LAB RATS INC.

PROJECT PLAN

Final Project

Date: April 24th, 2020

This Report was prepared by:

Levi Overstreet

levovers@uat.edu

Executive Summary

Introduction to the report

Overview of the requested project.

Project Report

Proposal for implementation of security program for the organization's new western region data center.

References for the report

Listed references and resources mentioned in the report.

Introduction

The following report is a proposal for the implementation of a security program for the organization's new western region data center. This proposal will address management's concerns regarding data security and the expectation of continuing growth for the organization. All recommendations within this proposal are meant to bring the company into scope with industry best practices.

Project Report

As the company continues to expand its business, the need for more data security and the ability to grow the digital footprint with that expansion will be ever-present. To maintain stability while supplying the resources needed by the organization, as well as the customers, significant business upgrades to the company network will be required. With this, management has requested that the IT department plan a network layout for the new western region data center that will cover the needs for security and expansion. These aspects are supported by Microsoft Server 2019 as the OS of choice for all servers in the network. The reason for this selection is due primarily to its complete selection of suites and services.

OS Selection

Microsoft Server 2019 is the most logical choice for implementation with longevity and expansion in mind for resources such as RAM and storage. Server 2019 is the current generation enterprise platform Microsoft offers to be used with existing and next-generation hardware that heavily utilizes multi-processor architecture, virtualization, and network teaming. Microsoft's Server series of OS's comes with many built-in features designed to ease and centralize the management of network resources and services.

Web Services, DNS, & DHCP

Microsoft covers the web services with its Internet Information Services, or IIS. IIS has been a staple of the Server OS since its initial release in 1995, and the current version of IIS on Server 2019 is IIS 10. This version has improved coalescing connections, upgraded HTTP/2's server-side cipher suites, wildcard host headers, and more (Azure, n.d.). IIS is also firmly implemented with Microsoft DNS and DHCP Server, the domain name system, and dynamic host configuration protocol services built-in standard with Server 2019. These services being standard features in Server 2019 help to tie in the centralized management of all internet-based features for any given enterprise. As for intranet-based features, Server 2019 comes equipped with suites loaded to get the job done.

Domain Services

One of the critical services Server 2019 has is Microsoft's Active Directory or AD. AD is a directory service developed by Microsoft for Windows domain networks. In its current iteration, is an umbrella title for a broad range of directory-based identity-related services, and one of those services is Active Directory Domain Service or AD DS. AD DS allows admins to manage users and computers on a network while giving them the ability to organize the data into logical hierarchies (Petters, 2019). AD, being an all-in-one suite, has other functions.

Software Update Services

AD is also responsible for the management of software updates with built-in group policy rules under Windows Server Update Services, or WSUS. WSUS acts as the central repository on your network, which downloads and maintains updates from Microsoft and distributing the updates to all clients on the network (Buzdar, 2017). With this, a business can reduce the bandwidth and traffic on a network because every client computer does not need to download

updates directly from Microsoft.

File Services

AD is also able to oversee file services under File Server Resource Manager, or FSRM. FSRM is used to help admins manage stored data in file servers, but, usually, due to size, it is recommended that file storage be handled by other means such as the structuring of a database for your network. A database offers easy organizing, storing, and retrieving large amounts of data. To achieve this, Server 2019 has Microsoft SQL Server. SQL Server is a relational database management system that handles aspects like data redundancy/inconsistency, file sharing, data concurrency, searching, security, and data integrity (Geeks, n.d.). Databases are also one of the main areas where clustering is a primary focus in network topology.

Network Map & Ordering Core Equipment

After we have selected our network-wide OS, we begin with a diagram of our new infrastructure to help map the layout of equipment as well as giving us direction on which parts of the network to build out first.

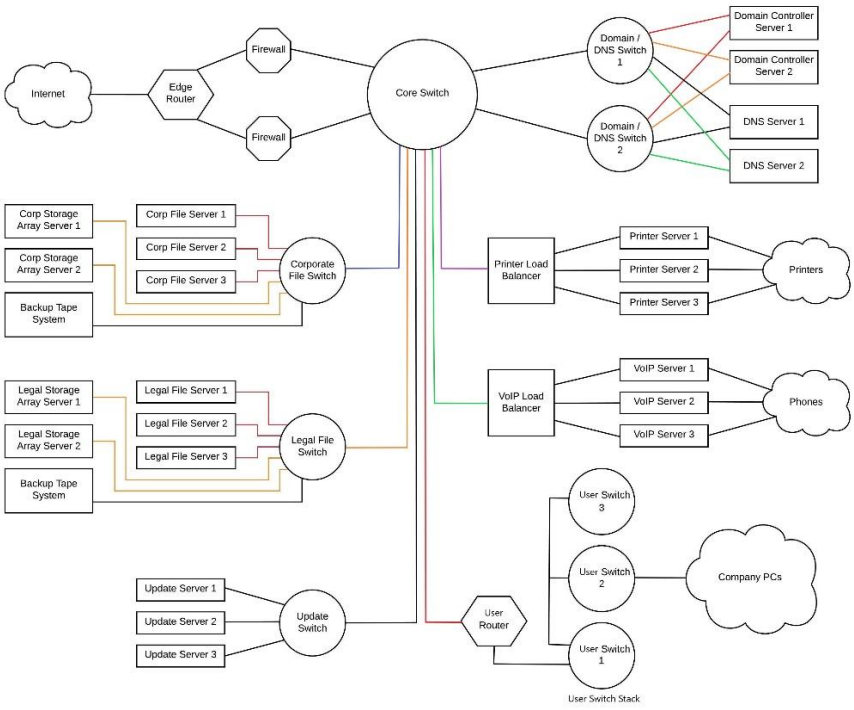

Figure 1. Proposed Network Diagram

This project assumes that all the equipment installed will be new, including the servers that are ordered arrive built to spec from the distributor. To address the build specs for our servers, redundancy must be considered at every level that is controlled to keep downtimes as low as possible while maintaining uninterrupted access to key resources. With that, servers will be ordered built out with hard drives set in RAID configurations best suited for redundancy and failover protection while maintaining high data transfer speeds. Usually, this will be something such as a RAID 5 configuration which consists of a minimum of three drives. This configuration allows for the failure of one drive without any data loss. This failure tolerance can also be increased with a RAID 6 configuration which consists of a minimum of four drives and allows for the failure of two. The servers ordered will also have redundant power supplies to help maintain uptimes. The next step will be to start by setting up the main networking equipment for our infrastructure, the Edge Router, the Firewalls, and the Core Switch as well as the equipment

for the User Switch Stack. The Edge Router and Firewalls will be the first pieces of equipment that come into contact from our uplink to the Internet and the Core Switch along with the User Switch Stack functioning as the backbone for the network. Once the core of the network is installed and servers ordered and delivered, work will begin on the list of network components. The main two components are Domain and DNS. The setup of our dedicated domain controllers and DNS servers will lay the foundation for the network and the remaining equipment to be installed and configured.

Domain Services

Active Directory Domain Service allows admins to manage users and computers on a network while giving those admins the ability to organize the data into logical hierarchies (Petters, 2019). As such AD DS has a complex makeup which includes Users and Computers, Administration Center, Domains and Trusts, Sites and Services, as well as PowerShell module functionality. Almost all control of all other services is covered under the umbrella of AD DS. Making sure that the proper installation of the base environment is key, Server 2019 must be installed with the needed hardware resources and configured for secured administrator access. As stated previously, AD DS sits as an umbrella for all services under it. Because of that, a server running AD DS is considered a domain controller, assigning and enforcing security policies for all systems on their designated domain as well as maintaining the main other parameters. As a directory service, Active Directory instance consists of a database and corresponding executable code responsible for servicing requests and maintaining the database. Active Directory structures are arrangements of information about objects. The objects fall into two broad categories: resources (e.g., printers) and security principles (user or computer accounts and groups). The framework that holds the objects are the forest, tree, and domain. These are the logical divisions

in an Active Directory network. Within a deployment, objects are grouped into domains. Multiple domains are grouped into a tree. Moreover, a collection of trees that share a common global catalog, directory schema, logical structure, and directory configuration is called a forest. As a function, web services fall under that collection and sit within the domain layer.

Web Services

Web services are often considered a broad grouping of the main services of internet-based functions such as DNS, DHCP, HTTPS, FTPS, and more. The service that covers the majority of internet service functionality is Internet Information Services. IIS supports HTTP, HTTP/2, HTTPS, FTP, FTPS, SMTP, and NNTP as well as boasting improved coalescing of connections, upgraded HTTP/2's server-side cipher suites, wildcard host headers, and more with the current generation (Azure, n.d.). Nevertheless, again, it is important to have configurations set to optimize your network best and support your environment. This optimization means making sure that the domain is configured in AD and that the proper IPs are set to ensure utilization across the network works.

File Servers

According to the network diagram, two separate file server clusters have been set up, one for all corporate data to be used by the whole company and one for all legal data to be used by just the legal department. This structure is designed with a need for complete and uninterrupted access to all documentation for all employees. For file servers and databases, it is always a good idea to have backups as well because redundancy is not a replacement for backups. However, given the amount of volume that can be accumulated in any given time frame, it is best to set the backup systems in multiple layers. The file servers, running redundantly as previously stated, will also have attached storage array servers with 24 drives each as well as being configured in a

RAID 6. However, for the main bulk of data, a policy must be established for maintaining backup copies. This backup will require that we use tape drive storage. Tape drives are not the ultimate backup medium, but they are one of the best options when it comes to ensuring long-term data retention and the building of offsite archive storage (Reed, 2019). Furthermore, to take this a step further, these backups will run in a way that takes a full back up weekly then an incremental backup daily. Daily changes are then copied over to the weekly, and from there, it goes to tape. Nevertheless, the implementation of a file server is very in-depth and requires the repetition of several steps. Once finished, management is made easier with Server 2019's build-in file management tools.

File Foundation

To start managing files and folders, you need to place them in separate and secure areas. This separation is meant to make it easier for the manager tool to function as well as keep the data organized. The start is navigating to the Disk Management tool within Windows. Next, the team needs to locate the free space on the designated hard drive and right-click. This will bring up a submenu where we will select *New Simple Volume*.

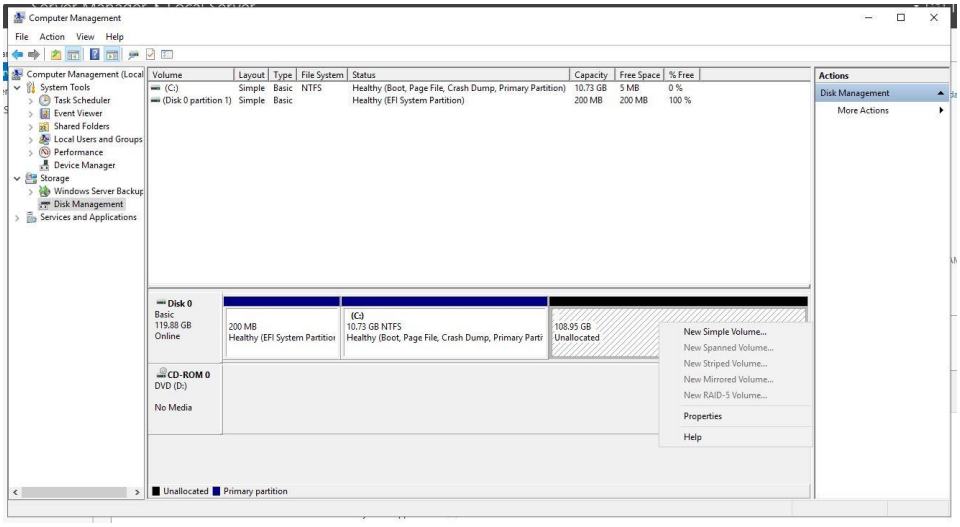

Figure 2. Disk Manager

Afterward, the wizard will be used to select the volume letter, the size of the volume, and how the team defines it. These series of steps will need to be repeated for the appropriate number of volumes that are needed.

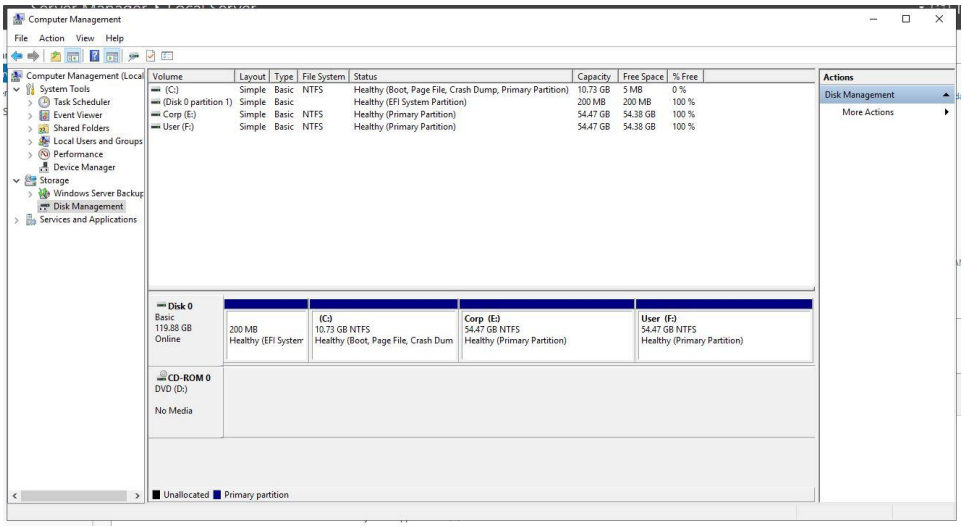

Figure 3. Volumes Created

User Creation

The next course of action is to set up different user groups within the domain. These groups are meant to hold the domain access rules for multiple users that have the same needs without having to configure each user account. To add new user group profiles, you must bring up the Active Directory Users and Computers tool within the Server Manager. After that is up, navigate to the domain and locate the Users subfolder. You can right-click on this subfolder to bring up a submenu where you will select New and then the type of user profile you want to create, which in this case would be *Group*.

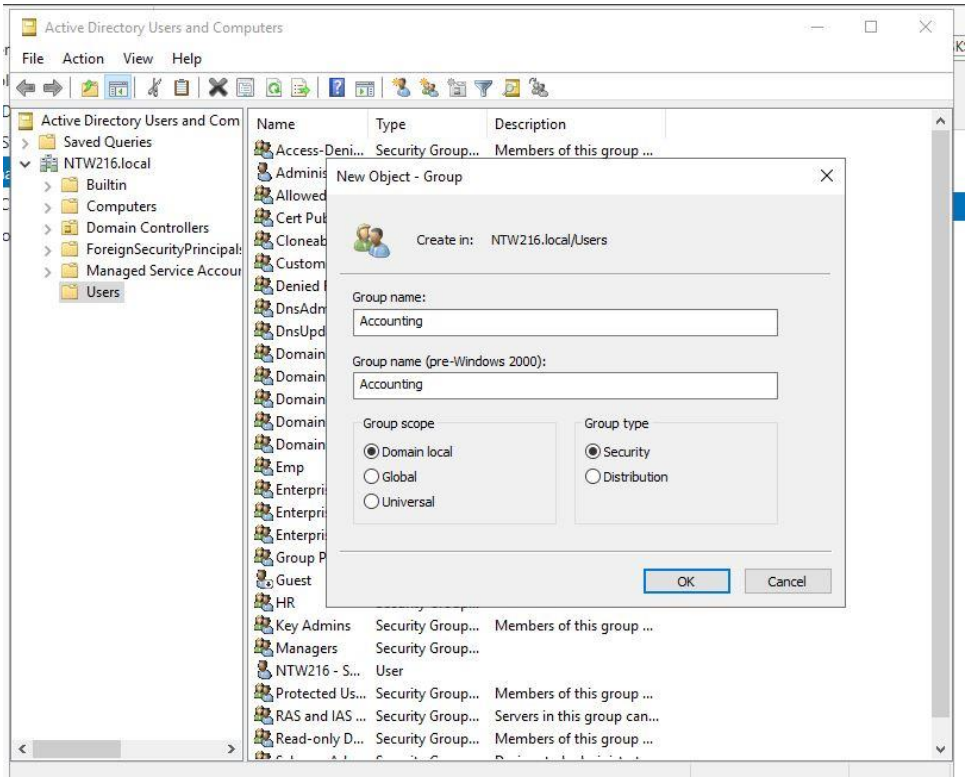

Figure 4. Adding User Groups

A New Group creation window will come up, and there you will name the group, group type as well as selecting the scope. It is very important to make sure that *Domain local* is selected for scope, and *Security* is selected for type. These steps will be repeated for each group needed, as well as any new users.

Building Fold Structure

After the needed volumes and the new user groups are created, you can begin to build out the folders. Creating them in their designated volumes as well as setting the sharing permissions for those folders. You will want to start with the volumes and work your way down in the folder tree configuring any subfolders as needed.

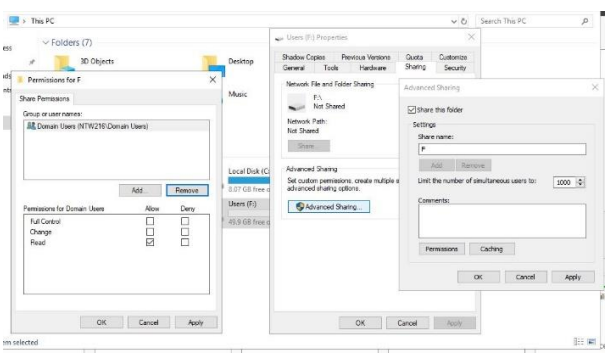

Figure 5. User Volume Permissions

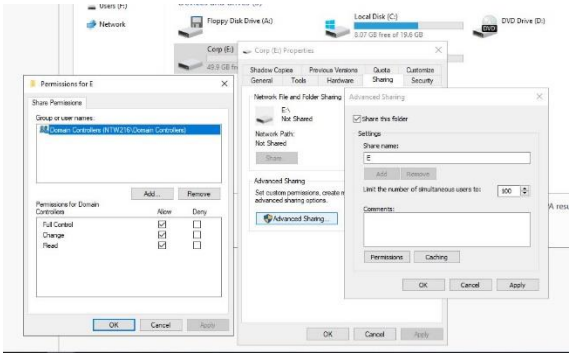

Figure 6. Corp Volume Permissions

Starting by right-clicking on the volume, select the *Properties* menu. Once that is open, go to the *Sharing* tab and click the *Advanced Sharing* button. A new menu will open, click on the box marked *Sharing this folder*, set the limit for how many users can access the folder simultaneously if applicable, then click the *Permissions* button. Another menu will come up where you can determine the users and groups allowed to access the folder. After adding or removing users and groups as needed, make sure to set the permissions for the domain controllers about each group or user. Once those are set, click the OK button for each menu to accept the changes. Once the volumes are completed, you can then proceed to confirm and configure the subfolders and the groups as needed.

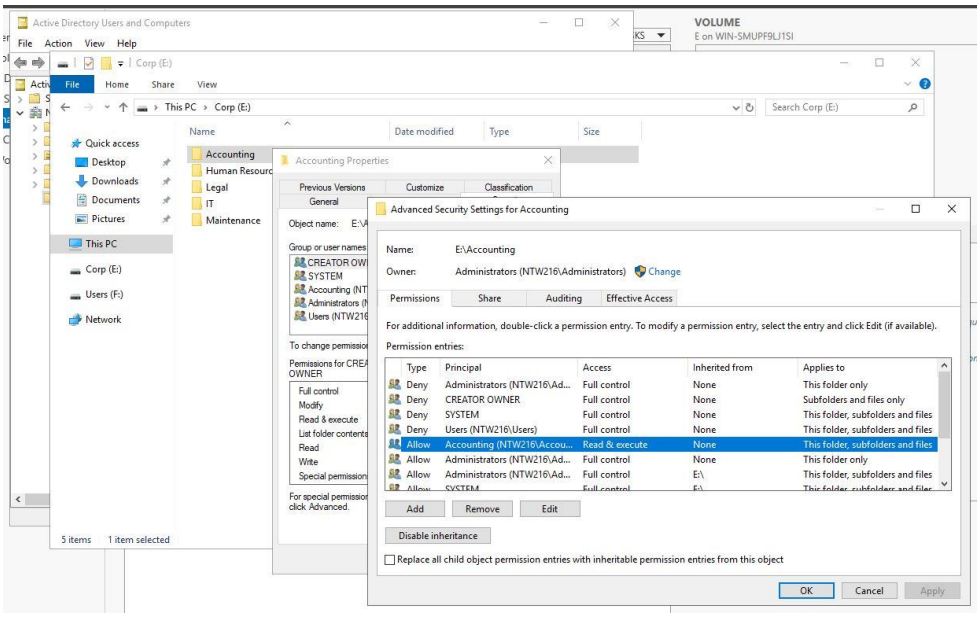

Figure 7. Corp Subfolder Configuration

This will need to be done for each subfolder within each volume that requires further securing and access control. Not all users will have access to every folder, and it is considered the best security practice to only allow authorized users access to sensitive data. This compartmentalization helps to secure corporate data as well as keep files organized.

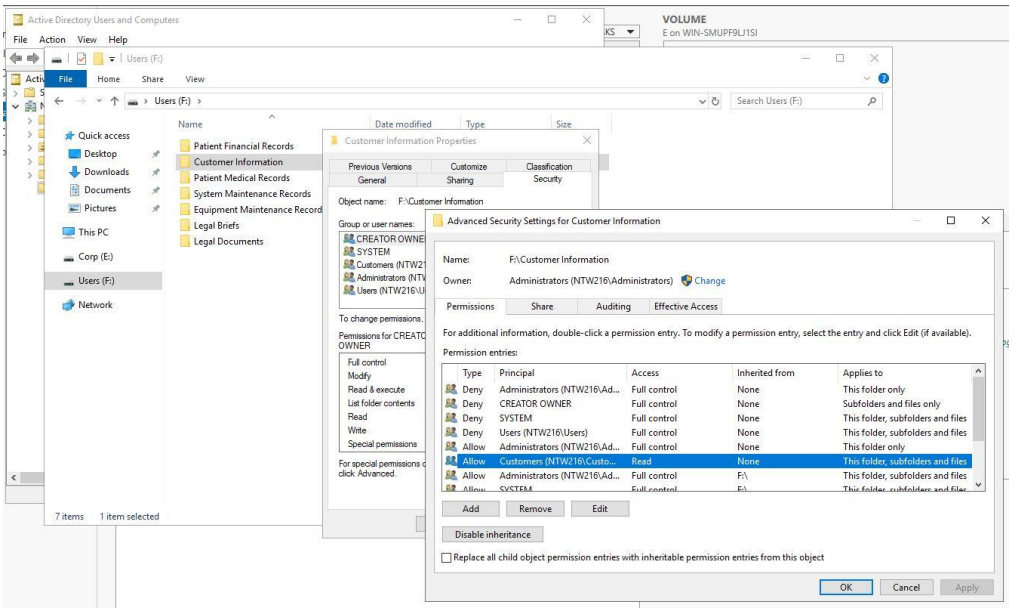

Figure 8. User Subfolder Configuration

Securing Folders

During this whole process, the team has been securing the folders and the file within varying levels of access control. Once that is completed, the team will need to secure the volumes further. In the Server Manager, navigate to the File and Storage Services and then Shares. Here you will find a list of all the associated volumes found by the server and domain.

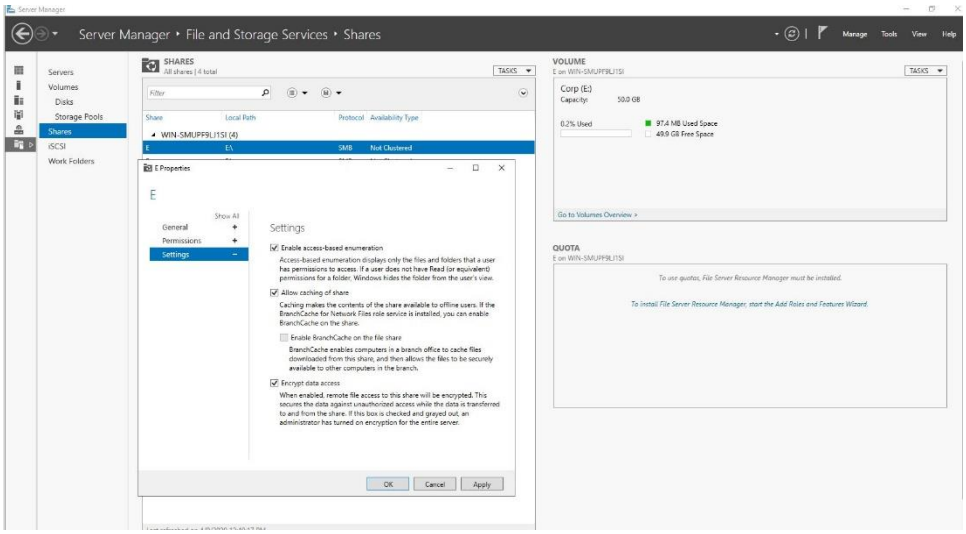

Figure 9. File Services Shares Properties

Right-click on one of the volumes listed and select *Properties*. This list will open another menu where you will review permissions set as well as set other options like enabling *Encrypt data access*. Once the needed settings are enabled, click *OK* and exit from the File and Storage Services. After setting up the file server clusters for both corporate and legal, we can move on to set up load balancers for the most heavily used company resources, printers, and phones.

NLB Nodes

The initial setup for network load balancing nodes is rather simple. You simply need to install the NLB feature by navigating to the Server Manager and running the Add Roles and Features wizard, clicking the *Next* button until you get to the Features submenu, and clicking on the box for *Network Load Balancing*, adding the feature, and installing.

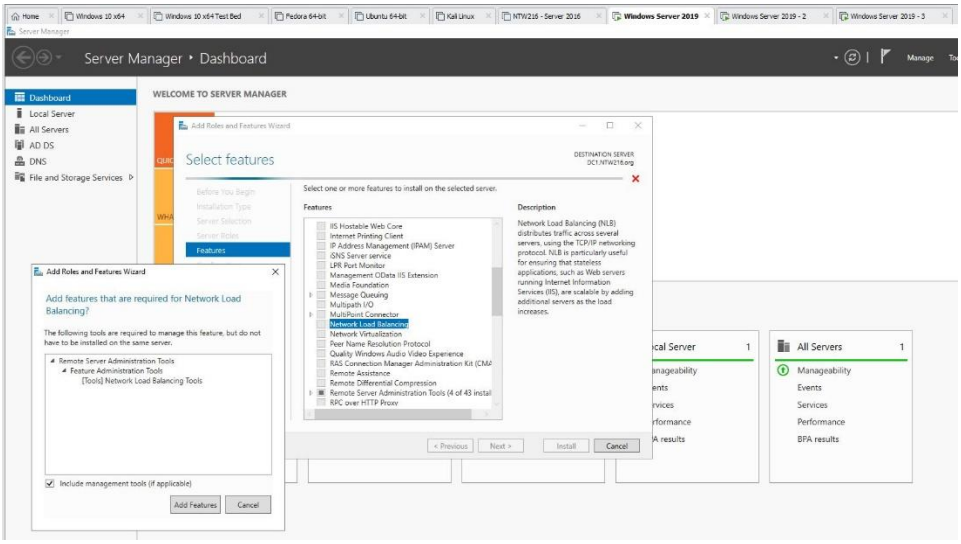

Figure 10. NLB Install

The process needs to be done on every server that you wish to have involved with the cluster. So, make sure to install the feature on the domain controller and all subsequent servers within that domain. Once all the servers have the NLB feature installed, open the Network Load Balancing Manager on the domain server. Once opened right click on the Network Load Balancing Cluster on the left of the manager and select *New Cluster*. The New Cluster wizard will open, and here is where you can list all the hosts for the nodes that will be in this new cluster. After the nodes are listed and connected, you will be taken through other options for setting up the cluster.

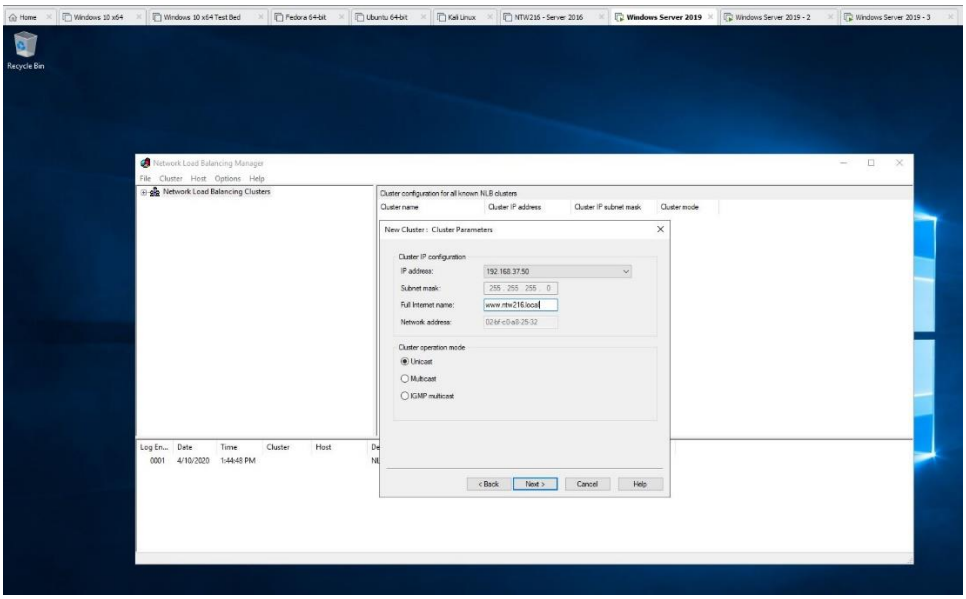

Figure 11. Configuring New Cluster

Adding or disabling any additional IPs and setting IP priority levels are just a few of the options to go through. Then you will need to specify the cluster IP that allows clients of the NLB cluster to use to contact it. After setting the cluster IP, you will then need to set the cluster operation mode and list the Full Internet Name for the cluster. After that, the next thing is setting port rules. By default, it is set up to be wide open, so make sure that the ports are closed and set according to company guild lines. You will also be able to configure filtering mode at this point if needed.

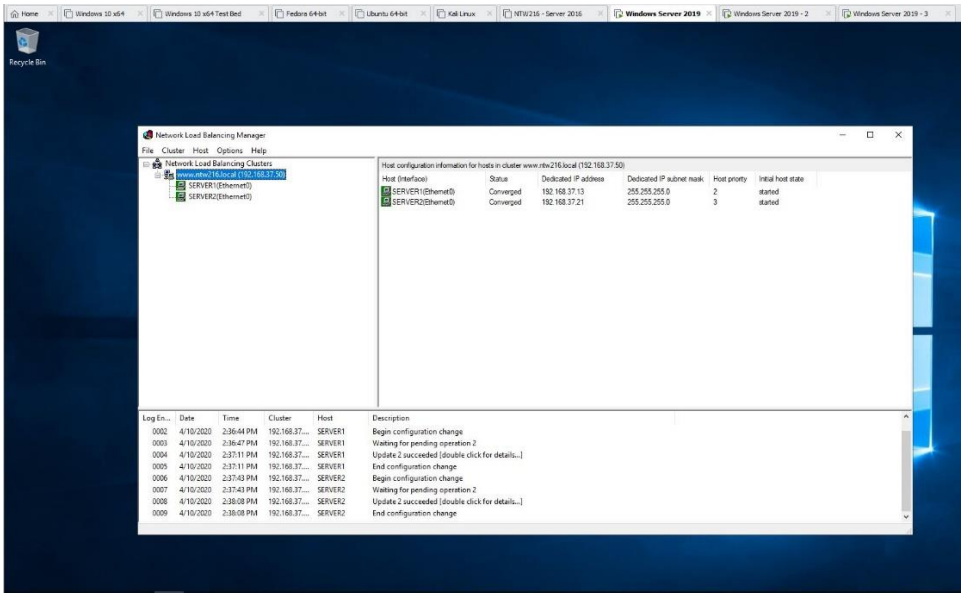

Figure 12. Finished New Cluster

It's at this point you can click the *Finish* button and create the new cluster. You will then see the cluster and all the servers within it listed.

Print Servers & VoIP Servers

A print server acts as an intermediary between computers and printers, accepting printing jobs from computers and sending them on to the right printer. This is done by storing and queueing print requests locally and to avoid overloading a busy printing device (Chris, 2016). Dedicated print servers are set up in a similar redundant fashion similar to all our other servers. The only difference is that with a print server we can keep the overhead low for hard drives given that we would only need to run it as a RAID 1 at most. This is a configuration that requires a minimum of two drives. Print servers will not run solely as a primary/backup setup but run multiple print servers in a failover configuration while connected to the load balancer. Print servers will be enabled to process any requests as needed, and should one fail; the others can pick up the slack. This redundancy will maintain the backup quality we need while also addressing high volume for print jobs. The print server setup will be applied to the VoIP servers

as well. With load balancers handling the amount of traffic, our VoIP and Print servers will be receiving; this will ensure that company communication systems will remain up.

Update Servers

The servers that will handle the downloading and pushing of updates across the network will also be set up in a low overhead by redundant configuration, much like the Print servers and VoIP servers. Multiple servers in a failover configuration with all of them having hard drives in a RAID 1.

Security

The security of the network needs to be maintained for both our internal and external employees. This maintenance is the basis of security policies that will need to be configured on the domain controllers.

Domain Password Policy

One of the first security policies that needed to be set before rolling out the remote connections was the enforcement of proper password protection for all devices on the domain. Do that required logging into the Domain Controller and navigating to the Group Policy Management tool. The next step required is to edit the Default Domain Policy's password policy settings to reflect the new password standards for the company.

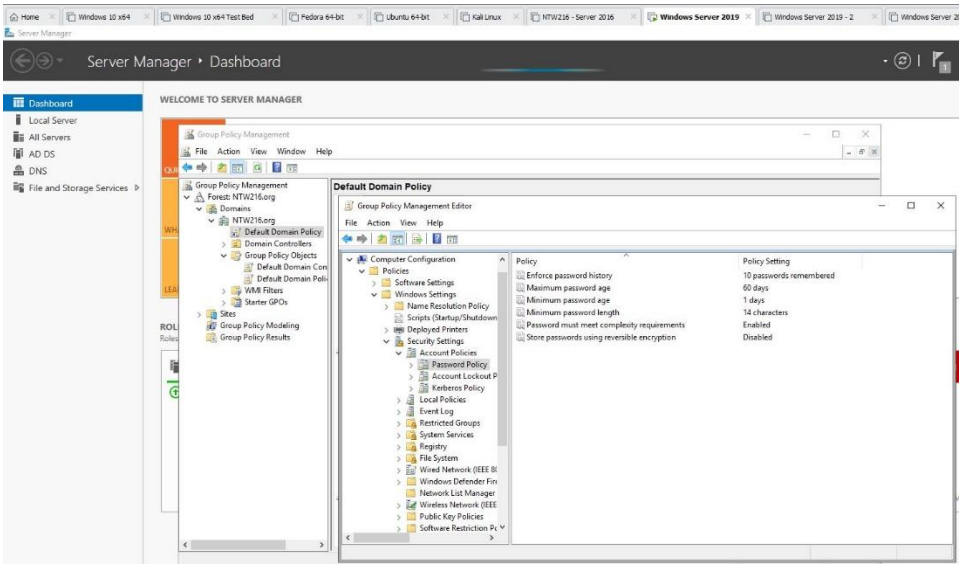

Figure 13. New Password Standards

The new password standards for the company domain are; passwords are to be changed every 60 days, must be a minimum of 14 characters and meet complex requirements, and passwords will not be repeatable for 10 iterations.

Domain Browser Policy

Another new policy that management has requested was setting Google Chrome as the only approved web browser to be used on the domain. Setting up this policy was done the same way as the others, by going to the Group Policy Management tool, right-clicking on the domain and selecting the option for a new policy in the submenu. After naming and creating the new policy, the Group Policy Management Editor was opened and used to navigate to the File Explorer subfolder to find the *default associations configuration file*. From there, the team would enable it and set the location of the XML file that will hold the configuration for setting Chrome as the default browser on the domain.

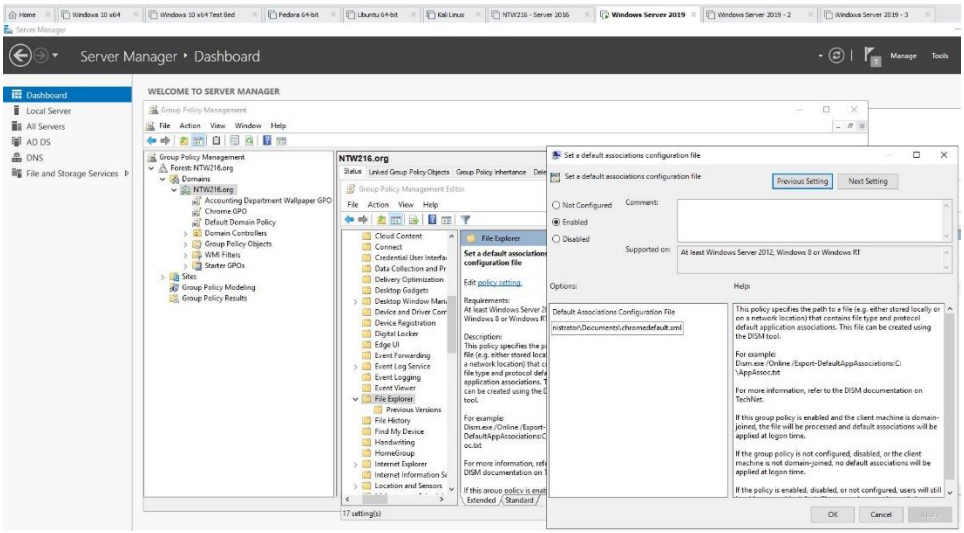

Figure 14. Chrome Default Browser

Domain Anti-Virus Policy

As a part of the comprehensive security policies that management requested, is the push for the installation of anti-virus software as well as the scheduled upkeep. Again, open the Group Policy Management tool, right-clicking on the domain and selecting the option for a new policy in the submenu, name and create the new policy and then open the Group Policy Management Editor.

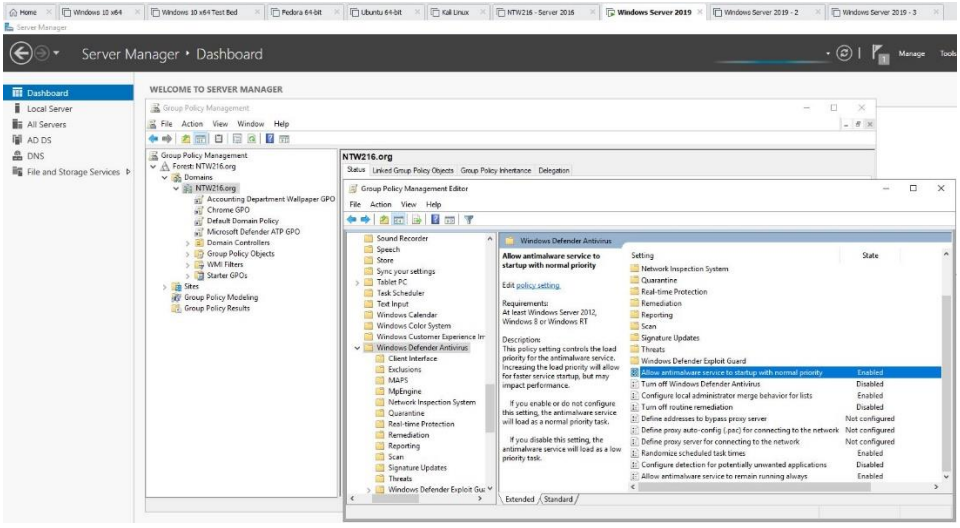

Figure 15. Anti-Virus Policy

For this policy, we opted to use the included software that Microsoft provides, Windows Defender Antivirus. Setting up Defender entails enabling and disabling a few settings within the Windows Defender Antivirus policy folder. This pushes out the enforced policy to the whole domain.

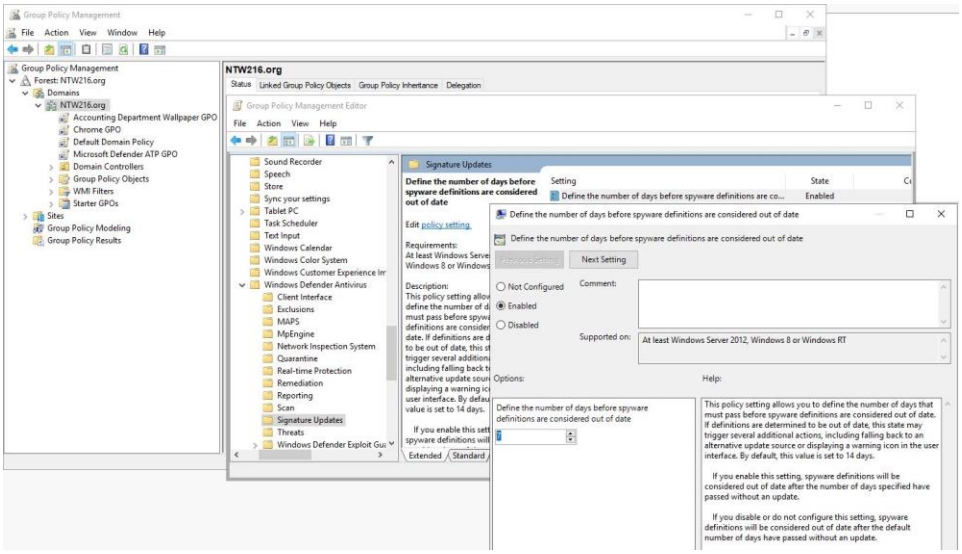

Figure 16. Anti-Virus Update Setting

Domain Routing and Remote Access

Once that is completed, the next step is to set up and configure the VPN so that any remote employees and the new kiosk machine can connect to the domain security. We must install the Routing and Remote Access Service on the servers that will act as access nodes for the domain.

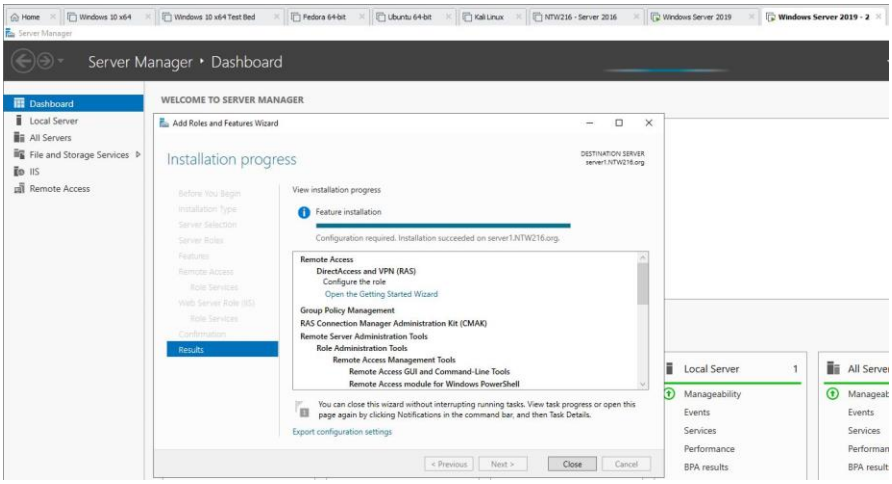

Figure 17. Routing and Remote Access Service Install

This helps to limit how many access points and the amount of traffic can connect to the domain from the outside. After the service is installed, we need to configure the VNP to the network. We need to open the RRAS tool and then right-click on the server that is listed and select the configure and enable the option in the submenu.

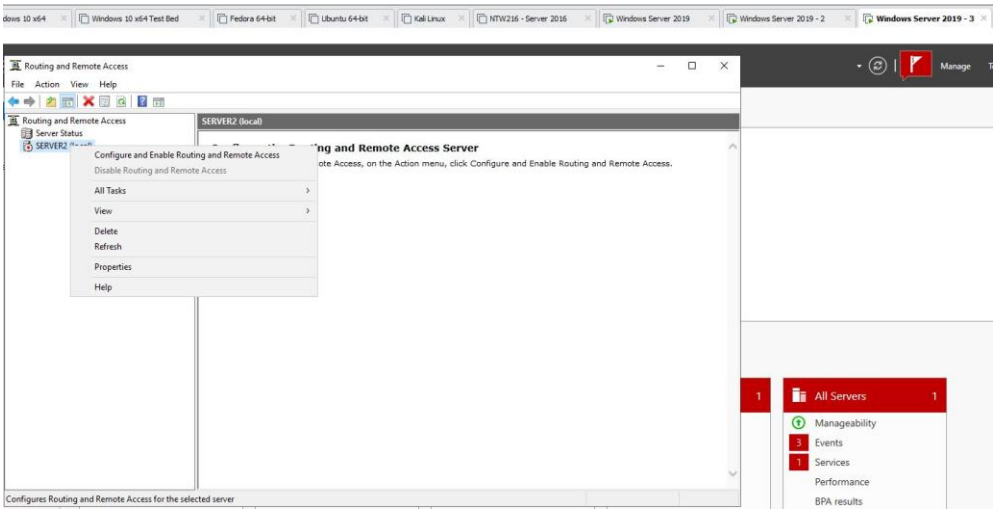

Figure 18. Configure VPN

Another wizard will walk you through the initial setup to start running the service.

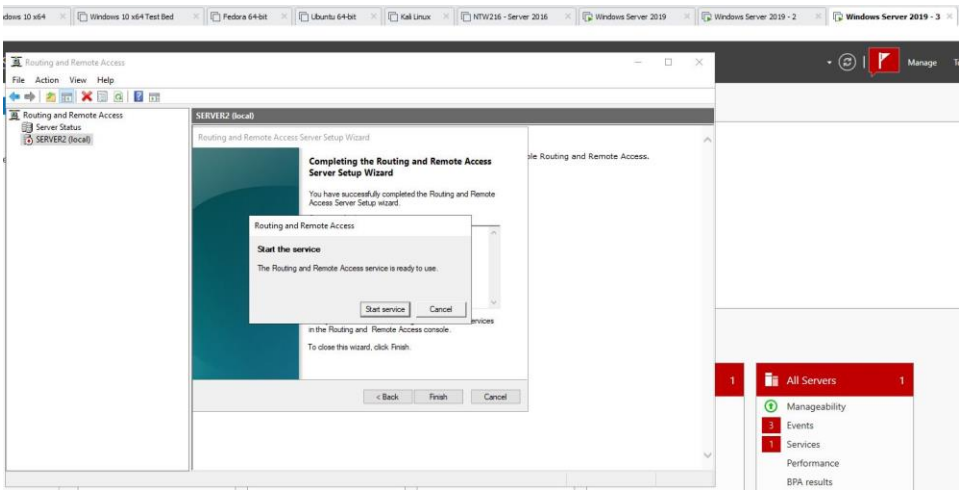

Figure 19. Service Starting

Immediately following the VNP is constructed, and all that is needed is to configure the IP for the VPN access. Right-clicking on the server shown and selecting the option for Properties will bring up the Properties window. Clicking on the IPv4 tab, we can configure the IP range for the new VPN. This IP range will exist outside the current domain IP range but will still be able to connect due to the routing functions with the RRA service.

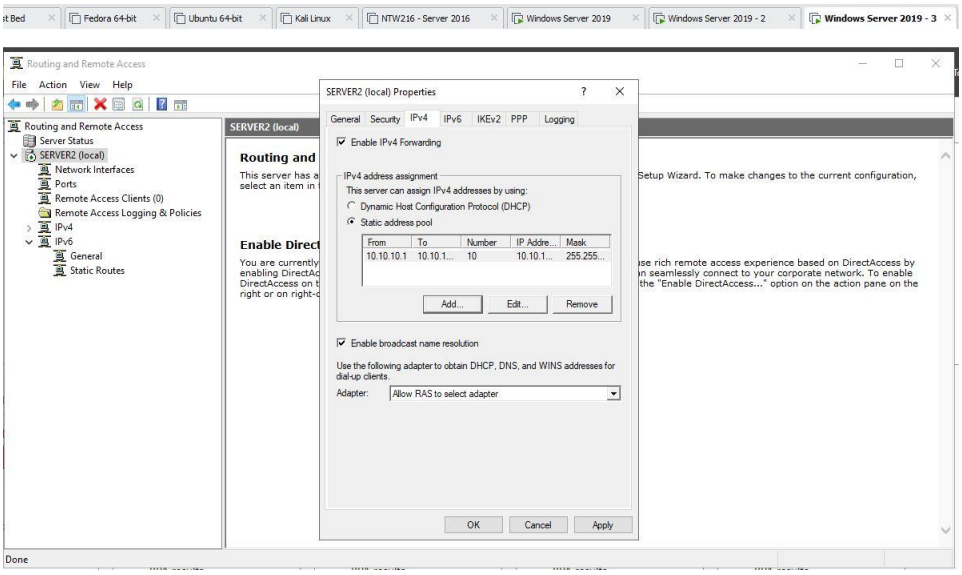

Figure 20. IP Configuration

Facility and Power

We also need to look at where the servers for our network will be housed. We need to make sure that the servers have redundant power connections and that those connections are also on sperate circuits. The facility will have UPS banks, uninterruptible power supplies, and backup power able to maintain the power needed for the server as well as the cooling of the server environments. The facility will also have redundant cooling to ensure the equipment is not degrading due to overheating and that the facility is connected by two separate power transformers fed from opposite sides of the facility.

Proposed Timeline for Implementation

The IT department has come up with an estimate for how long building this new network would take. This is only a rough estimate and is based on the experience of installing similar equipment. The network will be broken up into parts to allow for a better estimate of time to completion, and by using these groupings, we can see the breakdown for installing each group. The Edge Router, Firewalls, Core Switch, User Router, and User Switches will fall under the Core Networking Group.

The Domain / DNS Switches, Domain Controller Servers, and DNS Servers will be in the Domain Group.

The Corporate File Switch, Corp File Servers, Corp Storage Array Servers, and Backup Tape System will be in the Corp File Group. We will also group the file server cluster for legal in the same way and will be labeled the Legal File Group.

The Update Switch and Update Servers will be in the Update Group.

The Printer Load Balancer and Print Servers will be in the Printer Group.

The VoIP Load Balancer and VoIP Servers will be in the VoIP Group.

- To Rack & Stack and cable up the Core Networking Group will take an estimated 12

hours for 2 people. Add 8 more hours and 1 more person for the configuring of network equipment.

- To Rack & Stack and cable up the Domain Group will take an estimated 6 hours for 1 person. Add 1 hour per device for OS installation/configuration.
- To Rack & Stack and cable up the Corp File Group will take an estimated 9 hours for 1 person. Add 1 hour per device for OS installation/configuration.
- To Rack & Stack and cable up the Legal File Group will take an estimated 9 hours for 1 person. Add 1 hour per device for OS installation/configuration.
- To Rack & Stack and cable up the Update Group will take an estimated 5 hours for 1 person. Add 1 hour per device for OS installation/configuration.
- To Rack & Stack and cable up the Printer Group will take an estimated 6 hours for 1 person. Add 1 hour per device for OS installation/configuration.
- To Rack & Stack and cable up the VoIP Group will take an estimated 6 hours for 1 person. Add 1 hour per device for OS installation/configuration.

It would take an estimated total of 93 billable man-hours at the given figures above to complete this project, barring no issues. Note, the time to completion will be different depending on the number of people assigned to the project.

Proposed Labor Costs

Labor costs for this project are based on industry-standard labor rates, which are listed below.

- Jr. System Administrator hourly rate: $64
- Sr. System Administrator hourly rate: $94

Salary (Hourly)	$ 55.00	$ 37.50
Medicare Tax (1.4%)	$ 0.77	$ 0.53
Social Security Tax (6.2%)	$ 3.41	$ 2.33
Federal Unemployment Tax (6.2%)	$ 2.86	$ 1.95
State Unemployment Tax (5.4%)	$ 2.97	$ 2.03
Profit (5%)	$ 2.75	$ 1.88
401K plan cost (5%)	$ 2.75	$ 1.88
Medical Plan cost (25%)	$ 13.75	$ 9.38
Dental plan cost (1.5%)	$ 0.83	$ 0.56
Insurance costs (15%)	$ 8.25	$ 5.63
Total Labor Rate	$ 93.34	$ 63.64

Figure 21. Labor Rate Brake Down. (Benton, 2020)

Based on the proposed timeline figures above and accounting for having at least one Sr System Administrator on for OS installs and configurations during each group implementation, the minimal estimated projected costs for man-hours will come out to $7,920.00. Note, the cost for completion will be different depending on the number of people assigned to the project.

Cost-Benefit Analysis

Based on the requested items for implementation and the company profile, from a cost-benefit standpoint, the IT department feels that this proposal is the best means to implement the requested network infrastructure. While other solutions may have lower out-of-the-box costs,

over time, the company would see increased support costs as the need to expand increased. This solution will maximize all aspects of the company's operation while maintaining a stable foundation for any additional services or assets the company already has outside the of this proposal. These upgrades are not short-term gains, but long-term protections that can be scaled up as the company grows over the next 10 years.

In conclusion, the best option for this project is the proposed network infrastructure along with Microsoft Server 2019 as the chosen OS across the network. Out of the box, Server 2019 comes ready to configure for all required parameters, and this infrastructure solution covers all the company's needs while laying the foundation for continued growth.

References

Azure Marketplace. (n.d.). IIS on Windows Server 2019. Retrieved from https://azuremarketplace.microsoft.com/en-us/marketplace/apps/apps-4-rent.iis-on-windows-server-2019

Benton, R. (2020). Figure 21. *Labor Rate Break Down*. [screen capture]. Retrieved from https://synchronic.uat.edu/courses/3100/assignments/113404

Buzdar, Karim. (2017). Deploying Windows Server Update Services in Domain Environment and Using Group Policies on Windows Server 2012 R2: Step by Step Guide. Retrieved from https://www.itprotoday.com/windows-78/deploying-windows-server-update-services-domain-environment-and-using-group-policies

Chris. (2016). How Does a Print Server Work? Retrieved from https://www.printerland.co.uk/blog/2016/11/how-does-a-print-server-work/

Figure 1. *Proposed Network Diagram* [screen capture]. (2020).

Figure 2. *Disk Manager* [screen capture]. (2020).

Figure 3. *Volumes Created* [screen capture]. (2020).

Figure 4. *Adding User Groups* [screen capture]. (2020).

Figure 5. *User Volume Permissions* [screen capture]. (2020).

Figure 6. *Corp Volume Permissions* [screen capture]. (2020).

Figure 7. *Corp Subfolder Configuration* [screen capture]. (2020).

Figure 8. *User Subfolder Configuration* [screen capture]. (2020).

Figure 9. *File Services Shares Properties* [screen capture]. (2020).

Figure 10. *NLB Install* [screen capture]. (2020).

Figure 11. *Configuring New Cluster* [screen capture]. (2020).

Geeks for Geeks. (n.d.). Advantages of DBMS over File system. Retrieved from https://www.geeksforgeeks.org/advantages-of-dbms-over-file-system/

Petters, Jeff. (2019). Active Directory Domain Services (AD DS): Overview and Functions. Retrieved from https://www.varonis.com/blog/active-directory-domain-services/

Reed, Jessie. (2019). Debunking Tape Backup Myths in 2019: Full Overview. Retrieved from https://www.nakivo.com/blog/debunking-tape-backup-myths-in-2019-overview/