**Assignment: Server monitoring, auditing, remote access, and IIS.**

**Required Resources**

* Windows 10 workstation (As created in Assignment 1)
* Domain Controller and Member Server (As created in Assignment 1)
* Windows 10 KMS Key
* Course Resources documentation as found on BrightSpace

**Professional Documentation**

All documentation must be done in a **professional style**. It must include:

* Title page
* **Updateable** Table of Contents
* Document introduction
* Section introductions or description, each section must be clearly identified
* Graphics or screenshots MUST include a title with a short description
* Any direct or copied quotes or graphics MUST be properly credited in a footnote
* ALL sources MUST be properly cited (APA format) and placed at the end of your document in a bibliography.
* **NO** embedded, zipped or compressed files. \*\* All scripts must be converted to text before including them in your documentation. \*\*
* **1 Professional Word Document ONLY.**

**Research and documentation sections** -Please complete all research and question responses in your own words. Research sections not completed in your own words may result in a mark of 0 for the section.

**NOTE:** Please do NOT copy and paste responses from internet, **even with a citation**. I expect each section or response to be in your own words. Be prepared to explain your responses and demonstrate your comprehension.

**No marks** will be given for cited or credited information included in document.

***\*\* I recommend completing any research section before completing any required task listed below as you will have a much better understanding of the material and data.***

**Evaluation:** This assignment is markedas per the attached Rubric (marks will be deducted for deviating from Requirements). \*\*You may be asked to demonstrate some of your assignment to show your comprehension of the material.

**Marking and Assignment Notes:**

* ScreenshotsMUST include user or device identifying information.
* Screenshots MUST be added to your document in the order of creation.
* Documentation must meet Professionalism requirements.
* **Automatic mark of 0 - Assignment not submitted or work not original.**

<http://www.nscc.ca/docs/about-nscc/policies-procedures/policy-studentcodeofconduct.pdf>

<https://www.nscc.ca/docs/about-nscc/policies-procedures/policy-academicintegrity.pdf>

**NOTE: This assignment may require some adaption, research and troubleshooting.**

We have now created a small domain with a DC and a Member Server. Let’s build in a test some management and security options for our network.

**Task1 – Preparing your domain management environment.**

Using your Server Manager and RSAT tools (we will confirm they are installed if required) on your Member Server complete the following.

* Log into your member server with your **system operator** account.
* Do **NOT** add any new ROLES to your Member Server, we will add ONLY Features at this time.
* Ensure you have the following RSAT tools and features:
  + Group Policy Management
  + AD DS and AD LDS Tools (All)
  + Remote Desktop Service Tools
  + Windows Server Update Services Tools (All)
  + DHCP Server Tools
  + DNS Server Tools

\*\* Do **NOT** promote your member server to a Domain Controller.

* Let’s confirm al our required tools where installed by running the following command in an elevated PowerShell console:
* Get-WindowsFeature | where {($\_.Name -like “RSAT\*”)} | Select-Object -Property Name, InstallState | Sort-Object -Property InstallState > C:\Reports\RSATReport.txt
* **Stop**. Add a copy of the RSATReport.txt to your documentation.

Now that we have confirmed our RSAT tools are available, we will use them to create a new Group Policy to help us better manage and secure our domain.

* If required login to your Member Server as your System Operator
* In your Group Policy Management Tool

*HINT. If you do not have your Group Policy Management Tool available, you may have forgotten to add this “Feature” to your Member Server.*

* Under your Domain, remove the “**Linked”** Default Domain Policy shortcut (Do NOT remove the actual Default Domain Policy)
* **Copy** the Default Domain Policy \*\***Preserve the existing permissions**
* Rename your **new** Group Policy Object “YourInitials NETW Domain Policy” (*ex. MAD NETW Domain Policy*)
* **Link** your new policy to your Domain in place of the Default Domain Policy you removed in an earlier step.
* **Stop.** We want to make sure we have a copy of our policy for reference and troubleshooting. Selected your new Linked policy and save a report to C:\Reports\GPReports\”NameOfPolicy.vMM.DD.YY”.**html**.

*Example C:\Reports\GPReports\MAD Default Domain Policy v.09.27.19*

* We are done with our Group Policy for now, we will make some more modifications later.

**Task 2 - System monitoring**

**Part 1**

* Log onto your Member Server as your Systems Operator
* In your Server Manager Tools open your Event viewer and “create a custom view” with these options:
  + Filter:
    - Logged: Any time
    - Do NOT filter by an Event Level so all events are logged.
    - By log - Event Log:
      * GroupPolicy (including Operational)
      * DNS Client Events (including Operational)
      * RemoteDesktop Services-RdpCoreTS (including Admin and Operational)and RemoteDesktop Services-SessionServices (including Operational)
    - Keep your remaining default settings
    - Save your filter in your Custom Views as:
      * Name = CustomLog2024
      * Description = Created by and your name (ex. Created by Marie Dutka)
* Select your CustomLog2024 from your Custom Views list and sort by Source.
* **Stop.** Be prepared to **demonstrate** your new Custom Log with the correct sort option selected.

*Additional Learning: Windows Event Forwarding (WEF) reads any operational or administrative event log on a device in your organization and forwards the events you choose to a Windows Event Collector (WEC) server. In order to accomplish this, you must subscribe to events from one or more servers or devices.*

*Additional Reading:*

[*https://learn.microsoft.com/en-us/windows/win32/wes/subscribing-to-events*](https://learn.microsoft.com/en-us/windows/win32/wes/subscribing-to-events)

[*https://learn.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection*](https://learn.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection)

* Now let’s create a new Subscription
* In your Event Viewer, create a new Subscription
  + You must be running the Windows Event Collector Services, if you are not already doing so, select “yes” when asked to start the service.
* Create your Subscription with these settings:
  + Name = Errors and Warnings
  + Description = Created by and your name
  + Collector Initiated = Select your Member Server and Domain Controller – and test each computers connection. Repair connection if required. If your test passes say “Ok” and add it to your list.
  + Edit your Events to collect and filter by:
    - Logged: Any time
    - Event Level = Critical, error and warning
    - By Event Log = Windows Logs (all)
    - Keep your remaining default settings
  + Under advanced set your user account to specify the domain administrator
    - Keep your remaining default settings
* Confirm your Subscription is working by selecting Subscription in your Event Viewer and select Runtime Status from your Actions windows.
  + Repair any issues with your subscription until your status is “Active”
* Let’s test our subscription to confirm it is capturing our errors and warnings.
* Log into your Domain Controller server as the domain administrator
* Run the following PowerShell command to create a log entry

*Eventcreate /T Error /ID 88 /L Application /D “Error test event 1.2024”*

* Run the following PowerShell command to confirm the event was recorded

*Get-EventLog Application | Where InstanceID -eq 88*

* **Attention**: you may run the Event Create more than once but please change the test event version each run. Ex. “Error test event 2.2024”

Now that we have successfully created an error in our Application log lets confirm our subscription has captured and forwarded it.

* In your Event Viewer (on your Member Server) under Windows Logs, select Forwarded Events. It may take some time (5+ minutes) for the event to transfer over so you may have to refresh your Forwarded Events.
* **NOTE:** *In some cases it took several minutes to forward the event, feel free to move forward with the assignment but do not forget to return to this portion to confirm your event was forwarded and either troubleshoot the issue or capture your successful results.*
* **Stop.** Be prepared to **demonstrate** your new you successfully captured events report with the correct options selected.

**Part 2**

We will now use some additional monitoring tools to create a server baseline.

* On your Member Server create a new User Defined Collector Set in your Performance Monitor with these settings:
  + Name = YourIntitals.NETW2500 (*ex. Mad.NETW2500*)
  + Created from template
  + Template Data Collector Set = System Performance
  + Accept the default Root directory and User.
  + Accept all other default options.
* Run your new Collector Set at least once for a minimum 1 minute.
* View the results in your Reports.

Now that we have confirmed our Collector Set is working correctly, we will set up a schedule to run our Collector Set on a regular basis to start building our baseline.

* Right Clink on your Collector Set and select properties.
* Create a Schedule with these setting:
  + Starts (Day you created your schedule)
  + Expiration Dec 31, 2025
  + Launch Start Time (first NETW2500 class of the week), make sure to give your self-time to get your system and VM up and running so have it start 15 minutes into the class.
    - Example 10:45 am Every Tuesday
* Now let’s configure how long our collector set should run by setting the Stop Condition.
  + Overall Duration = 2 minutes
  + Limits = Restart the data collector set at limits, Duration = 1 minutes, maximum size 2 mb.
  + Stop when all the data collectors have finished.
* **Stop.** Be prepared to **demonstrate** your new Collector Set report with the correct options selected.

*Additional Reading:*

[*https://learn.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/configure-performance-monitoring*](https://learn.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/configure-performance-monitoring)[*https://www.howtogeek.com/devops/how-to-set-up-monitoring-to-alert-on-windows-high-system-usage/*](https://www.howtogeek.com/devops/how-to-set-up-monitoring-to-alert-on-windows-high-system-usage/)

**Part 3**

Now that we have setup log and system monitoring, we will setup a new directory and configure monitoring and auditing for the directory.

* Create the folder C:\scripts
* Edit YourInitials NETW Domain Policy (created in Task 2)
  + Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit Object Access - audit success and failure
* In an elevated Command Prompt run the command to force your Group Policy to run on your Domain Controller (remember, you may need to create a session)
* Open the properties of c:\scripts
* Under Security/Advanced/Auditing add:
  + Principal: Authenticated User
  + Type: All
  + Applies to: This folder, subfolders and files
  + Basic Permissions: Full Control
* Confirm your Audit setup is correct but opening your new C:\scripts directory (if already open close and open again)
* In Event Viewer, check your Security Log confirm you have a successful audit recorded for **c:\scripts**.
* Notice the Audit Policy uses and Event ID 4907, filter your Security Log to see how many Audit Policy events you have captured since you installed your Member Server.
* Copy your Audit Event for **c:\scripts** to text and paste in Notepad++and save it as c:\Reports\scripts\_audit.txt.
* **Stop.** We want to make sure we have a copy of our script\_audit.txt for reference of we will save a copy of our script (in text format) to our documentation.
* **Stop**. Be prepared to **Demonstrate** your scripts\_audit.txt report.
* **Stop.** We want to make sure we have a copy of our policy for reference and troubleshooting. Selected your new Linked policy and save a report to C:\Reports\”NameOfPolicy.vMM.DD.YY”.**html**.

Now that we have set up monitoring and auditing let’s look at remote access.

**Task 3 – VPN and Remote Management**

*Most servers are not managed locally and may even sit in an entirely different physical location, or there may be times the System Administrator does not have immediate physical access to the servers. The best solution to allow for management is to setup Secure Remote Access to the servers.*

* Since we will be making significant modifications to our Member Server take a new Snapshot in the off position.
* **STOP**. While your server is shutdown, add a second NIC (NAT) to your Member Server.
* If required, log into your Member Server as your System Operator
* Setup the IP information for you second NIC, we will use a Class A Private IP with a /24 Netmask
  + Make your new NIC IP match your existing IP convention

example xxx.xxx.xxx.13= Class A private

* + Set Gateway set to domain gateway (ex.192.168.208.2).
  + Set DNS to domain DNS.

**Attention**: You should receive a warning that your Gateway is in a different network and a warning regarding default gateways but that is exactly what we are requesting so say yes to both warnings.

Before we are able to use Remote Access we must add the Remote Access Role

* If required, log onto your Member Server as the System Operator.
* Add the Remote Access role to your Member Server.
  + Accept all defaults until you get to the Role Services
  + Add the first two Role **Services** offered, do not add Web Application Proxy service
  + Install your new role
  + Complete your install through the Configure Remote Access “Getting Started Wizard”.
    - Deploy VPN Only, this will open our Routing and Remote Access console.

Now we will need to configure the Routing and Remote Access

* Right Click on Member Server and “Configure and enable Routing and Remote Access”
* Select Remote Access (dial-up or VPN)
* Select VPN
* Select the IP address for **NIC 1** (Class C address)
* **\*\* Uncheck “Enable security on the selected interface……”**
* Since we do not have a DHCP server for this network select “From a specified range of address”
* We will use **Class A Private** IP addresses, starting IP Address with .2 as your final octet example xxx.xxx.xxx.2
* Number of address = 20
* In Managing Multiple Remote Access to Authenticate connection requests select **NO**. We currently do not have a RADIUS server.
* **NOTE**: When the message pops up stating that a computer can’t be added to the list of valid remote access servers in Active Directory click OK and then OK again for supporting relaying of DHCP messages.

*Learning Reminder: Review the KB Article you created in NETW1500 and refresh your memory on DHCP, how it works and DHCP Relay.*

Now we will need to create a secure user for remote access as we want to make sure only designated users have remote access and we can monitor the user as required.

* Open your Computer Management console and create a new **local** user:
  + Named = RUser
  + Full name = Remote User
  + Description = Special account
  + Password = Remote@2024
  + **Password never expires**
  + Modify user to set Dial-in options:
    - Network Access Permissions = Allow Access

Now let’s test our VPN

* Log into your **workstation** as the **LOCAL** default user
* Change your workstation IP for NIC 1 to match the settings used on your Member Server Class A addressing scheme. (Make sure you are in the designated range)
* In your Network and Sharing - Setup a new connection or network
* Set up a dial-up or VPN connection to your workplace
* Connect using your Internet connection (VPN)
* Setup your Internet Connection later
* Put in the Class A IP Address for your Member Server NIC 2
* Accept the default to remember your credentials (for testing)
* Create your new connection
* You will now need to open your new VPN connection and login with your Remote User account created earlier

**NOTE:** Remember to add your servername\before your username as this is a local user account.

\*\* See **Appendix A** for troubleshooting support.

Now we have setup a VPN connection between our workstation and server but we still can’t manage our server, we will need to setup remote management.

* On your Member Server in your Server Manager enable **Remote desktop** with these settings:
  + Allow remote connections to this computer
  + Allow connections only from computers running Remote Desktop with Network Level Authentication
  + Select users = Remote user, Systems Operators Groups and Domain Administrator (Notice the Local Admins are allowed by default)

Now we will test our connection to our server.

* From your workstation connect your VPN
* Open your Remote Desktop Connection (MSTSC)
* Computer = Member Server NIC2 IP
* User = remote user created earlier
* **Stop**. Be prepared to **demonstrate** your VPN and Remote Desktop Connection from your workstation.

We have successfully setup auditing and monitoring on our server and domain, we have setup an option for remote management.

**Task 4 – IIS Service**

**Part 1 – Understanding IIS Service**

*IIS Manager is a utility that integrates IIS, ASP.NET, FTP, and SharePoint services.*

Before proceeding with configuring our IIS services lets learn a little more about the IIS structure. Answer the following questions in paragraph form and place in your professional documentation.

Question 1. What is a Web Farm? Name three advantages of a Web Farm.

Question 2. What is a Web Garden? Name three advantages of a Web Garden.

Question 3. What is an Application Pool?

Question 4. What is a Worker Process?

Question 5. In your document, complete the following.

Copy or create the Summary Table below and complete the required information for each IIS Authentication Type listed.

**Summary Table:**

|  |  |
| --- | --- |
| **Authentication Name** | **Description of Authentication type** |
| Active Directory Client Certification Authentication |  |
| Anonymous Authentication |  |
| ASP.NET Impersonation |  |
| Basic Authentication |  |
| Digest Authentication |  |
| Forms Authentication |  |
| Windows Authentication |  |

**Part 2 – Creating our first website**

Now that we have created a small domain environment let’s add some features to our Member Server by creating our first web site using IIS.

* If required log into your Member Server as your System Operator
* Add/Modify the **web Server role** including FTP (accept all other default options) to your Member Server
* Copy the Assign2Sample.html script from your BrightSpace scripts folder to your Member Server C:\inetpub\wwwroot
* Modify the supplied HTML code to create a webpage.
* Your new webpage should be done in a professional style and include:
  + Modify the background colour to your favorite colour (if white is your favorite colour, select your second favorite).
  + Modify heading to “Welcome to Company Inc.”
  + Replace my company image with an image of your choice.

\*\*Please ensure you do NOT use a copy righted image. I recommend you take or create one yourself.

* + Add Subtitle under your image with our course name and number
  + Modify the webmaster email to link to your NSCC email
  + Modify the Web Master name to your name.
  + Modify “Modified:” date
  + **Save page as index.html**

So we have a webpage but we still don’t have a website to host our page. We will need to create an application pool and our first site.

* If required log onto your Member Server as your System Operator
* Open your Internet Information Services (IIS) Management console on your Member Server
* Create an application pool “**NETWPool**”
  + Accept all defaults
* Modify the settings for your Default Web Site as follows:
  + Application Pool = NETWPool
  + First default document is index.html
* Test your new Web Site page by selecting **Browse \*:80 (http)** from within your IIS Manager.
* If successful test your web page by opening an Internet Explorer or Chrome browser on your host machine and connect to your Member Server using the Class C IP.
* **Stop.** Be prepared to **demonstrate** your comprehension of IIS management and new web page with the correct options selected.

**Task 5 – Backups and Documentation**

It is important to keep an up to date record of all changes and modifications made to your servers and have a reliable copy available as backup.

* Take a snapshot of ALL your server and workstations in the **OFF** state.
* Create a Gold Copy of **each** server. \*\* Remember, we do not need a gold copy of our workstation.
* **Stop**. Take a screenshot of your Gold Copy properties for each server and add it to your documentation.
* **Stop**. Since we have made changes to our DC and Member Server, we will need to create a change management log.
* **Upload your change management log to BrightSpace**.
* **Upload your Group Policy report as a separate HTML document to BrightSpace**. **NOTE**: You ONLY require the final version of your policy, the first one was for reference and tracking only.
* **Upload your professional documentation to BrightSpace.**

Marking Rubrics:

|  |  |
| --- | --- |
| **Value** | **Task** |
|  | **In class marking** |
| 2 | YourInitials NETW Domain Policy correctly linked. |
| 5 | Open CustomLog2024 in Event Viewer to show correct settings.   * + Filter by:     - Logged: Any time     - Do NOT filter by an Event Level so all events are logged.     - By log - Event Log:       * GroupPolicy (including Operational)       * DNS Client Events (including Operational)       * RemoteDesktop Services-RdpCoreTS (including Admin and Operational)and RemoteDesktop Services-SessionServices (including Operational)     - Keep your remaining default settings     - Save your filter in your Custom Views as:       * Name = CustomLog2024       * Description = Created by and your name (ex. Created by Marie Dutka)   + Sort by Source. |
| 6 | View Errors and Warnings subscription for correct settings and configurations.   * + Name = Errors and Warnings   + Description = Created by and your name   + Collector Initiated computer = find your Domain Controller server – and test your computer connection. Repair connection if required. If your test passes say “Ok” to select your File Server.   + Edit your Events to collect and filter by:     - Logged: Any time     - Event Level = Critical, error and warning     - By Event Log = Windows Logs (all)     - Keep your remaining default settings   + Under advanced set your user account to specify the domain administrator     - Keep your remaining default settings |
| 1 | Subscription Status = Active |
| 10 | Show at least one successful capture of Event Error 88 in Captured Events. |
| 6 | Open Yourinitials.NETW2500 Collector Set and demonstrate you successfully captured the correct events in your Report.   * Collector Set Report has evidence of correct runs. * Performance Resource Overview results **details** and Schedule. * CPU * Network * Disk and Memory   + Starts (Day your created your schedule)   + Expiration Dec 31, 2025   + Launch Start Time (first NETW2500 class of the week), make sure to give your self-time to get your system and VM up and running so have it start 15 minutes into the class.     - Example 10:45 am Every Tuesday * Now let’s configure how long our collector set should run by setting the Stop Condition.   + Overall Duration = 2 minutes   + Limits = Restart the data collector set at limits, Duration = 1 minutes, maximum size 2 mb.   + Stop when all the data collectors have finished. |
| 1 | Demonstrate **c:\Reports\scripts\_audit.txt** was created with content. |
| 10 | Demonstrate a successful VPN access from workstation to member server. |
| 2 | Demonstrate a success Remote Desktop connection from workstation to member server with Remote User. |
| 5 | Open Web Page in local browser with all the correct setting |
| 2 | Open Web page in host machine browser. |
| 3 | Snapshot created for each VM. (DC, MS, Client) |
| **53** | **SUB TOTAL** |
|  | **Documentation Submitted to Brightspace** |
| 4 | Captured correct events in: **c:\Reports\scripts\_audit.txt** |
| 4 | “Gold” copy properties for each server. |
| 4 | GPReports\”NameOfPolicy.vMM.DD.YY”.html with correct configurations |
| 2 | Question 1 |
| 2 | Question 2 |
| 2 | Question 3 |
| 2 | Question 4 |
| 5 | Question 5 (Summary Table) |
| 5 | Change Management log contains all required changes, configurations and notes but is NOT a copy paste from assignment. |
| 2 | Document meets professionalism requirements as per page 1 of assignment. |
| **32** | **SUB TOTAL** |
| **85** | **Total Marks possible** |
|  |  |

**Appendix A**

VPN connection failed with error:



Troubleshooting steps:

1. Make sure you restarted your Member Server after making the IP change to allow all your tables to update.
2. Make sure you restarted your client after the IP change to all your tables to update.
3. Confirm you added the Member Server hostname before the username for your login credentials.
4. Disable Routing and Remote Access and reconfigure. Rebuild the connection following the settings required closely.