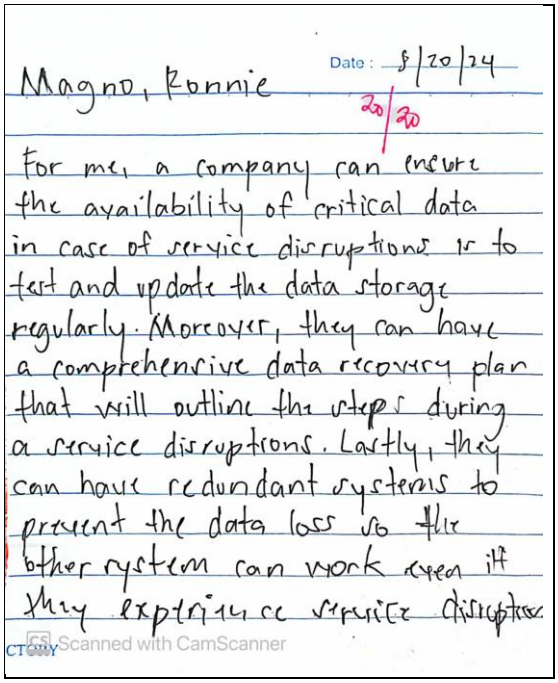
(SYSADM1) PORTFOLIO

Table of Contents

Quizzes			
Assignment 1	Oct 08, 2024	28/40	11
Seatwork 1	Oct 10, 2024	30/40	12
Other Activities			
Laboratory Activity 1	Sept 26, 2024	/50	13-14
Laboratory Activity 2	Oct 10, 2024	/50	15
Laboratory Activity 3	Oct 17, 2024	/50	16-17
Midterm Exam: Lecture	Nov 07, 2024	42/60	18
Midterm Exam: Laboratory	Nov 07, 2024	53/80	18
Finals			
Quizzes			
Assignment 1	Nov 28, 2024	/50	19
Assignment 2	Dec 05, 2024	/50	20
Seatwork 1	Nov 05, 2024	/60	21
Quiz 1	Nov 21, 2024		22
Other Activities			
Laboratory Activity 1	Nov 14, 2024	/50	23-24
Laboratory Activity 2	Nov 21, 2024		25
Final Exam			
Course Reflection			26-17

First Grading Lecture:

Quiz 1:

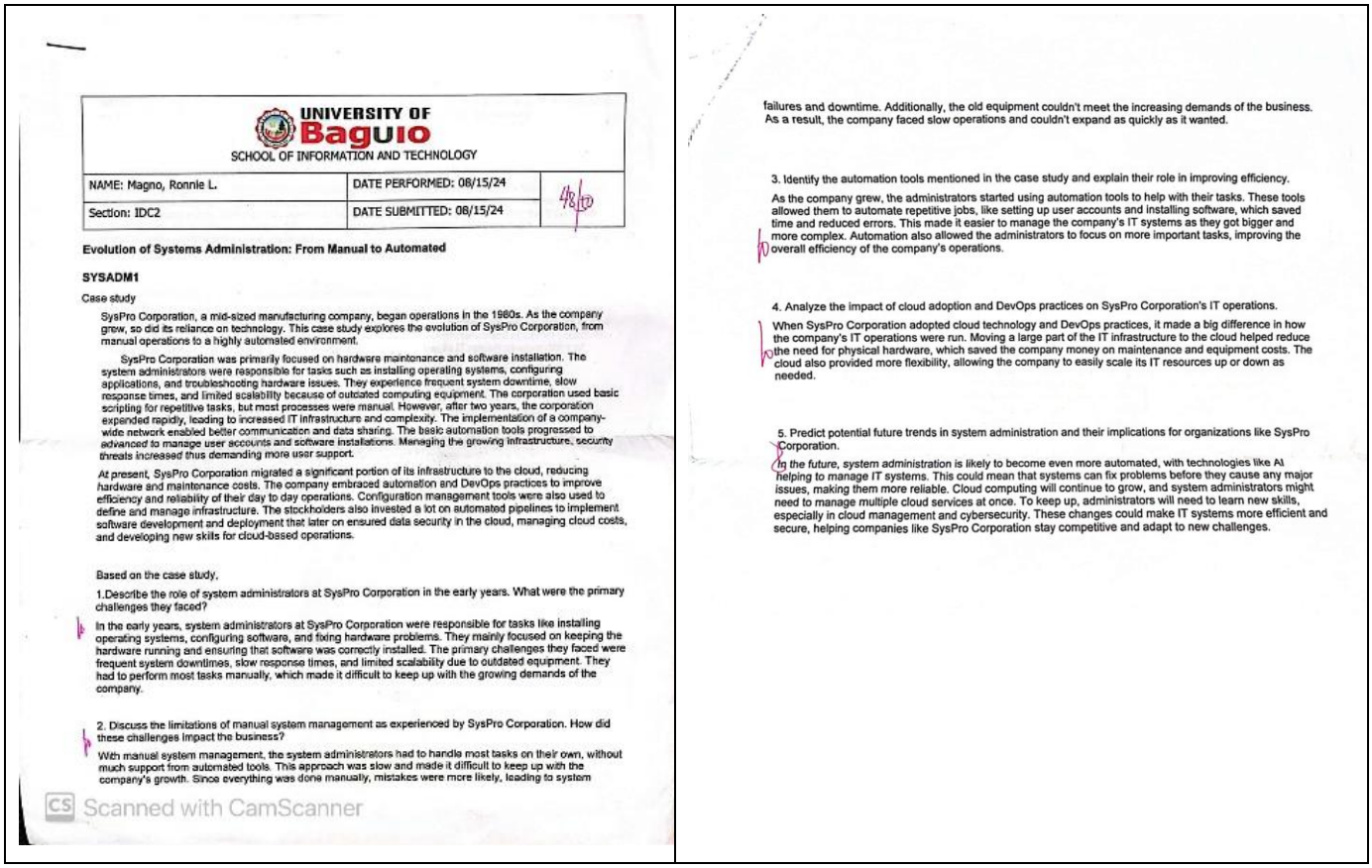


Magno, Ronnie Date : 8/20/24

20/20

For me, a company can ensure the availability of critical data in case of service disruptions is to test and update the data storage regularly. Moreover, they can have a comprehensive data recovery plan that will outline the steps during a service disruptions. Lastly, they can have redundant systems to prevent the data loss so the other system can work even if they experience service disrupt

Assignment 1:



UNIVERSITY OF BAGUIO
SCHOOL OF INFORMATION AND TECHNOLOGY

NAME: Magno, Ronnie L.	DATE PERFORMED: 08/15/24	48/50
Section: IDC2	DATE SUBMITTED: 08/15/24	

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, system administrators at SysPro Corporation were responsible for tasks like installing operating systems, configuring software, and fixing hardware problems. They mainly focused on keeping the hardware running and ensuring that software was correctly installed. The primary challenges they faced were frequent system downtimes, slow response times, and limited scalability due to outdated equipment. They had to perform most tasks manually, which made it difficult to keep up with the growing demands of the company.

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

With manual system management, the system administrators had to handle most tasks on their own, without much support from automated tools. This approach was slow and made it difficult to keep up with the company's growth. Since everything was done manually, mistakes were more likely, leading to system

failures and downtime. Additionally, the old equipment couldn't meet the increasing demands of the business. As a result, the company faced slow operations and couldn't expand as quickly as it wanted.

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

As the company grew, the administrators started using automation tools to help with their tasks. These tools allowed them to automate repetitive jobs, like setting up user accounts and installing software, which saved time and reduced errors. This made it easier to manage the company's IT systems as they got bigger and more complex. Automation also allowed the administrators to focus on more important tasks, improving the overall efficiency of the company's operations.

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

When SysPro Corporation adopted cloud technology and DevOps practices, it made a big difference in how the company's IT operations were run. Moving a large part of the IT infrastructure to the cloud helped reduce the need for physical hardware, which saved the company money on maintenance and equipment costs. The cloud also provided more flexibility, allowing the company to easily scale its IT resources up or down as needed.

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

In the future, system administration is likely to become even more automated, with technologies like AI helping to manage IT systems. This could mean that systems can fix problems before they cause any major issues, making them more reliable. Cloud computing will continue to grow, and system administrators might need to manage multiple cloud services at once. To keep up, administrators will need to learn new skills, especially in cloud management and cybersecurity. These changes could make IT systems more efficient and secure, helping companies like SysPro Corporation stay competitive and adapt to new challenges.

Assignment 2:

UNIVERSITY OF BAGUIO
SCHOOL OF INFORMATION AND TECHNOLOGY

NAME: Magno, Ronnie L.	DATE PERFORMED: 08/29/24	
Section: IDC2	DATE SUBMITTED: 08/29/24	

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

- **Outdated Hardware and Software-**

  Old computers and software can slow down systems and make them less secure, which can lead to higher maintenance costs and downtime. To fix this, organizations should plan to replace old systems every 3-5 years, which helps spread out costs. They can also improve the performance of existing hardware by optimizing software. Using cloud storage can save money and provide more flexibility without needing to buy new hardware right away.

- **Insufficient Data Storage-**

  Not having enough storage space can make it hard for organizations to work efficiently and manage their data. To improve this, they can use fast solid-state drives (SSDs) for important data and slower hard disk drives (HDDs) for less critical information. They can also use techniques to reduce the amount of data stored, like deleting duplicates or compressing files. Adopting cloud storage can help manage data without needing to invest heavily in new hardware.

- **High Energy Costs-**

  To save energy, organizations can use energy-efficient hardware and cooling systems that reduce power consumption while still performing well. Virtualization can help by allowing multiple tasks to run on fewer servers, which cuts down on energy use. Additionally, using power management features can automatically turn off systems that aren't being used, further saving energy.

- **Security Vulnerabilities-**

  Weaknesses in security can put organizations at risk of data breaches and other issues. To improve security, organizations should set up strong access controls, regularly check their systems for vulnerabilities, and train employees on best practices for cybersecurity. Keeping software updated with the latest security patches is also crucial to protect against known threats. Investing in proactive security measures can help prevent costly problems and using cloud security services can simplify management.

- **Network Bottlenecks**

  Slow network connections can hurt productivity and frustrate users. To improve this, organizations should regularly check and upgrade their network bandwidth to keep up with growing data needs. They can also set up Quality of Service (QoS) policies to prioritize important applications, ensuring they run smoothly.

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?

   - To support a smart city or digital transformation project, we need data management systems to collect and analyze data from various sources. Cloud services are important for storing and accessing this data easily, while fast networks like fiber optics or 5G ensure quick communication between devices. Additionally, GIS tools help visualize and understand the city's layout, and security tools protect sensitive information from hackers.

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

   - Using a modular approach allows the IT infrastructure to be broken down into smaller, independent parts that can be updated or expanded without affecting the entire system. Cloud services provide on-demand scalability, enabling the project to adapt as the city's needs change. By combining on-site servers with cloud solutions, we can choose the best option for each part of the project, making the infrastructure flexible enough to handle fluctuations in demand.

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

   - When implementing a smart city project, we face security risks like data breaches or attacks on connected devices. Using strong passwords and two-factor authentication protects accounts, while regularly updating software fixes security holes. Conducting security checks helps identify and address weaknesses in the system. Training city employees and residents on good security practices prevents mistakes that could lead to problems.

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

   - To smoothly integrate new IT infrastructure with existing systems, we first need to understand how current systems work and find ways to connect them with new technology. Using APIs helps different systems communicate easily. Involving people from various departments ensures that everyone's needs are considered, making the transition smoother. Lastly, providing training and support helps users adapt to the new systems without causing too much disruption to their work.

Page 2 of 2

First Grading Laboratory:

Labwork 1:

UNIVERSITY OF Baguio SCHOOL OF INFORMATION AND TECHNOLOGY		
NAME: MAGNO, RONNIE	DATE PERFORMED: 08/22/24	
Section: IDC2	DATE SUBMITTED: 08/22/24	50/50

SYSADM1 – Introduction to File Systems in Windows and Linux

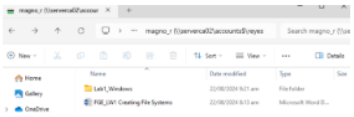
Requirement:

- A virtual machine running Linux and Windows OS

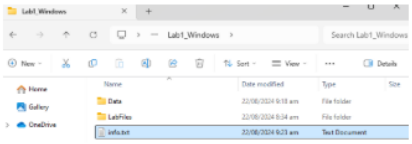
Instructions:

Part A: Windows File System

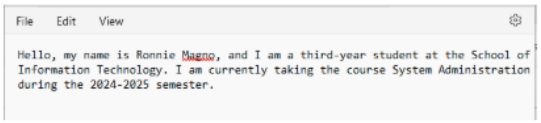
1. **Open File Explorer:** Click the File Explorer icon on your desktop or press the Windows key + E.
2. **Navigate to your Documents folder:** This is usually the default location for user files.
3. **Create a new folder:** Right-click in an empty space, select "New," then "Folder." Name it "Lab1_Windows."



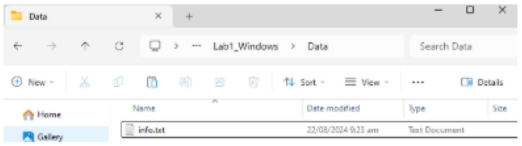
4. **Create a text file:** Right-click in the "Lab1_Windows" folder, select "New," then "Text Document." Rename it to "info.txt."



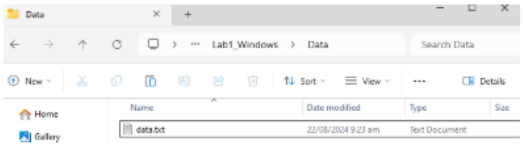
5. **Open the text file:** Double-click the "info.txt" file to open it in Notepad.
6. **Type some text:** Write a short paragraph about yourself or the purpose of the file.



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."

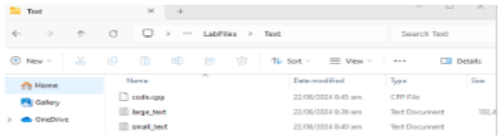


11. Create a folder named "LabFiles" with subfolders for each file type. Use the internet for the resources of the files listed below.

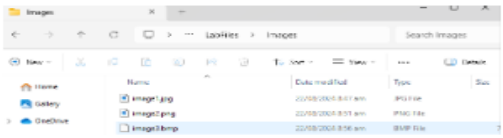
LabFiles

1. **Text**
    1. large_text.txt
    2. small_text.txt

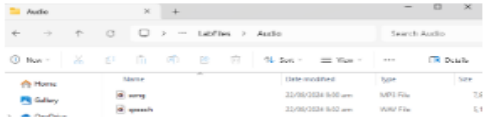
3. code.cpp



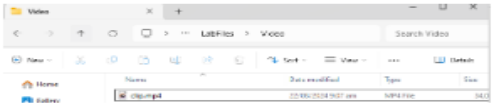
2. **Images**
    1. image1.jpg
    2. image2.png
    3. image3.bmp



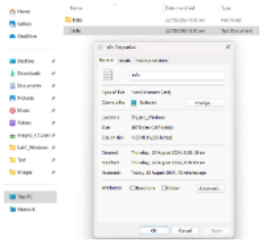
3. **Audio**
    1. song.mp3
    2. speech.wav



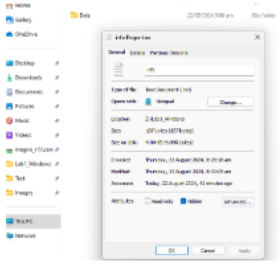
4. **Video**
    1. clip.mp4



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.

LOG REPORT					
STEP #	TASK	DESCRIPTION	RESULT	DURATION	STATUS
1	Open File Explorer	Click the File Explorer icon or press Windows key + E	File Explorer opened	2 minutes	Completed
2	Navigate to Documents folder	Go to default user file location	Documents folder accessed	1 minute	Completed
3	Create a new folder	Right-click, select New Folder, name it "Lab1_Windows"	Folder "Lab1_Windows" created	3 minutes	Completed
4	Create a text file	Right-click in "Lab1_Windows," select New Text Document, and rename to "info.txt"	Text file "info.txt" created	3 minutes	Completed
5	Open the text file	Double-click "info.txt" to open in Notepad	Notepad opened with "info.txt"	1 minute	Completed
6	Type some text	Write a short paragraph about yourself in Notepad	Text written and saved	6 minutes	Completed
7	Save the file	Close Notepad and save changes	File saved with changes	1 minute	Completed
8	Create a subfolder	In "Lab1_Windows," create a folder named "Data"	Subfolder "Data" created	2 minutes	Completed
9	Copy the text file	Copy "info.txt" to "Data" subfolder	File copied to "Data"	2 minutes	Completed
10	Rename the copied file	Rename the copied file in "Data" to "data.txt"	File renamed to "data.txt"	2 minutes	Completed
11	Create "LabFiles" folder	Create "LabFiles" with subfolders for Text, Images, Audio, Video	"LabFiles" and subfolders created	3 minutes	Completed

11.1	Text files	Download or create files: large_text.txt, small_text.txt, code.cpp	Text files added	5 minutes	Completed
11.2	Images	Download or create files: image1.jpg, image2.png, image3.bmp	Image files added	7 minutes	Completed
11.3	Audio	Download or create files: song.mp3, speech.wav	Audio files added	5 minutes	Completed
11.4	Video	Download or create file: clip.mp4	Video file added	3 minutes	Completed
12	Check file properties	Right-click "info.txt," select Properties, review General, Details, Security tabs	File properties reviewed	4 minutes	Completed
13	Change file attributes	Modify attributes (e.g., read-only, hidden) via Properties dialog	Attributes changed	4 minutes	Completed
14	Share the folder	Right-click "Lab1_Windows," select Properties, Sharing tab, set permissions			Failed
15	Create an archive	Use WinRAR or 7-Zip to create a compressed archive of "Lab1_Windows"	Archive created	3 minutes	Completed

Labwork 3:

UNIVERSITY OF Baguio

SCHOOL OF INFORMATION AND TECHNOLOGY

NAME: MAGNO, RONNIE L.	DATE PERFORMED: 08/29/24	
Section: IDC2	DATE SUBMITTED: 08/29/24	

SYSADM1 – Managing Services in Windows

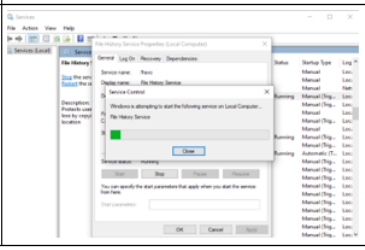
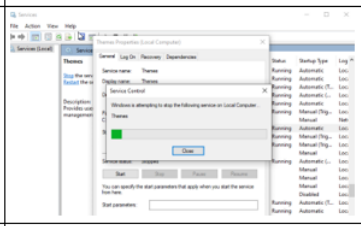
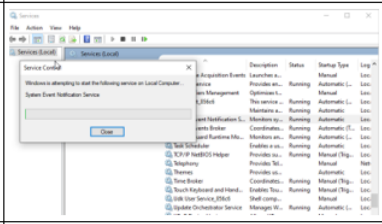
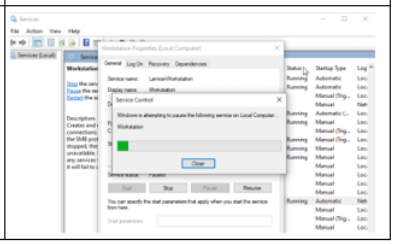
Requirement:

- 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.

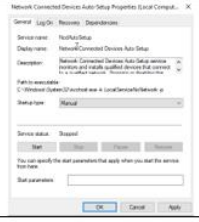
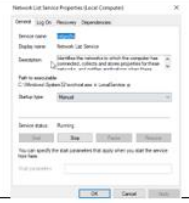
Instructions:

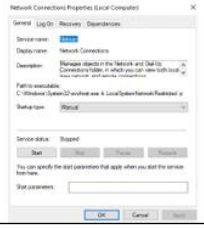
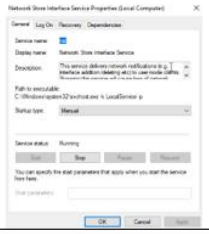
1. Open the Start menu and search for "Services"
2. Familiarize yourself with the columns, including Service Name, Display Name, Status, and Startup type.
3. Right-click on a service and select "Start", "Stop", or "Restart". Fill out the table below

Status	Name of Service	Screenshot
Start	File History Service	
Stop	Themes	
Restart	System Event Notification	
Pause	Workstation	

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

SS:

Network Connected Devices Auto-Setup	
Network Setup Service	
Network List Service	

Network Connections	
Network Store Interface Service	

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

Name	Date modified	Type	Size
magno_timer	8/29/2024 10:44 AM	Windows Batch File	1 KB

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

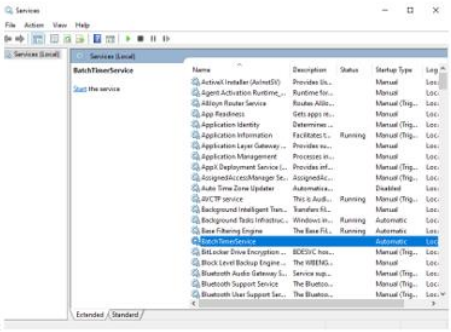
8. Use the sc command to add timer.bat service in the command line interface.

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.

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

Labwork 4:

UNIVERSITY OF BAGUIO
SCHOOL OF INFORMATION AND TECHNOLOGY

NAME: MAGNO, RONNIE L.	DATE PERFORMED: 09/12/24	
Section: IDC2	DATE SUBMITTED:	

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
procps	uuidd
cron	bluetooth
apport	ssrd
kmod	sanod
sysstat	rsync

   SS:

```
ubuntu@ubuntu: $ service --status-all
[ + ]  alsa-utils
[ - ]  anacron
[ - ]  apparmor
[ + ]  apport
[ - ]  bluetooth
[ - ]  console-setup.sh
[ + ]  cron
[ - ]  cryptdisks
[ - ]  cryptdisks-early
[ + ]  cups
[ + ]  dbus
[ + ]  gdm3
[ - ]  grub-common
[ + ]  kerneloops
[ - ]  keyboard-setup.sh
[ + ]  kmod
[ + ]  openvpn
[ - ]  plymouth
[ + ]  plymouth-log
[ + ]  procps
[ - ]  rsync
[ - ]  sanod
```

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?
   The status of Bluetooth is inactive
   SS:

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

4. Check the status of the cups services. Since when was it running?
   It was running 6 minutes ago
   SS:


```
ubuntu@ubuntu: $ sudo systemctl status cups
● cups.service - CUPS Scheduler
     Loaded: loaded (/usr/lib/systemd/system/cups.service; enabled; preset: ena
     Active: active (running) since Thu 2024-09-12 01:15:09 UTC; 6min ago
TriggeredBy: ● cups.path
             ● cups.socket
       Docs: man:cupsd(8)
   Main PID: 1819 (cupsd)
     Status: "Scheduler is running..."
      Tasks: 1 (limit: 4547)
     Memory: 4.2M (peak: 4.4M)
        CPU: 64ms
     CGroup: /system.slice/cups.service
             └─1819 /usr/sbin/cupsd -l

Sep 12 01:15:09 ubuntu systemd[1]: Starting cups.service - CUPS Scheduler...
Sep 12 01:15:09 ubuntu systemd[1]: Started cups.service - CUPS Scheduler.
```

5. Stop cups services.

6. Verify if the service was stopped.

```
ubuntu@ubuntu: $ sudo systemctl stop cups
ubuntu@ubuntu: $ sudo systemctl status cups
○ cups.service - CUPS Scheduler
     Loaded: loaded (/usr/lib/systemd/system/cups.service; enabled; preset: ena
     Active: inactive (dead) since Thu 2024-09-12 01:27:01 UTC; 31s ago
   Duration: 11min 51.628s
TriggeredBy: ○ cups.path
             ○ cups.socket
       Docs: man:cupsd(8)
    Process: 1819 ExecStart=/usr/sbin/cupsd -l (code=exited, status=0/SUCCESS)
   Main PID: 1819 (code=exited, status=0/SUCCESS)
     Status: "Scheduler is running..."
        CPU: 66ms

Sep 12 01:15:09 ubuntu systemd[1]: Starting cups.service - CUPS Scheduler...
Sep 12 01:15:09 ubuntu systemd[1]: Started cups.service - CUPS Scheduler.
Sep 12 01:27:01 ubuntu systemd[1]: Stopping cups.service - CUPS Scheduler...
Sep 12 01:27:01 ubuntu systemd[1]: cups.service: Deactivated successfully.
Sep 12 01:27:01 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.


```
ubuntu@ubuntu: $ sudo systemctl status cups
● cups.service - CUPS Scheduler
     Loaded: loaded (/usr/lib/systemd/system/cups.service; enabled; preset: ena
     Active: active (running) since Thu 2024-09-12 01:30:28 UTC; 16s ago
TriggeredBy: ○ cups.path
             ● cups.socket
       Docs: man:cupsd(8)
   Main PID: 4836 (cupsd)
     Status: "Scheduler is running..."
      Tasks: 1 (limit: 4547)
     Memory: 1.7M (peak: 1.9M)
        CPU: 6ms
     CGroup: /system.slice/cups.service
             └─4836 /usr/sbin/cupsd -l
```

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 89/100

Name: Magno, Ronnie Date: 09/19/24
Course and Year: BSIT - 3rd Section: 10C2

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) (6)

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

A. IaaS
B. SaaS
C. NaaS
D. PaaS

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) (7)

A,B 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

C,A 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

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

D 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

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

C 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

C 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

C 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)

Physical Infrastructure Services 1. It is the management and upkeep of computer systems, especially multi-user computers such as servers.

Virtualization 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 System 3. It is an advanced operating system that has necessary features and subsystems to operate in a client-server architecture.

DNS 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?

Network 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. Main frames
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. Storage Area Network (SAN)
b. Direct-attached Storage (DAS)
c. Network-attached Storage (NAS)

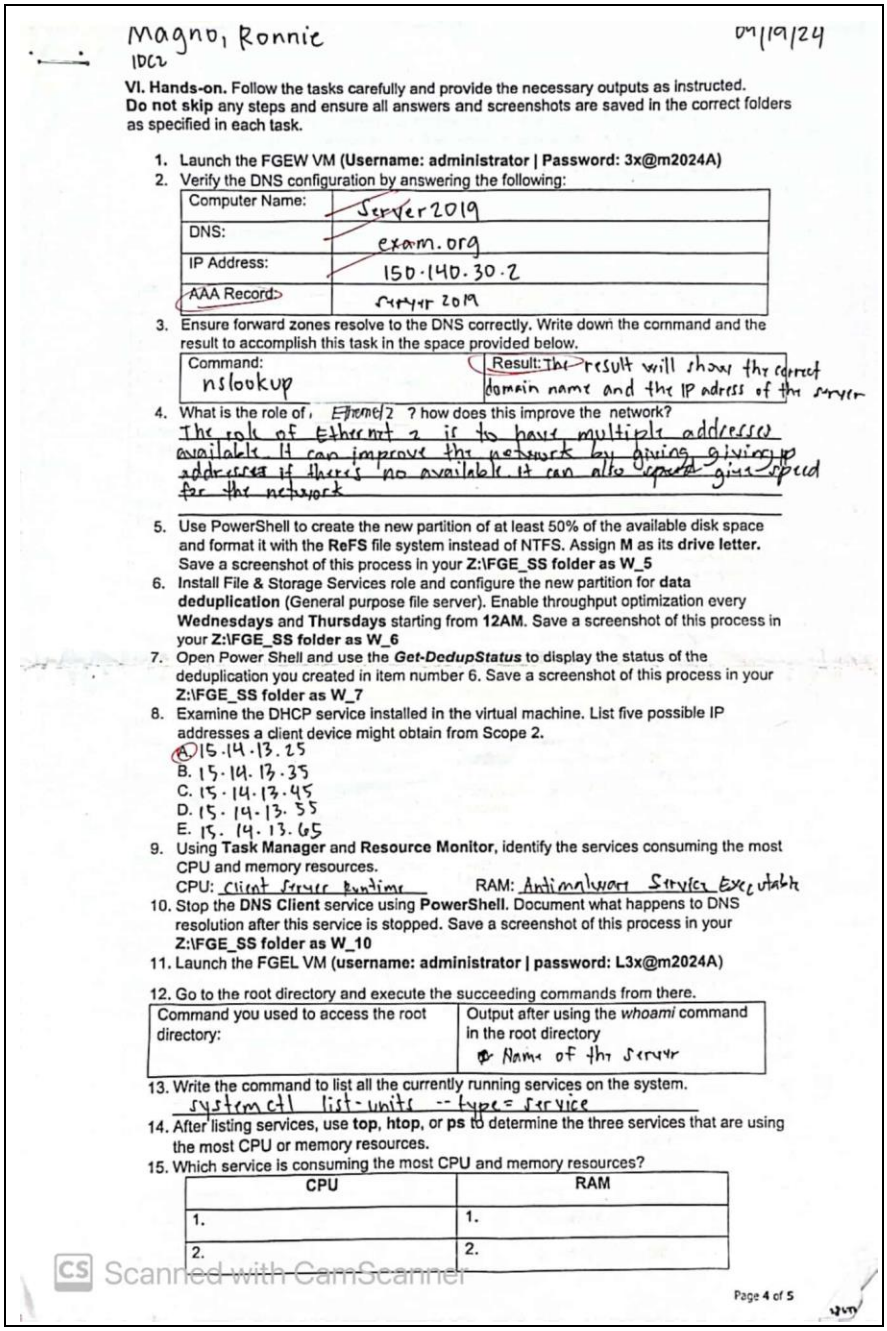
V. Discussion. Express your answers in English. All answers should be in paragraph form. Place your answers at the back of this sheet. (8 points each)

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. I ~~think~~ think if the company prohibits employees from using social media during work hours will help to minimize distractions. Avoiding distractions such as browsing on facebook watching contents from tiktok will surely help the employees to focus on their tasks that will result to higher quality of works. Moreover, this policy can encourage better collaboration among the employees that can lead to the success of their company. However, there should be exceptions like if there's an emergency and they need to communicate using some of the social media like messenger. I believe this policy will help the company but they should also consider the situation of the employees.

2. The potential security risks associated with cloud migration is that it is prone to data breaches. The company will also rely on the ~~to~~ cloud provider. Also, by using public cloud means employees can access the files (or applications) of the company from different locations using the internet. Moreover, the size of the cloud storage may not be enough if they want to transfer applications. On the other hand to mitigate potential security risks associated with cloud migration is to ~~back up have to~~ have contingency plan. The company should back up the applications and other important files so that if there's a data breaches or there's an unauthorized access in that and remove everything they still have the access. ~~back~~



Magno, Ronnie 09/19/24
IDC2

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:	exam.org
IP Address:	150.140.30.2
AAA Record	server 2019

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:
nslookup	The result will show the correct domain name and the IP adress of the server

4. What is the role of Ethernet 2 ? how does this improve the network?
The role of Ethernet 2 is to have multiple addresses available. It can improve the network by giving addresses if there's no available. It can also speed for the network

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. 15.14.13.25
   B. 15.14.13.35
   C. 15.14.13.45
   D. 15.14.13.55
   E. 15.14.13.65
9. Using **Task Manager** and **Resource Monitor**, identify the services consuming the most CPU and memory resources.
   CPU: Client Server Runtime RAM: Antimalware Service Executable
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
	Name of the server

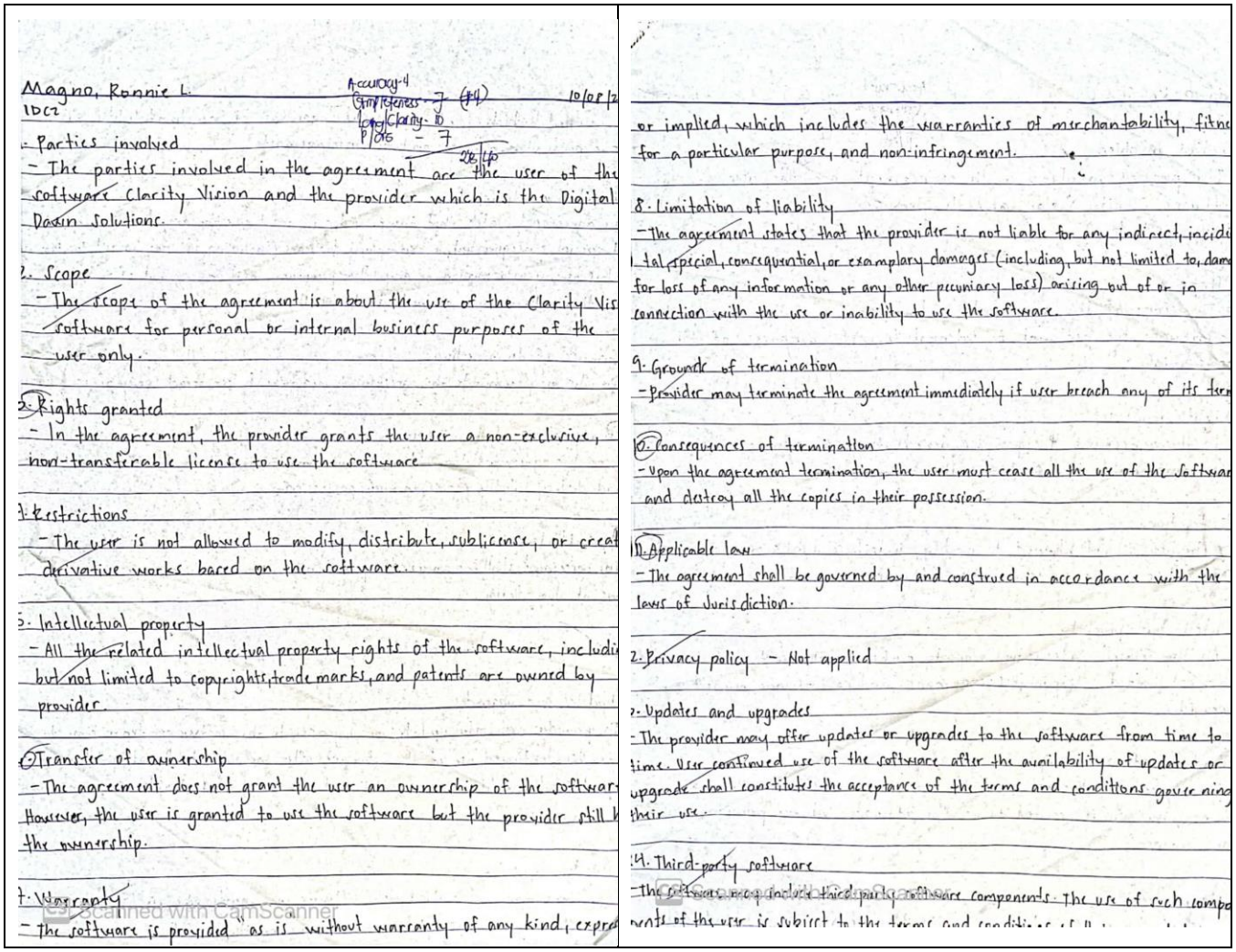
13. Write the command to list all the currently running services on the system.
systemctl list-units --type=service
14. After listing services, use **top**, **htop**, or **ps** to determine the three services that are using the most CPU or memory resources.
15. Which service is consuming the most CPU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

CPU	RAM
1.	1.
2.	2.

Page 4 of 5

Midterm Lecture:

Assignment 1:



Magno, Ronnie L. 10/08/2
IDC2

Accuracy-4
Completeness-7 (11)
Logic/Clarity-10
P/05 - 7
28/40

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

2. Scope
- The scope of the agreement is about the use of the Clarity Vis software for personal or internal business purposes of the user only.

3. Rights granted
- In the agreement, the provider grants the user a non-exclusive, non-transferable license to use the software

4. Restrictions
- The user is not allowed to modify, distribute, sublicense, or creat derivative works based on the software.

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

6. Transfer of ownership
- The agreement does not grant the user an ownership of the softwar However, the user is granted to use the software but the provider still h the ownership.

7. Warranty
- The software is provided as is without warranty of any kind, expre

Scanned with CamScanner

or implied, which includes the warranties of merchantability, fitne for a particular purpose, and non-infringement.

8. Limitation of liability
- The agreement states that the provider is not liable for any indirect, incide tal, special, consequential, or examplary damages (including, but not limited to, dam for loss of any information or any other pecuniary loss) arising out of or in connection with the use or inability to use the software.

9. Grounds of termination
- Provider may terminate the agreement immediately if user breach any of its ter

10. Consequences of termination
- Upon the agreement termination, the user must cease all the use of the softwar and destroy all the 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 - Not applied

13. Updates and upgrades
- The provider may offer updates or upgrades to the software from time to time. User continued use of the software after the availability of updates or upgrade shall constitute the acceptance of the terms and conditions gover ning their use.

14. Third-party software
- The software may include third-party software components. The use of such compo nents of the user is subject to the terms and

Seatwork 1:

Magno, Ronnie L. 10/16/24
IDC2

30/40

1. How do you monitor web server statistics?
> To monitor web server statistics, you can use special tools or software that keep track of how the server is doing. These tools look at things like how fast the server responds to requests like how fast the server responds to requests and how many people are using it at once. Moreover we can also check logs, which are records of everything that happens on the server.

2. What are key metrics that you need to monitor in a web server?
> the key metrics that we need to monitor in a web server are response times, error rates, request rate, CPU usage, Memory usage, Disk I/O, Network Traffic, and Uptime. Monitoring these metrics is essential because it helps to ensure optimal server performance.

3. Analyze the provided web server statistics to determine what is being asked for below.

A. Average response time > 738 ms
B. Request per second > 1 second/request or 1.125 request/second
C. Memory usage > 97.78 mb
D. Error Rate > 22.22%
E. Common error types > 404 Not Found
500 Internal Server Error

1. What are the possible issues in the web server statistics above?
High Average Respons Time - 738 ms suggests potential performance issues particularly with the 5000 ms respons time for one request
Error Rate - A 22.22% error rate is important and indicates issues with server err
> Resource Usage - Memory usage spikes 200 mb for one request
> Specific URLs causing Issues - The URLs that triggered errors (404 and 500) should investigate to resolve underlying problems

Midterm Laboratory:

Labwork 1:

UNIVERSITY OF Baguio

SCHOOL OF INFORMATION AND TECHNOLOGY

NAME: Magno, Ronnie L.	DATE PERFORMED: September 26, 2024	
Section: IDC2	DATE SUBMITTED:	/50

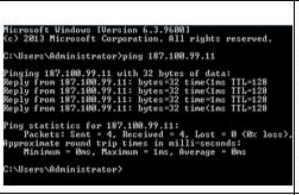
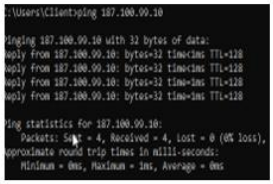
SYSADM1 – Monitoring Print Services in Windows Server 2019

Requirement:

- A virtual machine running Linux and Windows OS

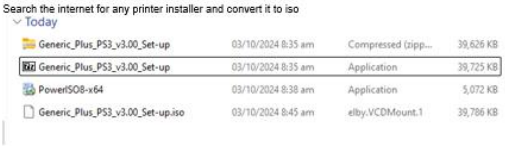
Part 1: Setting Up Print Services

1. Install and configure **print.srv** domain
2. Connect one client to the recently created domain

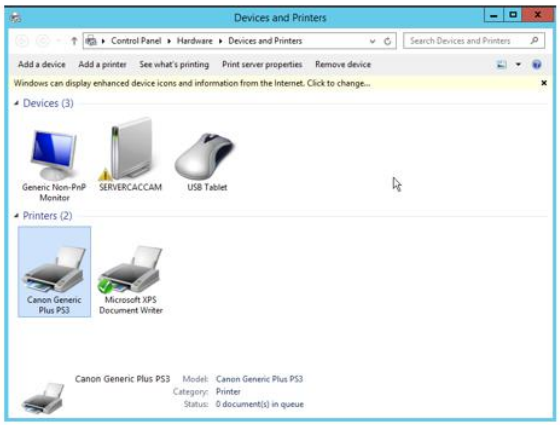
Server	Client
	
	

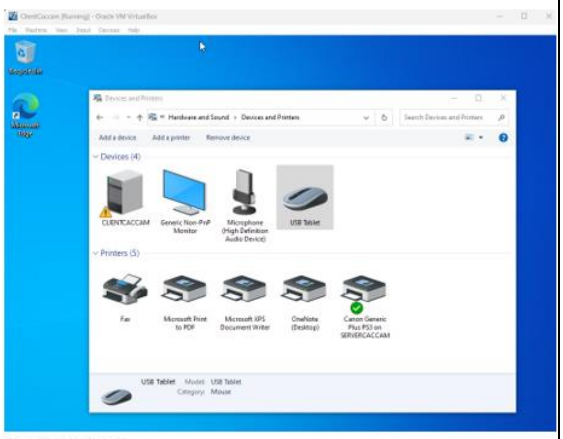
3. Install Print Services Role:

4. Search the internet for any printer installer and convert it to iso



5. Install and deploy it as network printer

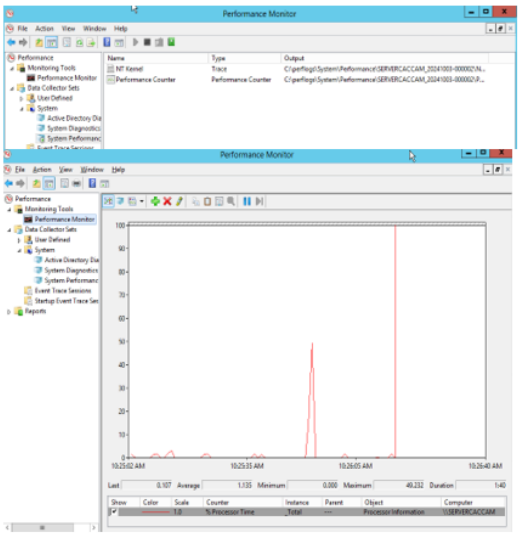




Part 2: Monitoring Print Services

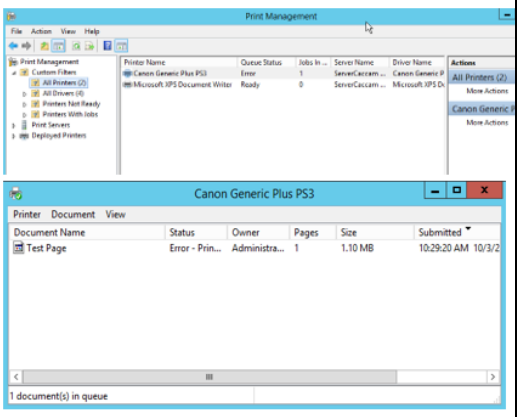
Objective: Familiarize yourself with monitoring tools available in Windows Server 2019.

1. Event Viewer:
   - Open Event Viewer (run **eventvwr.msc**).
   - Navigate to Applications and Services Logs > Microsoft > Windows > PrintService.



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.

- MangeEngine OpManager
The features of this third party tool is, it has a comprehensive monitoring, tools,and print queue monitoring. And when it comes to its price it is base on the numbers of devices that are being monitored. And It is compatible for server 2019 and above.

-PaperCut Print Logger
The features of this third party tool is it has a real time activity logging, export options, automatic printer detection, and multi language support. And for it's pricing, it is free. However the usage will be limited and may not receive daily updates

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: Magno, Ronnie L.	DATE PERFORMED: October 10, 2024	
Section: IDC2	DATE SUBMITTED: October 10, 2024	/50

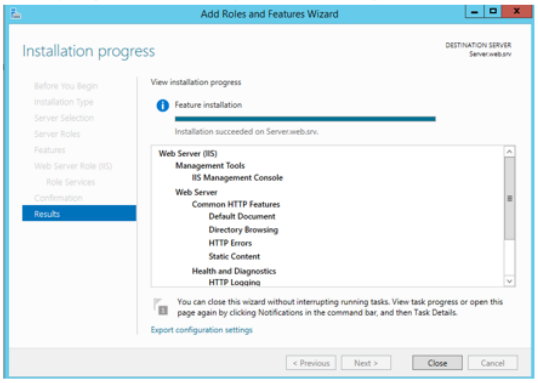
SYSADM1 – Setting Up Webserver

Requirement:

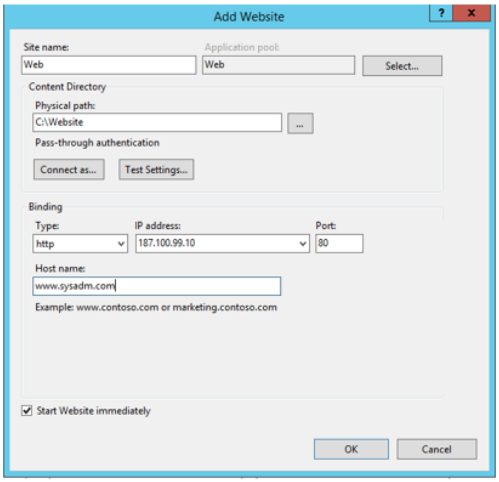
- A virtual machine running Linux and Windows OS

Task Instructions:

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



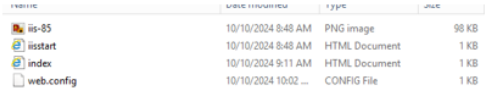
2. Create a website by opening IIS Manager
   - Right-click on the server's name and select Internet Information Services Manager.
   - Right-click on Sites and select Add Website.
   - Enter a name, description, physical path (where your website files will reside), IP address, port, and host name.



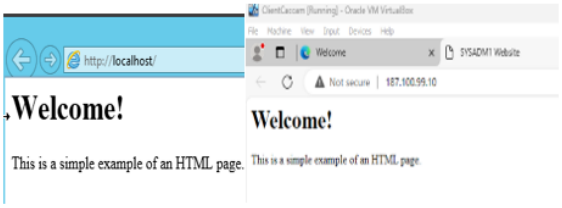
3. Configure the Website:
   - Right-click on your website and select Edit.
   - Set the Default Document to the name of your main HTML file >default.html
   - Configure other settings as needed (e.g., SSL certificates, authentication)
4. Create a Web Page:
   - Create an HTML file in the physical path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



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.



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.
Sucoessful 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: Magno, Ronnie L.	DATE PERFORMED: 10/17/2024	
Section: IDC2	DATE SUBMITTED: 10/17/2024	/50

SYSADM1 – Platform Services

Requirement:

- A virtual machine running Windows Server

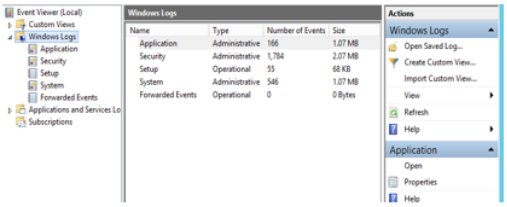
Objective/s:

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

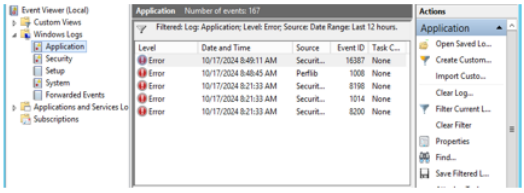
1. Access the event viewer in the server.
2. From the event viewer, explore the windows log and list down its major categories

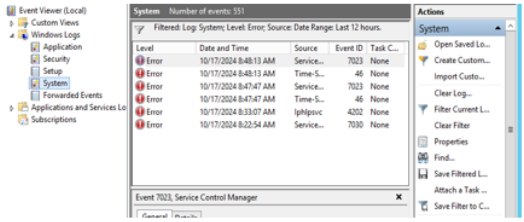


- **The Major list categories are Administrative and Operational**

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 events or recurring events that I encounter are Source and EventID. And the events that I encounter are:**

-Service Control Manager – Event 7023

-Time-Service – Event 46

-Iphlpsvc – Event 4202

- Perflib – Event 1008

- Security-SSP – Event 16387, 8198, 8200, 1014

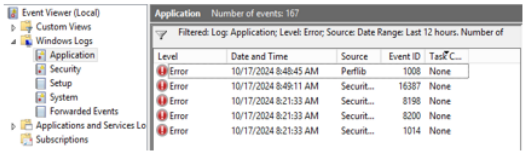
3. **Analyze the Events**:
   - For each critical or recurring event, **record the following details**:
     - **Event ID**
     - **Source**
     - **Timestamp**
     - **Description**

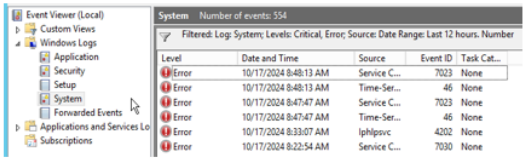
Event ID	Source	Timestamp	Description
1008	Perflib	10/17/2024 – 8:48 AM	Performance data for this service will not be available.
16387	Security-SPP	10/17/2024 – 8:49 AM	Failed to run task
8198	Security-SPP	10/17/2024 – 8:21 AM	License Activation (slui.exe) failed.
8200	Security-SPP	10/17/2024 – 8:21 AM	License acquisition failure: hr=0xC004C003
1014	Security-SPP	10/17/2024 – 8:21 AM	Acquisition of End User License Failed.
7023	Service Control Manager	10/17/2024 – 8:48 AM	An attempt was made to logon, but network logon service was not started.
46	Time-Service	10/17/2024 – 8:48 AM	Time service encountered an error and was forced to shut down.
7023	Service Control Manager	10/17/2024 – 8:48 AM	An attempt was made to logon, but network logon service was not started.
46	Time-Service	10/17/2024 – 8:48 AM	Time service encountered an error and was forced to shut down.
4202	Iphlpsvc	10/17/2024 – 8:33 AM	Unable to update the IP address on Isatap Interface Local Area Connection *11 Update Type: 0. Error Code: 0x57.
7023	Service Control Manager	10/17/2024 – 8:48 AM	An attempt was made to logon, but network

			logon service was not started.

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 a specific time and pattern to these errors. When a source generates an error, even if the event ID is different, the error time is consistent across all event IDs.**

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.
  - ❖ The summary of my documentation is to use the Event viewer and analyze the errors that are critical and errors that are recurring. And based on my findings, Errors like Security Control Manager, Security-SPP, and Time-Service. These errors occurred on the same time but with different Event IDs. So with these errors, I learned that event viewer helps a system administrator to fully monitor and check errors in its server and to easily troubleshoot any errors may encounter.

2. Key Findings

- ❖ **Event ID 1008** – Data Section Contains error code at 8:48 AM.
- ❖ **Event ID 16387** – BITS Service failed to run task at 8:49 AM.
- ❖ **Event ID 8198** – License Activation (slui.exe) Failed with hr=0xC004C003 error code at 8:21 AM.
- ❖ **Event ID 8200** – License Acquisition Failed at 8:21 AM.
- ❖ **Event ID 1014** – Acquisition of End User License Failed at 8:21 AM.
- ❖ **Event ID 7023** – Time service terminated due to attempt to logon but network service was not started at 8:48 AM.
- ❖ **Event ID 46** – Time service encountered an error and was forced to shut down at 8:48 AM.
- ❖ **Event ID 4202** – Unable to update IP address on Isatap Interface Local Area Connection at 8:33 AM.
- ❖ **Event ID 7030** – Printer Extension and Notifications service was marked Inactive services at 8:22 AM.

3. Root Causes and Solutions

- ❖ **Service Control Manager**

Errors:

- An attempt was made to logon, but the network logon service was not started.

Likely Causes:

- Network logon is not running
-Service dependencies not started
-Configuration issues

How to fix:

-Restart network logon service
- Check Server Dependencies
- Review Network Configurations

- ❖ **Security-SPP**

Errors:

- License Activation (slui.exe) failed" and "License acquisition failure: hr=0xC004C003.

Likely Causes:

-Issues with the licensing server.
- Corrupted license files.
- Insufficient permissions for the activation process.

How to fix:

- Run activation as Administrator
- Check internet Connectivity
- Check Event Viewer
- Reinstall Licensing Components

- ❖ **Time-Service**

Errors:

-Time service encountered an error and was forced to shut down.

Likely Causes:

- Incorrect time zone settings.
- Issues with the Windows Time service configuration.
- Network connectivity issues preventing time synchronization

How to fix:

- Restart the Windows Time Service
- Check Time Zone Settings
- Reconfigure Time Service
- Review Event Logs

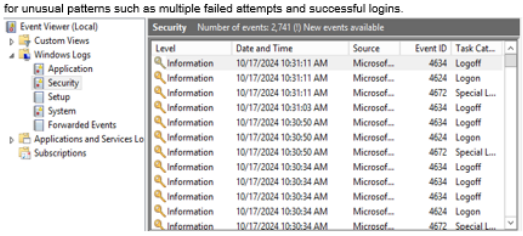
Part 4: Reflection Questions

1. What are the most common causes of a **Security-SPP** and **Service Control Manager** errors?

- The common causes of Security-SSP and Service Control manager errors are often due to corrupted files, which occurs when you shut down your device improperly or because of malwares. It is also causes when you have incomplete windows update or failed update which may also leads to compatibility errors that affects the service management. And lastly, it may also cause to other third party tools or software, which may conflict and causes to interfere the normal operation and management.

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

- To monitor login attempts, you can use the Event viewer to enable auditing logon events. And in the event viewer you can expand in Windows Logs and Select Security. This logs will contain events related to login attempts. And by filtering, you can see the Event id like 4624 and 4625, which these serve as the successful logins and logoff events. You can also review these events for unusual patterns such as multiple failed attempts and successful logins.



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

- Monitoring logs in Event Viewer is crucial for administrators because it helps them keep track of system activity and identify potential security issues. By regularly reviewing these logs, admins can spot unusual behaviors, like repeated failed login attempts, which may indicate attempted breaches or unauthorized access. This proactive approach allows them to respond quickly to threats and take necessary actions to protect sensitive data. Additionally, monitoring logs helps ensure compliance with security policies and regulations, as it provides a clear record of user activity and system changes. Overall, using Event Viewer is an essential practice for maintaining system security and stability in any organization.

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

2 ~~sets~~ 6
35 copies each set

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
Lec - 42
Lab - 53

Name: Magno, Konnie L Date: 11/07/24
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.

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

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

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

(16) 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)

Answer	Column A	Column B
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

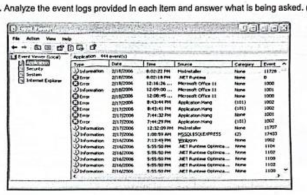
(12) III. **Scenario Based**
Your organization uses an in-house email server, and employees have been reporting issues with spam emails slipping through the filters. Additionally, the company has a web server and several network shares for internal file storage. Recently, the IT manager decided to introduce 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)
   3 The one of the challenge is network traffic or too much request that is the possible error we might encounter when redirecting in a wrong path. The ~~s~~ we can
2. Recommend appropriate email protocols for the employees' remote access. (7 points)
   The appropriate email protocols for the employees remote access is IMAP because it allows them to access emails from multiple device with the use of internet they can open the emails from different locations with their devices. It will help every employee in the company to stay in touch for every urgent email.
3. Propose two strategies to mitigate spam in the organization's email system issue (6 points)
   The strategy is to change the setting of email to limit who sends email in an organization. Next is blocked emails that is identified as spam to prohibit them from sending email again.

Midterm Exam: Laboratory

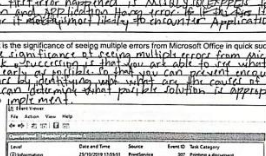
(45) IV. **Analysis.** Analyze the event logs provided in each item and answer what is being asked. (7 points each)

A.



1. What specific time pattern or frequency do you observe in the 'Application Hang' errors?
   The time pattern I observe is that the errors happened with 1 minute time difference for the first 2 application hang error and 1 hour for the next error.
2. Look at the timestamps. What conclusion can you draw about the relationship between 'Application Hang' errors and the information logs from 'MSSQLSQLEXPRESS' and 'Winlogon'?
   The first error happened is MSSQLSQLEXPRESS followed by Winlogon and application hang error. So if the first of the two error occur it more likely to encounter Application Hang error.
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 that you are able to see what are the errors as early as possible. So that you can prevent encountering additional errors by identifying what are the causes of that error. Moreover you can determine what possible solution is appropriate for you to implement.

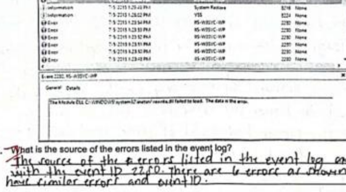
B.



4. What specific action does Event ID 307 indicate, and what can you infer from the fact that it is marked as "Information"?
   7 The Event ID 307 indicates that the action made by this event based from the task category are printing document, print job diagnostics, isolating printer driver and print job diagnostics. Also, the event printed a document that is owned by brent on WIN-LAPTOP and was printed on Microsoft Print to PDF through port C. It is marked information because the task is completed accordingly.
5. Based on the log details, what file size and page count were associated with this print job?
   Based on the log details the file size associated with this print job is 2905389 in terms of bytes. While the number of page count based from the pages that is printed is 7.

6. Look at Event ID 842. What could happen if these checks were skipped or failed?
   7 If the Event ID 842 were skipped or failed, it is possible that the printing task will be interrupted or simply an error could possibly cause, that will result to unsuccessful printing job.

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 with the event ID 2280. There are 6 errors as shown above and they have similar errors and event ID.
8. According to the event description, what file failed to load, and what type of error is this?
   The module DLL C:\WINDOWS\system32\inetsrv\rewrite.dll failed to load. Based from the event description the type of error encountered is data error.
9. What time did the errors occur, and is there any noticeable pattern in the timing? What does this indicate?
   The errors occur in 7/5/2013 1:23:54PM followed by 1:23:52, 1:23:52, 1:23:51, 1:23:50, and 1:23:48. I notice that there's only 1 second time between the errors but in the first to second error there's a 2 sec time difference. It indicate that the error is consistently affecting the task.
10. What is the cause of the most recurring error?
    7 The cause of the most recurring error is IIS-W3SVC-WP or because there's an error in the data of the module they are trying to load.

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."

(8)

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	3/4
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.	3/4
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 Reyes
Instructor

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

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

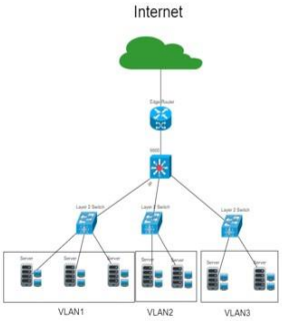
Assignment 2:

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.

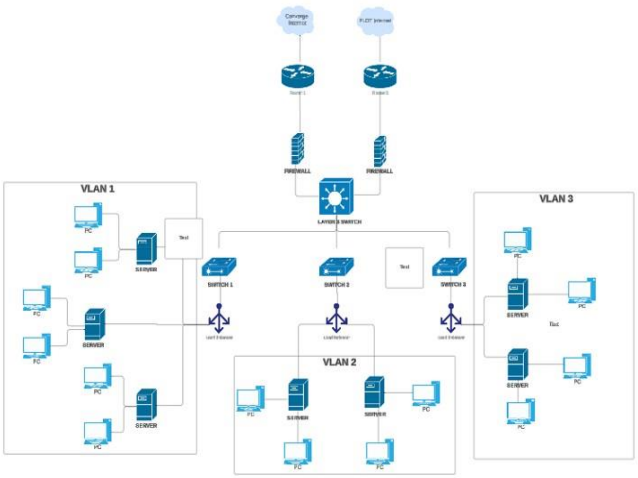
SOLUTION:

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: MAGNO, RONNIE L.	DATE PERFORMED: 11/05/24	
Section: IDC2	DATE SUBMITTED: 11/05/24	

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	Provides thorough guidelines on data security, privacy, and TechLease's compliance with laws, emphasizing user data responsibility.	Includes basic 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.	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.	Mentions an appeal process but lacks clarity or specific steps.	Missing or lacks an appeal process.
Score:	/60			

TechLease Acceptable Use Policy (AUP)

1. Purpose and Scope

The purpose of this Acceptable Use Policy (AUP) is to guide users on the responsible use of TechLease's rental devices and accessories, ensuring the safety, integrity, and longevity of these resources. This policy is essential to TechLease's mission of providing accessible, affordable technology solutions to students and educators. It is designed to support a productive educational environment and reliable service for all users.

Scope:
This policy applies to all TechLease clients, including students, teaching staff, and any other individuals who rent devices and accessories.

2. General Usage Guidelines

2.1 Permitted Uses
- **Academic and Educational Purposes:** Devices are provided for legitimate educational activities, such as attending online classes, conducting research, completing assignments, and collaborating with peers or educators.
- **Pre-Approved Software Use**: Users may access any software or applications pre-installed by TechLease, which are selected to support educational and academic functions.
- **Internet Usage for Learning**: Users are allowed to use the internet on these devices solely for educational purposes, accessing learning platforms, academic resources, and communication tools approved by TechLease.

2.2 Prohibited Uses
- **Non-Educational and Personal Activities**: Devices must not be used for activities unrelated to academics, such as streaming entertainment content, playing games, or engaging in personal activities.
- **Unauthorized Installations**: Users are strictly prohibited from downloading, installing, or modifying any software without TechLease's explicit permission. Unauthorized installations can compromise device security and functionality.
- **Access to Malicious Websites**: Users are restricted from accessing websites known for harmful content or malware. Any attempt to bypass security filters or access restricted sites will result in penalties.

3. Device Care and Maintenance

3.1 User Responsibilities
- **Safe Handling**: Users must handle all devices with care, avoiding rough use and ensuring the device is not exposed to extreme temperatures or moisture.
- **Secure Storage**: Devices should be stored in secure, safe environments when not in use, reducing the risk of damage or theft.
- **On-Time Return**: Devices must be returned to TechLease in their original condition by the specified due date to ensure availability for other clients. Late returns are subject to an additional fee of ₱100 per day.

3.2 Prohibited Actions
- **Physical Alterations**: Users are prohibited from making any physical modifications to the device or attempting self-repair. Such actions void any warranty and may incur fines.
- **Environmental Risks**: Devices must not be exposed to water, excessive dust, or extreme conditions that could harm their functionality.
- **Negligent Behavior**: Leaving devices unattended in unsecured areas or using them carelessly is strictly prohibited.

3.3 Consequences of Neglect
Negligent actions, such as failing to maintain the device, damaging it through misuse, or not returning it on time, may result in additional fees, repair costs, or, in severe cases, a suspension of rental privileges. Repeated neglect may lead to a requirement for full replacement of the device if deemed necessary by TechLease.

4. Data Security and Privacy

4.1 User Data
- **Data Backup**: Users are responsible for backing up personal data as devices will be reset to factory settings upon return. TechLease is not responsible for any data loss that may occur.
- **Data Removal Upon Return**: All personal information should be erased by users prior to device return. TechLease will also perform secure data wipes to protect user privacy.

4.2 Privacy Compliance
TechLease is committed to complying with relevant privacy laws to protect client data. Any personal information collected during the rental process is confidential and will only be used to improve service or as required by law. TechLease does not share client information with third parties unless legally mandated.

5. Penalties for Policy Violations

5.1 Consequences
Consequences for violating the AUP include:
- **Warnings**: Minor infractions may receive a written warning and a reminder of appropriate usage.
- **Fines**: More serious violations, such as unauthorized software installation or neglectful handling of devices, may incur fines or repair fees.
- **Service Suspension**: Repeated or severe violations may lead to suspension of rental privileges or a permanent ban from TechLease services.
- **Legal Action**: Deliberate and malicious damage to devices, such as intentional destruction or theft, may result in legal action as deemed appropriate by TechLease.

6. Appeal Process

If a user believes a penalty was applied unfairly, they may file an appeal within 14 days of receiving the penalty notice. The appeal process is as follows:
1. **Written Appeal Submission**: Submit a written appeal via email to TechLease's support, explaining the incident and providing any supporting evidence.
2. **Review Process**: TechLease will review the appeal within seven business days and may request additional information if necessary.
3. **Decision Notification**: TechLease will notify the user of the appeal outcome within seven business days of completing the review. If the appeal is successful, the penalty may be reduced or waived.

POLICIES:
1.If the client fails to return the rented device by the specified due date, an additional late fee of ₱100 per day will be charged. This fee covers potential inconvenience and the unavailability of the device for other clients. Clients must ensure timely returns to avoid additional fees and ensure device availability for others.

2. TechLease requires full payment for all rentals before the device can be released to the client. This "Payment First" policy ensures that rentals are processed efficiently and helps maintain a secure transaction environment for all users.

3. To protect both company resources and user safety, TechLease reserves the right to block access to websites that are identified as malicious or high-risk for viruses and malware. This restriction minimizes the risk of device infections, preserves device integrity, and ensures a safer user experience.

Quiz 1:

UNIVERSITY OF BAGUIO
SCHOOL OF INFORMATION AND TECHNOLOGY

NAME: Magno, Ronnie L.	DATE PERFORMED: 11/21/24	
Section: IDC2	DATE SUBMITTED: 11/21/24	

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. Th

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 signs of a malware attack during their routine cybersecurity audit. The malware was equipped with ransomware capabilities that posed a significant threat to the confidentiality and integrity of client data which can be steal. The main challenges were stopping the malware from spreading and to protect the client's sensitive data.
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?
   - Before the cybersecurity incident occurred, TechGuard Solutions had already implement preventive measures such as robust cybersecurity protocols, routine system audits, and employee training programs. By implementing these proactive measures, TechGuard was prepared to detect and respond to potential threats.
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?
   - TechGuard Solutions used recovery disks that went beyond standard restoration tools which was a critical part of their preparedness for any cybersecurity threat. These recovery disks included offline backup copies of essential client databases and proprietary threat intelligence. This setup allowed the company to respond swiftly and effectively in the event of a cyberattack. The recovery disks also contained decryption tools specifically designed for the ransomware used in the attack. By using these recovery disks, TechGuard could quickly restore data and ensure that sensitive information was not compromised or lost. The inclusion of offline backups was also crucial for protecting the data because it allows the company to restore operations without relying on potentially infected network resources.
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?
   - The team used the recovery disks to boot the infected workstations in an isolated environment. This isolation helped prevent the malware from spreading further within the network. The recovery disks also contained decryption tools, which were essential for decrypting the files encrypted by the ransomware. Using these tools, the IT team restored the encrypted files from the offline backups stored on the recovery disks. This allowed TechGuard to efficiently recover the critical data without paying the ransom or allowing the attackers to gain access to the company's systems.

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 offline backups stored on the recovery disks played a pivotal role in ensuring data protection during the ransomware attack. Since these backups were stored offline, they were not accessible to the malware, which typically targets online or networked data. The offline backups allowed TechGuard to restore critical client data without worrying about the ransomware affecting the files. With redundant copies of client data safely stored offline, TechGuard was able to restore files quickly and efficiently. This approach minimized data loss and helped the company avoid the pressure of paying a ransom to the attackers.
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 cybersecurity incident, TechGuard Solutions conducted a thorough post-incident analysis to evaluate their response and identify areas for improvement. The insights gained from this analysis helped the company enhance its security measures going forward. One of the key actions taken was the implementation of regular updates to threat intelligence on the recovery disks. Additionally, the analysis highlighted the need for more targeted employee training programs to prevent future phishing attempts and improve staff awareness of evolving cyber risks. This commitment to continuous improvement in their cybersecurity protocols not only strengthened the company's defenses but also had a positive impact on client services.
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?
   - After the post-incident analysis, TechGuard Solutions took several steps to improve its security. They started by regularly updating the threat intelligence on the recovery disks, which helped ensure the company was ready for future ransomware attacks. The company also made changes to its employee training programs, focusing on preventing phishing and other cybersecurity threats. In addition, TechGuard updated its cybersecurity protocols to make their systems stronger and more resistant to attacks. These changes improved the company's overall security and better prepared them to handle any future threats.
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?
   - TechGuard Solutions quick response to the ransomware attack had a positive effect on its client services and client relationships. By minimizing downtime and restoring operations

quickly, they reduced the impact of the attack on clients. This fast action helped maintain client confidence and showed the company's commitment to protecting sensitive information. As a result, TechGuard not only minimized the immediate damage but also improved its reputation and strengthened client trust in the long run.

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?
   - In response to the incident, TechGuard Solutions improved its employee training programs. These programs focused on preventing phishing and other cybersecurity threats. TechGuard provided targeted training to help employees recognize phishing attempts. The company also implemented regular awareness initiatives to keep staff updated on the latest risks. These steps ensured employees were better prepared to handle future threats.
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 incident taught TechGuard Solutions several important lessons. One key lesson was the need for offline backups to protect data during a ransomware attack. The company also learned that keeping threat intelligence and recovery tools up to date is important to fight new types of malware. The attack also showed the importance of training employees to spot threats like phishing. Going forward, TechGuard has improved its cybersecurity protocols and recovery strategies to better handle future attacks. The company is also focusing on continuous improvement to keep its defenses strong.

Finals Laboratory:

Labwork 1:

UNIVERSITY OF Baguio

SCHOOL OF INFORMATION AND TECHNOLOGY

NAME: Magno, Ronnie L.	DATE PERFORMED: 11/14/24	
Section: IDC2	DATE SUBMITTED: 11/14/24	/50

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

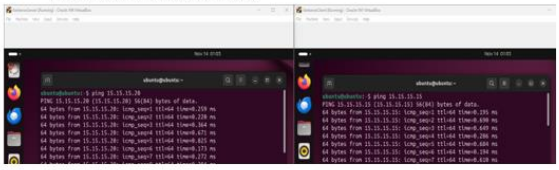
Objective:

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

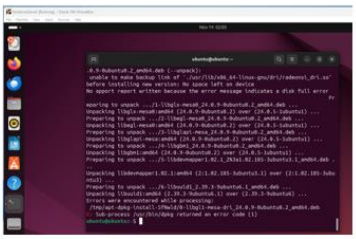
Step 1: Initial Setup and Package Installation

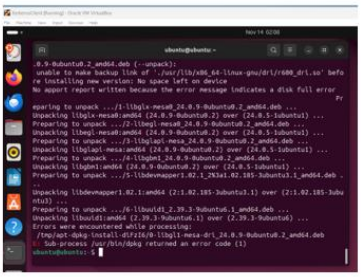


1. **Update Packages on Both VMs:**
   - Open a terminal on each VM and run:

bash

sudo apt update && sudo apt upgrade –y

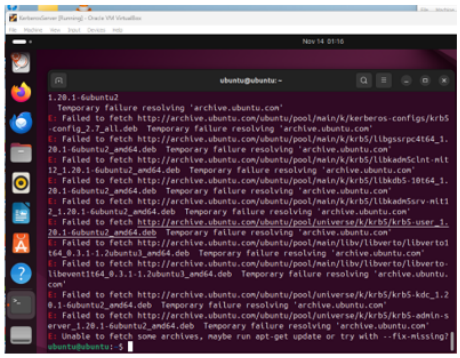




2. **Install Kerberos Server Packages on VM1 (Kerberos Server):**
   - In VM1, install the Kerberos Key Distribution Center (KDC) and admin server:

bash

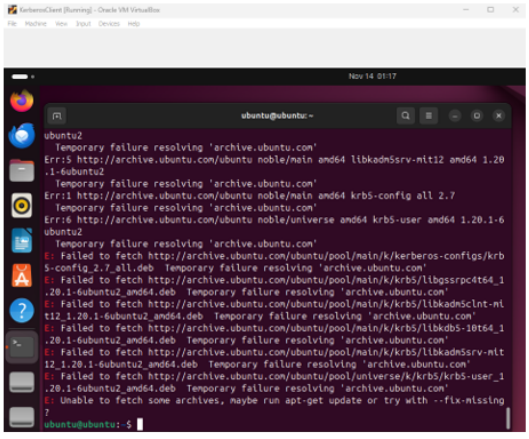
sudo apt install krb5-kdc krb5-admin-server –y



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

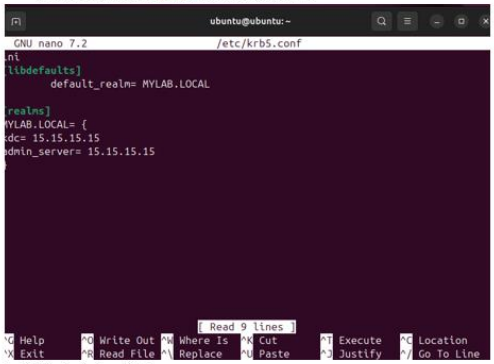
   - Set the realm as MYLAB.LOCAL. You should also specify the KDC and admin server as VM1's hostname or IP address:

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

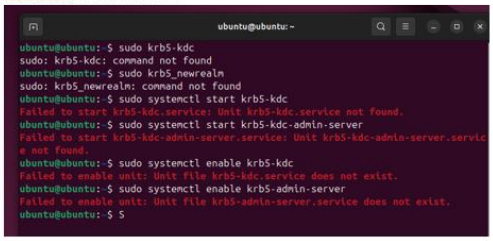
```
sudo krb5_newrealm
```

   - 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
```



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

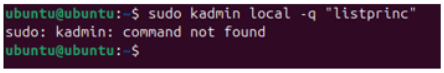
```
sudo kadmin.local -q "addprinc testuser@MYLAB.LOCAL"
```

   - Set a password for testuser.

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

bash

```
sudo kadmin.local -q "listprincs"
```

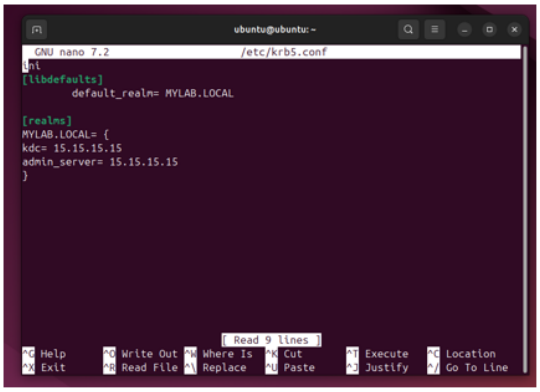
Step 4: Configure the Kerberos Client (VM2)

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
```

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

Labwork 2:

UNIVERSITY OF Baguio
SCHOOL OF INFORMATION AND TECHNOLOGY

NAME: Magno, Ronnie L.	DATE PERFORMED: 11/21/24	
Section: IDC2	DATE SUBMITTED: 11/21/24	

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 distributed version control system designed to efficiently track changes in source code during software development. Created by Linus Torvalds in 2005, Git allows multiple developers to collaborate on projects without interfering with each other's work. Each developer has a complete local copy of the repository, which includes the entire history of changes, enabling them to work offline and perform operations quickly. Git supports non-linear development through branching and merging, allowing developers to experiment with new features or fixes in isolated environments before integrating them into the main codebase
   - The importance of Git in software development lies in its ability to enhance collaboration and streamline workflows. By providing a robust framework for tracking changes and managing different versions of code, Git minimizes the risk of conflicts and errors that can arise when multiple developers work on the same project. Approximately 85% of developers believe that Git simplifies collaboration, making it easier to implement features and fix bugs efficiently. Additionally, Git's integration with continuous integration/continuous deployment (CI/CD) tools facilitates faster release cycles and more responsive development processes, allowing teams to adapt quickly to feedback and changing requirements
2. How does Git track changes in a project?
   - Git tracks changes in a project by utilizing a structured system comprising the working directory, the staging area, and the repository. When developers modify files, Git categorizes them as either tracked or untracked. Tracked files are monitored for changes and can be in states such as modified or staged. To begin tracking a file, developers use the `git add` command to move it to the staging area, indicating that it is ready to be committed. Once staged, changes can be committed to the repository using the `git commit` command, which saves a snapshot of the project along with metadata like author and timestamp. This process allows Git to maintain a comprehensive history of all changes, enabling developers to review modifications, revert to previous versions, and collaborate effectively on projects.
3. What is the difference between a local repository and a remote repository in Git?
   - A local repository in Git is a version-controlled directory that resides on an individual developer's machine. It allows developers to perform all Git operations, such as adding files, committing changes, and creating branches, without needing an internet connection. This local setup provides the full benefits of version control, enabling users to track changes, revert to previous versions, and experiment with new features in isolation. When a developer initializes a Git repository using the command git init, a hidden .git folder is created within the directory, containing all the necessary metadata for tracking changes. Since all operations are performed locally, developers can work at their own pace and manage their code independently before sharing it with others.

     In contrast, a remote repository is hosted on a server or a cloud platform (such as GitHub, Bitbucket, or GitLab) and serves as a centralized location for collaboration among multiple developers. Remote repositories allow team members to share their code and changes with one another through commands like git push to upload local commits and git pull to download updates made by others. Unlike local repositories, remote repositories are accessible over the internet and facilitate collaboration by allowing multiple contributors to work on the same project simultaneously. They also provide features for managing contributions, such as pull requests and code reviews, which help maintain code quality and streamline integration processes among team members working from different locations.
4. What are the basic Git commands?

   Basic Git commands:
   - **git init** - Initializes a new local Git repository in the current directory.
   - **git clone** <repository> - Creates a local copy of a remote repository.
   - **git add** <filename> - Stages changes to be included in the next commit. You can stage all changes using git add .
   - **git commit -m** "message" - Records the staged changes in the repository with a descriptive message.
   - **git status** - Displays the state of the working directory and staging area, showing which files are staged, modified, or untracked.
   - **git push origin** <branch> - Uploads local commits to the specified branch of a remote repository.
   - **git pull** - Fetches and merges changes from the remote repository into the current branch.
   - **git branch** <branch-name> - Creates a new branch or lists existing branches when used without an argument.
   - **git checkout** <branch-name> - Switches to the specified branch, allowing you to work on it.
   - **git merge** <branch-name> - Merges changes from the specified branch into the current branch.
5. How do you check the status of a Git repository?
   - To check the status of a Git repository, you use the git status command. This command provides crucial information about the current state of your working directory and staging area. When executed, git status displays which files are tracked, untracked, modified, or staged for the next commit. It also indicates if there are any changes that have not yet been committed or if the working tree is clean, meaning there are no changes to commit. This command is essential for understanding what modifications have been made and what actions you may need to take next, such as staging files or committing changes.
6. What is the purpose of branches in Git, and how do you create and switch between them?
   - Branches in Git allow developers to work on different features or fixes independently from the main codebase, facilitating parallel development without interference. This isolation helps maintain a clean and stable codebase while enabling collaboration among team members.
   - To create a new branch, use `git branch <branch-name>`, and to switch to it, use `git checkout <branch-name>`. Alternatively, you can create and switch to a new branch in one step with `git checkout -b <branch-name>` or `git switch -c <branch-name>`. To switch between existing branches, simply use `git checkout <branch-name>` or `git switch <branch-name>`.
7. What are GitLab Desktop and GitHub, and how are they different from Git?
   - GitLab Desktop and GitHub are both platforms that facilitate version control and collaboration on software projects, but they serve different purposes and have distinct features compared to Git itself.
   - Git is a distributed version control system that allows developers to track changes in their codebase, manage versions, and collaborate with others. It operates primarily through command-line interfaces (CLI) and provides the foundational tools for version control without any built-in graphical user interface (GUI). Git can be used independently on a local machine or integrated with various hosting services.

   - GitHub is a cloud-based platform that builds on Git's capabilities by providing a user-friendly interface for hosting Git repositories online. It offers additional features such as issue tracking, project management tools, and collaboration functionalities, making it easier for teams to work together on projects. GitHub also supports integrations with third-party applications and services, enhancing its functionality for developers.
   - GitLab serves a similar purpose but distinguishes itself by offering a more comprehensive suite of tools that includes built-in Continuous Integration/Continuous Deployment (CI/CD) capabilities. GitLab allows users to manage the entire software development lifecycle within a single platform, from code repository management to deployment. Additionally, GitLab can be self-hosted, giving organizations greater control over their repositories and data.
8. How do you connect a local Git repository to a GitLab or GitHub repository?
   - To connect a local Git repository to a GitLab or GitHub repository, first create a new repository on the platform without initializing it with any files. Then, navigate to your local project directory in the terminal and run git init to initialize it as a Git repository if it isn't already. Next, stage your files with git add . and commit them using git commit -m "Initial commit". After that, add the remote repository URL with the command git remote add origin <repository-url>, replacing <repository-url> with the URL of your GitLab or GitHub repository. Finally, push your local commits to the remote repository using git push -u origin main (or master if applicable), establishing the connection between your local and remote repositories.
9. What are the steps to collaborate with others using GitLab or GitHub?

   STEPS:
   - **Create a Repository**: The repository owner sets up a new project space on GitHub or GitLab for collaboration.
   - **Add Collaborators**: The repository owner invites team members by adding their usernames, granting them access to contribute.
   - **Fork the Repository** (if applicable): Collaborators create a personal copy of someone else's repository to make changes independently.
   - **Clone the Repository**: Collaborators download a local copy of the repository (or their fork) to their machine for editing.
   - **Create a Branch**: A new branch is created by collaborators to work on features or fixes without affecting the main codebase.
   - **Make Changes**: Collaborators edit files in their local branch according to the project requirements.
   - **Stage and Commit Changes**: Changes are prepared for saving (staged) and then saved (committed) with a descriptive message.
   - **Pull Latest Changes**: Collaborators update their local repository with the latest changes from the remote repository to avoid conflicts.
   - **Push Changes**: Collaborators upload their committed changes from their local branch to the remote repository.
   - **Create a Pull Request** (GitHub) or Merge Request (GitLab): After pushing, collaborators propose their changes for review and merging into the main branch.
   - **Review and Merge**: The repository owner and team members evaluate the proposed changes and merge them if they meet project standards.
10. How do you resolve merge conflicts in Git?

    There are a few steps that could reduce the steps needed to resolve merge conflicts in Git.
    - Step 1: The easiest way to resolve a conflicted file is to open it and make any necessary changes.

    - Step 2: After editing the file, we can use the git add a command to stage the new merged content.
    - Step 3: The final step is to create a new commit with the help of the git commit command.
    - Step 4: Git will create a new merge commit to finalize the merge.
11. What is a pull request, and why is it used in GitHub?
    - A pull request (PR) is a proposal to merge changes made in one branch of a repository into another, typically from a feature branch into the main branch. It serves as a formal request for code review and integration, allowing developers to discuss and evaluate the proposed changes before they are incorporated into the main codebase. Pull requests provide a platform for transparent communication among team members, enabling them to review the differences between branches, leave comments, and suggest modifications.

      Pull requests are essential in GitHub because they facilitate collaboration and maintain code quality. They help teams manage contributions effectively, especially in larger projects where multiple developers may be working simultaneously. By using pull requests, teams can conduct thorough code reviews, ensure that new features or bug fixes meet project standards, and maintain a well-documented history of changes. This process enhances accountability and fosters learning opportunities within the team, as developers receive feedback on their code and can track discussions related to specific changes.
12. What are some best practices for writing commit messages?
    - **Be Clear and Concise**- A commit message should clearly summarize the changes made, avoiding vague descriptions.
    - **Include Relevant Context**- Include context such as issue numbers or discussions to explain the motivation behind the commit.
    - **Mention Bug Fixes**: Reference and describe any bugs fixed in the commit, providing details of the problem and the solution.
    - **Organize Commits logically**- Break changes into smaller, self-contained commits that are easy to review and manage.
    - **Use Imperative Verbs**- Start commit messages with action verbs like "Add," "Fix," or "Refactor" to describe the changes.
    - **Summarize with a Subject Line**- Begin with a brief, meaningful subject line (around 50 characters) that summarizes the commit's purpose.
    - **Test and Proofread**- Test your changes thoroughly and proofread your commit message for errors before committing.
    - **Follow a Template**- Use a consistent commit message template to maintain structure and clarity across your team or project.
    - **Update Commit Messages**- Use Git's --amend option to update a commit message instead of creating a new commit to avoid clutter.

REFERENCES:

Afreen, S. (2024, July 15). *How to resolve merge conflicts in Git?* Simplilearn.com.

https://www.simplilearn.com/tutorials/git-tutorial/merge-conflicts-in-git#what_is_a_git_merge_conflict

Course Reflection

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

At the start of the system administration course, I expected to learn the basics of managing computer systems, such as setting up servers, troubleshooting, and maintaining networks. I also hoped to understand how to secure systems and ensure they run smoothly. The course met my expectations because it covered a lot of topics, especially in Linux, which I wasn't familiar with before. It helped me understand how Linux works and gave me new skills in using it for system administration.

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 many important topics, such as managing services in Windows and Linux, setting up printers downloaded from the internet, understanding EULA, working with Kerberos, using GitHub, and many more. These topics helped me understand how to handle different tasks in system administration. Managing services taught me how to control and troubleshoot systems, while setting up printers showed me how to deal with hardware and drivers. Learning about EULA and Kerberos improved my knowledge of security and licensing. Using GitHub was also useful for version control and collaboration. Each topic gave me skills that are essential for system administration.

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

Reflecting on my learning process, the most effective strategies that helped me understand and remember the course material were reviewing the lessons regularly and asking for help from my classmates. Going over the lessons after class made it easier to understand the concepts better. Talking with my classmates and sharing ideas also helped me learn faster because we could explain things to each other in simple ways.

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

Yes, the activity about EULA where we had to create our own policies for users or customers significantly enhanced my learning experience. It was effective because it made me think critically about how policies are written and why they are important. Writing our own policies helped me understand the legal and ethical aspects of system administration, like protecting users' rights and setting clear rules for using a system or service.

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

Yes, I encountered challenges during the course, especially during the finals with the Kerberos activity. Even though I followed the steps and commands given, I still ran into problems, which was frustrating. I overcame this by seeking help from my friends. They helped me figure out what went wrong and guided me through the process. Through this experience, I learned the importance of patience and troubleshooting.

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

Yes, the course encouraged critical thinking and analysis because it involved troubleshooting and monitoring servers. These activities required me to identify problems, analyze their causes, and decide on the best solutions. For example, when a server had performance issues, I had to evaluate logs, check configurations, and find ways to optimize it.

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

Reflecting on my personal growth, I gained a lot of new knowledge and skills from this course. I learned how to manage services in both Windows and Linux, set up devices like printers, and work with tools like GitHub and Kerberos. These technical skills helped me understand the responsibilities of a system administrator better. I also developed problem-solving skills through troubleshooting and monitoring servers.

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

I plan to apply what I have learned in this course to my future studies and career by using the skills I gained in system administration, such as troubleshooting, managing servers, and using tools like GitHub and Kerberos. In my future IT studies, I'll be able to solve problems more confidently. For my career, these skills will be important in any IT-related job, especially in roles like system administrator. Personally, I can also apply these skills to manage my own devices and troubleshoot technical issues.