DESIGN DOCUMENT

Javier Duran

Svatoslav Pich

Ilia Baroff

Tutor: Mikaeil Shaghelani

TABLE OF CONTENTS

1. INTRODUCTION

Project Description

During the first phase of the project the company 'Make IT Work4U' is realizing improved infrastructure for its business clients. Current clients are small to medium businesses who need help adapting their infrastructure to satisfy the ever-rising needs of the end customer. The company provides a one-stop-solution that includes acquiring and installing hardware.

Moreover, during the second phase, the company is having hard time to monitor the distribution of their resources and they lack a real time dashboard with server and client's statistics. The company has an urgent request to create an application for them to manage their infrastructure and clients.

Deliverables

- Windows Server with Hyper-V
- Windows desktop machine connected to AD
- Backup policy using an extrenal server
- Internet connection of internal hosts through firewall (pfsense)
- Functional VPN server
- A management dashboard for all real-time statistics

2. INFRASTRUCTURE DIAGRAM

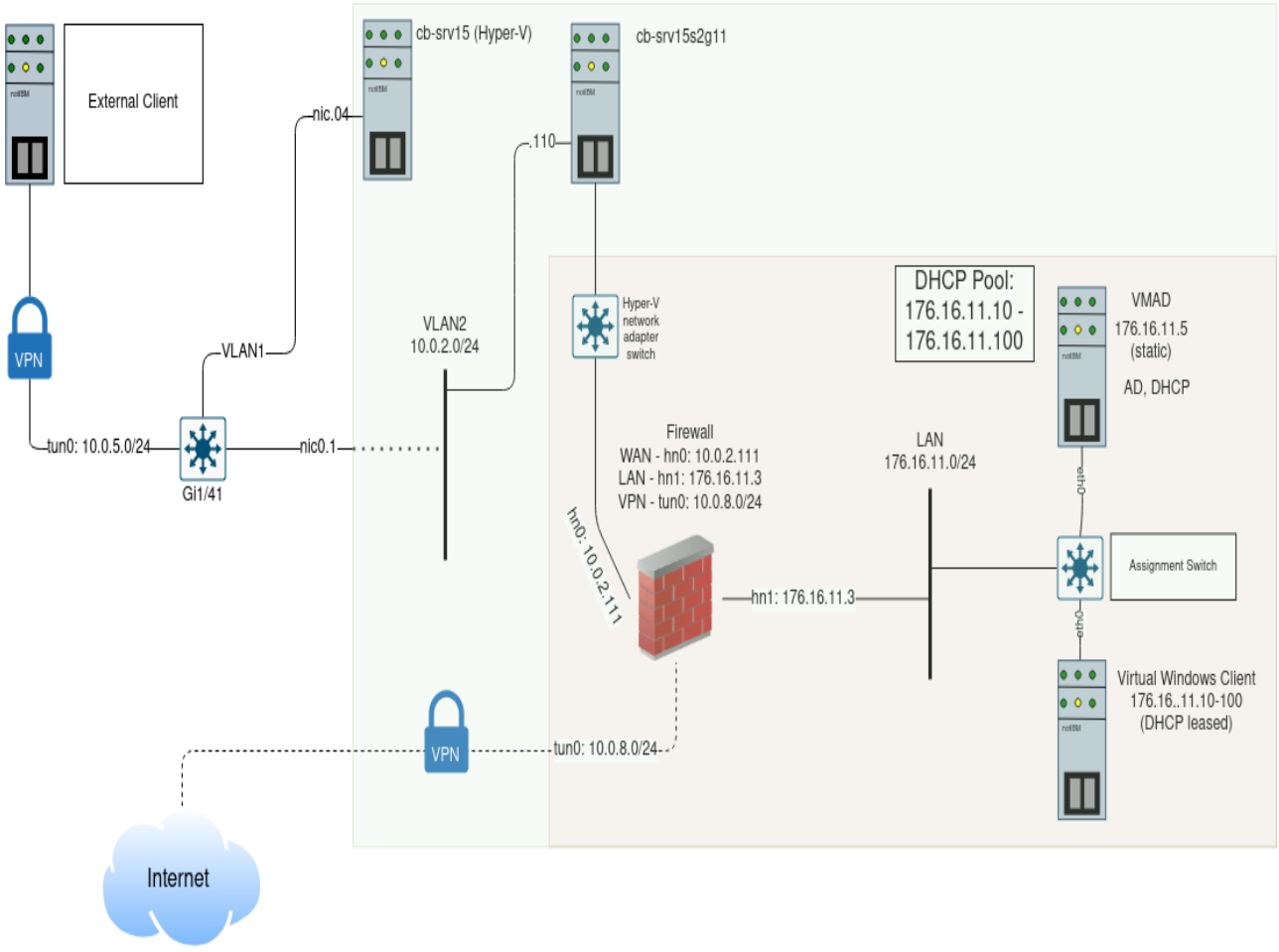

Figure 0.1

3. INFRASTRUCTURE DESCRIPTION

3.1 Windows Server

To mimic the company's infrastructure, we connected to a VPN and through Remote Desktop Connection to a Windows Server. Furthermore, after connection was established, Hyper-V was installed to be able to create a virtual environment and mimic the business infrastructure.

We are using the Windows Server OS, because it provides us with the tools and capabilities, we need to achieve our goals and furthermore is easy to use with an extensive community behind it always ready to help.

3.2 Hyper-V

The team installed Hyper-V, which is a software that is used to set up a virtual environment. In this environment we create virtual switches and machines with a given configuration such as RAM, Disk space, dynamic memory, and OS. The team installed a Windows Essentials 2019 Server operating system in a virtual machine. The virtual machine was later cloned, giving us a total of two VMS.

We decided to use this O/S because it is appropriate to the case study, as it suggests, it is best for small and medium sized business. Hyper-V will let us mimic the company being studied in a virtual environment due to the limited amount of hardware resources available. This software will be essentially used to create virtual servers and clients to install, configure and test different services.

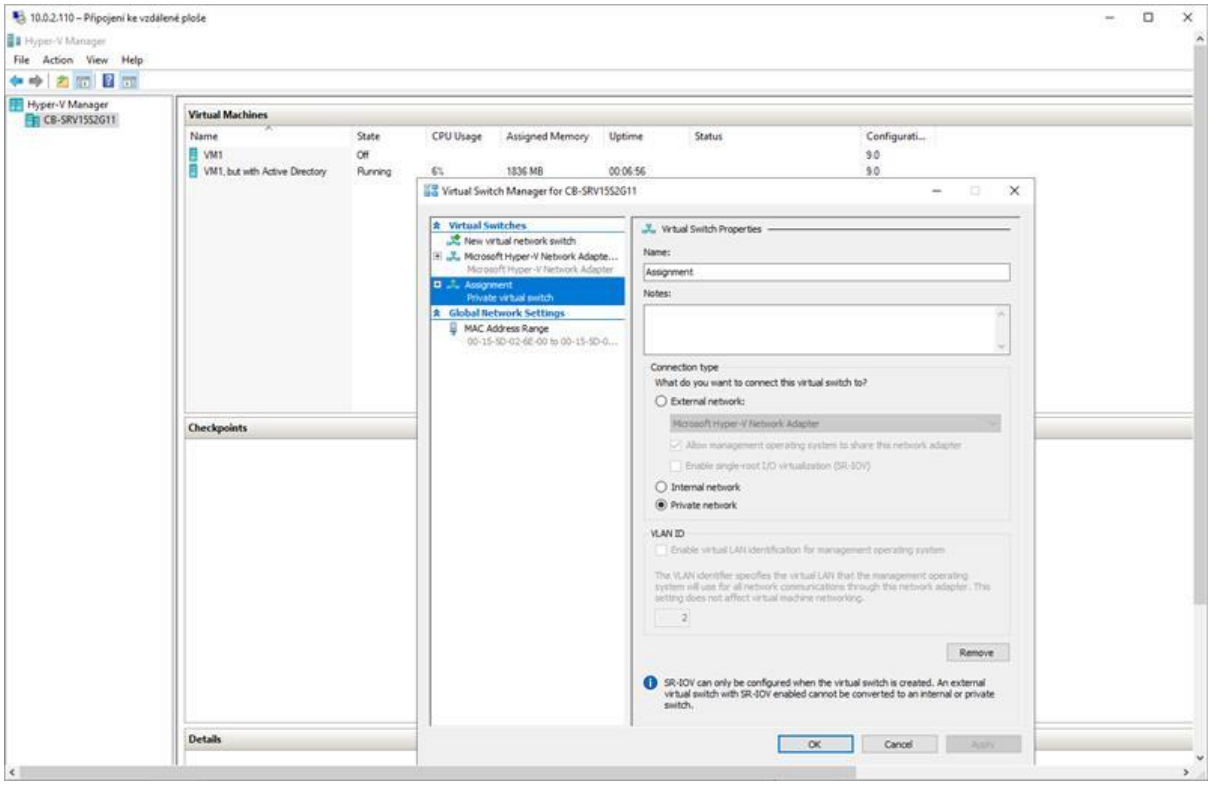

Figure 3.2

- On the above image, we can appreciate Hyper-V with a couple of virtual machines, some of which are running and some of them are turned off. VMAD is the virtual machine containing Active Directory and serving as a domain controller.

3.3 Active Directory

Active Directory is a service used on Windows Servers provided directly from Microsoft to manage and maintain accounts, groups, passwords, user rights and backups. It is an essential tool for managing the infrastructure. With this service it is possible to create new users and policies.

We are using it for automating the network, users and data management. The team will create test users, to create groups and to set up their policies. It is fundamental software for users, group management, domain management and variety of other managing tools.

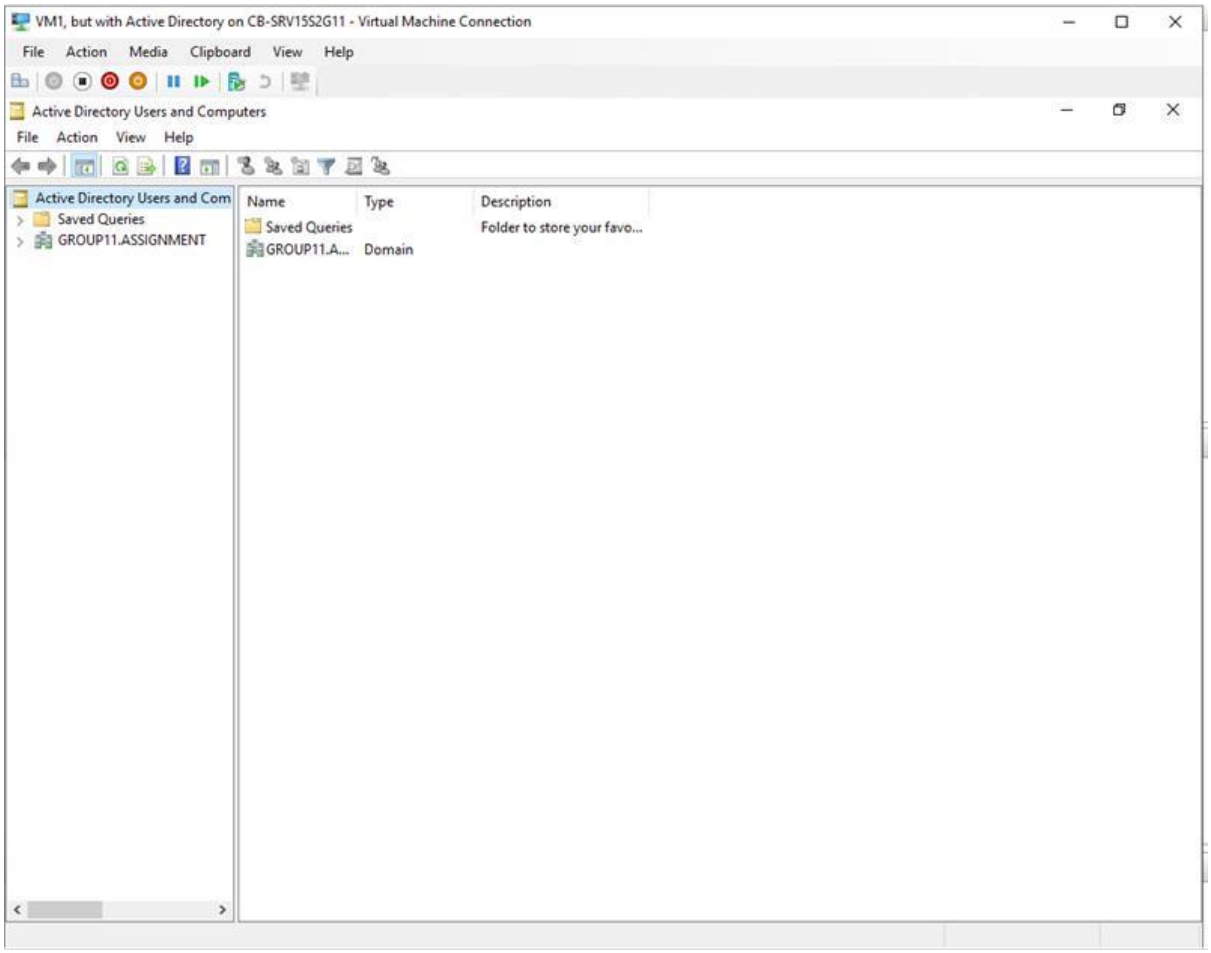

Figure 3.3

- In the image above, you can see the AD properly installed.

3.4 OpenVPN

VPN connection is a remote access protocol we are using to be able to connect to the virtual server on which we are doing all the project work. We use a personal credentials provided to us by Fontys to be able to connect to this VPN using OpenVPN service.

Without this remote connection we would not be able to connect to the network from which it is possible to remotely access our virtual environment, therefore rendering this service pivotal in our pursuits of project goals. We use VPN because the connection is stable and more secure than SSH for example.

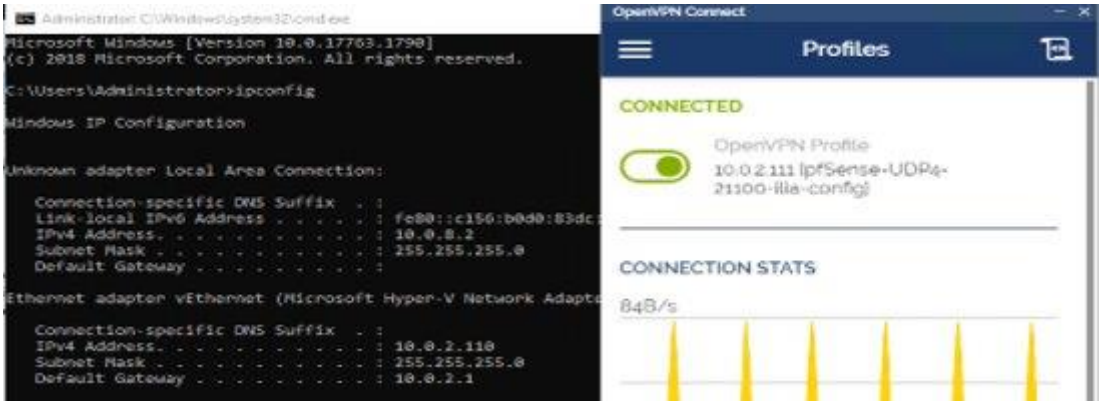

Figure 3.4

- In the image above we can see a successful connection to the VPN from outside the LAN.

3.5 Windows Server Manager

Server Manager is a management console in Windows Server that helps provision and manage both local and remote Windows-based servers from their desktops, without requiring either physical access to servers, or the need to enable Remote Desktop Protocol (RDP) connections to each server (Microsoft).

This software is used to install roles on the server, change its name, IP address, etc. It is the base tool for all the necessary installations of roles. Mainly Active Directory, DHCP, DNS and Hyper-V. For these reasons we deem this software necessary in most of steps we are undertaking during the project.

3.6 Firewall

A firewall is a network security software that monitors and controls incoming and outgoing network traffic based on predetermined security policies (Check Point Software Technologies, n.d.). Therefore, providing security to the nods and machines that are connected to the Internet. Pfsense firewall will be installed in one of the virtual machines to make a dedicated firewall/router for our private network.

We will use firewall to provide security and connectivity as it will work as gateway for our private network. This way the team will be able to properly install and configure services and a VPN so that employees have a remote connection to the server.

Not only that Pfsense firewall provides us with a needed security, it also provides us with the internet connection by connecting our private LAN to WAN with an internet using beforehand provided upstream gateway.

3.7 Backup

As for a backup software we decided to use Windows Server Backup feature that can be installed using Server Manager. We find this tool a very reliable software considering it is provided by Microsoft directly. You can specify a very detailed backup schedule using Windows Server Backup as either repeated or 'just once' backup and choose a partition or another specified place where the backup files would be.

Backing up the server data is a pivotal thing to have in case of disruptions from the outside, errors or a loss of important data. Therefore, we set up a recurrent backup at least once a day at 21:00.

4. GROUPS & POLICIES

Creating groups and policies is a utility widely used in almost all companies with any working infrastructure. They allow us to manage people's accounts and apply needed policies by groups.

4.1 Groups

We created groups of users by their department. IT, Sales, Production. All of which we created in AD and put some testing user accounts in there. Using command "gpresult /R" we

were checking whether the user was in fact in the applied group also what policies were applied to him.

We decided to use the groups for easier policy introduction to several users at one go.

4.2 Policies

By using GPO, we created a set of policies that are applied to our organization unit. We decided to ban access to command prompt and Powershell to production and sales groups as we saw it as a tool these departments will not be needing to use. Then we linked the policy to the main organization unit for it to work. Afterwards we tested it and checked that it worked. We also tried to look on the internet on which policies are usually applied to the certain departments and tried to introduce several of them.

The usage of group policies is by us seen as a mandatory thing in the network infrastructure and therefore we deemed it crucial to try and introduce at least basic policies to our infrastructure just to know how it works and how are they introduced.

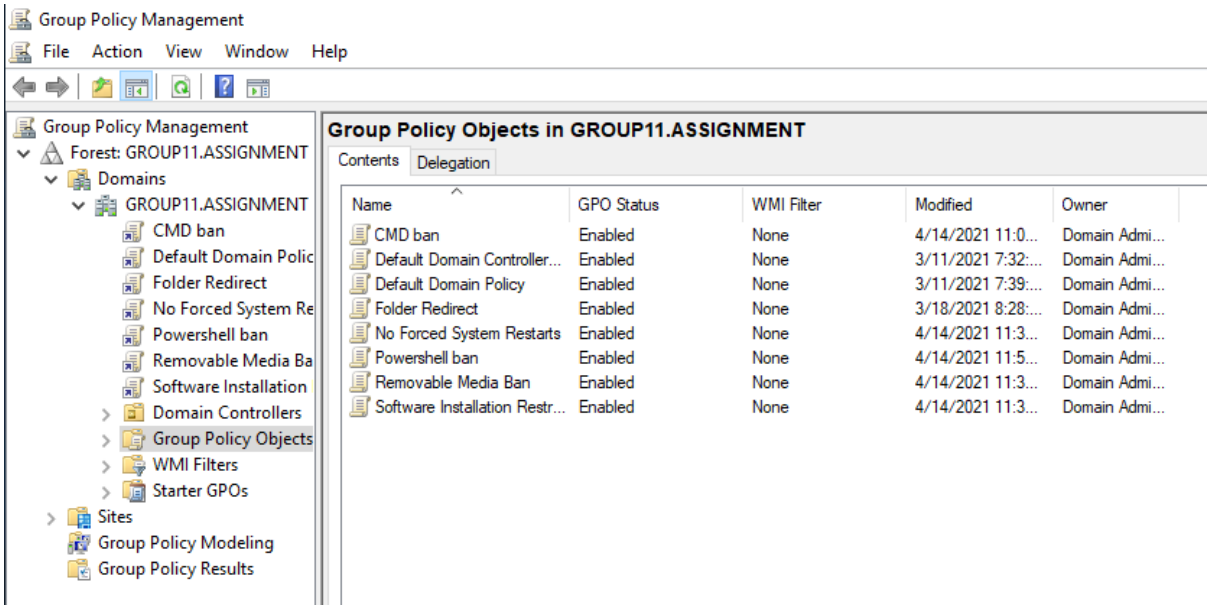

Figure 4.2

5. MANAGEMENT TOOLS

The team 'MakeIT Work 4U' developed a set of scripts and applications that will help the company manage and monitor some of the most important aspects of the infrastructure installed, such as, system key performance indicators, saving data system log entries to database and being able to perform CRUD operations and a DHCP log parser. All tools can be found in the following git repository: https://git.fhict.nl/I408431/casestudy1-group11.git

To make sure the applications properly work run the following command for the first time in a system: pip install -r requirements.txt.

5.1 System KPI Monitoring

The KPI Monitoring script gives us the basic information of the resources of the server such as CPU usage, memory availability and usage, disk information, and network interfaces information. The script takes information from the system and displays it in a Tkinter UI. This tool is uses psutil library which helps us take information directly from the system. It is useful mainly for system monitoring, profiling, limiting process resources and the management of running processes.

The tool is used by opening the file or from the command line by typing python kpi.py, after press enter.

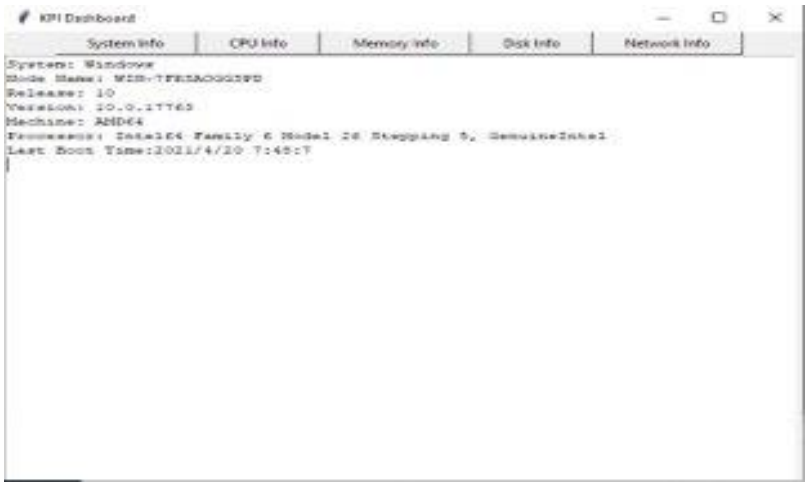

Figure 5.1

- In figure 5.1 we can observe the System Info section of the system KPI dashboard.

5.2 Events to Database

The script events.py will take user input to get the desired events from the main Windows logs, which are: Application, Security and System. Data can be filtered through different user input given in the script. For example, log, entry type and the number of latest entries to be sent to the database and a CSV copy.

This script can be used by running in it in the command line by writing and entering python events.py from the eventsToDB folder in git. Answer the questions to filter the data from the event logs and save them into the database.

5.3 Database Manager

As a compliment for the events.py script, which as mentioned above sends data from a specified event log like Application, Security or System logs, the team developed the database manager tool for this database. Giving the IT administrator the possibility to save the most important events saved or modify some data to remark and highlight important issues. The database manager tool performs the basic CRUD functions on the database created by events.py script.

The database manager tool can be launched from the command line typing and entering python manage.py or by double clicking the file in the folder.

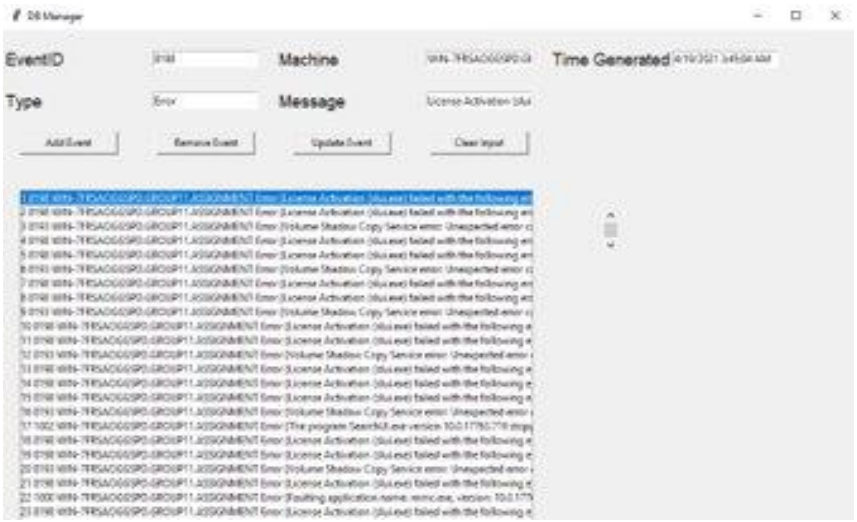

Figure 5.3

- In figure 5.3, the database manager application with some data. CRUD applications buttons.

5.4 DHCP Log Viewer

The DHCP Log Viewer tool takes a DHCP log from the desired day and prints it into a textbox. Sometimes data can be too much to be displayed in the textbox, therefore we made it possible for the user to input his or her email and receive a copy of the data in CSV format which can be easily read with excel. This will help the IT administrator get and save the data in his own personal computer for analysis if needed.

To make use of this tool run the script dhcp.py by double clicking on the file or running python dhcp.py in the command line.

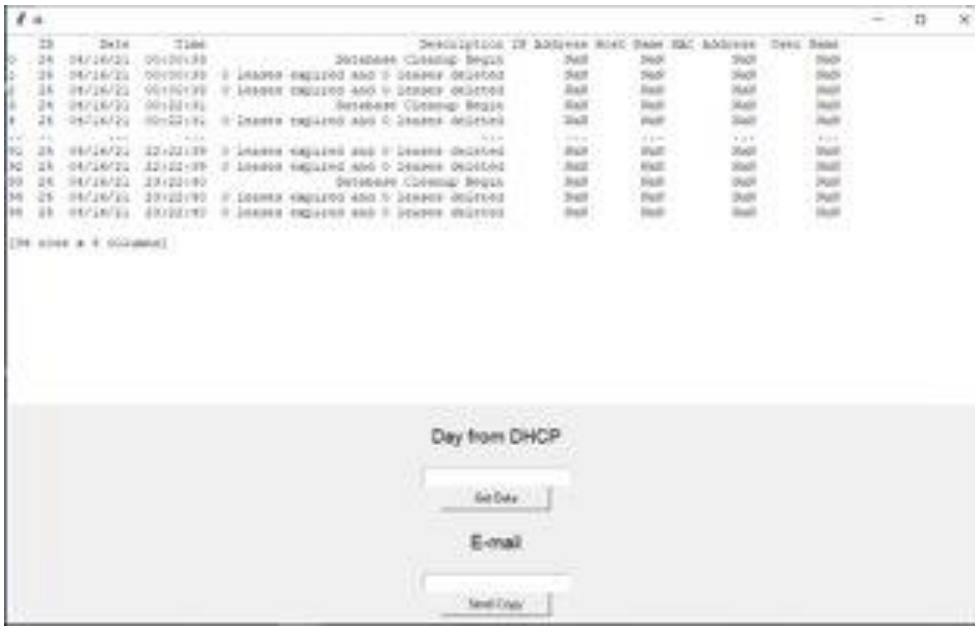

Figure 5.4

- In figure 5.4, the DHCP Helper has received data from a DHCP file and can be sent through email to the administrator.

5.5 Network Scanner

The network scanner script is used to get all the hosts (IP's) that are currently taken in network. It takes the input from the user to give a network IP, for example IP address will be 176.16.11.1 and IP range from 1 – 15 the script will check for all live hosts that are inside

range 176.16.11.1 – 176.16.11.15. This tool is useful to check what IP's are currently being used from our DHCP server.

To make use of this script we need to run the following command in the command line: python network.py and fill in the required input.

5.6 WinSCP & Task Scheduler

To automate some functionalities in our server we used WinSCP and Task Scheduler. We used it to run two tasks that will help our applications become more relevant and have automation in our server. First task will run a Powershell script that will get event logs from the main logs which are Application logs, Security logs, and System logs. After getting the log files it will convert them into CSV type files. Second task will run a batch file that will create a SFTP connection between client and server. After creating the connection, the files received by the first task will be sent to the main server. These tasks are scheduled to happen every day at 9:00pm.

6. MOSCOW

Must Have	1. Properly installed Hyper-V 2. Active Directory 3. Domain Controller 4. Firewall 5. Minimal viable product for management tools 6. DHCP Server 7. Scheduled backups
Should Have	1. Open VPN connection for remote access 2. Groups 3. Group policies for security 4. Use SCP to send monitoring activity log files 5. Some automation tools/tasks
Can Have	1. Extra security measures. 2. Proxy server 3. Centralized database 4. Multiple automation tools/tasks
Won't Have	1. Completely working/ no bugs or issues applications 2. All in one management tools

7. CONCLUSION

We believe we did a lot of work on this project and learnt a lot of new things about how to work and orient ourselves inside the actual network infrastructure. We faced an ample errors, hindrances, difficulties, and mistakes on our part but all in all we believe we were able to overcome the vast majority of those and in the end deliver a solid outcome on our part.

There are however still some matters that could get more attention given if we had more time. Be that the group policies where we all can imagine a couple of things that could require a user restrictions and rights or the time management of the group that we had. Some aspects certainly could do with some improvement.

To sum it all up, we believe we delivered a solid project outcome with certain aspects on which we could work further given more time and it gave us a lot of vital experience in the field of infrastructure that we deem quite interesting and mainly useful.

REFERENCES

Check Point Software Technologies. (n.d.). *What is Firewall?* From CheckPoint: https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/#:~:text=A%20Firewall%20is%20a%20network,network%20and%20the%20public%20Internet.

Microsoft. (n.d.). *Server Manager.* From Microsoft Docs: https://docs.microsoft.com/en-us/windows-server/administration/server-manager/server-manager#:~:text=Server%20Manager%20is%20a%20management,rdP)%20connections%20to%20each%20server.