

In-Class Practical Worksheet: PowerShell Automation for Windows Server 2022

Aim of the Activity

This activity is designed to help you **understand and implement PowerShell scripts** to configure core Windows Server services. You will apply automation techniques to install, configure, and verify services used in real-world enterprise environments.

By completing this worksheet, you will be able to:

- + Install Windows Server roles using PowerShell
- + Configure DHCP services and scopes
- + Deploy and configure IIS web services
- + Enable and test Remote Desktop access
- + Troubleshoot real-world configuration issues
- + Understand how automation improves system administration

Scenario

You are part of an IT administration team responsible for configuring a Windows Server 2022 machine (**S-DC**) that is already configured as a Domain Controller for:

yourname.acca

You must use **PowerShell scripts** to complete all tasks.

- ✓ Work in groups but ensure individual understanding
- ✓ Use **PowerShell (Run as Administrator)**
- ✓ Replace all values with your own where required

Part 1: Install Required Services

Install the following services using PowerShell:

Service	Marks <i>(Approx. in CW2)</i>
Firewall	2
DHCP Server	2
IIS Server	2
Remote Desktop Services	2

Write the PowerShell commands used:

+ Prerequisite

```
Get-NetFirewallRule -DisplayName "*ICMP*" | Format-Table
  DisplayName, Enabled, Direction, Action

Get-Service DHCPServer

Get-WindowsFeature DHCP

ipconfig /all
```

+ Firewall Configuration

Sample:

```
#Modify Firewall Rules
New-NetFirewallRule `
  -DisplayName "Allow ICMPNitheesh1" `
  -Direction Inbound `
  -Protocol ICMPv4 `
  -IcmpType 8 `
  -Action Allow
```

+ DHCP Installation

```
#DHCP Server Installation
Install-WindowsFeature DHCP -IncludeManagementTools
Get-WindowsFeature DHCP
```

+ IIS Installation

ACCA5023 – Network Operating Systems and Services

```
#IIS Server
Install-WindowsFeature Web-Server, Web-Mgmt-Tools, Web-
Scripting-Tools, Web-Windows-Auth -IncludeManagementTools
New-Item -Path "C:\inetpub\webs" -ItemType Directory -Force
```

+ Remote Desktop Services Installation

```
Install-WindowsFeature Remote-Desktop-Services -
IncludeManagementTools
```

Verification Evidence

- ☐ DHCP installed
- ☐ IIS installed
- ☐ Remote Desktop Services installed

Part 2A: Configure DHCP Server

Service	Marks <i>(Approx. in CW2)</i>
DHCP Server	5
IIS Server	5-8
Remote Desktop Services	5-7

Task: Configure S-DC as a DHCP Server with:

- IP Range: 192.168.1.10 – 192.168.1.20, Default Gateway: 192.168.1.1, DNS Server: 192.168.1.1, Domain: yourname.acca

```
Add-DhcpServerInDC -DnsName "S-DC.nitheesh.acca" -IPAddress
"192.168.1.1"
Add-DhcpServerv4Scope `
    -Name "Swansea Network Scope2" `
    -StartRange 192.168.1.40 `
    -EndRange 192.168.1.50 `
    -SubnetMask 255.255.255.0 `
    -State Active
Get-DhcpServerv4Scope

Set-DhcpServerv4OptionValue `
    -ScopeID 192.168.1.10 `
    -Router 192.168.1.1 `
    -DnsServer 192.168.1.1 `
    -DnsDomain "nitheesh.acca"
Get-DhcpServerv4OptionValue -ScopeId 192.168.1.0
```

Part 2B: Configure IIS Web Server

Task: Create a website: webs.yourname.acca

Enable: Windows Authentication, Disable Anonymous Authentication

```
Set-Content -Path "C:\inetpub\webs\index.html" `
-Value "<h1>Welcome to webs.nitheesh.acca</h1><p>This website
was created using PowerShell.</p>"

Import-Module WebAdministration

New-Website `
    -Name "webs.nitheesh.acca" `
    -Port 80 `
    -HostHeader "webs.nitheesh.acca" `
    -PhysicalPath "C:\inetpub\webs"
```

```
Set-WebConfigurationProperty `
    -Filter
"/system.webServer/security/authentication/windowsAuthenticat
ion" `
    -Name enabled `
    -Value true `
    -PSPath "IIS:\Sites\webs.nitheesh.acca"

Set-WebConfigurationProperty `
    -Filter
"/system.webServer/security/authentication/anonymousAuthentic
ation" `
    -Name enabled `
    -Value false `
    -PSPath "IIS:\Sites\webs.nitheesh.acca"

Add-DnsServerResourceRecordA `
    -Name "webs" `
    -ZoneName "nitheesh.acca" `
    -IPv4Address "192.168.1.1"
```

Verification

Open browser and test:

<http://webs.yourname.acca>

Part 2C: Configure Remote Desktop

Task: Enable Remote Desktop access to S-DC from another machine.

```
Set-ItemProperty `
    -Path "HKLM:\System\CurrentControlSet\Control\Terminal
Server" `
    -Name "fDenyTSConnections" `
    -Value 0

Set-ItemProperty `
    -Path "HKLM:\System\CurrentControlSet\Control\Terminal
Server\WinStations\RDP-Tcp" `
    -Name "UserAuthentication" `
    -Value 0

SystemPropertiesRemote.exe

Enable-NetFirewallRule -DisplayGroup "Remote Desktop"

Import-Module ActiveDirectory

Add-ADGroupMember `
    -Identity "Remote Desktop Users" `
    -Members "Domain Users"

Get-ItemProperty `
```

ACCA5023 – Network Operating Systems and Services

```
-Path "HKLM:\System\CurrentControlSet\Control\Terminal  
Server" `
-Name "fDenyTSConnections"
```

Verification

From Client Machine: type "mstsc" in run command

Connect to: 192.168.1.1

Troubleshooting (IMPORTANT)

If RDP fails, check:

- ✓ Can you ping the server?
- ✓ Is port 3389 open?
- ✓ Is RDP enabled?
- ✓ Is firewall configured?
- ✓ Are both VMs in the same network?

```
Restart-Computer
Get-NetFirewallRule -DisplayGroup "Remote Desktop"
Get-Service TermService
Restart-Service TermService
netstat -an | findstr 3389
```

Reflection Questions

1. Why is PowerShell preferred over GUI for administration?
2. What is the role of DHCP in a network?
3. Why is DNS important for web services?
4. Why should Remote Desktop access be restricted?
5. What was the most challenging part of this activity?

Note: PowerShell is a powerful tool that allows administrators to automate complex configurations efficiently. Mastering these skills will significantly improve your ability to manage enterprise systems.

End of Worksheet