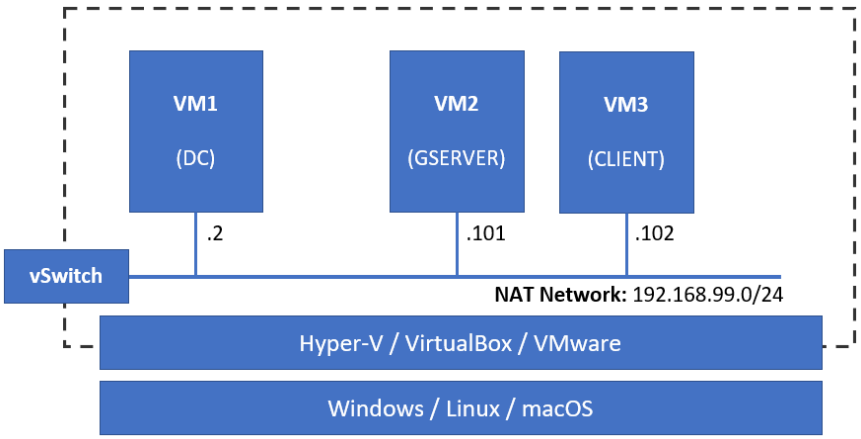
Practice M5: Additional Techniques in AD

The lab environment includes three machines, and the proposed network setup is the following:



- **DC.WSA.LAB** - Windows Server 2016/2019 Standard (with DE) with DNS and AD DS roles installed and with one network adapter connected to a common network
- **GSERVER.WSA.LAB** - Windows Server 2016/2019 Standard (with DE) with no additional roles installed and with one network adapter connected to a common network
- **CLIENT.WSA.LAB** - Windows 10 Enterprise - one network adapter connected to a common network

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

Part 1: Active Directory

Two tools one purpose

The logon name of every user should match the following pattern ***first_name.last_name***

Log on to the **DC** machine and execute the following set of tasks:

- Open **Server Manager** if not already open
- Open **Active Directory Users and Computers** (**ADUC**) tool
- Click on the domain and from the context menu choose **New > Organizational Unit**
- For name enter **Managed Computers** OU and click OK
- Repeat the procedure and create **Managed Users** OU
- Repeat the procedure and create **Managed Groups** OU
- Select the **Managed Groups** OU and from the context menu choose **New > Group**
- Create global security group **GS IT** in **Managed Groups** and make it member of **Domain Admins**
- Select the **Managed Users** OU and from the context menu choose **New > User**
- Create new user **Ivan T. Ivanov** with password **Password1**
- Now, select the user you just created, invoke its context menu, and select the option **Add to a group** to make it member of **GS IT**
- Now close this tool, and open **Active Directory Administrative Center** (**ADAC**) tool and continue there
- Note what two functions are available on the home screen – password reset and search
- Click on the domain
- Select the **Managed Groups** OU, open its context menu, and select **New > Group** to create a new global security group **GS IT HelpDesk**

SoftUni
© SoftUni – about.softuni.bg. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.
Follow us:

- Create new user **Stoyan I. Petkov** with password **Password1** and **Department** set to **DEPT_SALES** in **Managed Users** OU

Use PowerShell as well

- While still in the **ADAC** tool, let's check the PowerShell code by open **Windows PowerShell History** and examine what is there
- Copy the part related to group creation, paste it in a text editor, modify it to create a new **GS Sales** group in **Managed Groups** OU, and execute it in a PowerShell session
- Return to **ADAC** and check the PowerShell code again
- Copy the part (you can copy the whole set of related commands, or just the one for the user creation) related to user creation, paste it in a text editor, modify it to create new user **Rositsa T. Georgieva**, and execute it
- Return to **ADAC** and navigate to **Managed Users** OU to check if our new users are there
- Select the **Managed Users** OU and from the context menu choose **New > User**
- Create user template **_Template_Sales** with filled web page and address information (come up with a fictitious address) and a department set to **DEPT_SALES**
- Now switch to **ADUC** and use the template created earlier as a source. If the template user is not seen, then refresh
- Create **two more** users (**Gergana V. Petkova** and **Petya K. Georgieva**) out of the template user by selecting the **Copy** command
- Switch back do **ADAC** tool
- Create **Sales Department** OU both in **Managed Computers** OU and **Managed Users** OU

PowerShell in action

- Execute PowerShell commands to get and then move all **DEPT_SALES** user accounts to **Sales Department** OU
    - **Get-ADUser -Filter {Department -Like "DEPT_SALES"}**
    - **Get-ADUser -Filter {Department -Like "DEPT_SALES"} | Move-ADObject -TargetPath "ou=Sales Department,ou=Managed Users,dc=WSA,dc=LAB"**
- With PowerShell we can very easily check the indirect members of a group:
    - **Get-ADUser -Filter 'memberOf -RecursiveMatch "cn=Domain Admins,cn=Users,dc=WSA,dc=LAB"' | ft Name**
    - Of course, we can do it with a shorter command: **Get-ADGroupMember "Domain Admins" -Recursive**

Password Policies

- Return to **ADAC** tool
- Create **Password Policy** for all users in **System > Password Settings Container** and name it **PP-ALL**. It must be with minimum length of 10 and renewal every 30 days. Don't forget to set a precedence (lower number overwrites the higher), for example 10. Apply it to everyone (**Domain Users**)
- Try to set a simple password for one of the sales users
- Create **Password Policy** for **GS IT** group and name it **PP-GS-IT**. It must be with length of 15 and renewal every 15 days. Apply it to **GS IT** group
- Open PowerShell and list all password policies with: **Get-ADFineGrainedPasswordPolicy -Filter ***
- We can check to whom a password policy is linked with: **Get-ADFineGrainedPasswordPolicySubject -Identity "PP-ALL"**

SoftUni
© SoftUni – about.softuni.bg. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.
Follow us:

Recycle Bin

- Return to **ADAC** tool, select the domain, and in the right section (Tasks Section) click **Enable Recycle Bin**
- Now let's experiment. Delete **Sales Department** OU
- Go to the **Recycle Bin**, check if there is something there, and restore the **Sales Department** OU

Default Containers

- Redirect default **Users** container to **Managed Users** OU
    - Open CMD session with Run as Administrator and execute:
      redirusr "ou=Managed Users,dc=WSA,dc=LAB"
- Redirect default **Computers** container to **Managed Computers** OU
    - Open CMD session with Run as Administrator and execute:
      redircmp "ou=Managed Computers,dc=WSA,dc=LAB"
- The above two can be executed in a PowerShell session as well
- Now select the domain in either of both tools for AD objects manipulation (**ADAC** or **ADUC**) and create a user or computer. Check where it went
- Now open a PowerShell terminal and create a new user or computer. Check where it went
- In PowerShell we can easily check how the default containers are set:
  Get-ADDomain | Select UsersContainer, ComputersContainer | FL

Other actions or techniques

- Move **GSERVER** to **Managed Computers**
- Move **CLIENT** to **Managed Computers\Sales Department**
- Maybe you have noticed that some of the special containers are not available in **ADUC**. There is a way to show them. Select the domain and from the context menu choose **View > Advanced Features**

Export / import AD objects

- We can use the **ADUC** tool to export the content of a container. Select **Managed Users** OU and from the context menu choose **Export List** then select a file type and name and click **Save**
- To change what the export contains, first we must choose **View > Add/Remove Columns** from the context menu of the container and prepare the set we need
- Open a CMD shell and type:
  ldifde -d "cn=users,dc=wsa,dc=lab" -f c:\Temp\ad-export.ldif
  This will export the content of the **Users** container in a file named **ad-export.ldif**
- Open a CMD shell and type:
  csvde -d "cn=users,dc=wsa,dc=lab" -f c:\Temp\ad-export.csv
  This will export the content of the **Users** container in a file named **ad-export.csv**
- Open a PowerShell terminal and type:
  Get-ADUser -Filter * -SearchBase "CN=Users,DC=WSA,DC=LAB" | Select-Object Name | Export-CSV -Path c:\Temp\ad-all-users.scv
  This will export the content of the **Users** container in a file named **ad-all-users.csv**
- Now, let's import two new users. You should be **extremely careful** when importing objects in AD
- Use the simple **import.csv** file, provided with the practice files, and execute:
  csvde -i -v -f import.csv
- Now, we can see the newly imported users with:
  Get-ADUser -Filter * -SearchBase "OU=Managed Users,DC=WSA,DC=LAB" | Where -Property Enabled -Eq $false

SoftUni
© SoftUni – about.softuni.bg. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.
Follow us:

- Using an extended version of the above command, we can set a password for the users and enable them: **Get-ADUser -Filter * -SearchBase "OU=Managed Users,DC=WSA,DC=LAB" | Where -Property Enabled -Eq $false | Set-ADAccountPassword -NewPassword (ConvertTo-SecureString -AsPlainText "SomePassword-12345" -Force) -PassThru | Enable-ADAccount**

Alternative way to explore AD

- Active Directory PowerShell walk:
  - **Import-Module ActiveDirectory**
  - **CD AD:**
  - **DIR | Format-Table -Auto**
  - **CD "dc=WSA,dc=LAB"**
  - **DIR**
  - **CD "ou=Managed Users"**
  - **DIR**
  - **C:**
- Other providers can be seen with the **Get-PSProvider** command

Part 2: Group Policy Objects

GPO Techniques

Log on to the **DC** machine and execute the following:

- Start **Server Manager** if not already started
- Go to **Tools** and click on **Group Policy Management** tool to start it
- Even though we can change the **Default Domain Policy** it is not a good idea. Let's create a new one – **Global Policy**
- First, we will take care for turning off the Windows updates
  - **Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update** and set **Configure Automatic Updates** set to **Disabled**
- Enable firewall rules
  - We will set the profile of the network connections **Computer Configuration\Policies\Administrative Templates\Network\Network Connections\Windows Defender Firewall\Domain Profile** and set **Windows Defender Firewall: Protect all network connections** to **Enabled**
  - We will allow remote administration connections **Computer Configuration\Policies\Administrative Templates\Network\Network Connections\Windows Defender Firewall\Domain Profile** and set **Windows Defender Firewall: Allow inbound remote administration exceptions** to **Enabled**
  - Then we will enable few rules for remote management **Computer Configuration\Policies\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Inbound Rules** enable predefined rules **Windows Management Instrumentation** and **Windows Remote Management**
- Then we can change a few other things like
  - Add a group to the local Administrators group **Computer Configuration\Policies\Windows Settings\Security Settings\Restricted Groups** add a row for **Administrators** group. Then add **GS IT** and **Domain Admins** groups to it
  - Deny the right to log on locally for all members of the **GS IT Helpdesk** group

SoftUni
© SoftUni – about.softuni.bg. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.
Follow us:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment and add **GS IT Helpdesk** group to the **Deny log on locally**

- Link the newly created GPO to the domain
- Now you can check the **Link Order**. Our new GPO will be applied second. It is okay for the lab, but we could have situations in which we would like to rearrange the GPOs order of application
- If we want to avoid GPO application over specific organizational units, then we can set the **Block inheritance** on **Sales Department**. Now we can check the resulting policies (**Group Policy Inheritance**)
- There will be situations where we must set a GPO to be applied always. This can be achieved with **Enforce**. Let's enforce our GPO. And check again what happens with **Sales Department** the **Group Policy Inheritance** tab
- Remove **Inheritance Block** and **Enforce Rules**
- Other notable GPO settings are (feel free to skip them for now):
    - Enable/disable Task Manager
      User Configuration\Policies\Administrative Templates\System\Ctrl+Alt+Del Options\Remove Task Manager
    - Enable/disable PING (for IPv4)
      Computer Configuration\Policies\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Inbound Rules\File and printer Sharing (Echo Request - ICMPv4-In)
    - Restrict access to control panel. Normally this should be applied on user or group level, but for the sake of the experiment, we will change this setting in this GPO:
      User Configuration\Policies\Administrative Templates\Control Panel and set **Prohibit access to Control Panel and PC settings** to **Enabled**
    - Show/hide Control Panel items
      User Configuration\Policies\Administrative Templates\Control Panel\Hide specified Control Panel items
      User Configuration\Policies\Administrative Templates\Control Panel\Show only specified Control Panel items
    - Enable/disable USB storage devices
      Computer Configuration\Policies\Administrative Templates\System\Removable Storage Access
    - Special folders redirection
      User Configuration\Policies\Windows Settings\Folder Redirection

WMI Filtering

- Now, let's open again a PowerShell window and explore **WMI** with the following commands:
    - To examine the information about the system: **gwmi win32_computersystem**
    - To get some information about the firmware: **Get-WMIObject win32_bios**
    - To get information about the operating system: **gwmi win32_operatingsystem**

  *NOTE: **gwmi** is an alias to **Get-WMIObject**, so basically all three commands are using the same command with a different argument*

- Now let's expand the results returned by any of the above commands. For example:

Get-WMIObject win32_operatingsystem | Select -Property *

We can do the same for the other two. This way we will know what kind of information we can use to create WMI filters

- Let's return to the **Group Policy Management** tool and create two **WMI** filters. This can be done in the section **WMI Filters**

© SoftUni – about.softuni.bg. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.
Follow us:

- Filter for desktop machines
    - Right-click on **WMI Filters** and select **New**
    - Enter **Desktop Only** in the **Name** section and click the **Add** button
    - Make sure that the **Namespace** is set to **root\CIMv2**
    - Enter **select * from Win32_Operatingsystem where not caption like '%Server%'** in the **Query** field
    - Click **OK**
    - Click **Save**
- Filter for desktop machines
    - Right-click on **WMI Filters** and select **New**
    - Enter **Server Only** in the **Name** section and click the **Add** button
    - Make sure that the **Namespace** is set to **root\CIMv2**
    - Enter **select * from Win32_Operatingsystem where caption like '%Server%'** in the **Query** field
    - Click **OK**
    - Click **Save**
- If we are unsure, or we want to experiment with **WMI**, one valid option is to use the **wbemtest** tool. We can launch it by hitting **Win Key + R** , then enter **wbemtest**, and then hit **Enter**
- Alternative approach is to use PowerShell. For example, to test one of the above filters, we can execute the following:

  $WQL = "select * from Win32_Operatingsystem where caption like '%Server%'"

  $WMI = Get-WmiObject -Namespace Root\cimv2 -Query $WQL

  $WMI

  NOTE: Please note, that we are testing the filter against the system we are working on. So, if we want to know what it returns for example on Windows 10 machine, we must repeat the test there as well

GPO Software Distribution

- Now what if we want to distribute software with GPO? Let's do it
- First, we should download the package. Let's assume that we want to install **Paint.NET** application, so we must download it from here: https://github.com/paintdotnet/release/releases/download/v4.3.11/paint.net.4.3.11.winmsi.x64.zip
- Extract the archive you downloaded
- Create a network share. This one, we can do on the domain controller:
    - Create a folder **C:\Shared**
    - Open its context menu and choose **Properties**
    - Then switch to **Sharing** tab
    - Then click on the **Share** button
    - Select **Everyone** from the drop-down list and hit the **Add** button
    - You can change the permission level to **Read/Write** or leave it as **Read**
    - Click **Share** button and then **Done** button
    - As a result, if our domain controller is named **DC** and the folder is named **Shared**, our shared folder will be accessible to everyone on the network via the following URI **\\DC\Shared**
- Move the extracted **Paint.NET** installation files (just the 64-bit MSI file) to the share
- Create **Paint.NET Installation** GPO that assigns the package on computer
- Make it applicable only to **Desktop Computers** by using the WMI filter created earlier
- Finally, link it to the **Managed Computers** OU

© SoftUni – about.softuni.bg. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.

GPO Scripts Execution

Let's test the scripting delivery and execution capabilities with a simple example:

- Get the simple **welcome.ps1** file, provided with the practice files
- Store it on a share
- Create **Welcome Script** GPO that will execute a script when user signs in
- Navigate to **User Configuration > Policies > Windows Settings > Scripts (Logon/Logoff)** node
- Double-click on the **Logon** item
- Switch to the **PowerShell Scripts** tab
- Click the **Add** button
- Explore the default path (it points to a special share)
- Let's change the path to the place where we copied the script
- Confirm the file selection
- Click OK to confirm the changes and close the dialog box
- Close the GPO editor
- Finally, link it to the **Managed Users** OU

Apply WMI Filtering in GPO

- Create new GPO called **Manage User Experience (Server)**
- Enter in edit mode and navigate to **Computer\Policies\Administrative Templates\System\Server Manager\Do not display Server Manager automatically at logon**
- Set it to **Enabled** and close the editor
- Set the **WMI** filtering of the above GPO to **Server Only**
- Link it to the **Managed Computers** OU

Force and examine GPOs

On the command line, we can check and force GPOs:

- Log on to **GSERVER** or **CLIENT**
- Open a CMD shell
- To check what is currently applied, we can execute:
    - To display the resulting policy: **gpresult /R**
    - To produce a HTML report: **gpresult /H C:\gpo.html**
- We can force the GPO update (new/changed + old settings) with:
    - Only for the user part: **gpupdate /Force /Target:User**
    - Update and restart the system: **gpupdate /Force /Boot**

We can do the same with PowerShell (you can skip this step)

- Open a PowerShell session and:
    - To schedule a GPO refresh on the current PC:
      Invoke-GPUpdate
    - Or schedule only User update on a remote PC:
      Invoke-GPUpdate -Computer "WSA\CLIENT" -Target "User"

Of course, we can use a graphical approach to ask for the resulting GPOs:

- Return to the **DC** and open **Group Policy Management** console
- Navigate to **Group Policy Results** node
- Right-click and select **Group Policy Results Wizard** to create a **Group Policy Results** report

SoftUni

© SoftUni – about.softuni.bg. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.

Follow us:

- Click **Next**
- Select **Another computer** and either enter its name, for example **CLIENT** or click on **Browse** to find it, then click **Next**
- Select a user for which to display the resulting policy (it must have logged before) or select the option at the bottom – to not display user policy settings. Select the Administrator user and click **Next**
- Click **Next** to generate the report
- Click **Finish**
- Explore the resulting policy. Try to generate the same for the other machine as well

Extend GPO with Administrative Templates and Central Store

- We can download the latest **Administrative Templates** (.ADMX files) for different Windows versions from here: **https://support.microsoft.com/en-us/help/3087759/how-to-create-and-manage-the-central-store-for-group-policy-administra**
- Then install the package and follow the instructions:
    - Usually we must copy a folder (from the installation path) to the **Central Store** on the DC. Typically, this is something like **C:\Windows\SYSVOL\sysvol\WSA.LAB\Policies**
    - So, at the end we must have a folder named **PolicyDefinitions** which will contain our newly downloaded templates. Don't forget to copy the corresponding language files (for example en-us) together with the ADMX files
- You can check the GPO reference spreadsheet: **https://www.microsoft.com/en-us/download/details.aspx?id=57464**
- For example, if we want to control **MS Office**, we can extend our **Administrative Templates** from here: **https://www.microsoft.com/en-us/download/details.aspx?id=49030**

Part 3: Group Policy Preferences

Starter GPOs

- Mark the node **Starter GPOs** and click on the **Create Starter GPOs Folder** button to create the corresponding folder
- We can now examine the two starter GPOs that were created
- Why not create our own? Let's experiment a little bit
- Right click the **Starter GPOs** node and select **New**
- Enter **My Starter GPO** in the **Name** field and click **OK**
- Now, open it for editing
- Go and change a setting. For example, set the **Computer\Administrative Templates\Start Menu and Taskbar\Disable context menus in the Start Menu** to **Enabled** and close the editor
- Now, let's create a GPO based on our starter GPO. Right-click on **Group Policy Objects** and select **New**
- Enter a name, for example **Starter GPO Child**
- Select **My Starter GPO** from the **Source Starter GPO** drop-down list and click **OK**
- Now, if we enter in edit mode, we must see the setting that we set in the starter GPO is here with the same value. We can make some other changes or close the editor immediately

Export / import GPOs

We can back up a GPO by using the Export command

- Select a GPO, for example **Paint.NET Installation**

SoftUni
© SoftUni – about.softuni.bg. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.
Follow us:

- Right-click and select **Back Up**
- Type a location or click the **Browse** button to navigate to one
- Click the **Back Up** button to initiate the process
- Once, the process is done, click the **OK** button

We can back up all GPOs at the same time. This can be done by right-click on the **Group Policy Objects** folder and selecting the **Back Up All** item

We can restore a GPO from a backup of the same GPO made earlier. The option is called **Restore from Backup** and is found in the context menu of a GPO

On the other hand, we can overwrite a GPO if we want or need to, with the settings of a different GPO backup by following a similar procedure. The difference is the option, here it is **Import Settings**

Let's do a restore for our previously backed up GPO

- Select the **Paint.NET Installation** FPO
- Right-click and select **Restore from Backup**
- Click **Next**
- Select the folder where you saved the backup and click **Next**
- Select the GPO from the backup and click **Next**
- Click **Finish**
- Once the process is complete, click **OK**

We can also use the copy and paste actions to create alike copies of existing GPOs

There are also a set of PowerShell commands. For example, **Backup-GPO, Restore-GPO,** etc.

Migration Table Editor

When we move GPOs from one domain to another, there are adjustments that must be made. For example, user names, group names, path, etc.

- While still in the **Group Policy Management** tool, right-click either on the **Domains** folder or on the **Group Policy Objects** folder
- Select **Open Migration Table Editor**
- Click on the **Tools** menu and select **Populate from GPO**
- Select the **Global Policy** GPO and click **OK**
- You can see the items that we can make a mapping for
- Copy items from the **Source Name** column to **Destination Name** column and change the domain to **SULAB.LOCAL**
- Once done, click **File > Save** and save the migration table somewhere
- Close the editor

This table can be used when importing GPOs

Preferences

While still on the **DC**

- Create new share **\\DC\Common** by following the procedure we did earlier or reuse the existing one
- It must be accessible again by **Everyone** and the permissions can be either **Read** or **Read/Write**
- Create there a **Readme.txt** file there. It can be either empty or with some text for example, **Hello World!**

Now, open the **Group Policy Management** tool if not open already

© SoftUni – about.softuni.bg. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.
Follow us:

- Create GPP named **Managed User Preferences**
    - In **User Configuration\Preferences\Windows Settings\Drive Maps** add drive **Z:** mapped to the above share
    - In **User Configuration\Preferences\Windows Settings\Environment** add a system variable **APP_TEMP** with value **C:\TEMP**
    - In **User Configuration\Preferences\Windows Settings\Files** add step to copy file **Readme.txt** from **\\DC\Common\Readme.txt** to the **Desktop** of the logged user, which should be **%UserProfile%\Desktop\Readme.txt**
    - In **User Configuration\Preferences\Windows Settings\Folders** add step to create **C:\Temp**
    - In **User Configuration\Preferences\Windows Settings\Shortcuts** add step to create web page shortcut on the desktop
    - In **User Configuration\Preferences\Control Panel Settings\Regional Options** add a setting for regional options and select **Bulgarian (Bulgaria)**
- Link it to **Managed Users** OU
- Log on to one of the other machines (with someone from the **Managed Users** OU) and check if the GPO is applied

Now let's test if those changes are reversible

- Return to the **Group Policy Management** on the **DC**
- Remove the link of the **Managed User Preferences** GPO from the **Managed Users** OU
- Return on the station where you tried the changes
- Open a CMD shell and invoke a GPO update
- Check if the artefacts are gone
- Try to restart the machine, again the same, all changes made by the preference are still there

SoftUni
© SoftUni – about.softuni.bg. Copyrighted document. Unauthorized copy, reproduction or use is not permitted.
Follow us: