**Assignment:** Monitoring, auditing and system management.

**Required Resources**

* BrightSpace Course Resource Documents:
* Windows Server 2019 **Standard** from Assignment 1
* Windows 10 Education **22H2** Client from Assignment 1

**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.**

Now that we have set up a Domain Development environment, we will use our Windows Domain Server (DC) and our Windows 10 Client to learn more about some of the security and management requirements for a Windows Domain.

**Task 1**

**Part 1a - Performance Monitoring and Security**

<https://cyberpedia.reasonlabs.com/EN/system%20performance%20monitoring.html>

You can use the following site for additional information. <https://techcommunity.microsoft.com/t5/ask-the-performance-team/windows-performance-monitor-overview/ba-p/375481>

Requirements: Create a performance baseline of your Domain Controller and then adjust specified system parameters and observe the performance changes.

* Open your Performance Monitor from your Dashboard Tools
* Check the status of our computer by running a System Diagnostics test
  + Expand Data Collector Sets > System > Right-click System Diagnostics > Start.
  + When complete (green arrow disappears from System Diagnostics icon), **go to** Reports\System\System Diagnostics and select your computer for the list.
  + Confirm your workstation has passed all **Basic Systems Checks**, if you have failed any Basic System Check do not proceed, you must correct the failure first.
  + Take time to expand all the other results such as Performance, software configuration, Hardware configuration, CPU, etc. and review each section for what type of information is captured.

Requirement: Create a new Data Collector Set to monitor our system performance.

* Data Collector Sets 🡪 User Defined 🡪 Right Click 🡪 New 🡪 Data Collector Set
  + Set a name to Your “FirstMiddleLastInitials Collector Set” and ‘**Create Manually**’ Example: mad Collector Set
  + Select ‘Create data logs’ / Performance counter **and** Event trace data
  + Add the following Local Computer Performance Counters
    - Memory: Available KBytes,
    - Memory: Page Faults/sec.
    - Network Interface: Packets Received Errors (**All instances**)
    - Paging File: % Usage (**total**)
    - Paging File: % Usage Peak (**total**)
    - Physical Disk: % Disk Read Time (total)
  + Get a sample every 20 seconds
  + Save to **default** location
  + Accept default settings for everything else
* Start your new Data Collector Set and run for at least 2 minute then stop the set from running.
* Open your collector sets reports Reports/User Defined / “Initials” Collector Sets/ and review your results. To add clarity try viewing your report in Histogram Bar view. Now switch back to Line View.
* Select the icon in the top right of your graph to “View Current Activity”. Notice how the information is updated live. This is a great way to view the current state of your device and track any large or unexpected changes in your system.
* **Stop**. Be prepared to show and or demo your report(s) created above, be prepared to explain the information captured on the report(s).

**Part 1b – Security and Maintenance Center**

* Open the Security and Maintenance Center (use your search function if required)
* Expand the Maintenance option;

**Note** – if there are current system issues, you will see a message indicating this under Maintenance. **Talk to your instructor before proceeding if you have unresolved system issues.**

* Select “View reliability history” and review any recorded problems, issues or events. HINT: You may need to select a particular day.
* **Stop. Record** the details for one of the problems, issues or events noted and add your finding to your documentation. Your research MUST include:
  + Source:
  + Summary:
  + Date:
  + Action (View Technical Description):
* Return to the main “Security and Maintenance” window and select “Change maintenance settings”
* **Stop.** Review the description of “Automatic Maintenance” and **Record** the current Automatic Maintenance settings and add it to your documentation in the form of a screenshot.
* Set your maintenance task to run daily at 3:00 am but do not allow your schedule to wake-up your computer.
* **Stop.** Be prepared to demo your new maintenance schedule and setting.

Now that we have looked at some maintenance settings let’s look at our security settings.

* Return to the main “Security and Maintenance” window
* Expand the Security option
* Select your User Account Control and Change Settings.
* **Question 1: Review** the 4 UAC change settings available and **record** each option with a brief description, when the setting is recommended. \*\*Make sure to leave your UAC set to the default.

**Task 2 – System Events and error logs**

**Part 2a**

Event Logs, Security Logs and Event Viewer are critical to the security and management of any system. They are often your first flag that something is wrong, can track incidences and give details otherwise not identified. Review the following resources to get more information about logs.

<https://www.techtarget.com/searchsecurity/tip/Security-log-management-and-logging-best-practices>

<https://www.canada.ca/en/government/system/digital-government/online-security-privacy/event-logging-guidance.html>

**Question 2.** Copy the following table into your documentation and complete the missing information.

|  |  |
| --- | --- |
| Event ID | What is means / What it identifies |
| *4772* | *A Kerberos authentication ticket request failed.* |
|  | A user account was created. |
|  | Audit log was cleared. This can relate to a potential attack. |
|  | System audit policy was changed. |
|  | A user was added to a privileged global group |
|  | A user account was changed |
| 4782 |  |
| 4625 |  |
| 4737 |  |
| 4648 |  |
| 4720 |  |

Let’s have a closer look at our Event Viewer and log information.

* Open the Event Viewer tool
* In the “Summary of Administrative Events” pane, expand Error.
* In the **Action** pane on the right, under Error and select View All Instances of this Event.
* **Stop**. Take a screenshot that **records** the Number of events displayed and include in your documentation.
* Select any error with an ID other than Event ID 10 and review the entries in the General Pane at the bottom.
* Select the Details Tab in this pane. Toggle between Friendly and XML views
* From the Action Pane to the right, select Copy -> Copy Details as Text
* Minimize the MMC on screen. Start Notepad++ and paste the details into a new document.Save text document as **C:\Reports\Errors.txt**
* **Stop**. Add a copy of your Errors.txt converted to text to your documentation.
* Use the **Event ID** selected above in your Errors.txt and research your error to answer the following questions. *\*Remember to review the research and sources requirements from page 1 of this assignment.*
  + **Question 3:** What is the Error ID you selected and what is a symptom of this error?
  + **Question 4:** Based on your research, what is a possible cause of your error?
  + **Question 5:** Based on your research, what is a possible solution?
* Let’s look at some of the other options available by opening our Windows Logs/Security log.
  + **Question 6:** Filter your current log to search for any instance on 5 Event IDs identified in your Table in Question 2. Record the number of each one with a screenshot. \*\*Make sure to capture the total number of security events and the number of events with the filtered ID. See example below.

*Example:*

A screenshot of a computer

Description automatically generated

**Part 2b**

**Audit Policies**

* Using your Group Policy Management to set a new Windows Security policy for the Computer.
* Find the Advanced Audit Policy, configure the following security audit policies:
* Audit **failed** logon attempts
* Audit **failed** attempts to access shared files.
* Audit **successful** and **failed** changes made to security groups

Now that we have set up some audit policies, let’s test to confirm we are capturing the details. The audits we just created are written to the event logs, which we can view with *Event Viewer*.

* Log out and attempt to sign in as ABruce but use the password **FakePassword**.
* Oops, wrong password. Try again with the password **StillFakePassword**.
* Then log back in as your default user.
* Add the *Event Viewer (for the Local Computer)* snap-in to your custom MMC.
* Select your Event Viewer and navigate to:
  + *Windows Logs* -> *Security*.
  + Check your audit policies were set by:
    - Filtering current log by Event ID 4719
    - The **LAST** (by date) with Event ID 4719
  + Right click on the policy ->select Save Selected Events -> save it in your C:\Reports directory as **SuccessfulAudit.txt**
* **Stop**. Be prepared to Demo your Successful Audit report with the correct results.

We can also use the *Get-EventLog* cmdlet in PowerShell to gather this information as well. We will user parameters to specify the log’s name. We will then take the output and ***pipe it* ( | )** as input to another command which will grab only the logs with a failure entry type, we will then use a second pipe to output the results to a file. \*\* There may be some research and or troubleshooting required to get the results you need.

* *In an elevated PowerShell console, capture the results of your Event Log by using the following command:*

*Note: This is one line of code.*

***Get-EventLog -LogName Security -Message “\*Failure\*” -Newest 10 | out-file C:\Reports\FailureAudit.txt***

* **Stop**. Be prepared to Demo your Failure Audit report with the correct results.

**Task 3 – RSAT Tools Research Section**

In keeping with industry standards, we realize that most servers are managed via remote access. When working with Windows servers our best utilities for managing servers is called Windows RSAT (Remote Server Administration Tools). To help you better understand what RSAT tools are, you will have to do a little research.

You will find most the information required to complete this section either of the following Microsoft TechNet sites but use any site relevant to answer the following questions.

<http://social.technet.microsoft.com/wiki/contents/articles/2202.remote-server-administration-tools-rsat-for-windows-client-and-windows-server-dsforum2wiki.aspx>

<https://docs.microsoft.com/en-us/troubleshoot/windows-server/system-management-components/remote-server-administration-tools>

**Question 7.** Complete the following training resource on Windows Server Administration Tools.

<https://learn.microsoft.com/en-us/training/modules/describe-windows-server-administration-tools/>

* + **Stop**. Complete the knowledge Check at the end of the training and capture a screenshot of your checked answers. Add your screenshot to your documentation.
* **Question 8.** Create or copy the following summary table and complete it. For each Management or Resource Area please list the recommend RSAT tools you would recommend.

**Summary Table**

|  |  |
| --- | --- |
| **Remote Management Area** | **Required RSAT Tools** |
| DHCP Management |  |
| DNS Management |  |
| Routing and Remote Access Management |  |
| Remote Desktop Management |  |
| Group Policy Management |  |
| Domain User Management |  |
| File Services Management |  |

* **Question 9.** What are the steps to install RSAT Tools on a Windows 10 22H2 client?

**Task 4**

**Part 4a - Client RSAT tools installation**

Since we have decided we will be following the recommended industry standard and use RSAT tools when possible to manage our Windows Server remotely we will need to have a Windows 10 client in our domain. We will use the Windows 10 client we installed in our previous assignment.

* Use the steps identified in Questions7 and 8 to install the following **9 RSAT Tools:**

1. Active Directory Domain Services and Lightweight Directory Services
2. DHCP Server Tools
3. DNS Server Tools
4. File Services Tools
5. Group Policy Management Tools
6. Remote Access Management Tools
7. Remote Desktop Services Tools
8. Server Manager
9. Windows Server Update Services Tools

* Run the following command in an elevated PowerShell console to confirm your tools were successfully installed:

Get-WindowsCapability -Name RSAT\* -Online | Select-Object -Property DisplayName, State | sort-object -property state > C:\Reports\RSATReport.txt

* **Stop**. Add your RSATReport.txt that shows the successful install of the correct RSAT tools to your documentation.

**Part 4b – Working with RSAT, Remote Management and PowerShell Sessions**

Now that we have installed the tools required to support remote management of our server environment lets take some time to get familiar with the tools and options available to us for remote management.

* On your Windows 10 Client search for the Server Manager feature installed with your RSAT tools, since this is a tool we will use often, place a shortcut to the program on your **Task Bar**.
* Open your Server Manager from your Taskbar, notice that there are some differences in the dashboard then we are used to seeing in our Server Dashboard.
* Let’s add our Domain Controller server to your list of other servers to manage.
  + Make sure you move your server to the selected.
  + Notice your Server Manager is now updated with additional resource options based on the server we added.
* Using the Tools option in your menu bar of the Serve Manager have a look at some of the tools that are available on your client.
* Review the tools list available on your DC and see if there are any noticeable differences.

We have seen that by installing our RSAT tools we are able to use our client to preform most tasks required to manage our server and our domain. That will assist us when managing our servers from outside our Data Center or Server Farm but what about scripting? What if we need to create run scripts such as logon scripts or manage systems resources not available through our RSAT tools. Let’s look at our options for management in PowerShell.

* First we will need to create a PowerShell session between our client and our DC.
* Run the following commands in an elevated PowerShell console to setup a PowerShell session

New-PSSession -ComputerName “DCServerHostName” -Credential (Get-Credential)

* Supply your domain\backup administrator credential when prompted for authentication
* Now you will need to enter your PowerShell session using the following command

Enter-PSSession sessionID#Here

* Example: Enter-PSSession 1
* Notice that when you enter your PowerShell session your PowerShell now shows your sever name in the left hand of the console for confirmation you are working in the correct session.
* Use your PowerShell session to gather some information from Active Directory
* Run the follow command to get list of your Active Directory users on your server

Get-ADUser -Filter \* | Format-Table | Tee-Object -Filepath C:\Reports\ADReport.txt

**Question 10.** Notice that there are several accounts shown some are enabled and some are not. Identify each of the accounts that are not enabled, explain where the account came from and what it is used for.

* Have a look at a little more Active Directory information.
* Run the follow command to test your server

Get-ADUser -Filter \* -Properties MemberOf | Format-Table| Tee-Object -Append -Filepath C:\Reports\ADReport.txt

**Question 11.** Who is a member of the “Group Policy Creator Owners” and who is a member of the “Denied RODC Password Replication” Groups? Why are these two users members of these specialty groups?

* **Stop**. Add a copy of your ADReport.txt to your documentation. Remember to include it in text format, not screenshots allowed.

We have successfully installed RSTAT tools and tested our ability to connect to our server using a PowerShell session. The last method we will look at is setting up the ability to connect directly into our server using Remote Desktop Protocol (RDP). By default only Domain Admins have the ability to use RDP to access a server. Since our Backup Administrator is a member of our Domain Admins we do not need to worry about login security, we can simply enable the **protocol**.

* If required create a new PowerShell session and enter it. You can skip this step if you are still in your previous session.
* Run the following commands to enable RDP on our domain controller

Set-ItemProperty -Path ‘HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\‘ -Name “fDenyTSConnections” -Value 0 \*\*Note the space between Terminal and Server.

Enable-NetFirewallRule -DisplayGroup "Remote Desktop"

* Test your new connection by running the following command

Test-NetConnection YourServerIP -CommonTCPPort rdp

* Exit your PowerShell session by running the command.

Exit

* **Stop**. Be prepared to Demo a PowerShell sessions.

**Task 5 – Securing Active Directory**

In order to better manage our Domain we would like to be able to hire some casual staff. We would like our new staff to be able to *image* and add computers to our Domain but we do not want them to make any other changes in our Domain.

*Additional Learning: When managing dozens or even hundreds of computers, Imaging is an important tool for most System Management Professionals. Imaging allows for consistency in computer design and management as well as a backup for key systems.*

*Additional Reading:*

[*https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831764(v=ws.11)*](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831764(v=ws.11))

[*https://www.smartdeploy.com/blog/what-is-computer-imaging/*](https://www.smartdeploy.com/blog/what-is-computer-imaging/)

Before we make any new modification to our Active Directory we are going to take a minute to Enable our Recycle Bin.

* From your client launch your Server Manager RSAT tool.
* If required, add your Domain Controller to your severs to be All Servers list.
  + Make sure your Manageability is **Online**
* From your Tools, open your Active Directory Administrative Center.
* Select your domain (NetBIOS Name)
* From the Tasks window (on the right) Enable Recycle Bin
  + You will receive a warning letting you know we cannot disable the Recycle Bin once it is enabled, Say OK as we want it enabled.
* Let’s test our recycle bin.
  + Open your Active Directory Users and Computers
  + Create a user named **Test** in your Techs OU
  + Delete the user
  + Open your Deleted Items in your Active Directory Administrative Center
  + Restore the user.
* Close your Active Directory Administrative Center.
* **Stop**. Be prepared to Demo your Recycle Bin has been activated.

Now that we have enabled our recycle bin let’s create some new special permission users.

* From your Client, open your Active Directory Users and Computers.
* In your Techs OU
* Create a new Global Security group called **CasualTechs\_gp** with a description *Reduced Privileges Group*
* Create a new user:
  + OU = Techs
  + First Name = Bruce
  + Middle Name = Banner
  + Last Name = Brown
  + Full Name = Bruce Brown
  + User logon name = Sysop.BBB
  + Password never expires
  + Password = Passw0rd@2020
  + Groups = CasualTechs\_gp, Domain Users
  + Description = Casual Tech

Now we will give our Casual Techs group permission to add computers to our Domain

* From your Client.
* If required, open your Active Directory Users and Computers
* Right click on your Computer OU
* Select Delegate Control…
* Add your Casual Techs Group
* Choose Create a custom task to delegate
* Delegate control of: **Only the following object in the folder** 
  + Computer Objects
  + Create selected objects in this folder
  + Delete selected objects in this folder
  + **Stop**. Capture these settings in a screenshot before proceeding.
* Under Permissions/General, select the following:
  + Reset password
  + Read and write account restrictions
  + Validate write to DNS host name
  + Validate write to service principal name
  + **Stop**. Capture these settings in a series of screenshots before proceeding.

Now we will test your new Casual Techs abilities by adding our Windows 10 workstation to the domain

* Log into your workstation and
  + Remove your workstation from the domain and add it to a workgroup called test.
  + From your server, remove the computer account from AD/Computers
  + Log onto your client as your original default installer
  + **On your client, remane your computer by adding an A2 at the end of the client name**
  + Log back on to your client as your original default installer
  + Add you client back to your domain, **USE** your new **Sysop.BBB** account to add your workstation to the domain.
  + Confirm your client workstation is now a member of your domain by logging into your new client as regular Sysop User.
* **Stop**. Be prepared to demo your Sysop.BBB account by reconnecting your client back to your domain.
* **ATTENTION**: Now that we have added our Client to our Domain we will always need to ensure our Domain Controller is running before we start or stop our client or the Trust Relationship connection will be broken!
* **Create** a snapshot of the Server and workstation in the “off” state, following your naming convention for snapshots. Be prepared to demo your snapshots.
* Create “Gold” Copy of your Server and workstation since we have made changes to both.
* **Stop**. Capture a screenshot of the properties of your Server and Client Gold copies, ,make sure to include, creation date, size, location and name.

**Comprehensive and Documentation Submission Marking**

|  |  |
| --- | --- |
| **Value** | **Task** |
|  | **Comprehensive Marking** |
| 4 | Demo Performance monitor report(s) and explain the information captured on the report(s).   * Collector Set report * User defined report |
| 2 | Demo your new maintenance schedule and setting. |
| 2 | Demo your Successful Audit report with the correct results. |
| 3 | Demo your Failure Audit report with the correct results. |
| 2 | Demo a PowerShell Session. |
| 1 | Demo Recycle Bin with test user. |
| 5 | Demo domain Add with Sysop.BBB   * Sysop.BBB can add client to domain. * Client is in AD with correct modified name (A2) |
| 1 | Snapshot of Server with correct naming convention |
| 1 | Snapshot of Client with correct naming convention |
| **23** | **Total Marks for comprehensive marking** |
|  | **Submitted Documentation** |
| 4 | **Record** the details for one of the problems, issues or events noted and add your finding to your documentation. Your research MUST include:   * + Source:   + Summary:   + Date:   + Action (View Technical Description): |
| 1 | Screenshot of Automatic Maintenance setting. |
| 2 | Question 1. |
| 10 | Question 2. |
| 1 | Screenshot that records the Number of events displayed and include in your documentation. |
| 2 | Errors.txt converted to text |
| 4 | Question 3. |
| 3 | Question 4. |
| 2 | Question 5. |
| 5 | Question 6. |
| 3 | Question 7. Windows Server Administration Tools, knowledge Check at the end of the training and capture a screenshot of your checked answers. Add your screenshot to your documentation. |
| 7 | Question 8. |
| 1 | Question 9. |
| 4 | RSATReport.txt that shows the successful install of the correct RSAT tools. |
| 2 | Question 10. |
| 4 | Question 11. |
| 2 | ADReport.txt to your documentation. Remember to include it in text format, not screenshots allowed. |
| 2 | Gold copy **properties** of **server** with required details. |
| 2 | Gold copy **properties** of **client** with required details. |
| 1 | Document follows all Professional documentation requirements as per page 1 of assignment |
| **62** | **Total Marks for document submission** |
|  |  |
| **85** | **Total Assignment Marks.** |