Old Dominion University

IT 416 Network Server Configuration and Administration

IT 416 Advanced Network and Server Configuration Group Project

Dakota Bershers
Alec Kurek
Marcos Luchetti

Table of Contents

Introduction

The Strome College of Business is proposing to administer its network of computers used by its faculty and students. Microsoft Windows Server 2019 offers a wealth of features that meet the needs of the College. These include server roles, security, server management, and reliable computing. Components to be discussed in this report include specifications, Windows Server 2019 installation and configuration, implementation of Hyper-V, rapid server deployment, Active Directory, account management, as well as configuring and managing resource access, printing, data storage, and network services. This report will outline and justify the suggested server configurations and discuss the methodologies used in determining the different configurations, the domain, and users. The following conditions of the College are to be supported by the configurations:

- Strome College of Business
    - 100 full time faculty
    - 4000 students
        - 400 IT majors

- Business computer lab, IT computer lab (20 machines each)
    - IT majors use IT lab only, Business majors only use Business lab
    - Faculty can use both labs and their offices

- Business majors are allowed 100 MB of storage space on the network server
- IT majors are allowed 250 MB storage space

- Faculty must have at least 1 GB of network storage space allocated, ability to install/remove software but not configure critical components of their computer or access to the control panel

- All computers in the labs must be secured
    - Prevent unwarranted access, changes to the system (including access to the primary partition containing the OS and control panel)

- Installation and configuration of two domain controllers and three client computers representative of the three types of users (faculty, business, and IT students)
    - The NOS is Windows Server 2019 and the client OS is also Windows Server 2019

- Create a spreadsheet and a script that is used to generate about 10 accounts in each category

This report will further explain how to install, administer, and support Windows Server 2019 to deliver the most optimally efficient work and learning environment for the Strome College of Business.

System Specifications and Windows Server 2019 Installation

This section will cover the recommended system specifications and the installation of Windows Server 2019.

We recommend desktop systems that meet or exceed the following specifications:

- A 64-bit computer with a recent-generation processor that supports virtualization extensions (Intel VT + SLAT)
- 32 GB of memory
- 512 GB internal hard drive
- Built-in Network connector (RJ-45) 10/100/1000
- Microsoft Windows 10 Enterprise x64 for clients
- Microsoft Windows Server 2019 Datacenter Edition for servers

We have selected the Windows Server 2019 Datacenter Edition because it is designed for environments like the Strome College of Business that uses very large databases, very large virtualization requirements, cloud computing needs, and information access requiring high availability. To install Windows Server 2019 Datacenter Edition on the computer, insert the DVD or USB flash drive media containing the ISO image into the computer. Turn on the computer and wait for the POST splash screen. From there, press F2 or Del to access the BIOS utility, and then change the boot order so that it boots directly from the installation media. Once the Windows Setup screen appears, select the correct language, time and currency format, and keyboard or input type, and click Install now. Select Windows Server 2019 Datacenter (Desktop Experience) from the list of Windows Server 2019 editions and click Next. Accept the license terms, and click Next. After that, select Custom: Install Windows only (advanced), a window will be displayed, showing a list of storage devices within the computer. Highlight any partitions under Drive 0 and click Delete in turn until no more partitions exist under the storage device. Lastly, highlight the only remaining storage device and click Next to install Windows Server 2019 on it. After the installation has completed, click Restart now. When the Customize settings window appears, enter a secure password in the Password and Reenter password text boxes and click Finish. Then, log in to the Administrator account using this password.The system now has a fresh install of Windows Server 2019 Datacenter Edition.

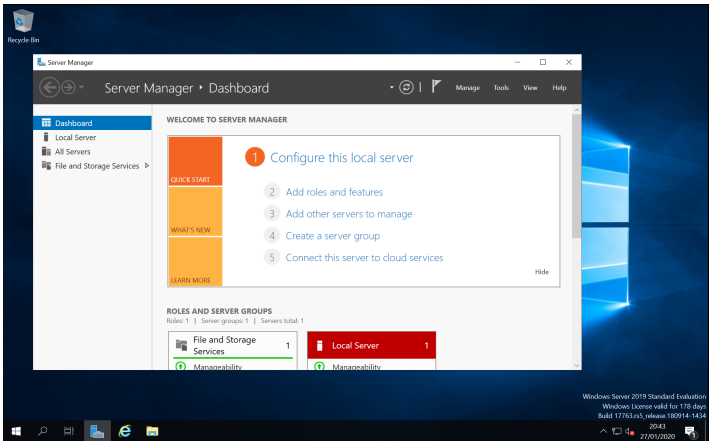

Figure 1 - Fresh installation of Windows Server 2019

After completing the installation process, the next step is to perform post-installation configurations. First, set the correct time and time zone on the computer. This will ensure that the server has the correct time and time zone that is required for many services that work with multiple computers on the network, such as Active Directory. The Server Manager allows us to monitor and manage the configuration of the local server it is running on and it can be used to centrally manage multiple servers on the network if we decide to add more servers to the Server Manager interface. To change the time, open the Server Manager, navigate to Local Server and select the hyperlink next to Time zone in the Properties window. To change the time zone, click Change time zone, select the correct time zone [(UTC-05:00) Eastern Time (US & Canada)], and click OK.

Now, to manually configure the IP on a network interface within Server Manager, navigate to Local Server and select the hyperlink next to the associated network interface (e.g., the Ethernet network interface). The Properties window will be displayed. Here, select IPv4 and click Properties. Supply the following information: IPv4 Address 10.1.130.1, IPv4 Default Gateway and DNS Server 10.1.1.1, and click OK. To make future troubleshooting of user access easier, disable the Windows Defender Firewall on the Domain, Private, and Public network. Next, change the default computer name to *SCB-SERVER-1*, for Strome College of Business. To make this change, navigate to Local Server on the Server Manager and select the hyperlink next to Computer name in the Properties window. From there, click the Change button and supply the new computer name in the Computer name field. After that, restart the server. Once rebooted, log in as Administrator, open the Server Manager and navigate to Local Server. Select the hyperlink next to Workgroup in the Properties window. Click the Change button, then select the Domain radio button and supply the domain name of the Active Directory domain (*SCB.com*) that will be configured later on.

Then, install a modern web browser such as Google Chrome. This is an important step in that the default Web browser is Internet Explorer, which is included for legacy application support only, and it does not support most modern Web tools such as the Windows Admin Center. In order to install a modern Web browser, we must first disable the Internet Explorer Enhanced Security Configuration (IE ESC). Navigate to the Local Server and select the hyperlink next to IE Enhanced Security Configuration in the Properties window. From here, we must disable IE ESC for all users. Now, activate the Windows Server 2019 operating system by opening the Server Manager, navigating to Local Server, and selecting the hyperlink next to Product ID in the Properties window. Here, enter the license key and click Activate to complete the activation process. Finally, open Windows Update and click Check for updates. Download and install any pending updates, and then restart the computer. It may take a few reboots to install all the updates. The next section will elaborate further on the Windows Server 2019 configuration.

Figure 2 - IPv4 settings

Configuring Windows Server 2019

This section will cover the different tools that can be used to monitor and configure Windows Server 2019 in more depth, including Server Manager, the Windows Admin Center, Control Panel, and Device Manager. Also detailed is the configuration of Roles and Features, Windows Admin Center, and Windows settings.

Use the Server Manager to monitor and manage the different Windows Server systems on our network and the roles that they provide. This tool is also to be used for configuring the local server, adding roles and features, adding other Windows Servers to manage from the Server Manager console, and creating groups to organize other Windows Servers as well as a wizard that allows us to connect Server Manager to servers and roles that we manage within the Microsoft Azure cloud. Use the Services tab under Local Server to find services that are not started, they should be flagged as red. It is a recommended configuration that this program shows detailed error information to help prevent and solve problems. To see more detailed error information, click on the Events pane, then click Tasks, Configure Event Data. Then, select Informational and click OK. Now, there will be additional events that are shown within the Events pane.

Now, to configure DHCP on the server, highlight the Roles and Features pane, click on Tasks, and then click on Add Roles and Features. Click Next on the Before you begin page, then click Next two more times. At the Select server roles page, select DHCP Server and then click Add Features. Click Next when it's done. On the Select features page, select Telnet Client and click Next, then click on Install to install the DHCP Server role and Telnet Client feature. Once the installation is complete, click Complete DHCP configuration, click Commit, and then click Close, finally closing out of the Add Roles and Features Wizard. After that, we must fix any errors in the DHCP feature. First, highlight DHCP in the navigation pane of Server Manager and head to the Best Practices Analyzer pane. Click on Tasks, then Start BPA Scan, and then click Start Scan, noting any Warning and Error that we receive. In the Services pane, right-click the DHCP Server service and click Stop Services. Then, right-click the DHCP Server service again, then click on Start Services, and click OK. After that, click on the Refresh button in the upper right of Server Manager. The BPA-related red flag disappears and the error should now be resolved. Now, click on Manage in the upper right of Server Manager, and click on Create a Server Group. Enter SCB-GROUP1 in the Server group name box. After that, select *SCB-SERVER-1* in the Server Pool tab and click OK. The new server group now appears in the Server Manager navigation pane.

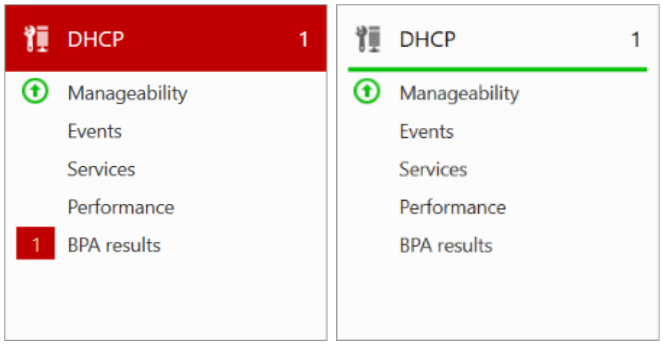

Figure 3 - BPA scan errors resolved

Next is the installation and configure of the Windows Admin Center, a tool which allows for managing the server remotely from any computer that has a modern Web browser. This will prove useful for the SCB because it is an environment that hosts a large number of remote Windows Server systems that must be managed centrally, including cloud environments. To install the Windows Admin Center, open Google Chrome and head to the following URL: https://aka.ms/WindowsAdminCenter. Download the latest non-preview version of the Windows Admin Center and begin the installation. Accept the terms in the License Agreement, and click Next four times, click Install and then Finish. Once installed, navigate to https://SCB-SERVER-1:443 within the Chrome Web browser. From here, it is possible to add servers by server name or import a list of server names. To assign a connection tag to *SCB-SERVER-1*, highlight it and click Edit tags. Then, type 2019HOST and click Save. Now, we are going to modify the power configuration of the server. On the All Connections page, highlight *SCB-SERVER-1* and click Connect. Click on Manage alerts, select Environment variables, and select Power configuration, then select the High performance power plan and click save. This will ensure that the server will perform at its greatest capacity. The Windows Admin Center also allows for the configuration of multiple functionalities, such as the Network feature, Firewall, Registry, Roles and Features, Virtual Machines, etc. The Control Panel and Device Manager can be used to install hardware devices. To scan the system for unsigned files, right-click the Start menu and click Run, then type sigverif in the Run dialog box and hit Enter to initiate the scan. This will verify the system and critical files to determine if they have a signature, including device drivers. The results are dumped into a log file called sigverif.txt, and if the tool finds a file without a signature that needs to be replaced, we must replace the file using the System File Checker. This can be done by obtaining the specific file from Microsoft's website, or by reinstalling the device driver or program with an up-to-date version.

The next step is to configure Windows settings. First, we must configure the performance options. This includes configuring processor scheduling and Data Execution Prevention, virtual memory, and file caching and flushing. With processor scheduling, we can configure how processor resources are allocated to programs. We will adjust the processor scheduling to adjust for best performance of background services rather than programs. This means that all programs running will receive equal amounts of processor time. In the event of a critical backup process, we will switch to the Programs setting, which refers to programs we will be running at the server console, such as a backup program. Furthermore, Data Execution Prevention (DEP) aids in assuring performance and security by monitoring how programs use memory to ensure they are not causing memory problems. DEP can essentially counteract malware, such as computer viruses, Trojan horses, and worms. If DEP notices a program trying to use system memory space, it stops the program and notifies the system administrator. Some applications, for instance, those that use dynamic code generation, might not work well with DEP. Programs such as these will often execute on the system, but will have much less performance. It is for that reason that we will exclude these programs from DEP, which include programs that run exception handlers, and code requiring executable locations in memory. This will help increase performance of the system. The default location of virtual memory paging files will be set to a separate hard disk that does not contain the Windows Server 2019 operating system, improving performance. File caching and flushing will remain turned on because in most cases, server performance is better with these options enabled. Another important feature to enable is PowerShell script support. To enable script support, we will open PowerShell and execute the following command:

Set-ExecutionPolicy unrestricted. This will become useful later on for executing the script that is used to generate user accounts. In the next section, we will cover the implementation of Hyper-V and rapid server deployment in Windows Server 2019.

Implementing Hyper-V and Rapid Server Deployment

This section is concerned with the configuration of Hyper-V to provide virtualization for Windows Server 2019, in addition to rapid server deployment of Windows Server 2019 systems using virtual machine templates and WDS.

With virtualization, server hardware can be used more efficiently by running multiple guest operating systems, or virtual machines, simultaneously. This will help reduce power and server cooling costs within the SCB, also reducing the energy and carbon footprint rendered onto the environment. To enable this feature, the computer must run a hypervisor that emulates a unique set of virtual hardware components for each virtual machine. Windows Server 2019 Datacenter Edition includes Hyper-V, a Type-1 hypervisor, which we will be installing using to create, configure, and manage virtual machines. Since our processor supports Intel VT virtualization extensions with SLAT support which helps VMs to run as efficiently as possible, we are ready for installation. To install Hyper-V, we will select the Hyper-V role when adding a role within Server Manager. The installation of Hyper-V hypervisor and its associated Hyper-V management tools (graphical Hyper-V Manager console and Hyper-V PowerShell cmdlets) will commence. During the installation process, an external virtual switch will be created within Hyper-V to allow virtual machines access to the physical network using the network interface. We will also enable live migration of virtual machines, which essentially allows us to copy a running Hyper-V virtual machine from one server (source server) across a network to another server in the same Active Directory domain (target server). After the virtual machine is copied to the target server, it will be started on the target server and stopped on the source server so as to not worsen service availability. At the Default Stores page, we will set the Default location for virtual hard disk files to be located in the C:\VMs folder and virtual machine configuration files will be stored within the C:\VMs\Virtual Machines subdirectory. On the Confirm installation selections page, we will select the option that restarts the destination server automatically if required, and then click Install to begin the installation. The system will reboot twice as it installs Hyper-V—the first is for adding Hyper-V in a Type 1 configuration, and the second allows Hyper-V to start the host operating system that is used to manage virtual machines. If the installation was successful, then our server should be listed within the navigation pane of Hyper-V.

Now we will create and configure a new internal virtual switch that will be used by the system. In the Network Connections settings, there will be a new network interface called vEthernet, which represents our Hyper-V external virtual switch. This will have the same IP configuration that was configured previously during the initial setup of Windows Server 2019. There is a Virtual Switch Manager in the Hyper-V Manager tool that we will use to configure this external virtual switch. We will rename it to “External Virtual Switch” so that it is discernible from the new “Internal Virtual Switch” that we are about to create. This represents a virtual network to which virtual machines and the host operating system can connect. The internal virtual switch can be used to create an isolated network for specific types of communication, providing enhanced security. Once created, we are going to right-click this vEthernet (Internal Virtual Switch) and edit the IPv4 address, changing it to 172.16.0.1, also changing the subnet mask to 255.255.0.0. This is important because it will be used to configure DHCP. We are also going to need to install and configure the Windows Deployment Services (WDS).

First, we must use the DHCP tool to add a new IPv4 scope with the dress range of 172.16.0.50 - 172.16.0.100. Once the scope is added, we can activate it. Now, we can proceed to configuring WDS, setting it up to install a standalone server at the default location, and have it respond to all client computers (known and unknown). After clicking Finish, we will insert the Windows Server 2019 installation media into the computer. We will then use WDS to add a boot image, selecting and opening boot.wim from the \sources folder on the USB drive, and also add an install image (\sources\install.wim), clicking Next until we finish the Add Image Wizard. Now, we can start the Windows Deployment Services on the server and use that, PXE, and the internal virtual switch, to install Windows Server 2019 on the virtual machines. The virtual machine setup is as follows. We will create a new Generation 2 virtual machine, which provides modern hardware emulation for guest operating systems. Virtual machines are to have 4 GB of memory and a 127 GB dynamically expanding hard disk (this can be modified to suit the needs of the SCB as time goes on). The names of the VMs will be "SCB-Server-VM-(number)." The VMs will be configured to use the Internal Virtual Switch for networking purposes. We will also configure it to install the OS from a network-based installation server. Once that is finished, we can connect to the VM and boot into it. We can then press F12 when prompted to boot from a network server, which will download the boot.wim file from the WDS server configured earlier to the VM, initiating the installation of Windows Server 2019 Standard to the VM. Once that is finished, we can restart the VM and the system will reboot twice to complete the installation process.

A virtual machine template will be configured with these settings so as to aid in the creation of VMs that need to be the same. For that, we will need to use the System Preparation Tool to create a template named "SCB-VM-Template." In the System Preparation Tool window, we will select the Generalize option, which will remove all unique information from the system and shut down the guest operating system when finished. When the VM is booted again, the Out-of-Box Experience (OOBE) wizard will create a new computer name and unique identifiers within the Registry, and prompt the user with entering specific regional options, accepting the Windows license agreement, and specifying a new password for the Administrator account. These templates can be stored in the C:\VMTemplates folder, where they can later be imported to create new virtual machines. We will also create production checkpoints, which are less resource-intensive than standard checkpoints. Moreover, since we enabled live migration during the installation of Hyper-V, it is possible to move a VM to another server running Hyper-V within the same Active Directory domain. In the next section, we will cover Active Directory and account management on Windows Server 2019.

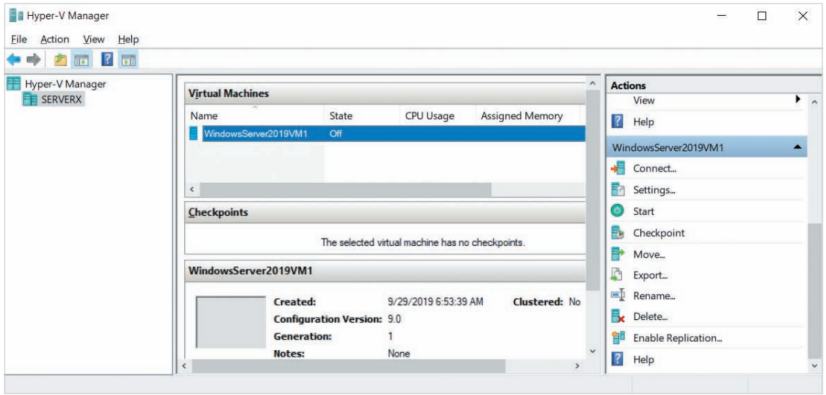

Figure 4 - Hyper-V Manager

Active Directory, Account Management, and Configuring Access

This section will encompass Active Directory and account management within our Windows Server 2019 environment.

Active Directory is used to set up user accounts, objects, and access. In our environment we will utilize a virtualized machine through HyperV in order to set up the domain controller for this environment. Using Server Manager, the virtualized machine will be set up with Active Directory as a domain controller, Active Directory Domain Services will be installed with a domain of scb.com and a functional level of Windows Server 2016 will be enabled. For the current project status we will only utilize one "site" called StromeCollege.

In our Windows Server 2019 environment we will utilize the Active Directory Users and Computers tools to create OU Groups to manage faculty, administrator, and student accounts. These OU groups will be named "Faculty", "Administrator", and "Student"; Templates of these OUs will be created for future use. Within these groups, identifiers for the departments of which they belong will be created for the departments to which they belong. For the Strome College of Business these departments are "Business" and "IT". This step will be important for setting up storage permissions and access rights going forward.

On the domain controller we will have to begin to add the authorized users to the OU groups. Due to the high volume of users on the system the time cost of adding users individually will be too expensive. Because of this, we will be using a .csv spreadsheet and an ADscript for Powershell to add bulk user lists to the domain. This list should be easy to keep up-to-date and allow for tracking changes to user information more easily. The .csv that has been created encompasses the most pertinent information for each user. Users will be tracked in the system by their SamAccountName, a unique identifier for each user account. The .csv has been set up to detect when there is a duplicate name generated based on similar first and last names. Once detected, the .csv file will add a numerical digit to the end of the account name in order to differentiate the name from similar names in order to keep it a unique identifier. The user email addresses are generated automatically from the SamAccountName and adds the domain name to the end of the SamAccountName as it will be generated on our mail server later in the user generation process. In this .csv the user's first time password will be generated as an eight character password with a mixture of Upper-case, lower-case, numbers, and special characters; however, once the user performs a login for the first time, the server will prompt the user to create a personalized, unique password to be updated every six months. IT services will not track this unique password and will only have the ability to generate password reset requests. An example of this .csv is provided below in Figure 6, as well as a link to the original file. Note that this file may not be completely functional without the Server 2019 environment.

	SamAccountName	password	path	GivenName	Surname	MiddleInitial	Name	UserPrincipalName	OfficePhone	EmailAddress	MemberOf	Department
2	Tony.Stark	UcwR848*		Tony	Stark	H	Tony.Stark	Tony.Stark@scb.com	757-240-1002	Tony.Stark@scb.com	Administrato	Staff IT
3	Ann.Doe	TizF923*		Ann	Doe	F	Ann.Doe	Ann.Doe@scb.com	757-240-7117	Ann.Doe@scb.com	Faculty	IT
4	Ann.White1	TjmF649+		Ann	White	H	Ann.White	Ann.White1@scb.com	757-240-8116	Ann.White1@scb.com	Faculty	Business
5	George.Potter	WgvY256*		George	Potter	W	George.Potter	George.Potter@scb.com	757-240-6119	George.Potter@scb.com	Faculty	Marketing
6	Ken.Potter	OmeN761+		Ken	Potter	J	Ken.Potter	Ken.Potter@scb.com	757-240-9118	Ken.Potter@scb.com	Faculty	Business
7	Mark.Doe	IjoQ884*		Mark	Doe	V	Mark.Doe	Mark.Doe@scb.com	757-240-4118	Mark.Doe@scb.com	Faculty	IT
8	Mark.Greene	ComU771*		Mark	Greene	Y	Mark.Greene	Mark.Greene@scb.com	757-240-5113	Mark.Greene@scb.com	Faculty	Business
9	Mark.Potter2	PfyT777*		Mark	Potter	H	Mark.Potter	Mark.Potter2@scb.com	757-240-6113	Mark.Potter2@scb.com	Faculty	IT
10	Matt.Doe	JbvB202+		Matt	Doe	S	Matt.Doe	Matt.Doe@scb.com	757-240-7115	Matt.Doe@scb.com	Faculty	Business
11	Sam.Brown	RhuM684*		Sam	Brown	M	Sam.Brown	Sam.Brown@scb.com	757-240-6511	Sam.Brown@scb.com	Faculty	Business
12	Sam.Doe	CokT504*		Sam	Doe	D	Sam.Doe	Sam.Doe@scb.com	757-240-8116	Sam.Doe@scb.com	Faculty	IT
13	Ann.Greene	DutQ400*		Ann	Greene	Y	Ann.Greene	Ann.Greene@scb.com		Ann.Greene@scb.com	Student	IT
14	Ann.White	AfaD251+		Ann	White	L	Ann.White	Ann.White@scb.com		Ann.White@scb.com	Student	IT
15	Ashley.Brown	TfrT728*		Ashley	Brown	T	Ashley.Brown	Ashley.Brown@scb.com		Ashley.Brown@scb.com	Student	Business
16	Ashley.Brown1	VaeM204+		Ashley	Brown	G	Ashley.Brown	Ashley.Brown1@scb.com		Ashley.Brown1@scb.com	Student	Business
17	Ashley.Doe	NipG940+		Ashley	Doe	R	Ashley.Doe	Ashley.Doe@scb.com		Ashley.Doe@scb.com	Student	IT
18	George.Brown	JgjD292+		George	Brown	T	George.Brown	George.Brown@scb.com		George.Brown@scb.com	Student	IT
19	George.Greene	LjiY718+		George	Greene	E	George.Green	George.Greene@scb.com		George.Greene@scb.com	Student	Business
20	George.White	QfuB418*	OU=Testir	George	White	Q	George.White	George.White@scb.com		George.White@scb.com	Student	Business
21	Jennifer.Brown	AogD385*		Jennifer	Brown	U	Jennifer.Brow	Jennifer.Brown@scb.com		Jennifer.Brown@scb.com	Student	IT
22	Jennifer.Greene	RnjQ510*		Jennifer	Greene	N	Jennifer.Greer	Jennifer.Greene@scb.com		Jennifer.Greene@scb.com	Student	IT
23	Jennifer.White	IzrT188*		Jennifer	White	H	Jennifer.White	Jennifer.White@scb.com		Jennifer.White@scb.com	Student	IT
24	Mark.Potter	SwzX222*		Mark	Potter	I	Mark.Potter	Mark.Potter@scb.com		Mark.Potter@scb.com	Student	Business
25	Mark.Potter1	SjyK656+		Mark	Potter	K	Mark.Potter	Mark.Potter1@scb.com		Mark.Potter1@scb.com	Student	Business
26	Mark.White	VnhZ117*		Mark	White	P	Mark.White	Mark.White@scb.com		Mark.White@scb.com	Student	Business
27	Matt.Potter	OnjC904*		Matt	Potter	A	Matt.Potter	Matt.Potter@scb.com		Matt.Potter@scb.com	Student	IT
28	Matt.Potter1	AdcT893+		Matt	Potter	C	Matt.Potter	Matt.Potter1@scb.com		Matt.Potter1@scb.com	Student	Business
29	Matt.Potter2	EheJ914*		Matt	Potter	R	Matt.Potter	Matt.Potter2@scb.com		Matt.Potter2@scb.com	Student	IT
30	Sam.White	CzuI510*		Sam	White	O	Sam.White	Sam.White@scb.com		Sam.White@scb.com	Student	Business
31	Sam.White1	UkxK979+		Sam	White	B	Sam.White	Sam.White1@scb.com		Sam.White1@scb.com	Student	Business

Figure 5: Snapshot of 31 Users in bulk_import.csv. Full file - https://drive.google.com/file/d/1xZ3zZOMURBsrc8nO84czOEfsF0AY3QJV/view?usp=sharing

The AD script for powershell is a baseline for completing a bulk import from the .csv file provided. The script scans the .csv file for user data and imports that into the user objects in AD while also checking for duplicate Usernames in order to prevent issues with user authentication. This script does not add a character to the end like the .csv did, however it does warn the technician doing the import of any duplicate entries into AD in the Powershell GUI. The script will also execute a few other commands such as converting the first time login password into a secure string instead of plain text, enable the account, and set the password to require a change on first login. This script is a strong foundation for getting accounts set up for initial and ongoing use on the system and is easy to expand upon if necessary. An example of the script used to implement the bulk import of users can be found in Figure 7 below.

```
#Import active directory module for running AD cmdlets
Import-Module activedirectory

#Store the data from ADUsers.csv in the $ADUsers variable
$Users = Import-csv c:\it\bulk_import.csv

#Loop through each row containing user details in the CSV file
foreach ($User in $Users) {
    # Read user data from each field in each row
    # the username is used more often, so to prevent typing, save that in a variable
   $Username       = $User.SamAccountName

    # Check to see if the user already exists in AD
    if (Get-ADUser -F {SamAccountName -eq $Username}) {
         #If user does exist, give a warning
         Write-Warning "A user account with username $Username already exist in Active Directory."
    }
    else {
        # User does not exist then proceed to create the new user account

        # create a hashtable for splatting the parameters
        $userProps = @{
            SamAccountName             = $User.SamAccountName
            Path                       = $User.path
            GivenName                  = $User.GivenName
            Surname                    = $User.Surname
            MiddleInitial              = $User.MiddleInitial
            Name                       = $User.Name
            DisplayName                = $User.DisplayName
            UserPrincipalName          = $user.UserPrincipalName
            Department                 = $User.Department
            OfficePhone                = $User.OfficePhone
            EmailAddress               = $User.EmailAddress
            MemberOf                   = $User.MemberOf
            AccountPassword            = (ConvertTo-SecureString $User.password -AsPlainText -Force)
            Enabled                    = $true
            ChangePasswordAtLogon      = $true
        }   #end userprops

         New-ADUser @userProps
       #  Write-Host "The user account $User is created." -ForegroundColor Cyan


    } #end else
```

Figure 6: Snapshot of bulk_import_script.ps1 for Powershell bulk entry of ADusers. Full file - https://drive.google.com/file/d/11Iuy51YhssZHx9bNm5WtyQ3_7LygJFbT/view?usp=sharing

Through the use of DFS Namespaces and Active Directory, the users will receive managed file access and storage allotments on the storage server provided by the institution.

In our configuration students will only receive access to Namespaces belonging to their degree field, “Business” and “IT”, and will only have access to computer labs assigned to these degree fields. Within these namespaces, students will have individualized folders in which only the account holder and IT Administrators will have access. Using user quotas, these folders will have limited, dynamically expanding storage for each user in the amount of 250MB for “IT” students and 100MB for “Business” students. Should a student be a member of both groups in the event of blended major programs, whichever group has the higher storage availability will take

precedence. Student accounts will have read, write, delete, and create access for their individual folder. File screens will be enabled for file types which may be damaging to the system these filetypes may consist of but are not limited to .exe, .msc, .js, .bat, .jsc, ect.. The only exception to this policy will be for “IT” students within a controlled environment. These exceptions will only be handled by an exception to policy handled by the professor of the class and ITS. Student accounts will not have access to introduce or run .exe files which have not been approved by the institution's ITS. Access to the primary partition, OS files, and the control panel will be denied for all student accounts.

Faculty accounts will have additional privileges not afforded to student accounts. Each faculty member will have access to 1GB of dynamically expanding storage hosted under the namespace “Faculty” and within a personalized file. Within this file, faculty will have modify access. Due to some faculty teaching under both “IT” and “Business” courseware, we do not want to limit the faculty to these namespaces. Faculty will have access to run .exe files, but will not have access to the system partition, control panel, or other potentially damaging file types. Exceptions to this policy can be petitioned with ITS and with review, these file types can potentially be utilized. Faculty accounts will not be restricted to specific computers or computer labs within the Strome College of Business and will have access to their namespace anywhere within the building.

Configuring Printing

This section describes the process for printing documents to a print device or shared printer and how to configure and monitor a print server using the Print and Document. It also explains how to Use the Print Management tool to add and configure shared printers, as well as how to Deploy shared printers using Group Policy.

After we configure resource access, configuring printers are next. Printers are one of the most common shared network resources within environments today. To set up a printer, you must first add the Print and Document Services on the host machine. At the select features page, select Internet Printing Client and LPR Port Monitor and click Next. At the select role services page, select Select Internet Printing and click Add Features when prompted. In addition, Select LPD Service and click Next. After clicking the next button a couple more times, we are asked to install. Click install to to install the Print and Document Services role, as well as the Internet Printing Client and LPR Port Monitor features.

The next step is to configure printing using the print management tool. On the host machine click tools, then print management. Continue the setup process by expanding print servers, and then expand SCB-SERVER-1. Go to drivers and click add drivers from the action plane. In the setup wizard click next until it says finish. The printers that we are using are generic/text only, this will be all we have to add for the drivers for our printers. All of them are PnP- capable and so they are already configured when they are attached to the physical port. We have 7 printers for the full time faculty, 4 printers in the IT computer lab, and 4 in the Business computer lab. This is the case because faculty are there every day and are likely to print more than students. They will have faculty only access so students cannot use them. It is to be noted also that faculty can use

any student printer as well. Most students are not there to print, however, if they need to they will have access to print in their labs that they are assigned to via their majors, Business or IT.To add these printers, go to more action, add printer from the action plane, and click add a new printer from an existing port. We are going to use LPT1 printer port for every single printer we set up for now, and later we will use printer pooling for bidirectional printing. At the Printer Driver page, select Use an existing printer driver on the computer, we will ensure that Generic/Text Only is listed in the associated drop-down box and click Next. At the Printer Name and Sharing Settings page, make sure that printer sharing is enabled by default, then type FacultyPrinter1 in both the Printer Name and Share Name text boxes. Next, type Faculty department in the Location text box, then type faculty printer in the Comment text box and click Next. We will then continue to add the remaining 6 of the faculty printers using the same method as described using the names FacultyPrinter2 and so on. When that is completed, we will add the 4 printers for the IT computer lab. Once at the Printer Driver page, select Use an existing printer driver on the computer, we will ensure that Generic/Text Only is listed in the associated drop-down box and click Next. At the Printer Name and Sharing Settings page, make sure that printer sharing is enabled by default, then type ITPrinter1 in both the Printer Name and Share Name text boxes. Next, type IT department in the Location text box, then type student printer in the Comment text box and click Next. We will then continue to add the remaining 3 of the IT printers using the same method as described using the names ITPrinter2 and so on. When that is complete, the last thing we need to do is add the printers for the Business lab. To do this, select Use an existing printer driver on the computer, we will ensure that Generic/Text Only is listed in the associated drop-down box and click Next. At the Printer Name and Sharing Settings page, make sure that printer sharing is enabled by default, then type BUSPrinter1 in both the Printer Name and Share Name text boxes. Next, type Business department in the Location text box, then type student printer in the Comment text box and click Next. We will then continue to add the remaining 3 of the Business printers using the same method as described using the names BUSPrinter2 and so on.

We will now allow access for all necessary users from each of their respective roles. To do this, highlight SCB-SERVER-1 and go to more actions, properties from the action plane. Highlight the security tap and click add. Type in the name of George White and click ok. The permissions for Business majors should already be set. It should only allow them to print, manage documents, and view server. There should be a check marked next to all of them. CContinue this process with the remaining Business majors by adding the correct names under the security tab. Next we will do the same thing for the IT majors. This time, type the name of Jennifer White.The permissions for IT majors should already be set. It should only allow them to print, manage documents, and view servers.There should be a check marked next to all of them. Continue this process with the remaining IT majors by adding the correct names under the security tab. Finally, we will add the permissions for faculty. Type in the name of Ann White and click ok. The permissions for Faculty members should already be set. It should only allow them to print, manage documents, and view server. There should be a check marked next to all of them. Continue this process with the remaining Faculty members by adding the correct names under the security tab.

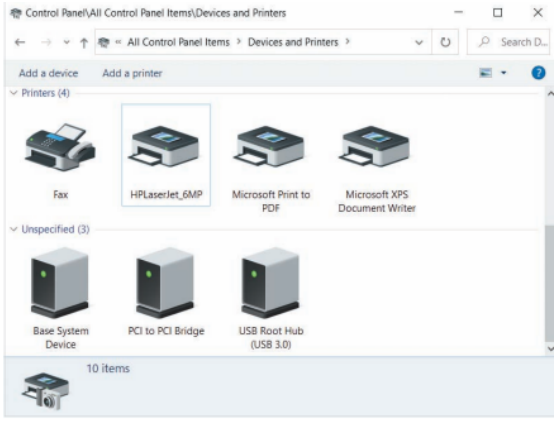

Figure 6-1 Viewing installed printers within the Devices and Printers utility

Configuring and Managing Data Storage

This section will introduce what data storage configuration we will use, as well as the procedures used to create and manage simple and software RAID volumes. Additionally, it will discuss how we will optimize, repair, and back up volumes.

After the printing is configured, we will then move to configure and manage our data storage. You can install two types of storage devices inside rackmount servers: hard disks and SSDs.We will be using a combination of the two to stay within company budget constraints. SSDs will be configured to store the operating system and applications, while hard disks may be used to provide storage for data. This will allow a configuration that provides fast performance for the operating system and applications while allowing for a large storage capacity for data at a low cost.

We will be creating one primary storage server that is hosted at the ip address of 172.16.0.51. There will be different volumes on the storage device to segregate the different types of data, allow for us to use more than one type of filesystem, reduce the change of filesystem corruption rendering all data on the storage device useless, and speed up access to stored data overall.

We will create 3 disks, one for each of the different OU groups. To do this, To add storage devices, login to the primary storage server and go to server manager. Then Under VIRTUAL DISKS, select the TASKS list, and then select New Virtual Disk. The New Virtual Disk Wizard will open, and we will be able to create them. At the Before You Begin page of the New Virtual Hard Disk Wizard, click Next. On the Choose Disk Format page, make sure that VHDX is selected by default and click Next. On the Choose Disk Type page, make sure that Dynamically expanding is selected by default and click Next. On the Specify Name and Location page, type AdminDisk1.vhdx in the Name text box and click Next. On the Configure Disk page, type 150 in the Size text box and click Next. Click Finish to create the new virtual hard disk file and associate it with your new SCSI virtual hard disk. Next we will continue by adding the rest of the disks for the OU groups. At the Before You Begin page of the New Virtual Hard Disk Wizard, click Next. On the Choose Disk Format page, make sure that VHDX is selected by default and click Next. On the Choose Disk Type page, make sure that Dynamically expanding is selected by default and click Next. On the Specify Name and Location page, type FacultyDisk1.vhdx in

the Name text box and click Next. On the Configure Disk page, type 125 in the Size text box and click Next. Click Finish to create the new virtual hard disk file and associate it with your new SCSI virtual hard disk. At the Before You Begin page of the New Virtual Hard Disk Wizard, click Next. On the Choose Disk Format page, make sure that VHDX is selected by default and click Next. On the Choose Disk Type page, make sure that Dynamically expanding is selected by default and click Next. On the Specify Name and Location page, type StudentDisk1.vhdx in the Name text box and click Next. On the Configure Disk page, type 500 in the Size text box and click Next. Click Finish to create the new virtual hard disk file and associate it with your new SCSI virtual hard disk.

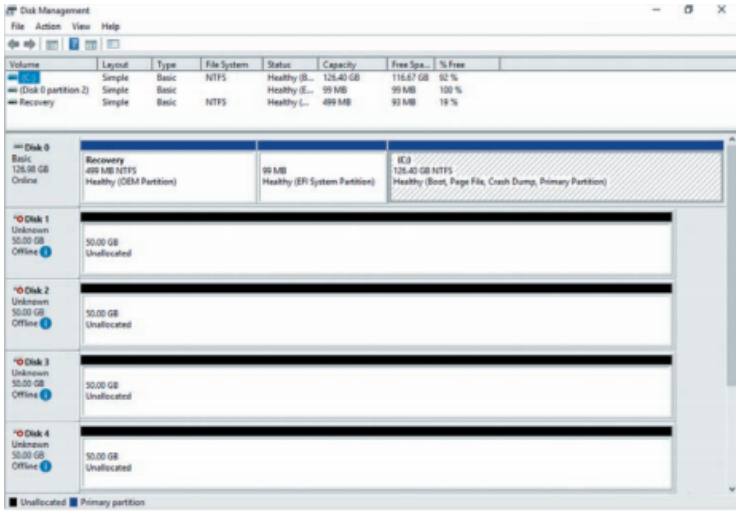

Figure 7-2 The Disk Management tool

When that is finished, it is now time to create simple volumes using the disk management tool. To do this, right click on the start menu of the server machine and select disk management. Right click all the disks that we created in the previous step, and click online. Next we will right click again and initialize the disk, if it asks to do so. We will not be partitioning the administrator disk because there is only one department for that OU group. This being staff IT and they can use all the storage on that disk for themselves if they need it. After initializing the disk, Right-click the 125.00 GB Unallocated space next to FacultyDisk1 and click New Simple Volume. At the New Simple Volume wizard, click Next. At the Specify Volume Size page, type 100,000 MB in the Simple volume size in MB text box and click Next. This will ensure that all 100 full time faculty can get 1 GB of storage. At the Format Partition page, type Faculty Volume in the Volume label text box, and click Next. Click Finish to complete your configuration. We will then do the same thing for the student OU group by Right-clicking the 500.00 GB Unallocated space next to StudentDisk1 and click New Simple Volume. At the New Simple Volume wizard, click Next. At the Specify Volume Size page, type 100,000 MB in the Simple volume size in MB text box and click Next. This will ensure that all 400 IT majors can get 250 MB of storage(400*250). At the Format Partition page, type Student Volume in the Volume label text box, and click Next. Click Finish to complete your configuration. After that, we will now do the same thing for the business majors. Right-click the now 400.00 GB Unallocated space next to StudentDisk1 and click New Simple Volume. At the New Simple Volume wizard, click Next. At the Specify Volume Size page, type 360,000 MB in the Simple volume size in MB text box and click Next. This will ensure that all 3,600 Business majors can get 100 MB of storage(3600*100). At the Format

Partition page, type Student Volume in the Volume label text box, and click Next. Click Finish to complete your configuration.

To make sure that we can backup and restore if something goes wrong, we will be adding this feature to our windows server 2019 host machine. Click on manage then add roles and features. We will continue to hit next until we are at the select features page where we will select windows server backup, then install. We will then go into our backup schedule and start the configuration wizard. It is generally ideal that backups happen once a day, and so everyday at 3AM this will happen. There should be minimal to no traffic on this day and hour, which is why we chose it. We will opt for a full server backup as well to make sure all data, applications, and systems are stable. This will be backed up to the administration hard disk, and should use about 86BG of the 150 allowed.

Configuring and Managing Network Services

This section discusses the procedures used to provide name resolution and IP configuration on the Windows network. More specifically, this covers the configuration and management of DNS, WINS

The reason we will be implementing a forward and reverse lookup zone is that Forward lookup zones resolve names to IP addresses and Reverse lookup zones resolve IP addresses to names. Forwarders can be used on our DNS server to forward requests for which our DNS server does not have an authoritative answer.

Our current server SCB-SERVER-1 will respond to DNS lookups that are received on all network interfaces by default. We then Highlight the Forwarders tab and note that our DNS server is configured as a default forwarder. To create a new forward lookup zone right click it and click new zone. At the New Zone Wizard, click next. At the Zone Type page, make sure that the default selection of Primary zone. Deselect Store the zone in Active Directory and click Next. At the Zone Name page we will be typing PrimaryFzone1.com and click Next. then create a new file with the filename PrimaryFzone1.com.dns At the Dynamic Update page, make sure the default option that does not allow dynamic updates and click Next, then finish.

The next step is to create a reverse lookup zone. We will do this by right clicking Reverse Lookup Zones in the navigation pane and click New Zone. Then at the New Zone Wizard, click Next. At the Zone Type page, make sure that an Active Directory-integrated primary zone will be created by default and click Next. At the Active Directory Zone Replication Scope page, make sure the default option that replicates the zone to domain controllers in SCB.com and click Next 2 times. At the Reverse Lookup Zone Name page, type 172.16.0 in the Network ID text box and click Next. At the Dynamic Update page, make sure the default option that allows only secure dynamic updates and click Next, then finish to create.

Next we will install WINS. We will do this to ensure that NetBIOS names can be resolved for computers on other LANs in our organization. The first thing we will do is to add roles and features on our windows host machine. Then we will click next until we get to the select features

page in which we will then select WINS server and click add features when prompted. After installation, we will open up WINS in the tool menu and expand our SCB-SERVER-1. Then we will go to our VM and go to the WINS tab in the properties of Internet Protocol Version 4 (TCP/IPv4). We will type the IP address of our host machine there and click add. This will allow us to use WINS capabilities.

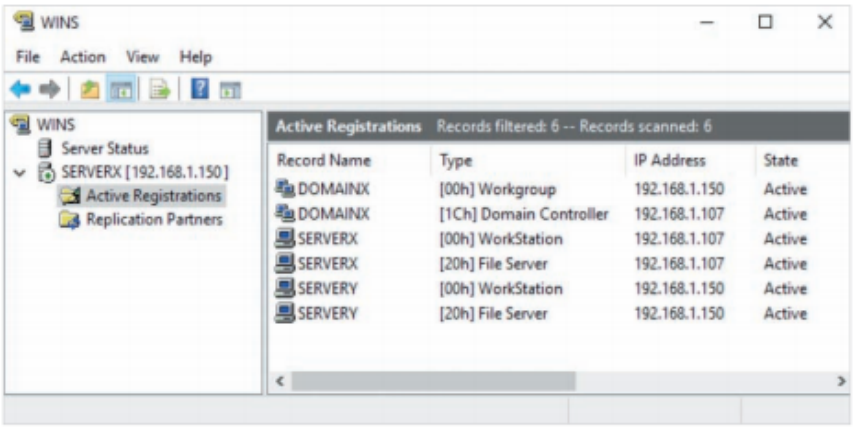

Figure 8-31 The WINS tool

Conclusion

In this report, we have outlined and justified the suggested server configurations and discussed the methodologies used in determining the configurations, the domain, and users on the network of computers used by the faculty and students of the Strome College of Business. We have provided a plan to prepare and install Windows Server 2019 on these systems with adequate hardware specifications, robust security, and optimal performance. We covered the installation and configuration of Windows Server 2019 Datacenter Edition, which included instructions for configuring the Ethernet network interface properties, as well as the server and domain name. We also used the Server Manager to scan and fix errors, configuring the Windows Admin Center, and optimizing the system. In addition, we detailed how DEP can be used to assure performance and security, and we enabled PowerShell script support which made it possible to execute the script that generates user accounts. Hyper-V and rapid server deployment were also discussed, and we provided details on the specifications, installation, configuration of virtual machines, as well as the creation of virtual machine templates and virtual switches. We also described the implementation of Windows Deployment Services and DHCP to install Windows Server 2019 on a VM over the WDS server that we configured.

In our Windows Server 2019 configuration we utilized Active Directory Services in order to generate, configure, and maintain OU objects. To generate OU objects for our wide base of users we have elected to utilize Faculty, Administrator, and Student user types with identifiers for the departments “Business” and “IT” and templates of these objects were created for future use. These objects will allow the organization to effectively manage varied access controls and allowances on the system. In order to efficiently add user objects we generated a .csv spreadsheet to store user information for bulk input. This spreadsheet contained most, if not all, of the information required to quickly get user objects inputted and enabled on the server with a unique first time password which will be changed on first login. In order to implement this, I had compiled a script to be used in Powershell which would import all information from the .csv as well as perform a check for duplicate users on the system. Once the appropriate OU objects were created I configured the namespaces for each user and user group for storage and user access privileges. To fit the parameters of the assignment I have chosen to attach storage quotas to the “Business”, “IT”, and “Faculty” objects in order to assign limited storage to these groups. File screens were attached to the “Student” and “Faculty” objects in order to screen certain file types from being stored and executed on the system. All objects with exception to “Administrators” have been blocked from OS system access and the control panel. Exceptions to these policies can be issued by ITS for academic reasons, primarily in the IT courseware, and within a strictly controlled environment. Our configuration and implementation of these principles should fulfill the needs of our organization and are able to be modified if required.

Through these parameters we were able to configure printing and data storage. We have detailed both the contents of how to meet these requirements and how the process will be done. For printing, we have decided that we will have different printers for each of the 2 members of the OS groups faculty and students. Student being subdivided by Business majors and IT majors. The printers will be located in or near the lab that each of them are allowed access to. There will be 4 printers for each student group. For the faculty, there will be a total of 7, each of which will be evenly distributed around the college of business, both upstairs and downstairs. It is to be noted that they are also allowed access to both students' printers as well in case of emergency. In

addition, Group policy will determine who has rights to do different things. The Data storage system we decided to go with is that of creating 3 disks on a primary storage server rack with the ip address of 172.16.0.51. From those disks labeled according to OU group, we will create partitions that separate the different faculty and students. The students will be partitioned into either business majors or IT majors, so they are allocated the correct amount of space. The same goes for faculty getting 1GB each. We also implemented a backup and restore feature in case something goes wrong. This will ensure that our data, applications, and system work as it should. The backup schedule is set to once a day, at 3AM to avoid traffic, however, is subject to change if another time works better. Lastly, we implemented a forward and reverse lookup zone, to be able to resolve names to IP addresses and resolve IP addresses to names. Forwarders will be used on our DNS server to forward requests for which our DNS server does not have an authoritative answer.