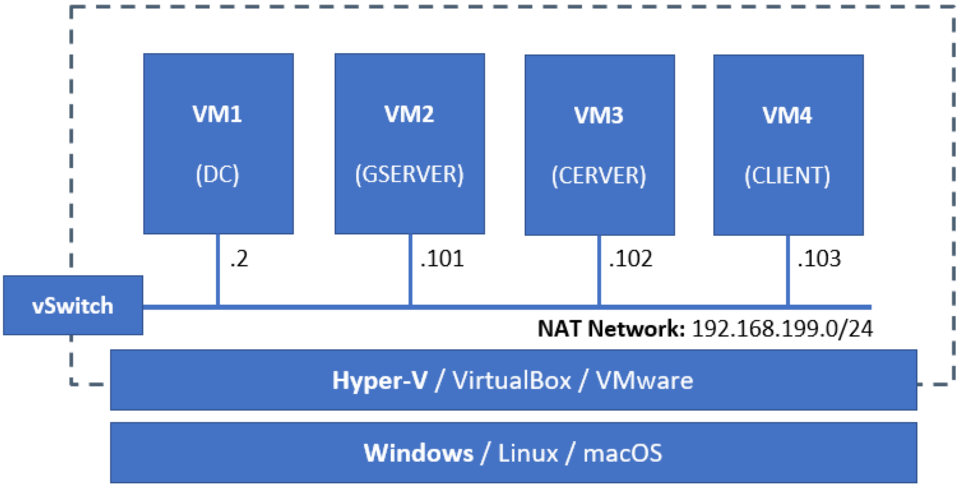
Practice M4: Additional Services

The lab environment has the following structure:



Of course, it could be limited to just the DC and one station (workstation or server). Be careful if you import virtual machines from templates (or appliances), do not forget to reinitialize their MAC addresses and if you are going to join them to the domain, run this command (if the sysprep procedure was not executed earlier) in a CMD shell as Administrator to reset all system settings before that:

sysprep.exe /oobe /generalize /shutdown /mode:vm

The AD hierarchy of objects is good to follow the structure bellow:

- Domain Controllers OU
    - DC
- Managed Computers OU
    - GSERVER
    - CSERVER
    - Sales Department OU
        - CLIENT
- Managed Groups OU
    - GS Help Desk
    - GS IT (member of Domain Admins)
    - GS Sales
- Managed Users OU
    - Ivan T. Ivanov (member of GS IT)
    - Sales Department OU
        - Gergana V. Petkova (member of GS Sales)
        - Petya K. Georgieva (member of GS Sales)
        - Stoyan I. Petkov (member of GS Sales)

For the organizational units, groups and users, you can use the preparation script provided with the practice

If due to any reason your setup is different, then you should adjust the steps and commands in the practice

Make sure that the following Windows Firewall rules ICMP, WMI, WRM, and COM+ are enabled on the machines you plan to administer remotely

The following tasks are executed on different machines. It is stated clearly on which machine a task is being executed

Part 1: File and Storage Services

One of the most common usage scenarios for a Windows server, either as a stand-alone dedicated server, or as part of a multiple role server, is the file and folder sharing functionality

Folder Sharing

Create Share (On DC)

Let's create a few shares on our DC server

Now open the **Windows Explorer** and go to **C:** drive:

- Create folder **C:\Shared**
- Create folder **C:\Shared\Common** and save a **Readme.txt** file with "Strictly forbidden to store personal stuff"
- Share **C:\Shared\Common** by choosing **Properties** and then select **Sharing** tab
- Click on the **Share** button
- Type-in **Everyone** and click **Add**
- Then click **Share**
- Finally, click **Done** and then **Close**
- Create folder **C:\Shared\Common\Management**
- Go to **Properties** and then select **Security** tab
- Click **Advanced**
- Then click **Add**
- Now click **Select a principal** link on the top part of the dialog
- Type **GS Sales**, click **Check Names**, and the click **OK**
- From **Type** drop-down choose **Deny**, you can mark individual permissions or mark **Full control**, and click **OK**
- Now click **OK**, when asked if you are sure, click **Yes,** and once again **OK**
- Create folder **C:\Shared\IT** and share it by choosing **Properties** and then select **Sharing** tab
- Click on the **Share** button
- In the drop-down list select **Find people**
- Then type **GS IT**, click **Check Names**, and then **OK**
- Set the permissions to **Read/Write**
- Then click **Share**
- Finally, click **Done** and then **Close**
- Create folder **C:\Shared\Sales**

The last share will be created from **Server Manager**, but before that we must install or extend a role if not already done (if the machine is promoted to DC, it most probably has the role), else skip this section:

- Open **Server Manager** if not already open
- In **Manage** choose **Add Roles and Features**
- Then click **Next**
- Then do not make any changes and click **Next**
- Leave the default selection (current server) and click **Next**
- In **Server Roles** expand the **File and Storage Services** section

- Then expand the **File and iSCSI Services** section
- Select **File Server** and click **Next**
- On the **Features** leave everything as is, and click **Next**
- On the summary screen click **Install**
- Once the feature is installed click **Close**

Open **Server Manager** if not already open and:

- Go to **File and Storage Services**
- Then select **Shares**
- Click on **TASKS** in the **SHARES** section and select **New Share**
- On the **Select Profile** screen leave the default selection **SMB Share - Quick** and click on **Next**
- In the **Share Location** screen select the **Type a custom path** option and click on **Browse**
- Navigate to the **C:\Shared\Sales** folder and click **Select Folder**
- Then click **Next**
- In the **Share Name** screen set **SALES** for a name and click **Next**
- On the next screen you can leave the default options and click **Next**
- Click **Customize Permissions**
- Then select **Share** tab
- Then click **Add**
- Now click **Select a principal** link on the top part of the dialog
- Type **GS Sales**, click **Check Names**, and the click **OK**
- Select **Read** and **Change** permissions and click **OK**
- Click **OK**
- Click **Next** and then **Create**
- Click **Close**

Mount Share (On CSERVER)

- Mount folder \\DC\COMMON as Z: with **net use z: \\dc\common [/persistent:yes /user:WSA\Administrator *]**
- Browse its contents by typing **z:** and pressing **Enter** key
- Then type **dir** and press **Enter**
- You can check the contents of the **Readme.txt** file with **type Readme.txt**
- Now, return to system drive with **c:** and then **Enter**
- Delete the mapping with **net use z: /delete**
- Check that there aren't any mapped drives with **net use**

Work with Share (On CLIENT)

- Log on as someone from **Sales Department**, for example **Petya Georgieva**
- Open **Windows Explorer**
- In the location bar type-in **\\DC\COMMON**
- Browse and try to write something
- By the way, did you see the **Management** folder?

Change Share Permissions (On DC)

- Open **Server Manager** if not open
- Select **File and Storage Services**, and then select **Shares**, and then **Common** share

- Click on **Properties**
- Then **Permissions**
- Now **Customize permissions**
- Click on **Share** tab and then **Add**
- Click **Select a principal**
- Enter **GS Sales** and click on the **Check Names** button
- Click **OK**
- Mark **Full Control** then click **OK**
- Click **OK** and once again, **OK**

Check Permissions (On CLIENT)

- Go to \\DC\COMMON
- Browse and try again to write something
- Still no luck

Change NTFS Permissions (On DC)

- Open **Server Manager** if not open
- Select **File and Storage Services**, and then select **Shares**, and then **Common** share
- Click on **Properties**
- Then **Permissions**
- Now **Customize permissions**
- Click on **Permissions** tab and then **Add**
- Click **Select a principal**
- Enter **GS Sales** and click on the **Check Names** button
- Click **OK**
- Check **Modify** (plus existing ones) then click **OK**
- Click **OK** and once again, **OK**

Check Permissions (On CLIENT)

- Go to \\DC\COMMON
- And hit refresh
- Try to create new text file
- Enter some content and save it

The moral is that even if **share** permissions allow for example **Full Control**, **NTFS** permissions have the last word

Register Shared Folder in AD (On DC)

Open the **Active Directory Users and Computers** tool and:

- Select the domain
- Right-click and from the context menu select **New > Shared Folder**
- In the **Name** field enter **Demo-Share**
- In the **Network path** field enter **\\DC\Common**
- Click the **OK** button to finalize the process

Use an AD Registered Share and Map It as a Drive (On GSERVER)

Open the **File Explorer** and:

- Select the **Network** node
- In the top menu select **Network** and then **Search Active Directory**
- Change the **Find** drop-down to **Shared Folders**
- Click on the **Find Now** button
- You should see a list of shares (only one item in our case)
- Select a share
- Invoke its context menu with right-click
- You can either select **Explore** or **Map Network Drive**
- Select the second option
- Adjust the settings, for example the **Drive** letter if needed
- Click on **Finish**

Additional Storage Techniques

Quotas (On DC)

It can be a good idea to set quota on the storage:

- Select drive **C:\**
- From context menu choose **Properties** and then **Quota**
- Mark **Enable quota management**
- Select **Limit disk space to** and enter **6 GB** for **limit**, and **4 GB** for **warning** level
- Mark both options for logging and click **OK**
- In the dialog window click **OK** again
- Now return to **Quota** window again and click on **Quota Entries** to check each user's entries
- You can experiment and try to copy several big files and check what will happen
- For example, you can create a big empty file with:
  fsutil file createnew test.bin 4000000000
- The above will create a file almost 4 GB in size which can be used to test the quota
- Now, we can disable the quota management, by going in the **Quota** tab of the **C:\** drive and removing the selection from **Enable quota management**
- Then click on **OK**, and once again **OK**

File Server Resource Manager (On DC)

Now we will install one additional feature, allowing us to do even better control over shared resources:

- Open **Server Manager** if not already open
- In **Manage** choose **Add Roles and Features**
- Then click **Next**
- Then do not make any changes and click **Next**
- Select the domain controller and click **Next**
- In **Server Roles** expand the **File and Storage Services** section
- Then expand the **File and iSCSI Services** section
- Select **File Server Resource Manager** and click **Next**
- If asked to confirm adding features, confirm with **Add Features** and click **Next** again
- On the **Features** leave everything as is, and click **Next**
- On the summary screen click **Install**
- Once the feature is installed click **Close**

We are ready to continue with the **FSRM**:

- From **Server Manager** > **Tools**, select **File Server Resource Manager**
- Browse **FSRM** console
- Check the quota related functionalities. It seems that now we have even more control over quotas

Instead of working with quotas, we will focus on filtering functionalities:

- Being in the **FSRM**, go to **File Screening Management** > **File Screens**
- From the context menu click **Create File Screen**
- Click **Browse**, navigate to **C:\Shared\Sales**, select it and click **OK**
- Leave other options with their default values and click **Create**

Now, let's create one storage report:

- Being in the **FSRM**, go to **File Screening Management** > **File Screens**
- From the context menu click **Create File Screen**
- Click **Browse**, navigate to **C:\Shared**, select it and click **OK**
- Select Define custom file screen properties
- Click on the **Custom Properties** button
- Switch **Screening type** to **Passive screening**
- In **File groups** select **Image Files**
- Switch to the **Event Log** tab
- Select the **Send warning to event log** option
- Switch to **Report** tab
- Mark **Generate reports**
- Select **Files by File Group** and **Files by Owner**
- Click **OK**
- Click **Create**
- Now we are asked if we want to create a template out of what we did or not
- Select **Save the custom file screen without creating a template** and click **OK**

Test Filters (On CLIENT)

Now let's see the screening filters in action:

- Log on as user from **GS Sales**
- Then go to **\\DC\SALES**
- Try to copy one **mp3** file
- Did you have success?
- Now try to copy one or more picture file(s)
- If you have troubles copying the files from the host to the VM and using Hyper-V, you can use a command like this:
  Copy-VMFile "VM-INT-WSTN" -SourcePath "C:\Temp\dog-and-cat-babies.jpg" -DestinationPath "C:\Temp\pic.jpg" -CreateFullPath -FileSource Host
- Alternatively, you can use the same command that we used to create a big file. After all, the file extension is the one thing that matters

Storage Reports (On DC)

First, open the **Event Viewer** and navigate to **Windows Logs > Application**. You should notice a warning about the illegal file that was copied

Then, navigate to the **C:\StorageReports\Incident** folder. There you should see both audit reports generated automatically when the copy of a monitored file happened

Now, let's generate an on-demand report about the situation in **C:\Shared**:

- Return in the **FSRM** console
- Select **Storage Report Management**
- From the context menu select **Schedule a New Report Task**
- Just enter a name for the report
- Deselect all selected reports but **Files by Owner** and **Files by File Group**
- Switch to the **Scope** tab
- There click **Add** and navigate to **C:\Shared**. Then click **OK**
- Now go to **Schedule** tab
- Select time and day and click **OK**
- Now select the report and from the context menu choose **Run Report Task Now**
- Select **Wait for the reports** and click **OK**
- First, open for example the **Files by Type** report and then the other one

Part 2: Remote Access and Management

Remote Administration

Don't forget to modify the firewall rules of every machine that you are about to administer remotely

MMC and Server Manager (On DC)

Let's try to control other servers from the **MMC** on the **DC**:

- Start **MMC**
- Add **Scheduled Tasks** snap-in for **GSERVER**
- Add **Computer Management** for **CSERVER**
- Browse the information
- Close **MMC**

We will register other servers in our **Server Manager** in order to be able to control them from a single tool:

- Start **Server Manager**
- In **Manage** click on **Create Serve Group**
- Then either in **Active Directory** or **DNS** tab find **GSERVER** and **CSERVER** and add them by clicking on the arrow button
- Set the group name to **THE-REST**
- Then confirm with **OK**
- You can see that after all roles, there is our new group
- We can click on it, choose a server, and examine what we can do
- Close **Server Manager**

Remote Server Administration Tools (On CLIENT)

One viable option for managing servers is to install a set of tools on a workstation and manage them from there. In fact, this is how it must be done:

- Logon either with Administrator or user with administrative privileges – for example Ivan Ivanov

- Depending on the target system and on the version of the systems that we are going to manage, we should pick up the corresponding version. Knowing our setup, let's download the package from here: https://www.microsoft.com/en-us/download/details.aspx?id=45520
- Alternative option, if our system is Windows 10 October 2018 Update or newer, to install the package is to use the Features on Demand section
- Install **RSAT** on the **CLIENT**
- Start **Server Manager** and connect to **DC**
- Browse the information and then close the application

PowerShell (On DC)

- Start **PowerShell** console
- Test remote management connectivity to **CSERVER** with **Test-WsMan CSERVER**
- Test remote management connectivity to **CLIENT** with **Test-WsMan CLIENT**

WinRM Preparation (On CLIENT)

- Start CMD Shell console
- Enable **WinRM** by executing **winrm quickconfig**

WinRM (On DC)

- Test remote management connectivity to **CLIENT** with **Test-WsMan CLIENT**

One option to work remotely in PowerShell environment is to establish a session and execute commands as if you are working locally on the remote machine and when ready, just close the session:

- Start PS session to **CLIENT** with **Enter-PSSession CLIENT -Credential WSA\Administrator**
- Execute **Get-Service bits** to get the status of the BITS
- Close the session with **Exit-PSSession**

Alternative approach is to execute single command or batch of commands on a remote computer:

- Now execute **Invoke-Command -ComputerName CLIENT,CSERVER -ScriptBlock { Get-Service bits }**

Remote Assistance

Remote Assistance Invite (On CLIENT)

Users can request remote assistance from the authorized personnel with the help of **Remote Assistance**.

Before using this functionality on a client computer, you should check if it is enabled first. This can be done either:

- On the start menu start typing **remote as**, click on the **Allow Remote Assistance invitations to be sent**, and then be sure that there is a check mark set, if not mark it and hit **OK**
- Alternative way is to initiate **System Properties** windows, go to the **Remote** tab, then ensure that **Allow Remote Assistance connections to this computer** is selected, and then click **OK**

And the corresponding firewall rule (**Remote Assistance**) for your current profile should also be enabled. If a PC is joined to a domain, it is usually enabled.

It can be started either way:

- Press **Windows Key + R**, in the dialog box enter **msra**, and click **OK**
- Or in the start menu start typing **remote assistance** or **invite** and click on the **Invite someone to connect to your PC**

Once the tool is started the request can be made:

- Click on the **Invite someone you trust to help you** option
- Then you can select **Save this invitation as a file**
- Select where to save it and click **Save**
- Leave the **Windows Remote Assistance** window open until the session is made and the task fulfilled
- Now transfer the file to the other computer (use one of the shared folders created earlier)

Remote Assistance Invite (On Server i.e. GSERVER)

Typically, on servers **Remote Desktop Connection** is used, but this does not mean that you cannot use **Remote Assistance**. In order to do so, you must first install the feature. This can be done by:

- Start **Server Manager** if not already started
- Click **Manage** and then **Add Roles and Features**
- Then click **Next**
- Then do not make any changes and click **Next**
- Leave the default selection (current server) and click **Next**
- Do not make any changes to selected roles and click **Next**
- On the **Features** screen find the **Remote Assistance** feature, select it, and click **Next**
- On the summary screen click **Install**
- Once the feature is installed click **Close**

It can be started either way:

- Press **Windows Key + R**, in the dialog box enter **msra**, and click **OK**
- Or in the start menu start typing **remote as** and click on the **Invite someone to connect to your PC**

Once the tool is started the request can be made:

- Click on the **Invite someone you trust to help you** option
- Then you can select **Save this invitation as a file**
- Select where to save it and click **Save**
- Leave the **Windows Remote Assistance** window open until the session is made and the task fulfilled
- Now transfer the file to the other computer

Remote Assistance Response (On DC)

In order to connect to the remote PC, you must open the invitation (file) received earlier:

- Then enter the password that the opposite side will dictate to you and click **OK**
- Now the opposite side, should allow the actual connection by answering with **Yes** on the screen that will appear
- Watch (or pretend to watch) what the end user is trying to do
- Disconnect from the station

Remote Desktop

Remote Desktop (On GSERVER)

The easiest way is to do it graphically through the **Server Manager**:

- Start **Server Manager** if not already started
- Select **Local Server** from the left section
- Click on the **Disabled** link next to **Remote Desktop** label

- Select the option **Allow remote connections to this computer**
- If you want to allow connections from older clients, remove the tick bellow (**Allow connection only from …**)
- By default, only members of **Administrators** group have the right to connect through remote desktop. If you want to add other users, you must add them by clicking on the **Select Users** button

There is, as always, an alternative way by using PowerShell. Open a PowerShell window as Administrator and execute the following commands:

- To allow the connections:
  ```
  Set-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\' -Name "fDenyTSConnections" -Value 0
  ```
- To restrict older clients from connecting (you can skip this step):
  ```
  Set-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\' -Name "UserAuthentication" -Value 1
  ```
- To enable the firewall rules to allow incoming RDP connections (when using the Server Manager, this is done automatically):
  ```
  Enable-NetFirewallRule -DisplayGroup "Remote Desktop"
  ```

Remote Desktop (On CSERVER)

On Server Core, again we have two options – by using the **sconfig.cmd**:

- Open CMD shell and execute
  ```
  sconfig
  ```
- Select option 7 and follow the instructions to enable Remote Desktop

Or by using the PowerShell (the procedure is the same as described above).

Remote Desktop (On DC)

If we have other machines added to Server Manager, then we can initiate remote desktop connection:

- Open **Server Manager** if not open
- Select **CSERVER** and from the context menu, choose **Remote Desktop**
- Browse and then disconnect

Alternative option is to open the Start menu and either search from **Remote Desktop** or select **Remote Desktop Connection** from **Windows Accessories** sub-menu.

Windows Admin Center

There is one new addition to the management stack – **Windows Admin Center**. It supports multiple configurations for installation. More info here: https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/understand/windows-admin-center

Direct download link: http://aka.ms/WACDownload

We will go with the simplest one – we will install it on a server machine with GUI – **GSERVER**:

- Download the installation on the domain controller and move it to a shared folder
- Log on as **Administrator** or someone from the **GS IT** group
- Open the shared folder and copy the installation package
- Double click on the package
- Click **Run**
- Select **I accept** and click **Next**

- Leave the default value and click **Next**
- Again, leave the default value and click **Next**
- On the last screen, modify the settings or use the default values, and click **Install**
- Click **Yes**
- Write down or memorize the address and click **Finish**

Log on to the domain controller and test the **Windows Admin Center**:

- Ensure that you have a supported browser. Currently only **Edge** and **Chrome** are supported
- Open browser and navigate to the address from the previous task. It should be something like: https://GSERVER.WSA.LAB:443 or https://gserver for short
- Accept the security warning
- Skip the tour
- Click on the **GSERVER** item
- Browse the available options

Part 3: Print and Document Services

Install the Role (DC)

Now we will install the Print and Document Services role:

- Open **Server Manager** if not already open
- In **Manage** choose **Add Roles and Features**
- Then click **Next**
- Make sure that **Role-based or feature based installation** option is selected and click **Next**
- Select the domain controller and click **Next**
- In **Server Roles** select the **Print and Document Services** option
- If asked to confirm adding features, confirm with **Add Features** and click **Next** again
- On the **Features** leave everything as is, and click **Next**
- Then on the role screen click **Next**
- On the **Role Services** screen accept the default and click **Next**
- On the summary screen click **Install**
- Once the feature is installed click **Close**

Now, we have the role installed

Create a Printer Object (DC)

We are ready to continue and configure our first printer

Create a Port

First, we must create a port:

- From **Server Manager** > **Tools**, select **Print Management**
- Explore different nodes of the tree
- Once done, select the **Ports** node
- Right-click and from the context menu select **Add Port** option
- Then select **Standard TCP/IP Port** and click **New Port**
- On the first screen of the wizard click **Next**
- Let's imagine that we have a network printer with an IP address of **192.168.199.201**

- Type its address in the **Printer Name or IP Address** field and click **Next**
- The wizard will initiate a search for the printer. As we do not have one, after a while the process will stop
- A dialog to set up the network connectivity will appear
- Select **Hewlett Packard Jet Direct** from the **Standard** drop-down list and click **Next**
- Finish the procedure by clicking **Finish**
- Finally, click **Close**

Add a Driver

Now, we must download the driver first from here:

https://support.hp.com/us-en/drivers/selfservice/hp-universal-print-driver-series-for-windows/503548/model/3271558

Download for example the **HP Universal Print Driver for Windows PCL6 (64-bit)** option

Next, we must extract the driver's files by double clicking on the downloaded file and selecting where the files to be stored

When the wizard is started, close it

Then, we must add a printer driver:

- Being in the **Print Management** tool, select the **Drivers** node
- Right-click and from the context menu select the **Add Driver** option
- On the first screen of the wizard click **Next**
- Make sure that **x64** is selected and click **Next**
- Click the **Have Disk** button
- Click the **Browse** button and navigate to the folder where the extracted files are and confirm with **Open**
- Then click **OK**
- Select the **HP Universal Printing PCL 6** option and click **Next**
- Close the wizard by clicking on the **Finish** button

Add a Printer

We are ready to add the printer:

- Being in the **Print Management** tool, select the **Printers** node
- Right-click and from the context menu select the **Add Printer** option
- Select the **Add a new printer using an existing port**
- Select the port created earlier from the drop-down list and click **Next**
- Select the **Use an existing printer driver on the computer**
- Select the **HP Universal Printing PCL 6** option from the drop-down list and click **Next**
- Enter **Printer Name**, for example **HP-LJ**
- Copy the same to the **Share Name** field
- Fill in the rest of the fields and click **Next**
- Check the information on the summary screen and click **Next**
- After a while, the installation process will finish. Click **Finish**

Printer Configuration

Now, that we have the printer installed, we can a few post-installation tasks:

- Being in the **Print Management** tool, select the **Printers** node
- Select the newly added printer and double click on it

- Explore the tabs
- Return on the **Sharing** tab
- Select the **List in the directory** option
- Close the settings with the **OK** button

Printer Object in AD

Let's check if the printer is present in the Active Directory:

- Open the **Active Directory Users and Computers** tool
- Select the domain
- Right-click and from the context menu select **Find**
- Select **Printers** in the **Find** drop-down list
- Click on the **Find Now** button
- You should see the printer we added earlier

Add a Printer (GSERVER)

We are ready to add our new printer on this machine:

- Navigate to **Control Panel**
- Click on the **View devices and printers** link
- Click on the **Add a printer** button
- You should see the printer we created earlier
- Select it and click **Next**
- After the printer is successfully added, click the **Finish** button

If the printer does not appear, then:

- Click on the link **The printer that I want isn't listed**
- Select the **Find my printer in the directory** option
- Click **Next**
- In the dialog box select the printer and doble-click on it
- Then click **Next**
- Finish the process by clicking on the **Finish** button