**PAMANTASAN NG LUNGSOD NG PASIG**

**COLLEGE OF COMPUTER STUDIES**

**SY 2024-2025, 2ND SEM**

**IT113 – System Administration and Maintenance**

**Activity # 2**

**Configuring Windows Server 2019**

**NAME: RAMOS, JENNYLYN ANNE O.**

**STUDENT ID NUMBER: 21-00042**

**COURSE CODE: IT 113**

**SECTION: BSIT 4A**

**SCHEDULE: 6:00 – 8:00 PM (THURSDAY)**

**INSTRUCTOR: MR. EUGENE EMBALZADO JR.**

1. **Introduction**

In this activity, you’ll examine the different tools that can be used to monitor and manage Windows Server 2019 in more depth, including Server Manager, the Windows Admin Center, Control Panel, and Device Manager. You’ll also learn how to check for and repair system files, as well as edit the Windows Registry. At the end of the module, you’ll learn how to work within Windows PowerShell, as well as how to create and modify PowerShell scripts to automate system configuration tasks.

1. **Program Activity (By Pair)**

**For the final output of this activity, provide a 10-to-15-minute video presenting the procedures of this activity. You can put the screenshots of each procedure to discuss it comprehensively. Please upload the link for both of your submission together with your file in PDF.**

**Activity 2.1 – Server Manager**

In this activity, you explore the different configuration and management features of Server Manager.

1. Boot your Windows Server 2019 host and log into the system as Administrator using the password **Secret555**. After a few moments, Server Manager will open. If prompted to try the Windows Admin Center, select **Don’t show this message again** and close the information window.

2. Within the Server Manager Dashboard, observe the roles and server groups shown. Note that your server is represented by Local Server, a member of the All Servers group and has the File and Storage Services role installed. Also note whether there are any services that are flagged red. If this is the case, click Services under your Local Server and note the services that are not started and the reason why.

3. Highlight **Local Server** in the navigation pane of **Server Manager.**

a. Observe the default events shown in the Events pane. Next, click **Tasks, Configure Event Data** within the Events pane. At the Configure Event Data window, select **Informational** and click **OK**. Note the additional events that are now shown within the Events pane.

b. In the Performance pane, click **Tasks, Configure Performance Alerts**. Note the default alert thresholds and graph display period and click Cancel.

c. In the Roles and Features pane, click **Tasks, Add Roles and Features**.

i. At the Before you begin page, select the **Skip this page by default** checkbox, and click **Next**.

ii. At the Select installation type page, click **Next**.

iii. At the Select destination server page, click **Next**.

iv. At the Select server roles page, select **DHCP Server**, and click **Add Features** when prompted. If prompted to continue after validation errors (because your system has a DHCP-assigned IP address), click **Continue**. Click **Next** when finished.

v. At the Select features page, select **Telnet Client** and click **Next**.

vi. At the DHCP Server page, read the information regarding best practices and click **Next**.

vii. Click **Install** to install the DHCP Server role and Telnet Client feature. viii. After the installation has completed, click **Complete DHCP configuration**, click **Commit**, and then click **Close**.

ix. Click **Close** to close the Add Roles and Features Wizard.

4.Highlight **DHCP** in the navigation pane of Server Manager.

a. In the Best Practices Analyzer pane, click **Tasks, Start BPA Scan**, and then click **Start Scan**. Note the Warning and Error that you receive.

b. In the Services pane, right-click the **DHCP Server** service and click **Stop Services**.

5.Click **Dashboard** in the navigation pane of Server Manager. Note that there is one service and one BPA result red flagged for the DHCP, Local Server and All Servers groups.

a. Click **Services** under Local Server and note that the DHCP Server service is stopped. Right click the **DHCP Server** service, click **Start Services,** and then click **OK**. Click the **Refresh** button in the upper right of Server Manager and note that the service related red flag disappears.

b. Click **BPA results** under Local Server and note the Predeployment error shown. Right click the error, click **Exclude Result,** and then click **OK**. Click the **Refresh** button in the upper right of Server Manager and note that the BPA-related red flag disappears.

6.In the upper right of Server Manager, click **Manage**, **Add Servers**. Note that you can add servers within your Active Directory domain, by DNS name, or import them from a file. Because your computer is not domain-joined, you do not see entries under the Active Directory tab. Click **Cancel**.

7.In the upper right of Server Manager, click **Manage**, **Create Server Group**. In the Create Server Group window, specify a name of **Building1** in the Server group name box. Next, highlight **SERVER*X*** in the Server Pool tab, click the arrow button to move it to the Selected pane, and click **OK**. Note that your new server group appears within the navigation pane.

8.Highlight **Building1** in the navigation pane of Server Manager. Right-click **SERVER*X*** in the Servers pane and note the options available on the menu. Select the **Windows PowerShell** option to open a Windows PowerShell console as Administrator. Close the Windows PowerShell console when finished.

9.In the upper right of Server Manager, click **Tools** and note the tools that are available. Next, click **Manage, Server Manager Properties**. In the Server Manager Properties window, select **Do not start Server Manager automatically at logon** and click **OK**.

10. Close the Server Manager window.

**Activity 2.2 – Windows Admin Center**

In this activity, you install and explore the different configuration and management features of the Windows Admin Center.

**1.** On your Windows Server 2019 host, open the Google Chrome Web browser and navigate to https://aka.ms/WindowsAdminCenter. Follow the prompts to download the latest non-preview version of the Windows Admin Center. When finished, the downloaded file will automatically be opened to start the installation.

a. At the Windows Admin Center Setup screen, select **I accept the terms in the License Agreement** and click **Next**.

b. At the Use Microsoft Update page, click **Next**.

c. At the Install Windows Admin Center on Windows Server page, click **Next**.

d. At the Installing Windows Admin Center page, click **Next**. Note that the installation program will generate a self-signed encryption certificate for use on port 443 (HTTPS) and click **Install**.

e. Click **Finish**.

**2.** Navigate to https://SERVER*X*:443 within the Chrome Web browser and click **Skip tour** when prompted. Maximize your Chrome Web browser screen.

**3.** At the All connections page, click **Add, Servers**. Note that you can add servers by server name or import a list of server names. Click **Cancel**.

**4.** Highlight **server*x*** within the All connections page and click **Edit tags**. At the Edit connection tags window, type **2019HOST** and click **Save**.

**5.** Highlight **server*x*** within the All Connections page and click **Connect**. Within the Overview tool, view the information shown and then click **Manage alerts**.

a. Select **Environment variables** and note that you can create and edit system and user environment variables.

b. Select **Power configuration**, select the **High performance** power plan and click **Save**.

**6.** Highlight **Devices** within the Tools pane. Note that you can disable existing hardware devices or update their device drivers.

**7.** Highlight **Network** within the Tools pane. Select your Ethernet adapter and click **Actions, Settings**. Note that you can configure IPv4 and IPv6 settings for your Ethernet adapter.

**8.** Highlight **PowerShell** within the Tools pane to open a Windows PowerShell prompt.

Type **exit** and press **Enter** to stop your Windows PowerShell session.

**9.** Highlight **Registry** within the Tools pane. Expand **HKEY\_CLASSES\_ROOT** and highlight **.ac3**. Note that you can add, modify, and delete values.

**10.** Highlight **Roles & Features** within the Tools pane. Select **DHCP Server** and click **Remove**. Click **Yes** to remove the role.

**11.** Optionally navigate to the other tools within the Windows Admin Center and note their functionality. Close Google Chrome when finished.

**Activity 2.3 – Configuration Utilities**

In this activity, you explore various Windows configuration utilities available within Windows Server 2019.

**1.** On your Windows Server 2019 host, click **Start** and then click **Control Panel**.

**2.** Navigate to **System and Security**, **System**, **Advanced system settings**. Under the Performance section of the System Properties window, click **Settings**.

a. Next, highlight the **Advanced** tab and note the default setting for Processor

scheduling.

b. Click **Change** and note the default size of the paging file that is currently allocated on your system. Because the paging file size is managed by the system by default, this value should be close to the recommended value shown.

c. Click **OK** to close the Virtual Memory window.

d. Highlight the **Data Execution Prevention** tab and note the default settings that apply DEP to all programs and services.

e. Click **OK** to close the Performance Options window.

**3.** Under the Startup and Recovery section of the System Properties window, click **Settings**. Note the default options and location of the dump file. Click **OK** to close the Startup and Recovery window when finished.

**4.** At the bottom of the System Properties window, click **Environment Variables**.

a. In the User variables for Administrator section, click **New**.

b. At the New User Variable window, supply a Variable name of VAR1 and Variable value of Sample Variable and click **OK**.

c. In the System variables section, note the values of the Path, TEMP, TMP, and windir variables and click **OK**.

**5.** In the System Properties window, highlight the **Hardware** tab and click **Device Manager**.

a. Devices that require attention will be marked with a yellow label and shown by default. If you see any Unknown devices, right-click the device, choose **Update driver** and follow the prompts to search for a driver on the Internet or from removable media supplied by your manufacturer.

b. Expand **Disk drives**, right-click your storage device, and click **Properties**. Highlight the **Policies** tab and note that write caching is enabled on the device by default but that flushing is not. Click **OK** to close the properties window.

c. Close Device Manager and click **OK** to close the System Properties window. If you are prompted to restart your computer to apply changes, click **Restart Later**.

**6.** In the Control Panel window, click **Control Panel** in the navigation bar to switch back to the Category view. Next, click **Add a device** under the Hardware category. Your system will search for devices that may not have been detected by PnP. Follow any prompts to install devices that are found. If no devices were found, click **Cancel**. Close Control Panel when finished.

**7.** Navigate to **System and Security**, **Power Options**.

a. Select the **High performance** power plan.

b. Click **Change plan settings** and note the defaults.

c. Click **Change advanced power settings**. Navigate through the detailed power plan settings that are available for your computer, making changes that you desire as necessary. Click **OK** when finished.

d. If you made changes to your power plan, click **Save changes**, otherwise, click **Cancel**.

e. Close Control Panel.

**8.** Right-click the Start menu and click **Run**. Type regedit in the Run dialog box and click **OK**. Expand **HKEY\_CLASSES\_ROOT** and highlight **.ac3**. Note that you can add, modify, and delete values. Double-click **(Default)**, supply the value audio, and click **OK**. Close the Registry Editor when finished.

**9.** Right-click the Start menu and click **Run**. Type sigverif in the Run dialog box and click **OK**. In the File Signature Verification tool, click **Start** to scan your system for unsigned files. When the scan has completed, click **OK** and then click **Close** to close the File Signature Verification tool.

**10.** Right-click the Start menu and click **Run**. Type cmd in the Run dialog box and click **OK**. At the command prompt, type sfc /scannow and press **Enter**. Note whether any system files were replaced with correct versions and close the command prompt window when finished.

**Activity 2.4 – Cmdlets**

In this activity, you work with common Windows PowerShell administrative

cmdlets.

**1.** On your Windows Server 2019 host, open the Google Chrome Web browser. Next, right-click the **Start** menu and choose **Windows PowerShell (Admin)** to open Windows PowerShell.

**2.** At the prompt, type Get-Process | more and press **Enter**. Note that there are

many processes with a ProcessName of chrome that comprise the Google Chrome Web browser. Press q to quit the more command. Next, type Stop-Process -name chrome and press **Enter**. Note that the Google Chrome Web browser app was closed.

**3.** At the prompt, type Get-Service | ogv and press **Enter**. Note that the App

Readiness service is called AppReadiness and is not started by default. Close the

GridView window. Next, type Start-Service -name AppReadiness and press **Enter** to start the service. Next, type Stop-Service -name AppReadiness and press **Enter** to stop the App Readiness service.

**4.** At the prompt, type Get-WindowsFeature | ogv and press **Enter** to view installed roles and features. Note that the Telnet Client feature that you installed earlier in Activity 2.1 is given the name Telnet-Client. Close the Out-GridView window. Next, type Remove-WindowsFeature -name Telnet-Client and press **Enter** to remove the feature.

**5.** At the prompt, type Test-NetConnection and press **Enter** to test your network connectivity to internetbeacon.msedge.net. Next, execute the following commands at the command prompt, in turn. For each one, note the network configuration information displayed.

Get-NetIPConfiguration

Get-NetAdapter

Get-NetAdapterStatistics

**6.** Close Windows PowerShell.

**Activity 2.5 – Cmdlet Output**

In this activity, you modify the output of Windows PowerShell cmdlets.

**1.** Right-click the **Start** menu and choose **Windows PowerShell (Admin)** to open Windows PowerShell.

**2.** At the prompt, type cd \ and press **Enter** to switch to the root directory. Next, type dir and press **Enter** to list the contents of this directory.

**3.** At the prompt, type alias dir and press **Enter**. Next, type alias gci and press

**Enter**. Note that dir and gci are aliases to the Get-ChildItem cmdlet. Execute the following commands at the command prompt, in turn. For each one, interpret the output (referencing the aliases and cmdlets within this module, as necessary).

Get-ChildItem

gci | sort –property name

gci | Format-List

gci | Format-List –property name,lastwritetime

gci | Format-Wide

gci | Format-Wide –column 3

gci | Format-Wide –column 3 –property length

gci | Format-Wide –column 3 –property name –groupby length

gci | Format-Table

gci | Format-Table –property name,length,lastwritetime

gci -recurse

gci –recurse –include \*.txt

**4.** Other cmdlets that generate a large amount of information may require that you use additional Windows PowerShell features to modify command output for organization and readability. Execute the following commands at the command prompt, in turn. For each one, interpret the output (referencing the aliases and cmdlets within this module, as necessary).

Get-EventLog System | more

Get-EventLog System | Group-Object eventid | more

Get-EventLog System | Group-Object eventid | Out-GridView

(Close the GridView window when finished.)

Get-EventLog System | Group-Object eventid | ogv

(Close the GridView window when finished.)

Get-Process | ogv

(Close the GridView window when finished.)

Get-Process | ConvertTo-HTML | Out-File C:\PList.html

Invoke-Item C:\PList.html

(Choose to open in Google Chrome, and close Chrome when finished.)

Get-Process | Export-CSV C:\PList.csv

Invoke-Item C:\PList.csv

(Choose to open in WordPad and close WordPad

when finished.)

**5.** Close Windows PowerShell.

**Activity 2.6 – Powershell Providers**

In this activity, you work with PowerShell providers.

**1.** Right-click the **Start** menu and choose **Windows PowerShell (Admin)** to open Windows PowerShell.

**2.** At the prompt, type Get-PSProvider and press **Enter** to view the available PowerShell providers. Next, type Get-PSDrive and press **Enter** to view the expanded list of PowerShell providers. Note that the filesystem provider is available for each drive letter on the system, and that registry provider is available for HKEY\_CURRENT\_USER and HKEY\_LOCAL\_MACHINE.

**3.** Each PowerShell provider treats each item that it works with as an object. At the prompt, type gci | Get-Member and press **Enter** to view the properties available for the objects within the current directory of the filesystem provider. Note that there is a PSIscontainer property that indicates that the object is a subdirectory. Next, type gci | Where-Object {$\_.psiscontainer} and press **Enter** to view only directories. Following this, type gci | Where-Object {!$\_.psiscontainer} and press **Enter** to view only non-directories (i.e., files).

**4.** Within the filesystem provider, you can create, edit, and remove objects, such as files and directories. Execute the following commands at the command prompt, in turn. For each one, interpret the output (referencing the aliases and cmdlets within this module, as necessary).

new-item –path C:\ -name mydir –type directory

new-item –path C:\mydir -name lala.txt –type file

get-content c:\mydir\lala.txt

add-content c:\mydir\lala.txt –value "This is line 1"

add-content c:\mydir\lala.txt –value "This is line 2"

add-content c:\mydir\lala.txt –value "This is line 3"

get-content c:\mydir\lala.txt

set-content c:\mydir\lala.txt –value "This is the only line"

get-content c:\mydir\lala.txt

remove-item c:\mydir –recurse

**5.** At the prompt, type sl env:\ and press **Enter** to switch to the environment provider. Next, type gci and press **Enter** to view the environment variables on the system. In many PowerShell providers, you can instead use the Get-Item cmdlet (alias gi) to view items. Type gi \* and press **Enter** to view all items within the environment provider.

Next, execute the following commands at the command prompt, in turn. For each one, interpret the output (referencing the aliases and cmdlets within this module, as necessary).

gi \* | sort-object –property name

gi windir

gi windir | format-list \*

new-item –path . –name lala –value "This is cool!"

gi lala

gi lala | format-list \*

rename-item –path env:lala –newname po

gi po

gi po | format-list \*

gi \* | sort-object –property name

remove-item po

**6.** At the prompt, type sl variable:\ and press **Enter** to switch to the variable provider. Next, type gci and press **Enter** to view the user-defined PowerShell variables on the system. Next, execute the following commands at the command prompt, in turn. For each one, interpret the output (referencing the aliases and cmdlets within this module, as necessary).

gci | sort {$\_.Name}

get-variable home

get-variable home | format-list

new-variable oobla

set-variable oobla –value "Toast"

get-variable oobla

set-variable tinky –value "Winky"

get-variable tinky

remove-variable tinky

**7.** At the prompt, type sl alias:\ and press **Enter** to switch to the alias provider. Next, type gci and press **Enter** to view the user-defined PowerShell variables on the system. Following this, type gci | Where-Object {$\_.name –like "c\*"} and press **Enter** to view aliases that start with c. Note that “clear” is an alias to Clear-Host.

**8.** You can also view aliases by their definition. At the prompt, type gci | Where-Object {$\_.definition –like "c\*"} to view aliases that point to cmdlets that start with the letter c.

**9.** At the prompt, type sl function:\ and press **Enter** to switch to the function provider.Next, type gci and press **Enter** to view the functions on the system. Note that Clear-Host is a function. Next, type Get-Content Clear-Host and press **Enter** to view the content of the Clear-Host function.

**10.** At the prompt, type sl cert:\ and press **Enter** to switch to the certificate provider. Next, type gci and press **Enter**. Note that the certificate provider can manage certificates for the current user and local computer. Next, type gci -recurse and press **Enter**. Note the self-signed certificate installed on your system by the Windows Admin Center is displayed in the list.

**11.** At the prompt, type sl 'HKLM:\software\microsoft\windows nt\currentversion' and press **Enter** to switch to the registry provider for HKEY\_LOCAL\_MACHINE and navigate to the currentversion subkey for your Windows server system. Next, type set-itemproperty –path winlogon –name legalnoticecaption –value "Hey!" and press **Enter** to set a legal notice caption for local logon attempts. Finally, type set-itemproperty –path winlogon –name legalnoticetext –value "What are you doing on my system?" and press **Enter** to modify the text message for local logon attempts.

**12.** Right-click the **Start** menu and click **Shut down or sign out**, **Sign out**. Press

Ctrl1Alt1Del (or Ctrl1Alt1End if you are running Windows Server 2019 within a Hyper-V virtual machine on Windows 10). Note your legal notice and click **OK**. Log into the system as Administrator using the password **Secret555**.

**Activity 2.7 – WMI**

In this activity, you query WMI using Windows PowerShell.

**1.** Right-click the **Start** menu and choose **Windows PowerShell (Admin)** to open Windows PowerShell.

**2.** At the prompt, type alias gwmi and press **Enter**. Note that gwmi is an alias to

Get-WmiObject. Next, execute the following commands at the command prompt, in turn. For each one, interpret the output (referencing the aliases and cmdlets within this module, as necessary).

gwmi win32\_bios

gwmi win32\_processor

gwmi win32\_processor | gm

gwmi win32\_computersystem

gwmi win32\_computersystem | fl \*

gwmi win32\_logicaldisk

gwmi win32\_logicaldisk | fl \*

gwmi win32\_diskdrive

gwmi win32\_diskdrive | fl \*

gwmi win32\_share

gwmi win32\_share | fl \*

gwmi win32\_networkadapterconfiguration

gwmi win32\_networkadapterconfiguration | fl \*

gwmi win32\_desktop

gwmi win32\_desktop | fl \*

gwmi win32\_share –filter name="'c$'"

gwmi win32\_logicaldisk –filter name="'c$'" |

Measure-Object -property freespace -Minimum –Maximum

gwmi win32\_logicaldisk -filter name="'c$'" |

Measure-Object -Property freespace -Minimum -Maximum |

Select-Object -Property freespace, maximum, minimum |

Format-Table –autosize

**3.** You can also query WMI using WQL syntax. Execute the following commands at the command prompt, in turn. For each one, interpret the output (referencing the aliases and cmdlets within this module, as necessary).

gwmi –query "Select \* from win32\_share"

gwmi –query "Select \* from win32\_share" | gm

gwmi –query "Select name,path,allowmaximum from win32\_share"

gwmi –query "Select name,path,allowmaximum from win32\_share where

name='c$'"

gwmi –query "Select name from win32\_share" | Sort-Object -property

name | Format-List -property name

gwmi –query "Select name from win32\_share" | Sort-Object -property

name | Format-List -property name > C:\scripts\ShareInformation.txt

notepad C:\scripts\ShareInformation.txt

**4.** Close Notepad and Windows PowerShell.

**Activity 2.8 – Powershell Customization**

In this activity, you enable script execution and create a PowerShell profile script that loads a custom alias and function. Next, you create a PowerShell console file to customize your Windows PowerShell experience.

1. Right-click the **Start** menu and choose **Windows PowerShell (Admin)** to open Windows PowerShell.

**2.** At the prompt, type Set-ExecutionPolicy unrestricted and press **Enter**. Type Y when prompted to confirm. Next, type Test-Path $profile and press **Enter**. Note that you do not have a PowerShell profile script configured.

**3.** At the prompt, type New-Item –path $profile –itemtype file -force and press **Enter** to create a PowerShell profile. Next, type notepad $profile to open your PowerShell profile script within Notepad. Add the following lines:

Write-Host "Hello"

Set-Alias lala Get-Service

function pro {notepad $profile}

**4.** Click **File, Save** within Notepad to save your changes. Close Notepad when finished.

**5.** At the prompt, type cd Desktop and press **Enter** to switch to your Desktop directory. Next, type export-console CustomPS and press **Enter** to create a CustomPS.psc1 file on your Desktop that can be used to open Windows PowerShell. Close Windows PowerShell when finished.

**6.** Double-click the **CustomPS** file on your desktop to open Windows PowerShell. Note that your PowerShell profile script executed and printed Hello to the screen. Type lala and press **Enter** to test your alias. Next, type pro and press **Enter** to test your function. Close Notepad when finished.

**7.** Click the PowerShell icon in the upper left of the Windows PowerShell window and click **Properties**. Navigate through the properties and make some visual changes to your liking (color, font, and so on). Click **OK** to close the Properties dialog box and close Windows PowerShell when finished.

**8.** Double-click the **CustomPS** file on your desktop to open Windows PowerShell. Note that your customizations are available. Close Windows PowerShell when finished.

**9.** Right-click the Start menu and choose **Windows PowerShell (Admin)** to open WindowsPowerShell. Note that your customizations are not available as PowerShell was not started via the CustomPS.psc1 file.

**10.** Close Windows PowerShell.

**Activity 2.9 – Powershell Scripting**

In this activity, you create and execute a basic PowerShell script using Windows

PowerShell ISE, and execute it on the system.

**1.** Click **Start**. Next, right-click **Windows PowerShell ISE** and click **More, Run as administrator**.

**2.** Click the **New Script** button above the Windows PowerShell pane, and enter the following contents:

#This script prints process information to the screen for

#a process that the user is prompted to supply during

#script execution

$ans=Read-Host "What process would you like to query?"

Get-WmiObject win32\_process -Filter "name='$ans'" | Format-Table

HandleCount,VirtualSize,UserModeTime,KernelModeTime,ProcessID,Name

**3.** Click the **Run Script** button (or press **F5**) to test your script in the Windows PowerShell console. Type the value svchost.exe and press **Enter** when prompted.

**4.** After your script executes properly, click **File, Save As**. Type C:\myscript.ps1 in the File name box and click **Save**.

**5.** Close Windows PowerShell ISE.

**6.** Right-click the **Start** menu and choose **Windows PowerShell (Admin)** to open Windows PowerShell.

**7.** At the prompt, type cd \ and press **Enter** to switch to the root of C:\. Next, type ./myscript.ps1 and press **Enter** to execute your script again. Type the value svchost.exe and press **Enter** when prompted.

**8.** Close Windows PowerShell.

**III. Question and Answer**

* **Is your activity complete?**  
  **Answer:** Yes, my activity is completed.
* **Does it conform to the target output?**  
  **Answer:** Yes, I conformed to the target output because my partner and I successfully completed all activities from 2.1 to 2.9.
* **Can we say that your system is functional?**  
  **Answer:** Yes, our system is fully functional as we clearly completed all the required activities.

**IV. Conclusion**

In conclusion, Windows Server Configuration offers a wide range of functionalities that users can utilize to modify the system according to their needs. It provides various syntax and commands to help users create, edit, and remove configurations, making the system easier to manage and adapt to specific requirements. With proper use of these tools, users can significantly enhance the performance and security of their systems.