BAIST COMP3000

Technical Documentation and KB Articles

Submitted By

Jithin Jose

200563286

Submitted to

Nichol Campbell

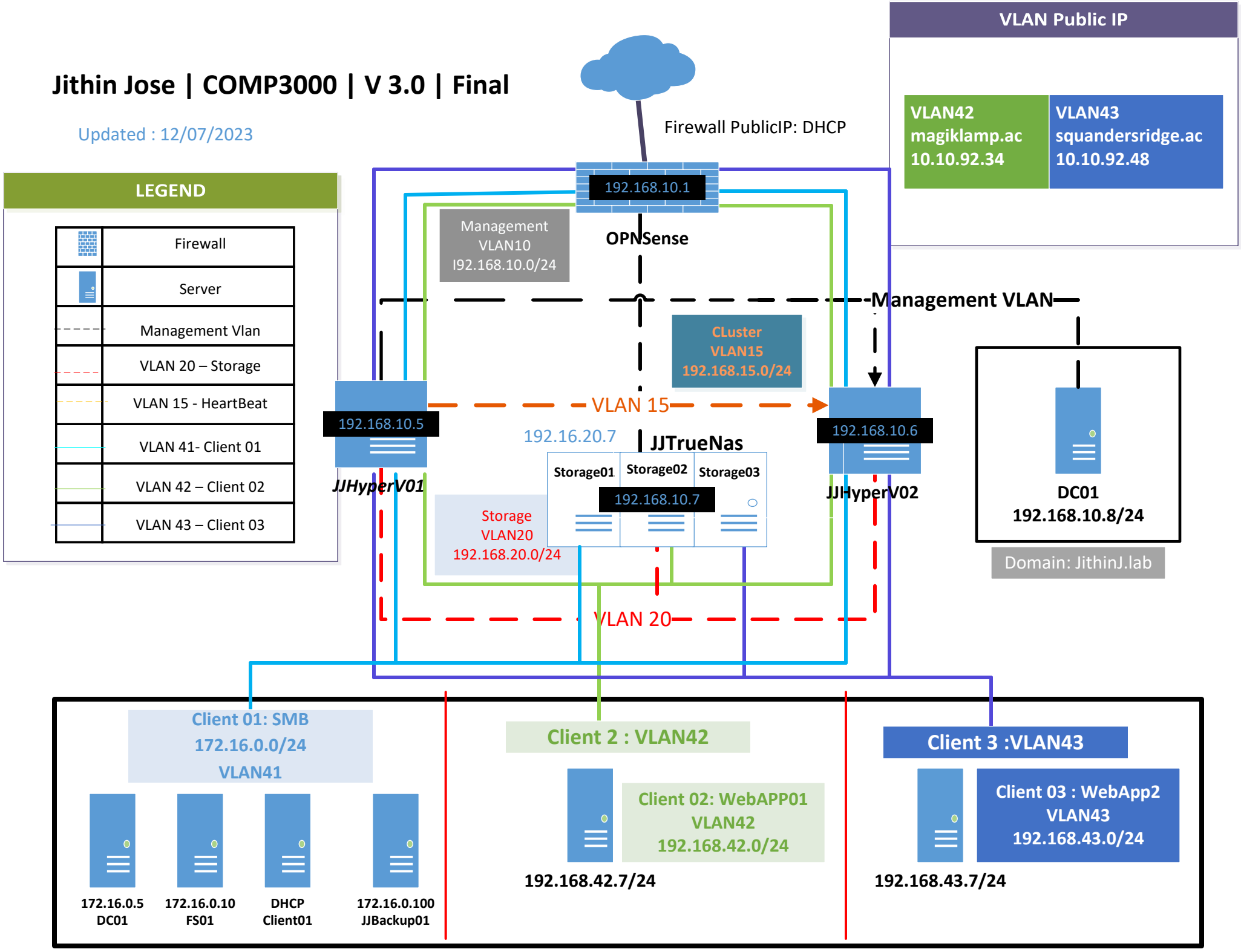
12/08/2023

Table of Contents

Table of Figures

Jithin Jose | COMP3000 | V 3.0 | Final

Updated : 12/07/2023



Introduction

I am Jithin Jose, a personable and dedicated IT professional with a proven track record of over 4 years in a dynamic and fast-paced IT company. I bring forth a strong ambition and comprehensive expertise in the realms of Windows server management, Azure cloud services, networking, and Linux administration.

In my previous role, I garnered recognition for achieving the highest company-wide quality satisfaction rating. Through strategic initiatives, I successfully reduced client wait time by 20%, resulting in a noteworthy enhancement of client satisfaction ratings. My commitment to excellence and a results-driven approach positions me as an asset in delivering optimal IT solutions and services.

Current State Overview

Domain Controller (DC):

The Domain Controller is set up to manage the network's user accounts, security policies, and directory services. The other features on this DC are DNS, DHCP

Server	IP Address
DC01	192.168.10.8

2 Nodes with Windows Server Hyper -V:

Windows Server Hypervisor clustering has been implemented to ensure high availability and fault tolerance.

Server	Roles	Management	HB	WebApp01	WebApp02	SMB
JJHyperv01	Hyper-V	192.168.10.5	192.168.15.5	192.168.42.5	192.168.43.5	172.16.0.6
JJHyperv02	Hyper-V	192.168.10.6	192.168.15.6	192.168.42.6	192.168.43.6	172.16.0.7

Client Virtual Machine (VM) for Testing:

A client VM has been created and stored on Storage 1 for testing purposes, likely to evaluate live migration and failover clustering.

Server	IP Address
Webapp1	192.168.41.7

Preconfigured Networks for Clients:

Networks have been preconfigured to meet the specifications outlined in the Cutsheet, involving IP addressing and routing configurations.

Management Network:

A dedicated network has been set up for managing and monitoring the infrastructure components such as Firewall, True Nas, 2 Nodes, and DC

Devices	Virtual Machine	Internal IP Address	Default Gateway
JJHyperV01	Windows Server 2022	192.168.10.5/24	192.168.10.1
JJHyperV02	Windows Server 2022	192.168.10.6/24	192.168.10.1
JJTrueNAs	FreeNAS	192.168.10.7/24	192.168.10.1
DC01	Window Server 2022	192.168.10.8/24	192.168.10.1
Firewall	OPNSense	192.168.10.1/24	192.168.10.1

Storage Area Network (SAN) or Virtual SAN (vSAN):

For SAN, True Nas has been configured with RAID 5 using four 100GB disks, ensuring data redundancy and fault tolerance with four separate storage pools. 3 for Clients and 1 for Witnesses.

Disk Witness	VOLUME	43.95 GiB	44.88 GiB	Inherits (lz4)	7.63
SMB01	VOLUME	92.3 GiB	93.23 GiB	Inherits (lz4)	7.66
WEBAPP01	VOLUME	68.12 GiB	69.05 GiB	Inherits (lz4)	7.78
WEBAPP02	VOLUME	69.22 GiB	62.64 GiB	Inherits (lz4)	1.59

Figure 1: Storage Zvol on the iSCSI storage

Target	LUN ID	Extent
smbtarget	0	smbextent
webapp1target	0	webapp1extent
webapp2target	0	webapp2extent
witnesstarget	0	witnesextent

Figure 2: Linked Extend to Target

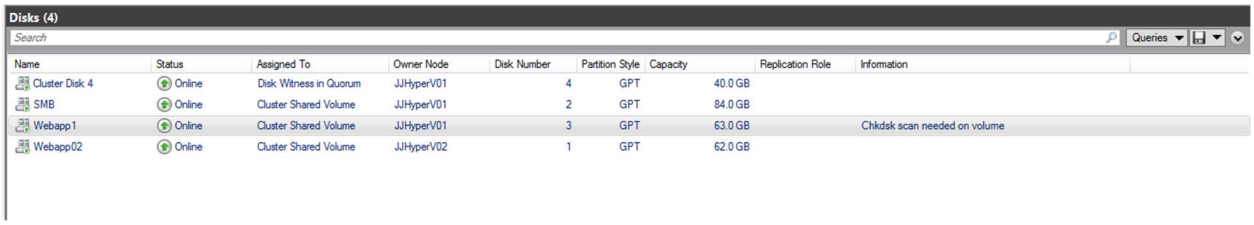


Figure 3: Segregated disk storage on the Hyper-V

Configured Firewall with OPN Sense

A firewall has been configured according to the Firewall Guide. It includes the NAT, VLAN, and Interface required for the Lab. Nat Forwarding accordingly.

			Source		Destination		NAT	
	Interface	Proto	Address	Ports	Address	Ports	IP	Ports
	LAN	TCP	*	*	LAN address	80, 443	*	*
	WAN	TCP	*	*	10.10.92.34/20	80 (HTTP)	192.168.42.7	80 (HTTP)
	WAN	TCP	*	*	10.10.92.48/20	80 (HTTP)	192.168.43.7	80 (HTTP)

Figure 4: Nat forwarding table in the firewall.

Configured Virtual Settings that connect public IP to each web app and assigned.

Address	VHID	Interface	Type	Description
10.10.92.34/20		WAN	IP Alias	Webapp01
10.10.92.48/32		WAN	IP Alias	Webapp02

Figure 5: Virtual IP settings on the firewall

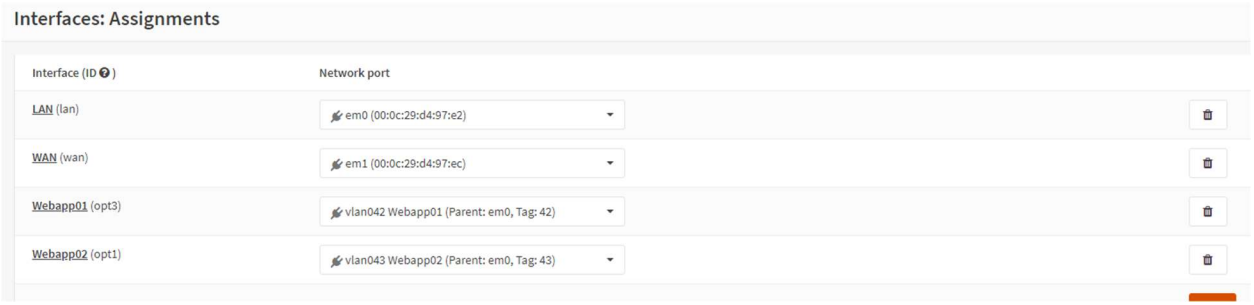


Figure 6: Assignment of the interface in the firewall

Connected to Ultra Cloud ISP:

The firewall is connected to the Ultra Cloud Internet Service Provider (ISP), enabling internet access for the network.

Preconfigured Networks for Clients (reflecting Cutsheet):

Network configurations for clients align with the specifications mentioned in the Cutsheet.

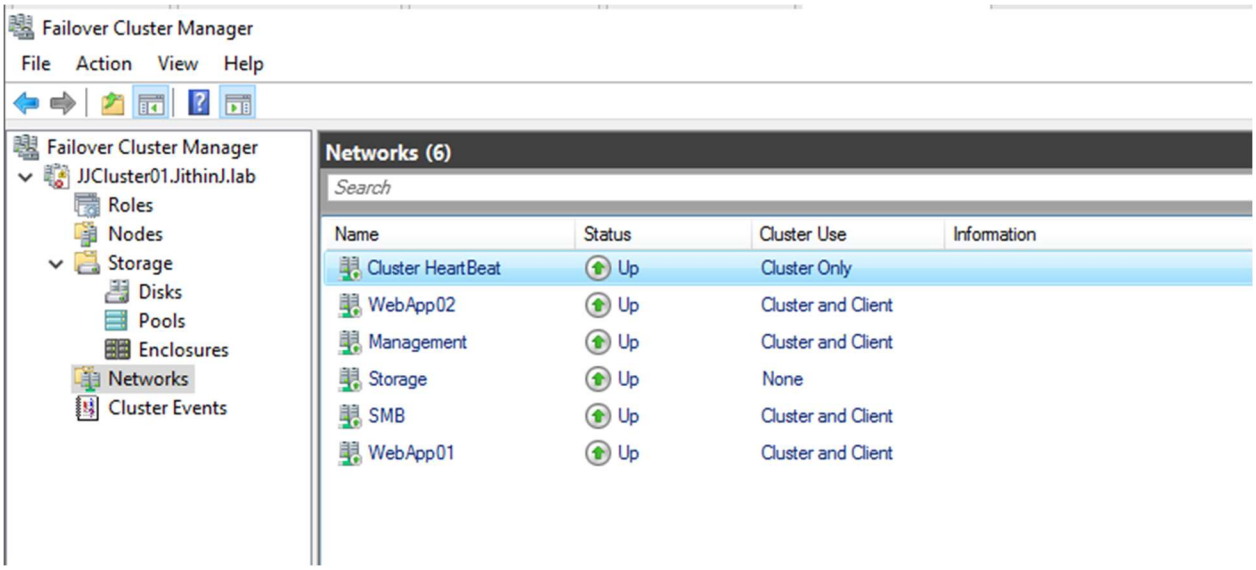


Figure 7: Preconfigured network for the clients

VLANs Created and Tagged (reflecting Cutsheet):

VLANs have been created and appropriately tagged to segment the network, enhancing security and network management.

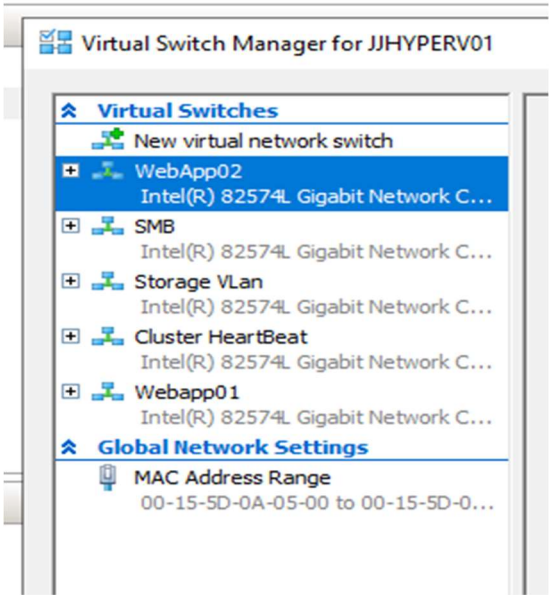


Figure 8: Created Switch with VLAN and tagged

IT Manager Account (Domain Admin):

An IT manager's account with domain admin privileges has been created on DC01.
Username: BAITSNM
Password: P@ssw0rd

Cient01:Dundermifflin. local

Client01 is configured with the Domain Controller, File Server, Backup Server, and Windows 10. All the servers in Client 01 are Windows servers, we have installed ADDS on DC01, and FS01 acts as the file server. The Backup server is named JJBAckup01. Also added a 40 GB drive to FS01 as K:/ and created share permission for the mounted drive. Users are also created inside the DCFS and added to eh separate group with different folder permissions.

DC Server here also acts as DHCP server and ADDS. Whereas FS01 is only used for file sharing within the domains There is also a backup server installed on this Domain which also contains the Monitoring Software. Backup Server backups up DC and File Server

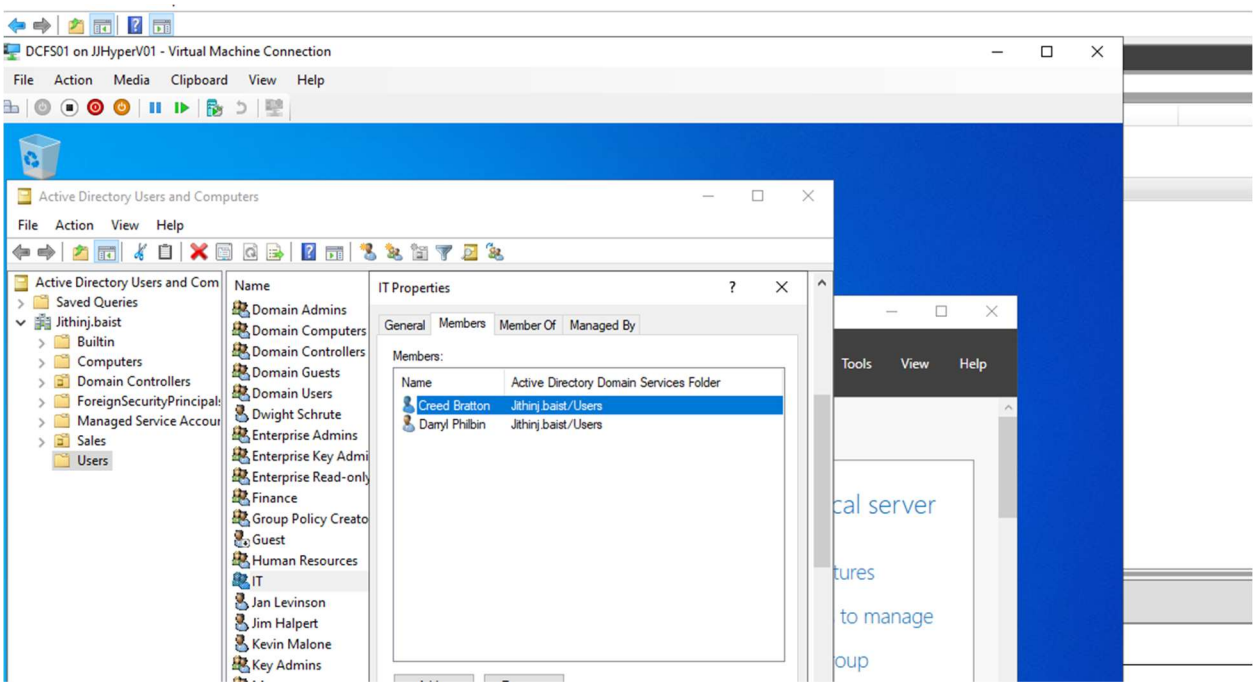


Figure 9: Windows Server(DCFS) and Windows Client

We used Acronis for the Backup Server and PRTG for Monitoring software. This is a third-party application and is installed with full support.

Client02

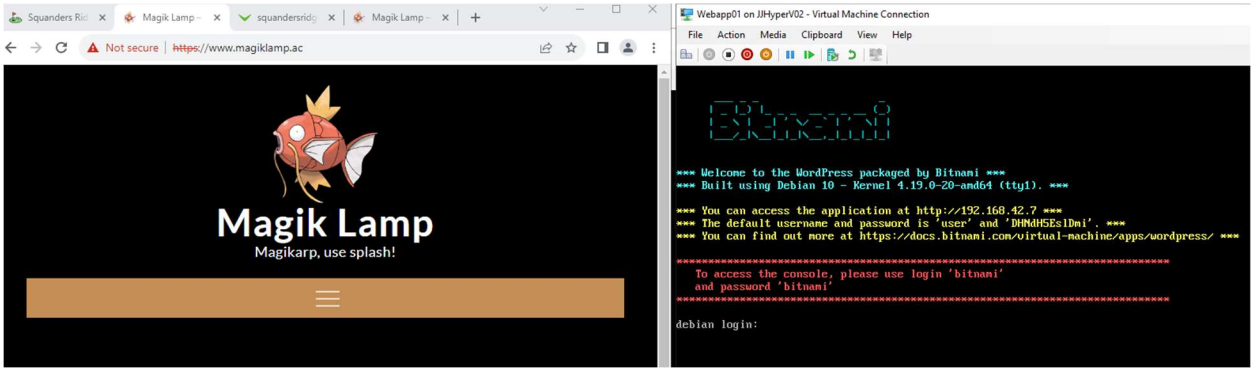


Figure 10: Webapp01 is configured with the External DNS(magic lamp.ac)

Webapp is configured using Hyper-V. Here, we had to convert the OVA to a VHD disk. I used the Star Winds V2V converter to convert Ova to VHD. Configure a static IP address on the web app with the internal IP address as 192.168.42.7. The Web app is a Debian-based Linux OS with Bitnami installed.

Client03

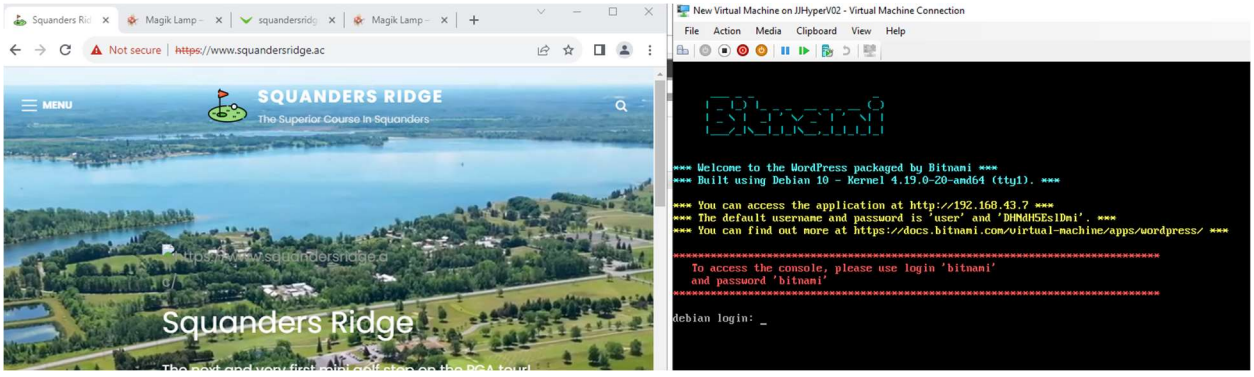


Figure 11: Webapp02 is configured with the External DNS(squandering.ac)

Webapp is configured using Hyper-V. Here we also had to convert the OVA to a VHD disk. I used the Star Winds V2V converter to convert Ova to VHD. Configure a static IP address on the web app with the internal IP address as 192.168.43.7. The Webapp are Debian based Linux OS with Bitnami installed.

External DNS

Internal Webapps are assigned with the public IP. Here, the web main DNS external server introduced on Ultra cloud is used to set up the DNS server. In this assignment, we log into the External DNS server using the Domain name and credential password provided. On the login page, we go to the DNS manager to set up the public IP address for the DNS server. Here we must 10.10.92.34 as the A name for magiklamp.ac as well

as 10.10.92.48 as a Squanderridge.ac. We are using the NAT translation on the OPN sense server to convert the Public I to the internal address.

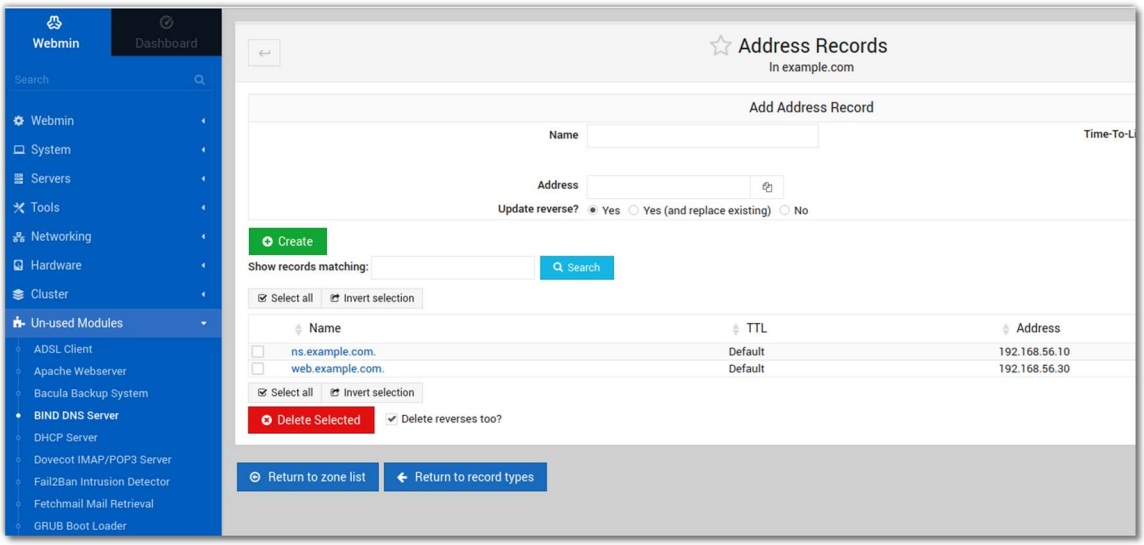


Figure 12: DNS server settings in the Webmin DNS server

Configured Reflection on the OPN Sense

This is the configuration that is enabled on the OPN Sense firewall to get the web apps working from the internal network. To set up the reflection, we need to allow traffic to go through the internal web app network. Also, make sure NAT is configured on the firewall which is pointing to the Internal Webapps. Reflection is configured according to the Guide. Technically, it asks the router to allow the public IP to go out and come back to the same network. So, when the client on a different try to access the website of another client, reflection on the firewall can allow the website to access using their public IP.

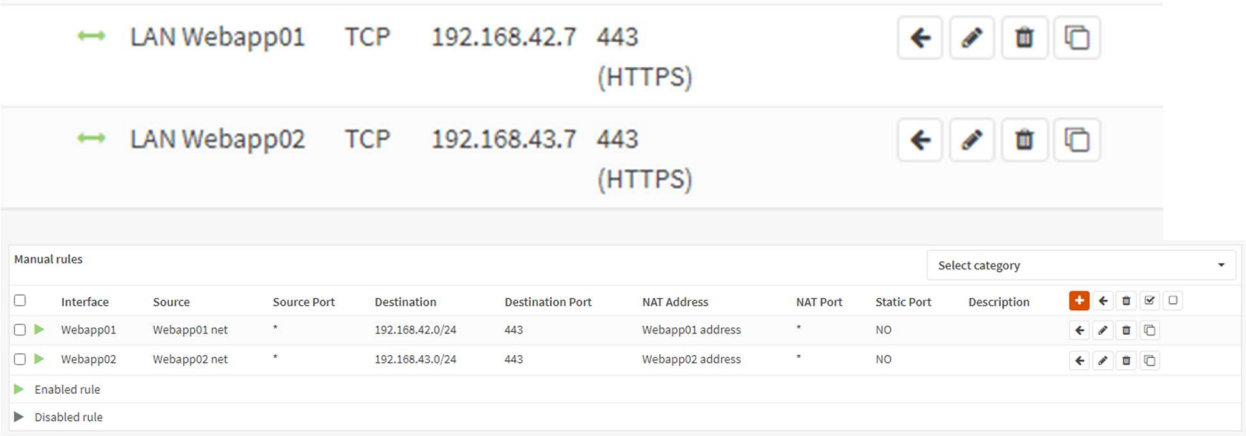


Figure 13: Firewall Settings with NAT and reflection

Client 1 Backup Documentation

Description of this Backup Software

Reasons for Choices:

- **Acronis:** Acronis is user-friendly and comes with different features and it also supports FTP and cloud backup. Acronis is known for its comprehensive backup solutions and ease of use.
- **Block Backup on DC:** This choice is likely driven by the need for a full system recovery in case of a disaster on the domain controller.
- **File-Level Backup on File Server:** For efficiency and to target specific critical data on the file server.

Backup Scope:

- **Block or Entire Machine Backup on DC:** I choose Block Level for the domain controller (DC) as it needs to be recreated from scratch if it fails. Therefore, an entire block-level backup ensures a complete system recovery in case of a failure.
- **K Drive Files on File Server:** For the file server, I chose the entire K drive because a new system can be created and recover files from that system easily. This is a more granular approach, focusing on essential data rather than the entire system.

Frequency:

- **Full Backup:** Scheduled for Friday evenings. This is a comprehensive backup that captures the entire system or selected data.
- **Incremental Backup:** Set every 15 minutes. Incremental backups capture changes made since the last backup, helping to minimize data loss in case of an incident.

Backup Type:

- **Local Backup:** This backup can be used for sudden recovery. If a file corrupts or is deleted accidentally, we can use this local backup on the site to recover the files on the server. The local backup is a fast and reliable backup for day-to-day life. It is backed up on the backup server on the same subnet and backed up on \\jjbackup\e drive. It is authenticated with a backup username and password.
- **FTP Backup:** This is an offsite backup. This backup is created away from the network. This type of backup can help if an organization is infected with different kinds of worms. Viruses and if an organization is hacked by phishing. It is backed up on the FTP server in the ultra-cloud. The FTP server is an offsite backup, and

the server IP is 10.11.8.20 and authenticated with a student ID username and password.

- **Cloud Backup:** This involves backing up your data to an online cloud storage service. The files are stored in Acronis Cloud Backup. This type of backup saves the organization if there is an economic disaster like a Tsunami or earthquake. This backup can be used to restore files to the systems. It is backed up on the one drive.

KB Article

Installing the Backup Software

Step 1: Install a new Windows Server VM on the same Network to act as a Backup Server.
Step 2: Create an Account on the Acronis Backup Website and register for the Cyber protection console.
Step 3: Download the client-side Installed from Download Acronis Cyber Protect So we can create a management Backup Server.
Step 4: On the Management Server, Choose it as the protection server and Management
Download Acronis Cyber Protect

Figure 14: Selecting the type of Agent.

Step 4: On VMs that need backup, just choose the protection agent. For Example, you must choose the protection agent on the FS01 and DC01.
Step 5: To get the registration token, we need to go to the management server and get the token using the **ADD** button on the top and Click Generate

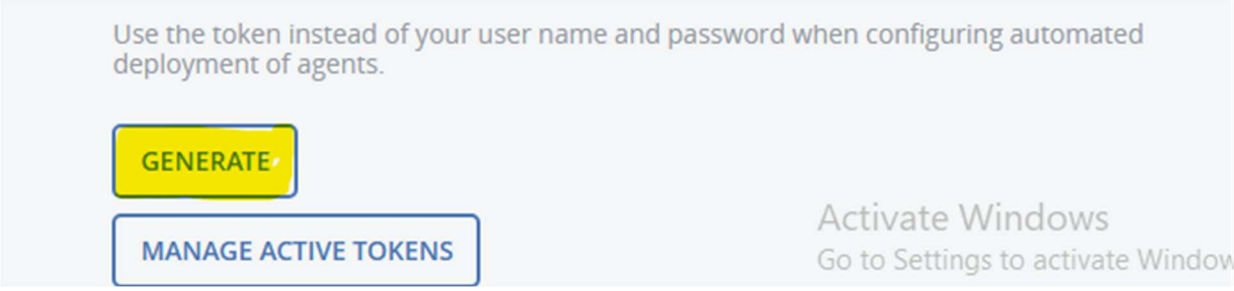


Figure 15: Creating a token for the clients

Step 6: While installing the protection Agent, you can link the protection agent using the registration token.

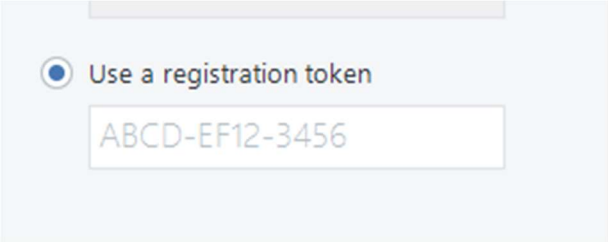


Figure 16: Adding the registration token to the Agent client

Step 7: After Installation, You should able to see all the devices on the Backup Agent.

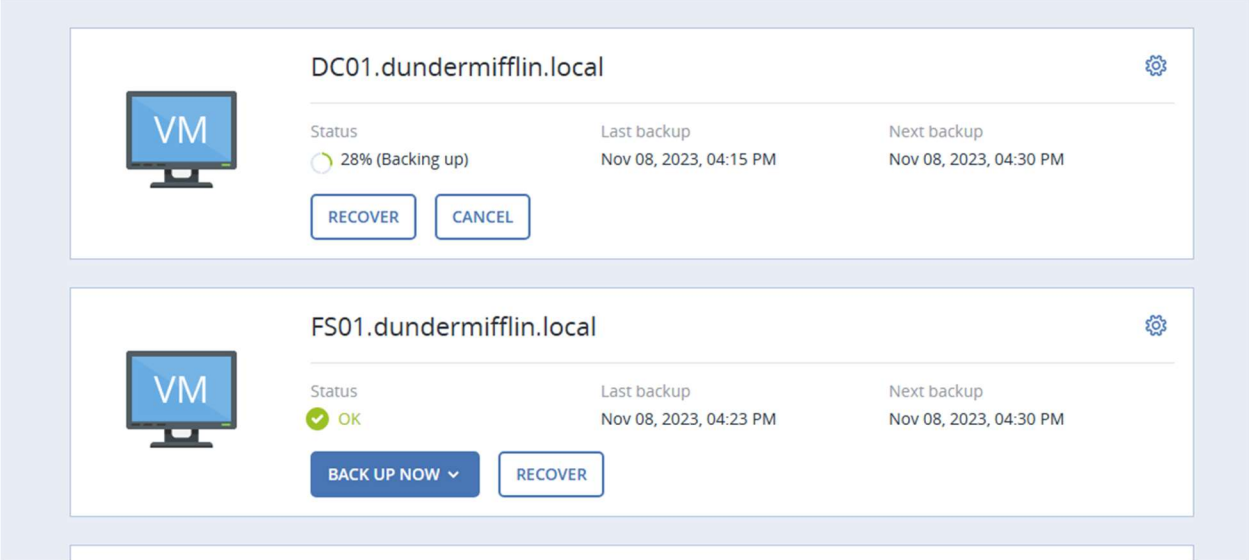


Figure 17: Shows all the devices in the Backup Agent

Creating the Backup Plan using the 3-2-1 methodology

Plan 1: Cloud Backup

Step 1: On the device that needs to be backed up, Click the settings bar on the right corner.

Step 2: Choose the option to **protect,** the first option
Step 3: On the right top corner, Click the **add plan** button.

Figure 18: Creating a new plan on the Backup Management Server

Step 4: Rename the Plan accordingly. Here for Example- Cloud Backup

Step 5: On the option **Where to Backup,** choose the **cloud Storage**(you might need to log into your account the first time)

Figure 19: Creating a plan for the Backup Server

Step 6: On the Schedule settings on the above change the **Backup Scheme** option to custom choose the incremental backup every 15 minutes.

Step 7: On the Schedule settings the above change the **Backup Scheme** option to custom and Under **Full Backup** select a day in the week

Step 8: Make sure all the backup settings are configured and choose the right location for the backup.

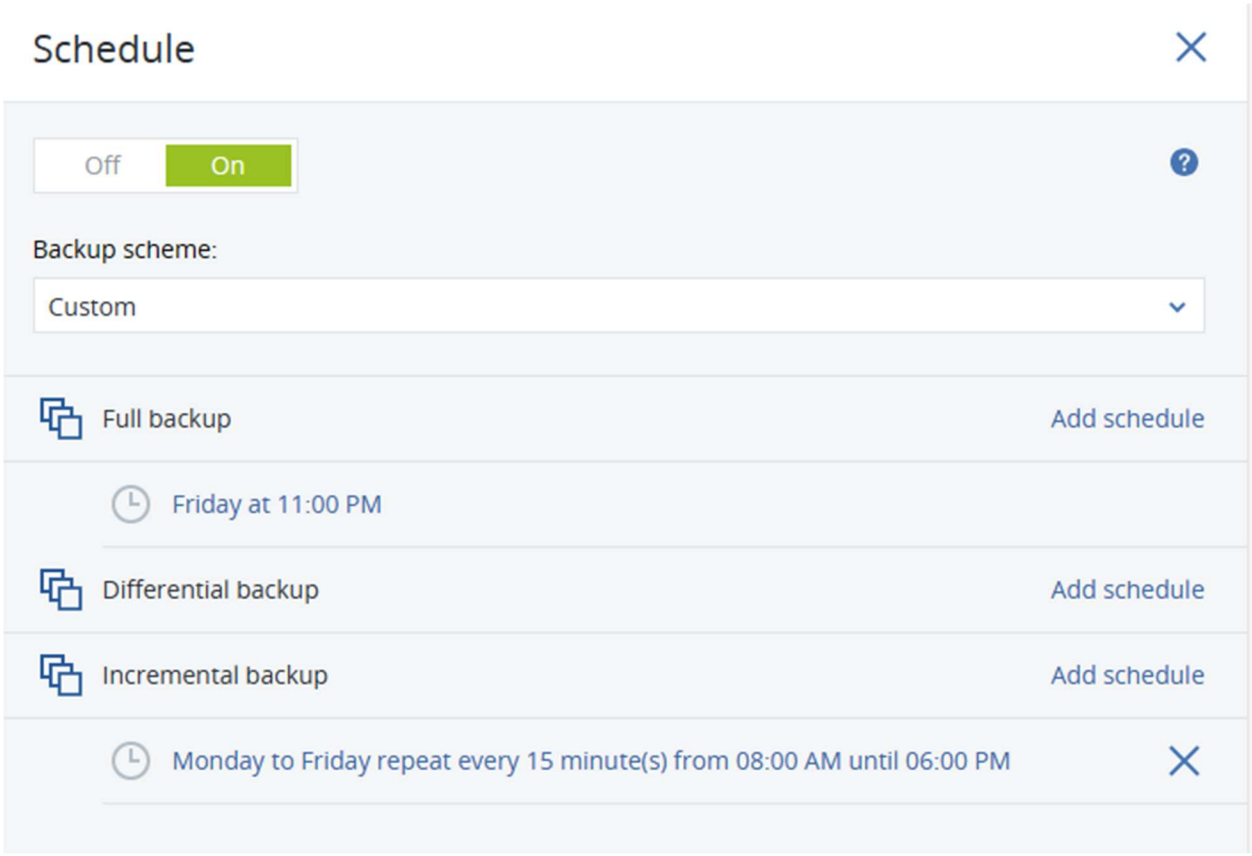


Figure 20: Creating a schedule using the Backup Management Server

Step 9: Click **Create** in the top corner, now the full backup plan is created.

Plan 2: FTP-Backup(offsite)

Step 1: On the device that needs to be backed up, Click the settings bar on the right corner.
Step 2: Choose the option to **protect,** the first option.

Step 3: On the right top corner, Click the **add plan** button.
Step 4: Rename the Plan accordingly. Here for Example- FTP-Backup
Step 5: On the option **Where to Backup,** click on the **Add location** on the right corner
Step 6: Select the **SFTP** from the right corner.
Step 7: Specify the FTP server name as **sftp://10.11.8.20/.**
Step 8: Credential Window pops up, type in **student-id** and **password.**

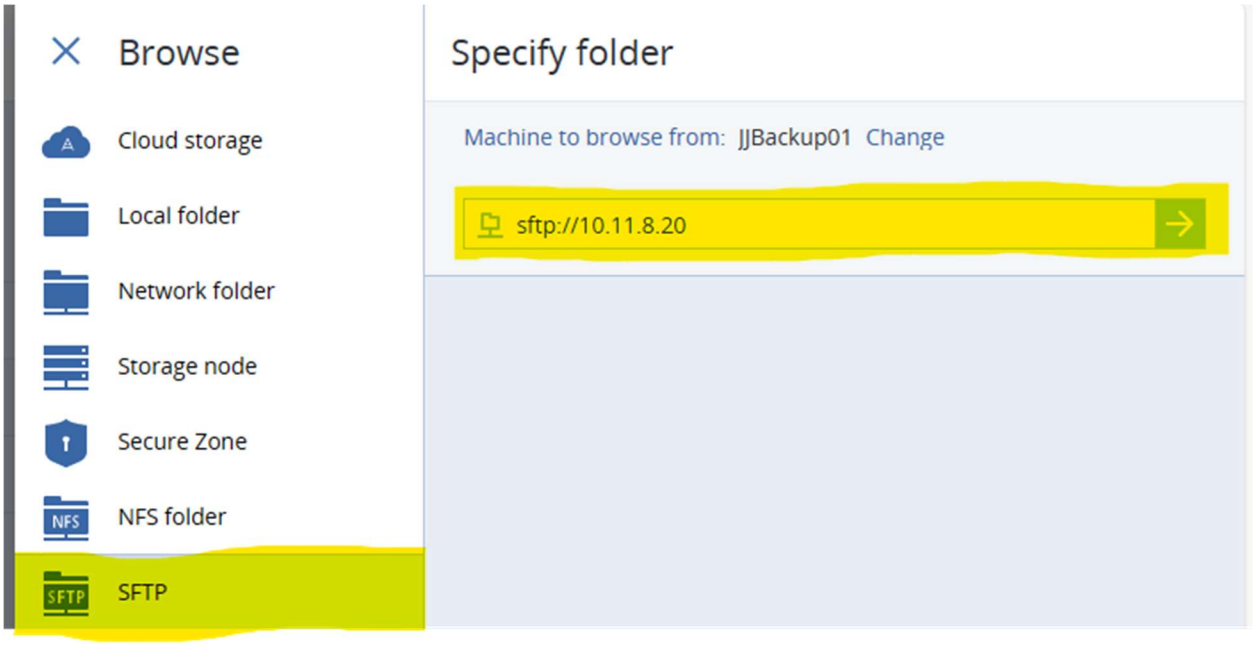


Figure 21: Choosing the SFTP server location for the FTP backup

Step 9: On the Schedule settings on the above change the **Backup Scheme** option to custom and Under **Full Backup** select a day in the week and choose the incremental backup every 15 minutes.
Step 7: Click **Create** in the top corner, now the full backup plan is created.

Plan 3: Local Backup

Step 1: Add a new backup drive on the Management Server. Initialize and format the hard disk.
Step 2: Share the drive and make sure the drive has set permission with full control.
Step 3: In the Acronis Backup Management console, On the device that needs to backup, Click the settings bar on the right corner.
Step 4: Choose the option to **protect,** the first option.
Step 5: On the right top corner, Click the **add plan** button.
Step 6: Rename the Plan accordingly. Here for Example- FTP-Backup
Step 7: On the option **Where to Backup,** click on the **Add location** on the right corner.
Step 8: Select the **Network Folder** from the right corner.
Step 9: Add the shared path that was created.

.

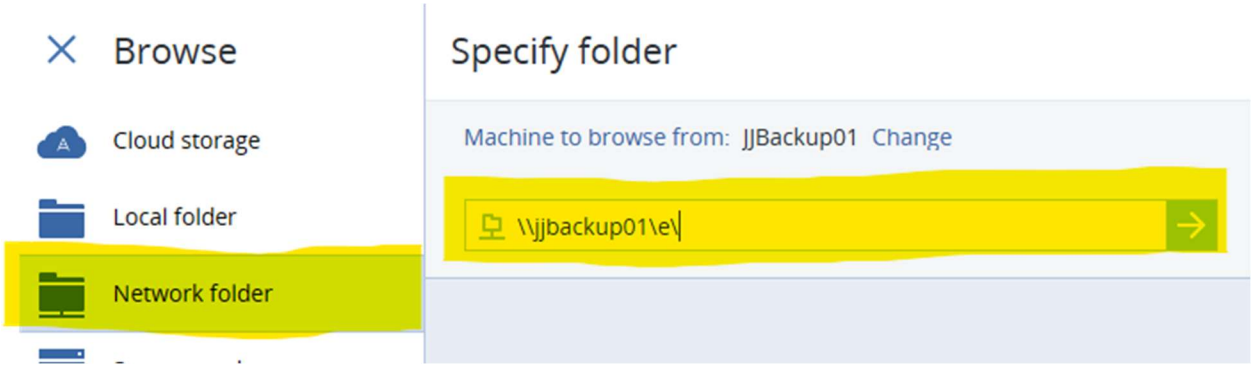


Figure 22: Selecting the network folder backup for the local backup.

Step 10: Type in Backup server credentials and save.
Step 11: On the Schedule settings on the above change the **Backup Scheme** option to custom and Under **Full Backup** select a day in the week and choose the incremental backup every 15 minutes.
Step 12: Click **Create** in the top corner, now the full backup plan is created.

Recovering files using the Backup Software

Step 1: On the right corner, **Devices,** Select the device that needs to be backed up.
Step 2: On the selected device, click **recover** below the device.

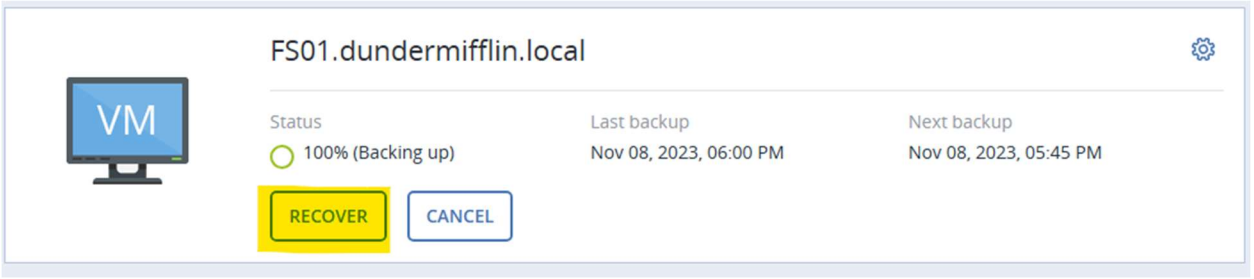


Figure 23: Recover button to restore the files.

Step 3: It allows you to choose the location that can be recovered, you can choose **sftp, cloud, or local.**
Step 4: Select the time you need to recover and click on the **recover** button on the time you would like to recover.
Step 5: Choose Files/Folder and select the files to recover.

Step 6: When you click on the file you need to recover, It gives two options recover and another one is Download.
Step 7: option **Download,** It downloads the file to the management server
Step 8: option **Recover,** again gives you two options. Options are custom or original destination. Where custom recovers to the location we specify and the original destination to the place file is located

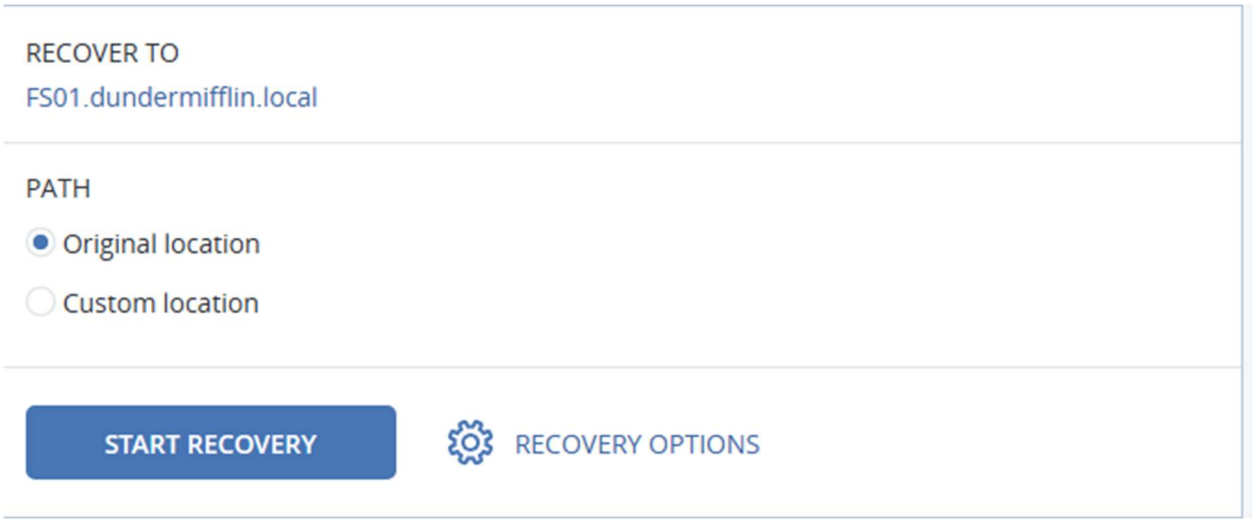


Figure 24: It says the location that needs to be restored

Step 9: Credentials might be requested for the restoration and it starts the restoration process.
Step 10: A successful message pops up if it is successfully restored.

Recovering the Entire System using the Backup Software

Step 1: On the right corner, **Devices,** Select the device that needs to be backed up.
Step 2: On the selected device, click **recover** below the device.
Step 3: It allows you to choose the location that can be recovered, you can choose **sftp, cloud, or local.**

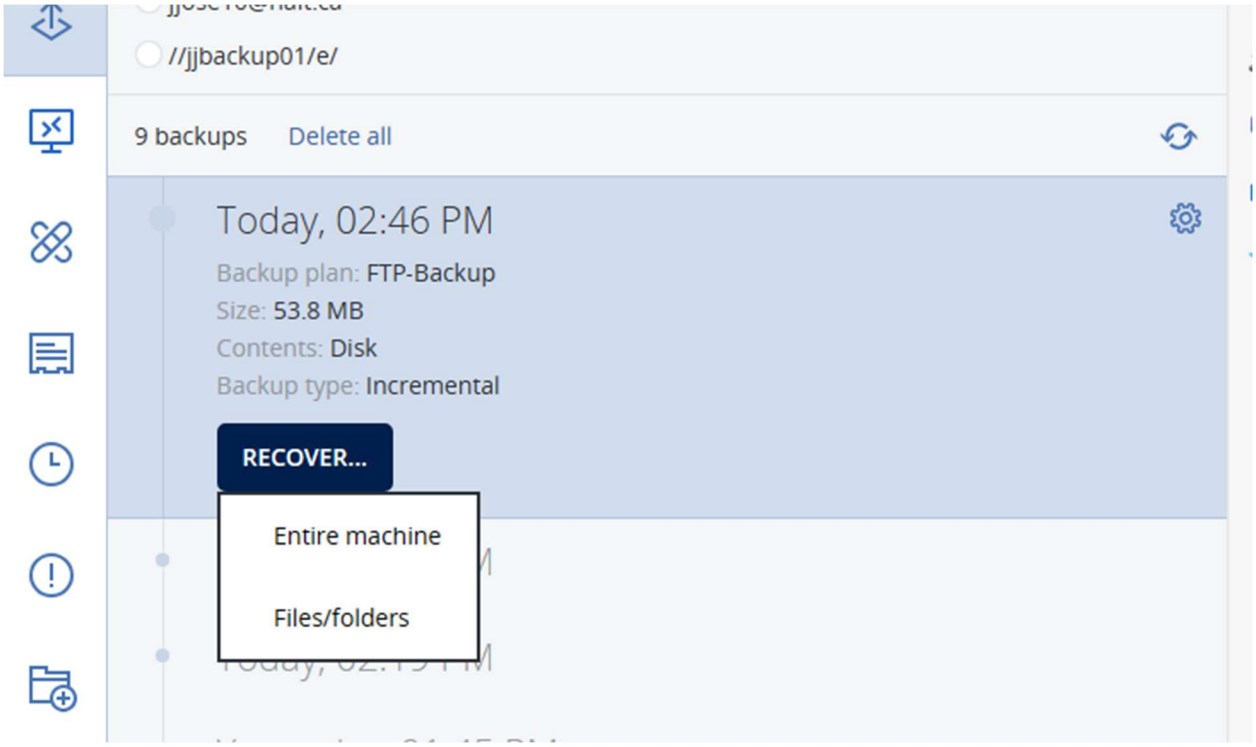


Figure 25: Selecting the restore point on the Acronis

Step 4: Select the time you need to recover and click on the **recover** button on the time you would like to recover.
Step 5: Choose Entire Machine and click recover.
Step 6: Credential of the Backup server is requested before the restore.
Step 7: Click confirm and the restore will start on the entire machine during the restore the Entire machine will turn Blue with just the option to see logs of the restore.

Password Reset

Step 1: Click **Ctrl + Alt + Delete** using the keyboard.
Step 2: Click on the **Change a Password** as shown in the picture below. The Chane Password Dialog appears.

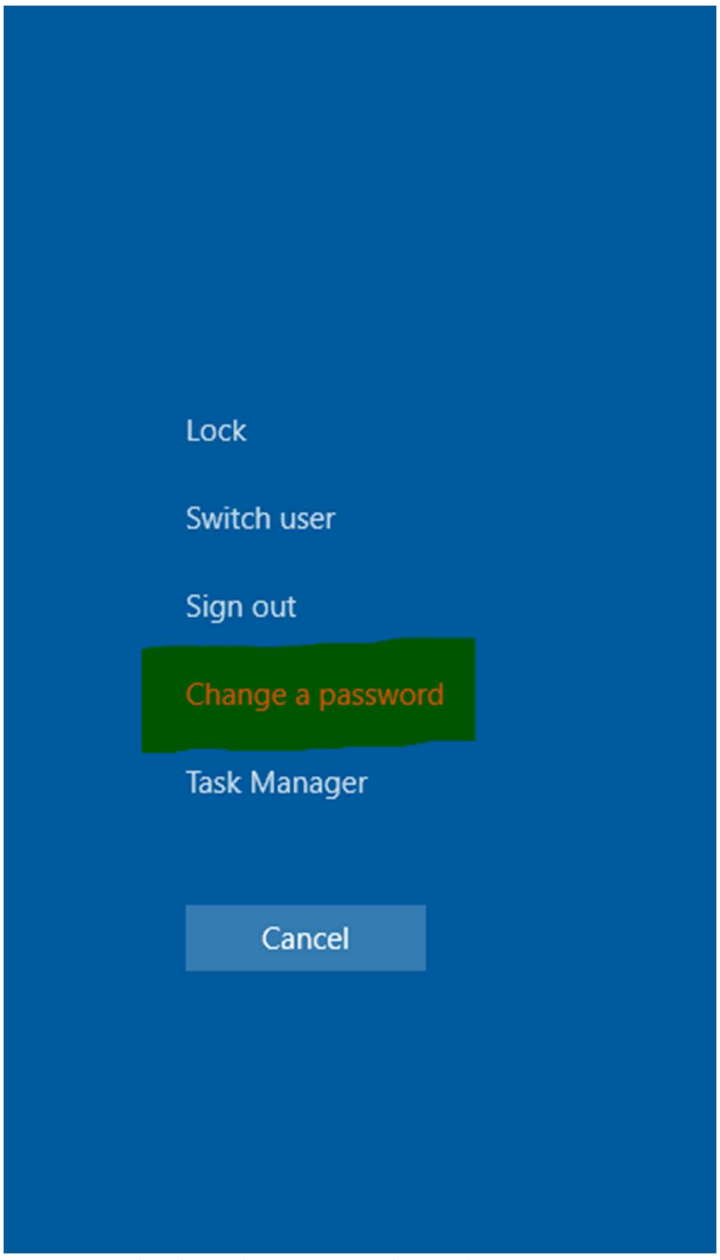


Figure 26: Ctrl + Alt + Delete Screen on the Windows

Step 3: On the Username box, type the username.
Step 4: On the old Password, type the existing password.
Step 5: On the New Password box, type your new password.
Step 6: On the Confirm New Password, re-type our new password
Step 7: Click OK.
Step 8: Confirm the password you typed is working by signing out and signing in to the Computer.

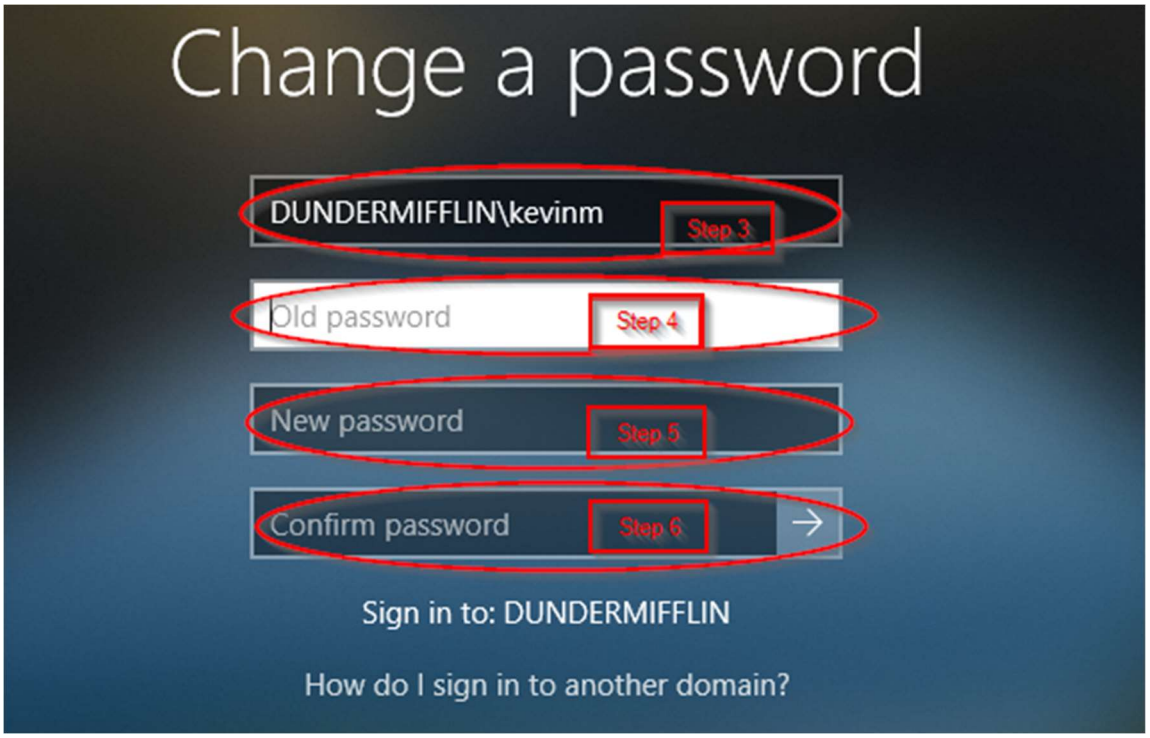


Figure 27: Step by Step to reset the password in Windows

Finding their Computer Name and IP address

Step 1: Click **Start**

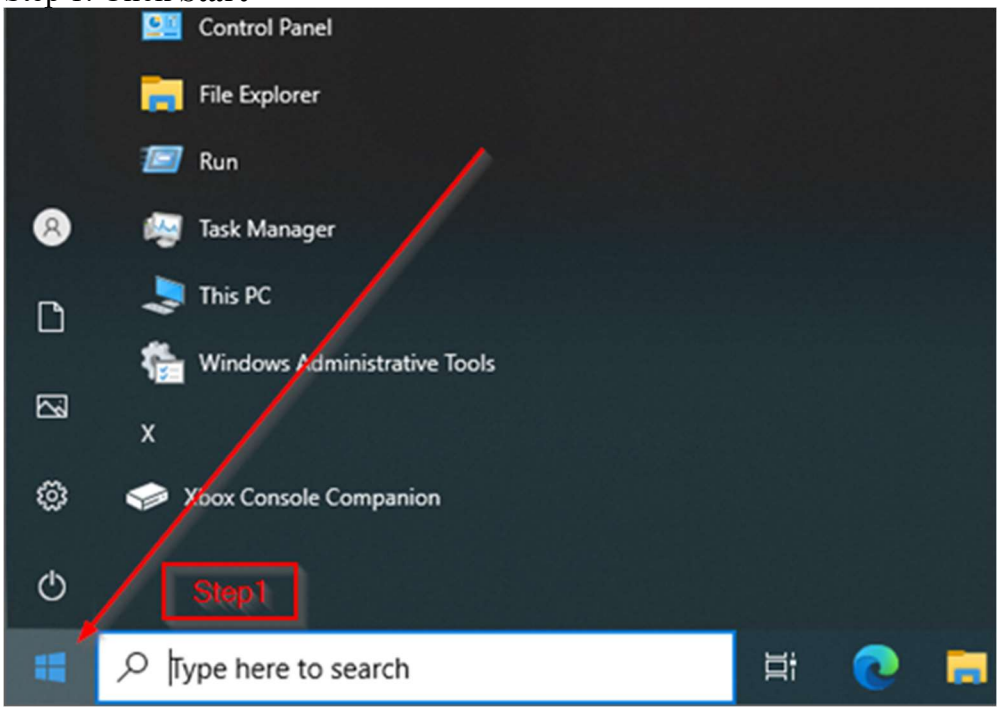


Figure 28: Start Button in Windows

Step 2: Type **CMD,** On the Search bar

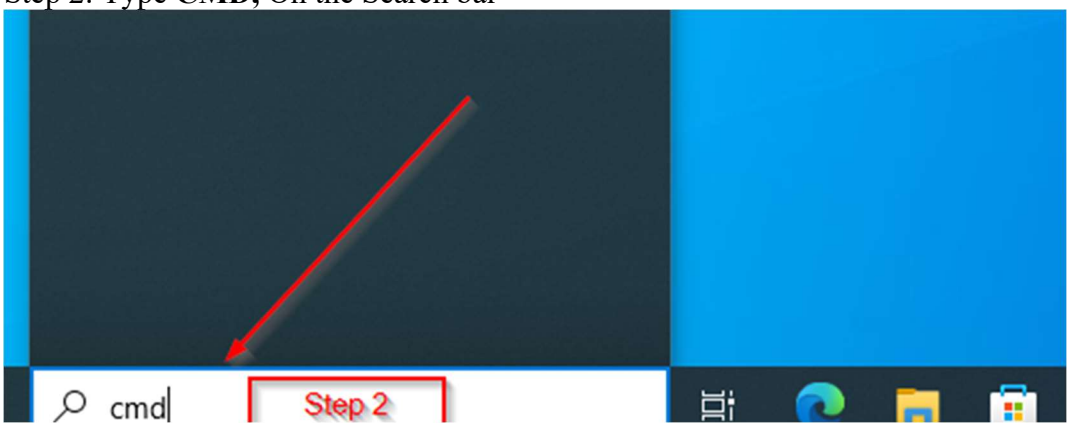


Figure 29: Looking for Command Prompt in Windows

Step 3: Open the **Command Prompt** application.

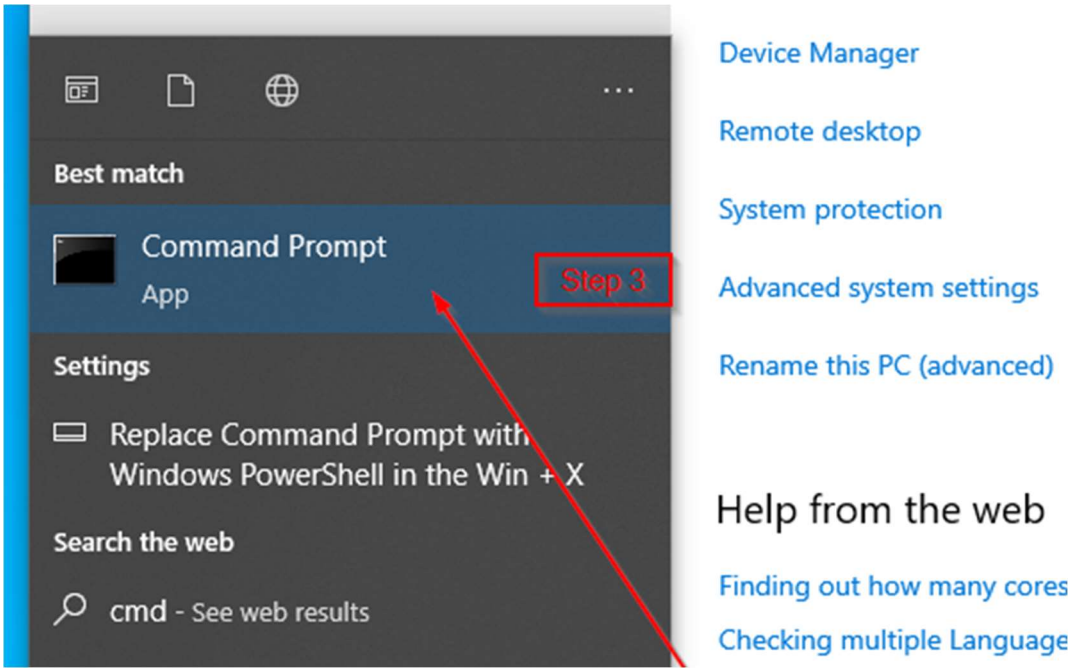


Figure 30: CMD application Windows

Step 4: On the CMD, type **ipconfig /all.** Below the screen, you will get a bellow screen.

Step 5: From the output, find out the IP Address and Hostname. See the screenshot for more details.

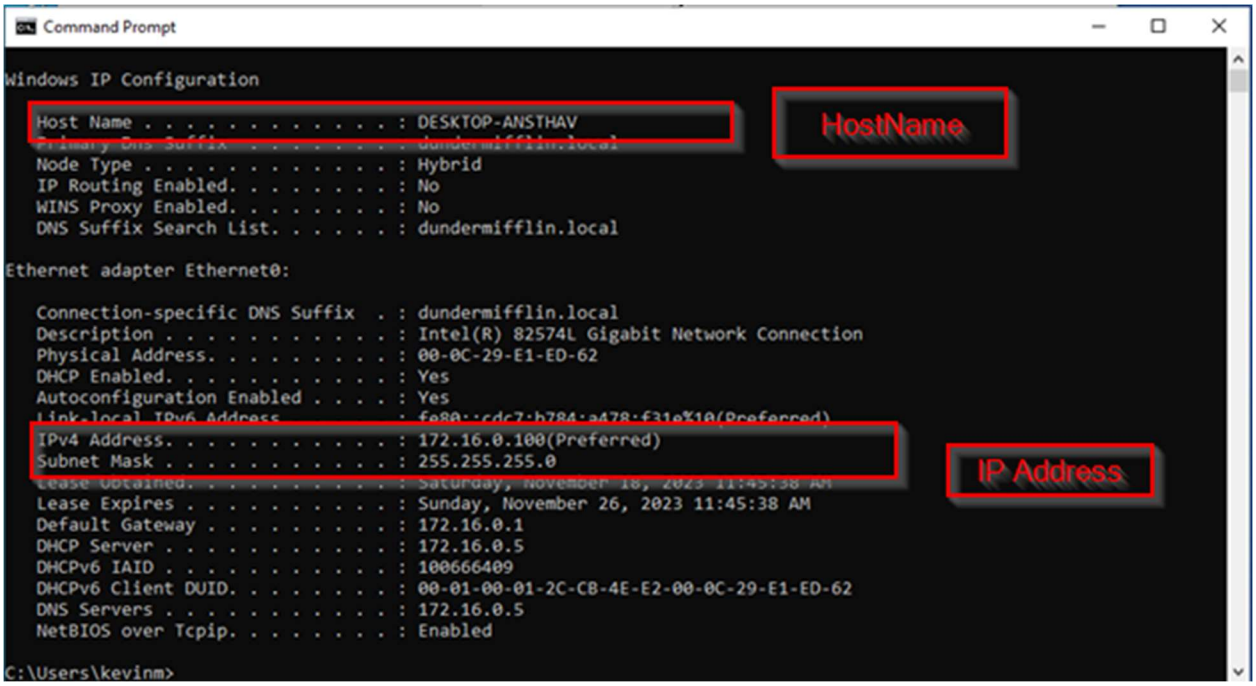


Figure 31: Command Prompt output in Windows

Denying the Access to a Folder

Step 1: On the FS server, On the K drive select **General** Folder, right click properties.

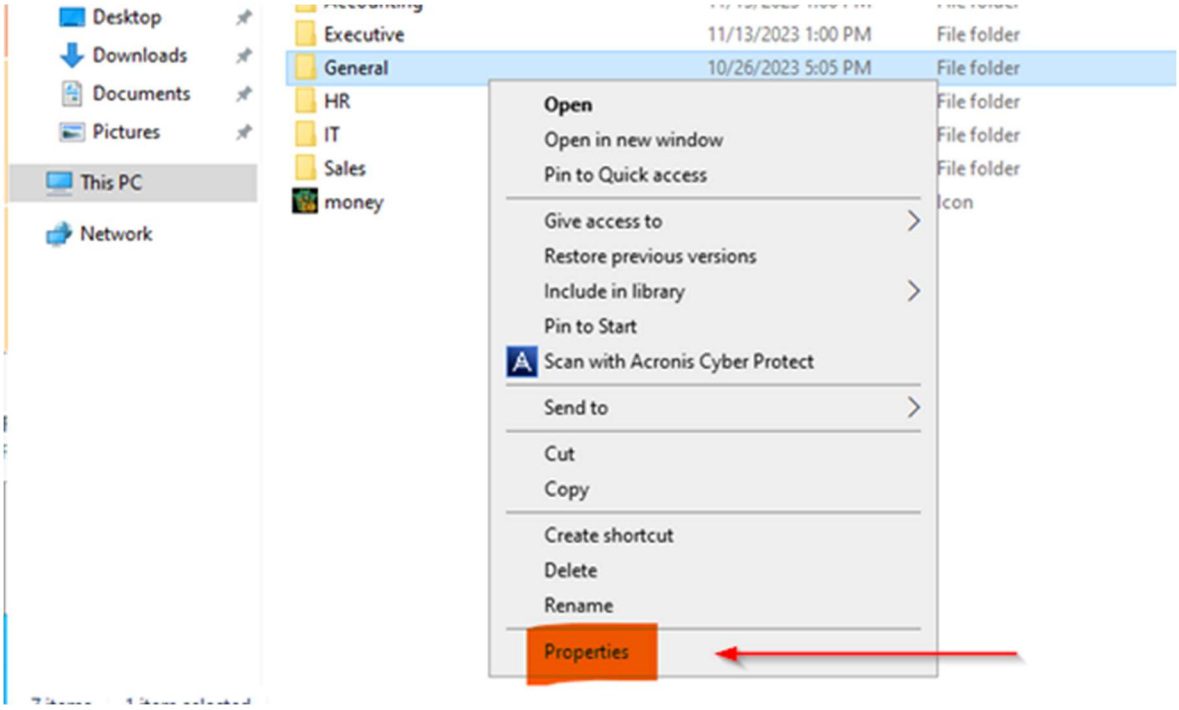


Figure 32: Properties of the File Explorer

Step 2: Under File Properties, Under the Security Tab

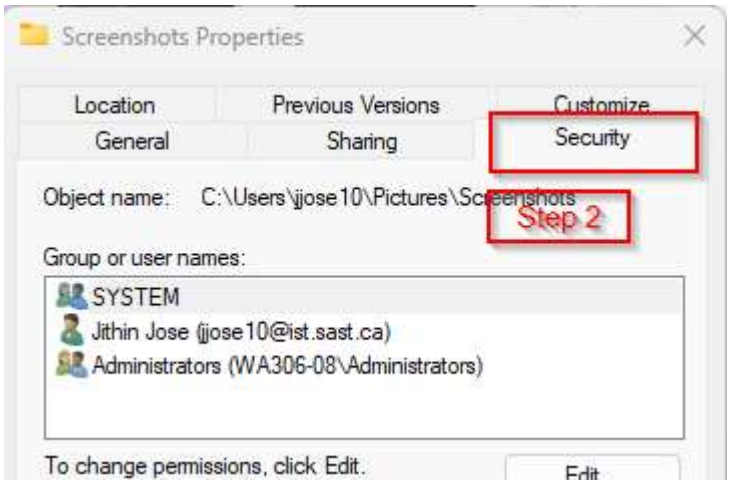


Figure 33: Security TAB options on the File Properties

Step 3: Click **Edit** and a window pops up with Permission for General
Step 4: An window poops up and makes sure the domain is selected on the location.
Step 5: Type the Username of the user whose permission is to be denied and Click **OK.**

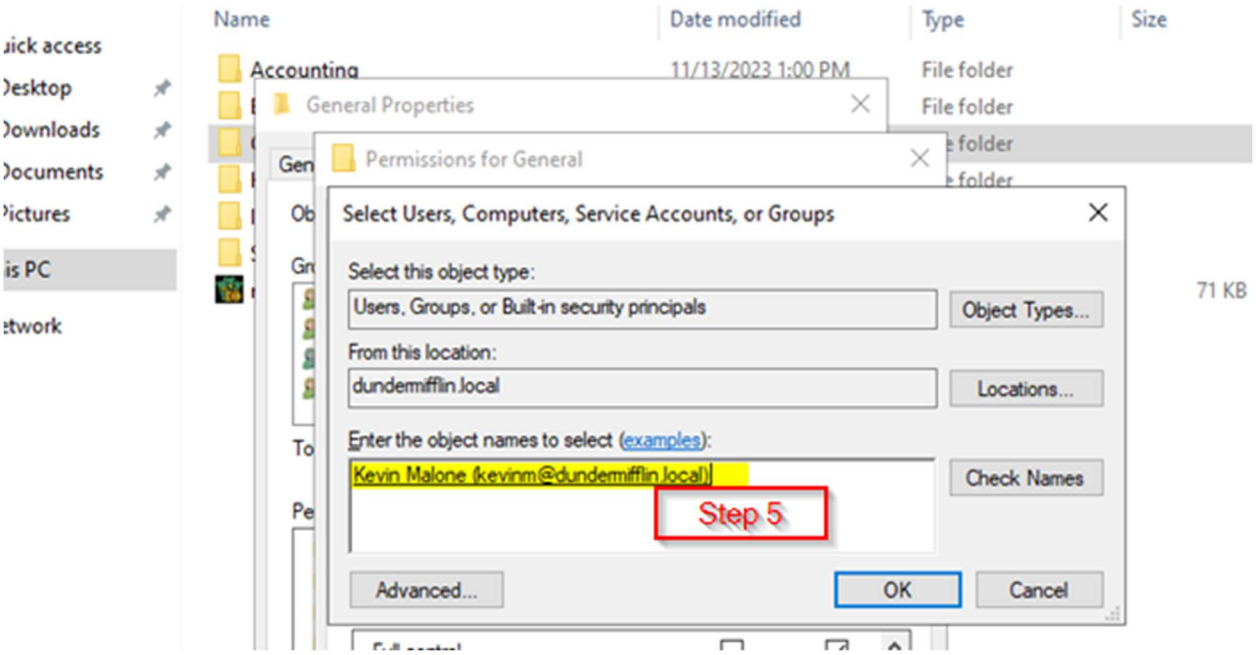


Figure 34: Username Detail on the Tab

Step 6: Under the Permission, check the deny full control as seen in the figure below.

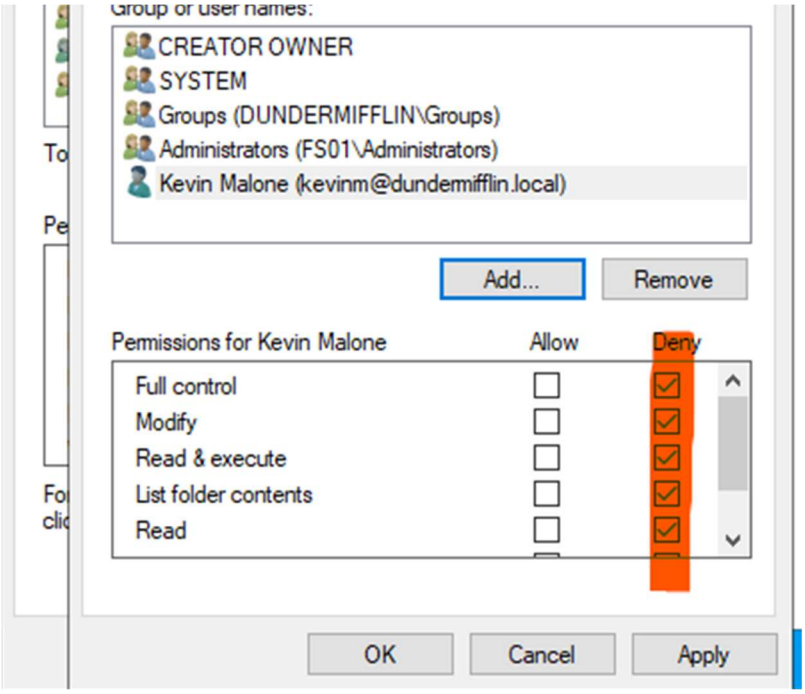


Figure 35: Denying the Permission of the User

Step 7 After setting the Permission, Click Apply and OK save Settings.

Client 1 Monitoring and Ticketing Solution

Monitoring Solution: PRTG Network Monitor

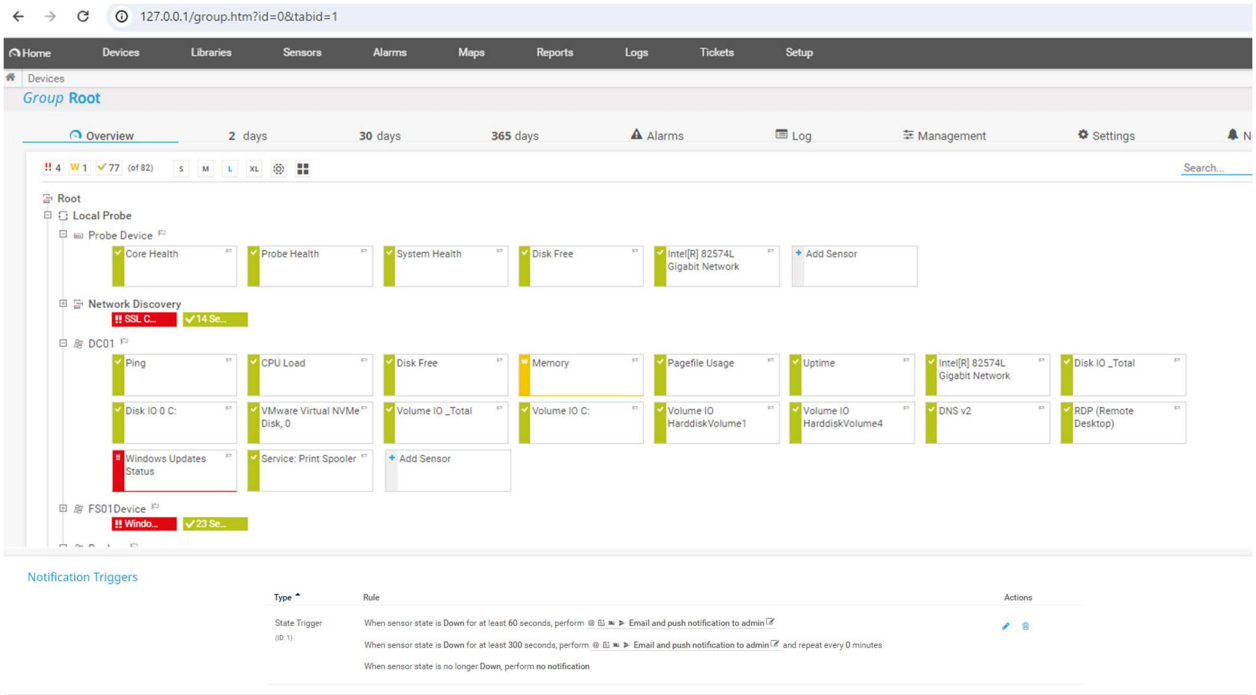


Figure 36: Screenshot of the PRTG Monitor

PRTG stands for Pressler Router Traffic Graph and is a monitoring tool that can monitor almost any object that has an IP address1. It was created by the company named Pressler AG and is designed to run on a Windows machine within your network.

The system consists of the PRTG core server and one or more probes. The core server is responsible for configuration, data management, and the PRTG web server. Probes collect data and monitor processes on devices via sensors. These sensors are the building blocks of PRTG and can provide information about various aspects of a device such as uptime, load, interface throughput, bandwidth usage, loading times, speed, hardware status, temperature, quality, resource consumption, user counts, record counts, log events, and database requests.

PRTG obtains monitoring data from target devices in two ways: the first method, either actively gathers data from a device in regular intervals and the other method that uses it passively receives data from a device or application. This includes, for example, device status, resource usage, performance metrics, unexpected events, Syslog and Simple Network Management Protocol (SNMP) traps, detailed data flow, and event log messages.

PRTG is important for ensuring that your computer systems are running smoothly and that no outages occur. It also helps to increase the efficiency of your network by understanding bandwidth and resource consumption.

For Installation, we need to install from the PRTG Website. The product we use is PRTG Network Monitor. In the management server, we install this product and add the device that needs to be monitored from the Web console. After adding the devices, we need to add more sensors to discover all the services. It came with a lot of sensors by default.

For Setup, we need to configure an SMTP setting in PRTG to send emails by the monitoring server. After that, we set a fresh desk email as administrator so that all triggers can be sent to that email using the SMTP settings initialized. Then Notification triggers are created within the console as shown in the screenshot below.

To Create a Notification Trigger, we select the device that needs to be triggered. From the device we have selected the service that needs to be monitored and under the service on the notification trigger we set up the state and threshold trigger, The state trigger will state if the service is up or down, and the threshold trigger will send a trigger if that reaches the threshold value. This trigger can be of any sort. It varies from the emails, logs, and critical alarms on the server.

The items that are triggered by the monitoring software are K:\ disk space Disk Health, print spooler monitor, RAM utilization, Ping, and DNS server. Also added a trigger for the Monitoring System to send an email if it is in an idle state and alerts are sent to support@jithin.freshdesk.com. When the alerts are sent to this email address it creates a ticket in the Freshdesk and the tickets are monitored by the IT Administrator.

Ticketing Solution: Freshdesk

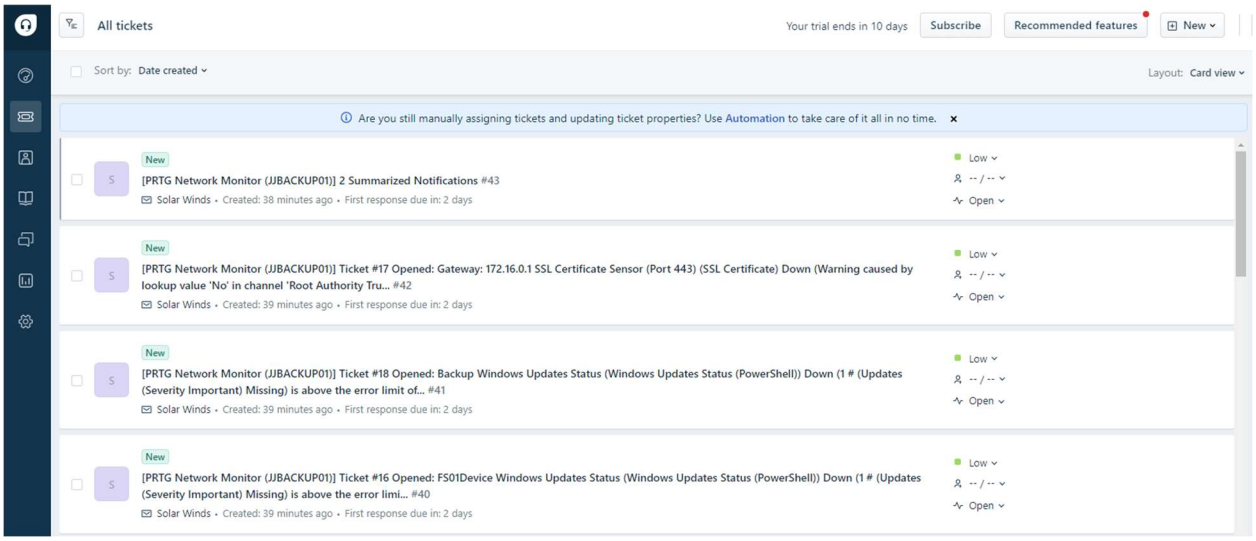


Figure 37:: Fresh Desk Motor in Windows

Freshdesk is a cloud-based customer service software that helps businesses of all sizes deliver customer support. It converts requests coming in via email, web, phone, chat, and social into tickets, and unifies ticket resolution across channels.

Freshdesk is designed to increase productivity so agents can easily send updates to customers. It stays on top of all tickets and works collaboratively with teammates to efficiently resolve customer issues. Customer issues from any channel can be converted into tickets in Freshdesk, ensuring none of your customer conversations slip through the cracks. The Fresh desk also allows you to prioritize, categorize, and assign tickets to the right agents. It also enables the automation of follow-ups, escalations, and other tasks using specific time and event-based triggers.

Moreover, Freshdesk offers features like a knowledge base to enable customers to help themselves by finding answers on their own and reporting tools to analyze trends and stay on top of tickets by allocating resources at the right time.

In summary, Freshdesk is a comprehensive ticketing system that streamlines customer service workflows, increases agent productivity, and enhances customer experience.

For the Freshdesk setup, It is straightforward as it starts with setting up a fresh desk email and adding that email address generated by the fresh desk to be added on the Monitoring server to send emails when there is a trigger. The email address assigned for my Freshdesk is support@jithin.freshdesk.com and can be accessed using jithin.freshdesk.com. All the emails received in this email are created as tickets. We have the opportunity to move to different priorities and states. Also, it allows you to send a reply to this ticket.

Cut Sheet

Cutsheet – Summarized

Devices	Virtual Machine	Internal IP Address	Public IP Address	Storage/Files Saved	VLAN
Firewall	OPNsense	192.168.10.1	N/A	N/A	N/A
DC01	Windows Server	192.168.10.8	N/A	N/A	VLAN 10
JJHyperV01	Windows Server	192.168.10.5	N/A	N/A	VLAN 10
JJHyperV02	Windows Server	192.168.10.6	N/A	N/A	VLAN 10
Client 1: SMB	Windows Server	172.16.0.5	10.10.92.61	Storage01	VLAN 41
Client 02: Web APP	Windows Server	192.168.42.7	10.10.92.34	Storage02	VLAN 42
Client03: Web APP	Windows Server	192.168.43.7	10.10.92.48	Storage03	VLAN 43
JJBackup01	Windows Serer	172.16.0.102			VLAN 41

Table 1.1: Summarized Cutsheet with the Basic information

Cutsheet – Detailed

VLAN untagged			
Management Network			
Devices	**Virtual Machine**	**Internal IP Address**	**Default Gateway**
JJHyperV01	Windows Server 2022	192.168.10.5/24	192.168.10.1
JJHyperV02	Windows Server 2022	192.168.10.6/24	192.168.10.1
JJTrueNAs	FreeNAS	192.168.10.7/24	192.168.10.1
DC01	Window Server 2022	192.168.10.8/24	192.168.10.1
Firewall	OPNSense	192.168.10.1/24	192.168.10.1

Table 1.2: Detailed Information of the VLAN 10

VLAN 20			
Storage VLAN			
Devices	**Virtual Machine**	**Internal IP Address**	**Subnet**
JJHyperV01	Windows Server 2022	192.168.20.5	255.255.255.0
JJHyperV02	Windows Server 2022	192.168.20.6	255.255.255.0
JJTrueNas	FreeNAS	192.168.20.7	255.255.255.0

Table 1.3:: Detailed Information of the VLAN 20

VLAN 15			
Cluster Heartbeat			
Devices	**Virtual Machine**	**Internal IP Address**	**Subnet**
JJHyperV01	Windows Server 2022	192.168.15.5	255.255.255.0
JJHyperV02	Windows Server 2022	192.168.15.6	255.255.255.0

Table 1.3: Detailed Information of the VLAN 15

Client 01: SMB

VLAN 41				
SMB				
Devices	**Virtual Machine**	**Internal IP Address**	**Default Gateway**	**Public IP Address**
DC01	Server 2022	172.16.0.5/24	172.16.0.1	10.10.92.61
JJHyperv01	Server 2022	172.16.0.6/24	172.16.0.1	
JJHyperV02	Server 2022	172.16.0.7/24	172.16.0.1	
Firewall	FreeNAS	172.16.0.1/24	172.16.0.1	
JJBackup01	Server 2022	172.16.0.100/24	172.16.0.1	
FS01	Server 2022	172.16.0.10/24	172.16.0.1	
Client01	Server 2022	172.16.0.101/24	172.16.0.1	

Table2.1: Detailed Information of the VLAN 41

Client 02: Webapp

VLAN 42\magiklamp.ac				
SMB\Public: 10.10.92.34				
Devices	**Virtual Machine**	**Internal IP Address**	**Default Gateway**	**Public IP Address**
Client02	Webapp	192.168.42.7/24	192.168.42.1	10.10.92.34
JJHyperv01	Windows Server 2022	192.168.42.5/24	192.168.42.1	
JJHyperV02	Windows Server 2022	192.168.42.6/24	192.168.42.1	
Firewall	FreeNAS	192.168.42.1/24	192.168.42.1	

Table2.2: Detailed Information of the VLAN 42

Client 03: Webapp

VLAN 43\ squandersridge.ac				
WebApp02\Public: 10.10.92.48				
Devices	**Virtual Machine**	**Internal IP Address**	**Subnet**	**Public IP Address**
Client03	Webapp	192.168.43.7/24	192.168.43.1	10.10.92.34
JJHyperv01	Windows Server 2022	192.168.43.5/24	192.168.43.1	
JJHyperV02	Windows Server 2022	192.168.43.6/24	192.168.43.1	
Firewall	FreeNAS	192.168.43.1/24	192.168.43.1	

Table2.3: Detailed Information of the VLAN 43

Server Cutsheet

Server	Roles	IP Address	Default Gateway	VLAN
JJHyperv01	Hyper V	192.168.10.5/24	192.168.10.1	VLAN 10
JJHyperv02	Hyper V	192.168.10.6/24	192.168.10.1	VLAN 10
DC01	AD DS DNS	192.168.10.8/24	192.168.10.1	VLAN 10
SMB01	SMB	198.168.41.5/24	192.168.41.1	VLAN41
Webapp01	Windows Server	192.168.42.5/24	192.168.42.1	VLAN42
Webapp02	Webserver (IIS)	192.168.43.5/24	192.168.43.1	VLAN43
JJTrueNas	TrueNAss	192.168.20.7/24	N/A	VLAN20
JJBackup01	Acronis Backup PRTG Monitor	172.16.0.102/24	172.16.0.1	VLAN 10

Table 3.1: Server Cutsheet

Reference

BTNHD. (2020, May 7). *Failover Clustering within Windows Server 2019 Hyper-V | TSR* [Video]. YouTube. https://www.youtube.com/watch?v=QfGnLHPbpwk

BTNHD. (2020a, April 30). *Creating iSCSI Storage with FreeNAS v11.3 | TSR* [Video]. YouTube. https://www.youtube.com/watch?v=XiEm8-oFuWM

Web Help for Acronis Backup 12.5. (n.d.). https://www.acronis.com/en-us/support/documentation/AcronisBackup_12.5/#38847.html

PRTG Manual. (n.d.). PAESSLER. https://www.paessler.com/manuals/prtg

Videos | Basic, Advanced, Tutorials | PRTG. (n.d.). https://www.paessler.com/support/videos-and-webinars/videos?lang=en

Knowledge base. (n.d.). Freshdesk. https://support.freshdesk.com/en/support/solutions/folders/272620

Freshdesk. (2022, July 21). *How to respond to a ticket | Freshdesk Tutorial* [Video]. YouTube. https://www.youtube.com/watch?v=GVX4OPQJD-8

APPENDIX

Appendix: Resources and References

1. **Video Tutorials:**

    - **"Failover Clustering within Windows Server 2019 Hyper-V" by BTNHD (Published on May 7, 2020):**
        - Description: This video provides insights into setting up Failover Clustering within Windows Server 2019 Hyper-V. It covers key aspects of creating a resilient virtualized environment.
    - **"Creating iSCSI Storage with FreeNAS v11.3" by BTNHD (Published on April 30, 2020):**
        - Description: This tutorial demonstrates the process of creating iSCSI storage using FreeNAS v11.3. It is a helpful resource for implementing network storage solutions.

2. **Acronis Backup 12.5 Documentation:**

    - **Web Help for Acronis Backup 12.5:**
        - Description: The official Acronis Backup 12.5 documentation provides detailed information on configuring and using the backup solution. It serves as a comprehensive reference for users seeking guidance on Acronis Backup.

3. **Appendix: Freshdesk**

    - The Freshdesk Android app offers various functionalities for managing tickets efficiently. Upon logging in, users are presented with the ticket list, displaying essential information such as priority, status, and assigned team.

4. **Appendix: PRTG Monitor**

    - PRTG Network Monitor is a comprehensive unified monitoring tool designed to oversee various network elements accessible via an IP address. Its architecture comprises the PRTG core server and multiple probes responsible for data collection and process monitoring via sensors.