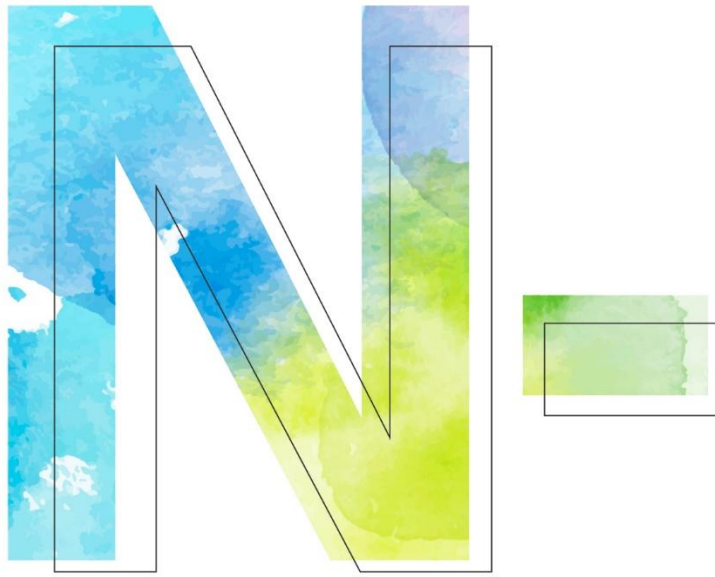




Partner

How to Configure Windows DHCP Log

V012

2025/08/14





Copyright Declaration

N- Copyright © N-Partner Technologies Co. All Rights reserved. Without written authorization from N-Partner Technologies Co., anyone may not in any way copy, plagiarize or translate this manual. The system is keeping upgraded; therefore, N-Partner reserves the right to revise it without informing.

Registered Trademark

All company products, names and trademarks mentioned in this manual belongs to their legally registered organizations.

Contents

Preface.....	2
1. NXLog.....	3
1.1 NXLog Installation	3
1.2 Download NXLog Configuration File	7
1.2.1 For Windows Server 2003 or earlier:	7
1.2.2 For Windows Server 2008 or later	8
1.3 NXLog Configuration	9
1.4 Starting the NXLog Service.....	12
1.4.1 For Windows Server 2003 or earlier	12
1.4.2 For Windows Server 2008 or later	15
2. Windows Server 2003	18
3. Windows Server 2008	21
3.1 DHCP IPv4	21
3.2 DHCP IPv6	24
4. Windows Server 2012	26
4.1 DHCP IPv4	26
4.2 DHCP IPv6	29
5. Windows Server 2016	31
5.1 DHCP IPv4	31
5.2 DHCP IPv6	34
6. Windows Server 2019	36
6.1 DHCP IPv4	36
6.2 DHCP IPv6	39
7. Windows Server 2022	41
7.1 DHCP IPv4	41
7.2 DHCP IPv6	44
8. N-Reporter	46
8.1 For Windows Server 2003 or earlier	47
8.2 For Windows Server 2008 or later	50
9. Troubleshooting.....	53
9.1 Adjusting the DHCP Log File Size	53

Preface

This document describes how N-Reporter users can configure Windows DHCP logging using the open-source tool NXLog.

NXLog converts Windows DHCP logs into syslog format and forwards them to N-Reporter for normalization, auditing, and analysis.

This document applies to Windows Server 2003, 2008, 2012, 2016, 2019, and 2022.

Note: This document is provided solely as a reference for configuring log output. It is recommended that you contact the device or software vendor for assistance with the appropriate log export methods.

1. NXLog

1.1 NXLog Installation

(1) Download NXLog CE (Community Edition)

Please go to: <https://nxlog.co/products/nxlog-community-edition/download>

Download the latest version of nxlog-ce-x.x.xxxx.msi.

Example Here: **nxlog-ce-3.2.2329.msi**



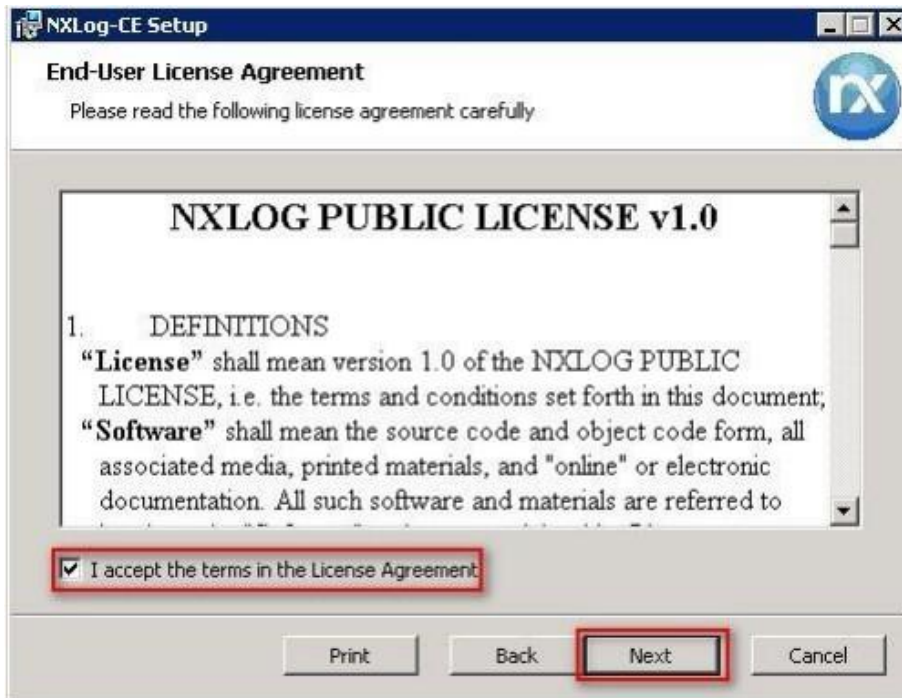
(2) Install NXLog

<2.1> For Windows Server **2008** or later:

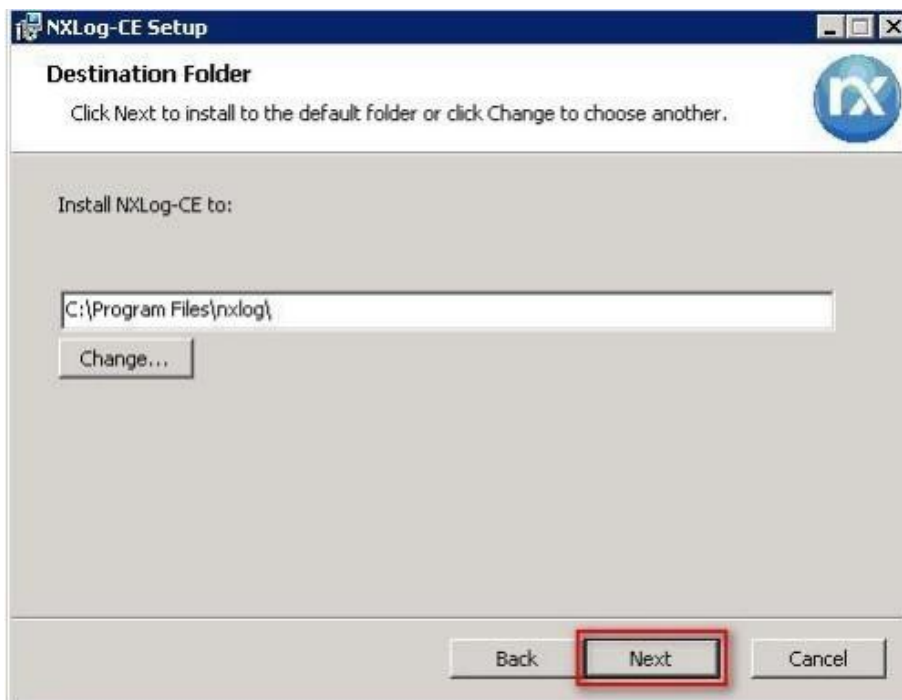
Double-click “**nxlog-ce-3.2.2329.msi.**”



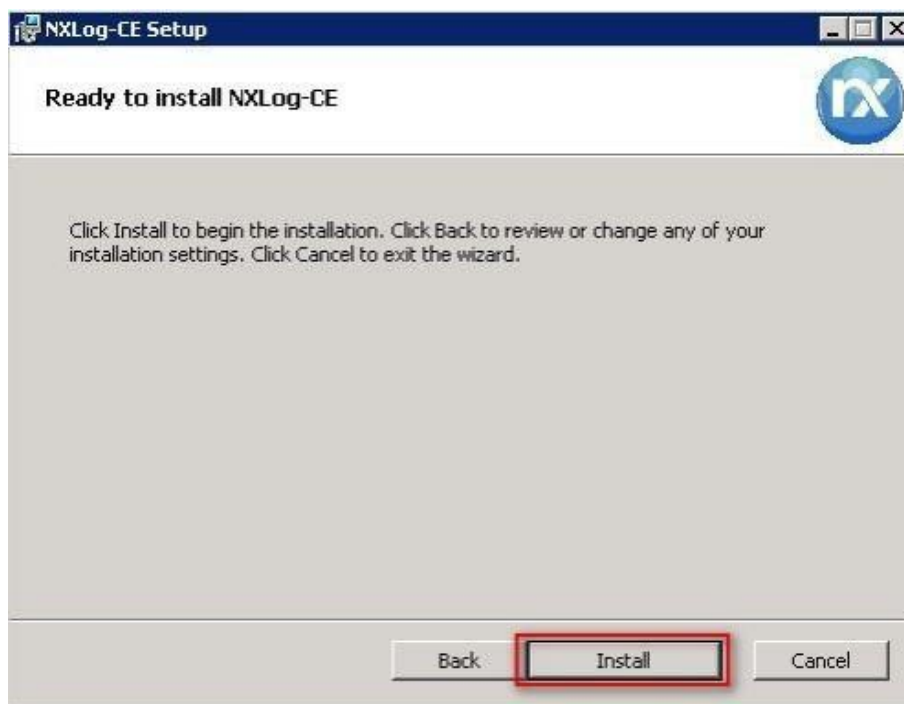
(3) Select "I accept the terms in the License Agreement," then click "Next."



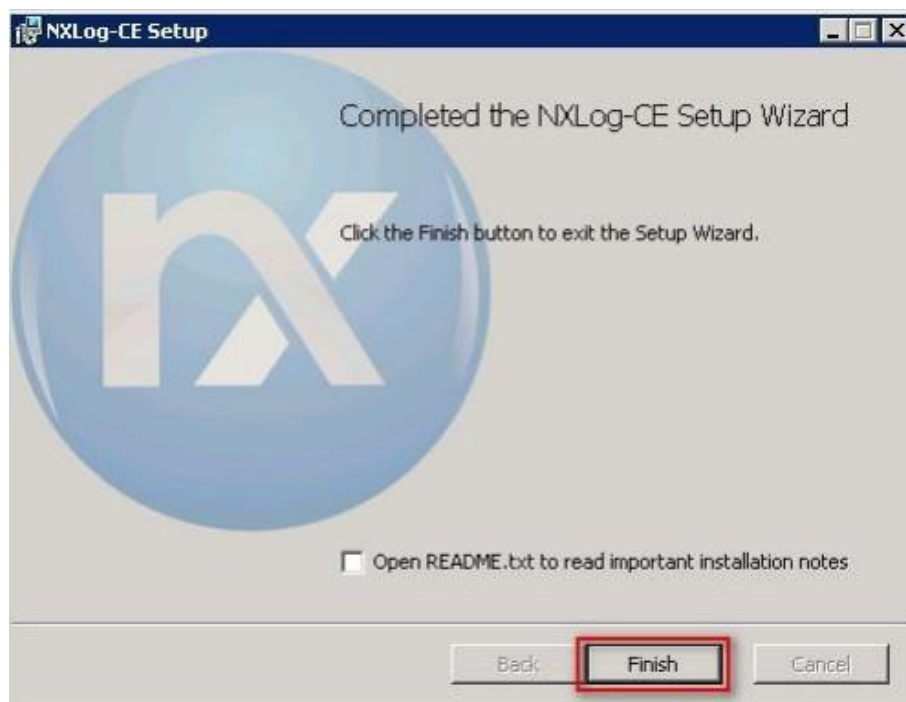
(4) Click "Next." (The default installation path is (C:\Program Files\nxlog\)).



(5) Click "Install."

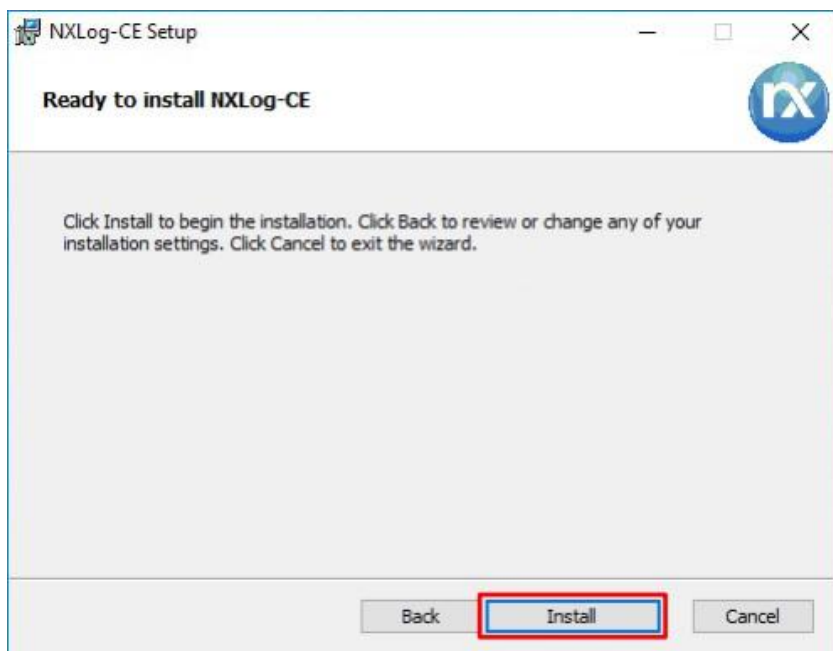


(6) Click "Finish."



<2.2> For Windows Server 2003:

Download File: **nxlog-ce-3.2.2329.msi**. → Select “Install” and proceed until the installation completes. → Click “Finish” to exit.

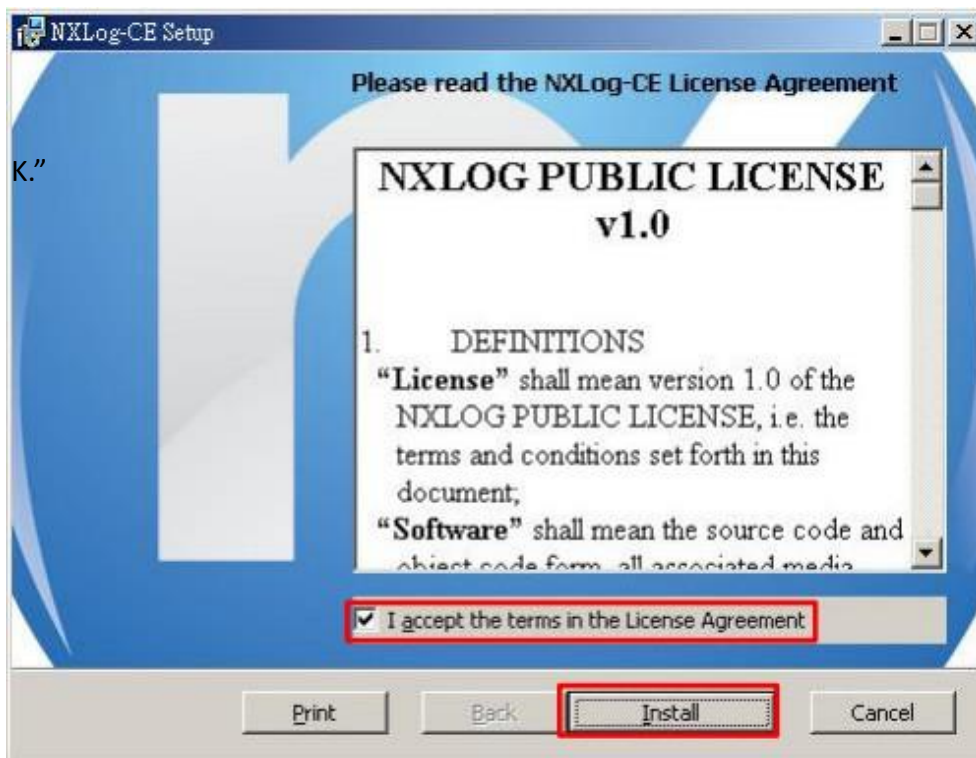


<2.3> For Windows 2000:

(1) Navigate to the NXLog CE legacy download page: <https://sourceforge.net/projects/nxlog-ce/>

(2) Click “See All Activity” and download the Windows 2000-compatible version “/nxlog-ce-2.8.1248.msi.”

(3) Launch “nxlog-ce-2.8.1248.msi,” and accept the license terms, click “Install,” and then “Finish.”



1.2 Download NXLog Configuration File

1.2.1 For Windows Server 2003 or earlier:

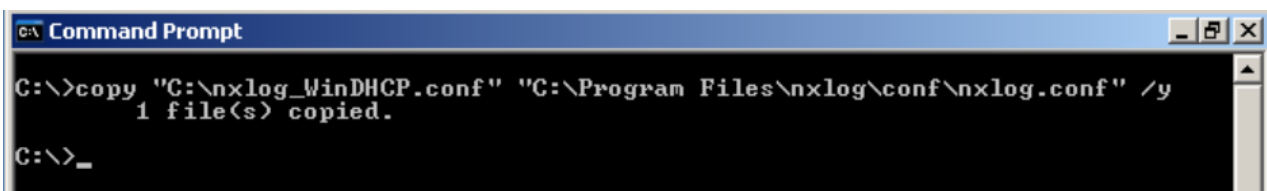
(1) Open "Command Prompt."



(2) Download the "NXLog DHCP configuration file" and overwrite the existing NXLog configuration file in the Windows system.

Download link: http://www.npartner.com/download/tech/nxlog_WinDHCP.conf

```
C:\> copy "C:\nxlog_WinDHCP.conf" "C:\Program Files\nxlog\conf\nxlog.conf" /y
```



Note: The example above is for a 64-bit operating system. For a 32-bit operating system, replace the highlighted text with: 'C:\ **Program Files (x86)**\nxlog\conf\nxlog.conf'

1.2.2 For Windows Server 2008 or later

(1) Open “Windows PowerShell.”



(2) Download the “NXLog DHCP configuration file” and overwrite the existing NXLog configuration file in the Windows system.

Download link: http://www.npartner.com/download/tech/nxlog_WinDHCP.conf

```
PS C:\> Invoke-WebRequest -Uri`http://www.npartner.com/download/tech/nxlog_WinDHCP.conf' -  
OutFile 'C:\ Program Files\nxlog\conf\nxlog.conf'
```



Note: This example is for a 64-bit operating system. For a 32-bit system, replace the highlighted text with: 'C:\ Program Files(x86)\nxlog\conf\nxlog.conf'

1.3 NXLog Configuration

```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud 192.168.8.4
define DhcpPath C:\Windows\System32\LogFiles\DHCP
define ROOT C:\Program Files\nxlog
define CERTDIR %ROOT%\cert
define CONFDIR %ROOT%\conf
define LOGDIR %ROOT%\data
define LOGFILE %LOGDIR%\nxlog.log
LogFile %LOGFILE%

Moduledir %ROOT%\modules
CacheDir %ROOT%\data
Pidfile %ROOT%\data\nxlog.pid

## Load the modules needed by the outputs
<Extension syslog>
  Module xm_syslog
</Extension>

## For DHCP log file use the following:
<Input in_dhcplog>
  Module im_file
  File '%DhcpPath%\Dhcp*.log'
  SavePos TRUE
  ReadFromLast TRUE
</Input>

<Output out_dhcplog>
  Module om_udp
  Host %NCloud%
  Port 514
  Exec $SyslogFacilityValue = 20;
  Exec to_syslog_bsd();
</Output>

<Route dhcplog>
  Path in_dhcplog => out_dhcplog
</Route>
```

```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
```

```
define NCloud 192.168.3.88
define DhcpPath C:\Windows\System32\LogFiles\DHCP
define ROOT C:\Program Files\nxlog
define CERTDIR %ROOT%\cert
define CONFDIR %ROOT%\conf
define LOGDIR %ROOT%\data
define LOGFILE %LOGDIR%\nxlog.log
LogFile %LOGFILE%

Moduledir %ROOT%\modules
CacheDir %ROOT%\data
Pidfile %ROOT%\data\nxlog.pid

## Load the modules needed by the outputs
<Extension syslog>
```

```

Module xm_syslog
</Extension>

## For DHCP log file use the following:
<Input in_dhcplog>
Module im_file
File '%DhcpPath%\Dhcp*.log'
SavePos TRUE
ReadFromLast TRUE
</Input>
<Output out_dhcplog>
Module om_udp
Host %NCloud%
Port 514
Exec $SyslogFacilityValue = 20;
Exec to_syslog_bsd();
</Output>
<Route dhcplog>
Path in_dhcplog => out_dhcplog
</Route>

```

Enter the N-Reporter system IP address in the blue text section.

```
define NCloud 192.168.3.88
```

This example is based on a 64-bit operating system.

For a 32-bit operating system, use the following setting instead:

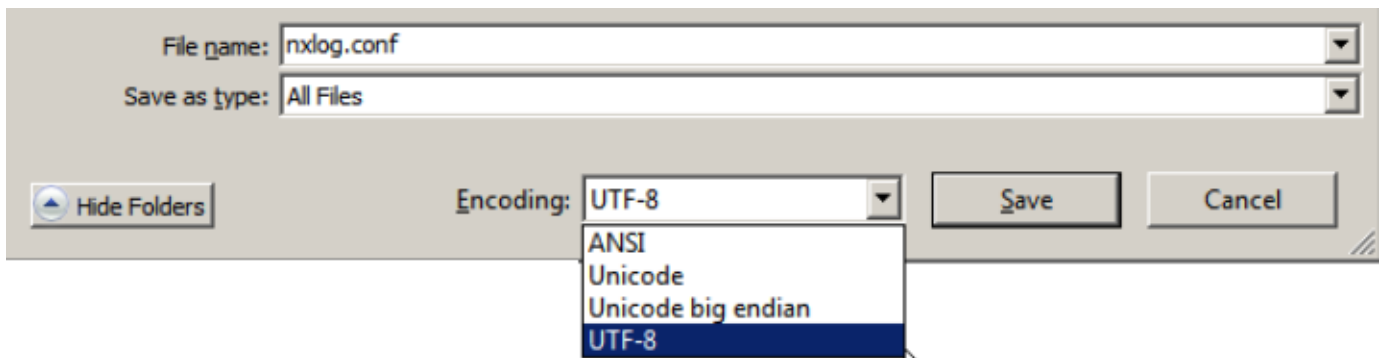
```
define ROOT C:\Program Files (x86)\nxlog
```

If NXLog cannot access the System32 folder path, specify “Sysnative”.

Sysnative is a redirected folder:

```
define DhcpPath C:\Windows\Sysnative\LogFiles\DHCP
```

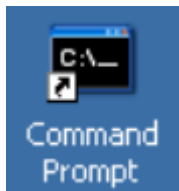
Note: After modifying the configuration file, save it as a new file to overwrite the original. For Save as type, select “All Files (*.*)”. For Encoding, select UTF-8 to avoid encoding errors that could prevent the service from starting.



1.4 Starting the NXLog Service

1.4.1 For Windows Server 2003 or earlier

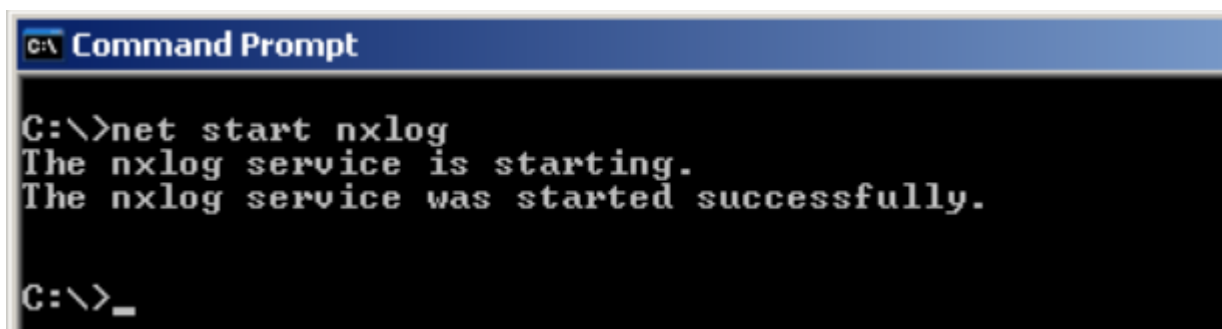
(1) Open "Command Prompt."



(2) Start the NXLog service and verify that there are no error messages:

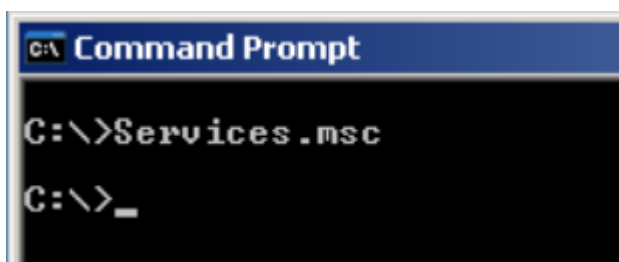
```
C:\> net start nxlog
```

```
C:\> type "C:\Program Files\nxlog\data\nxlog.log"
```

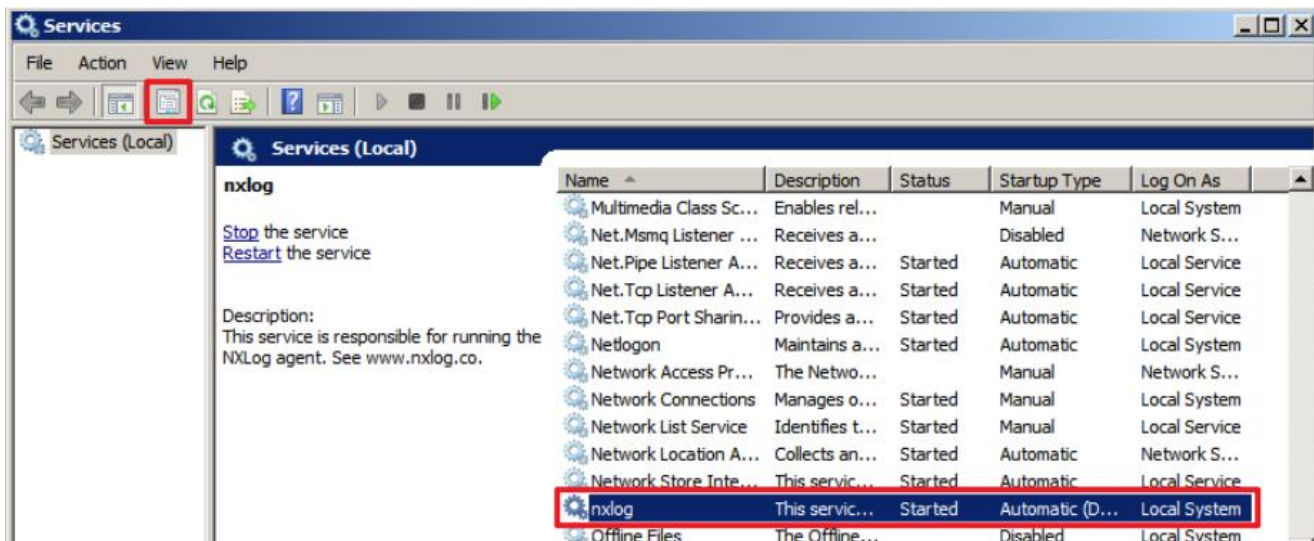


(3) Enter the command below to open the **Services** console:

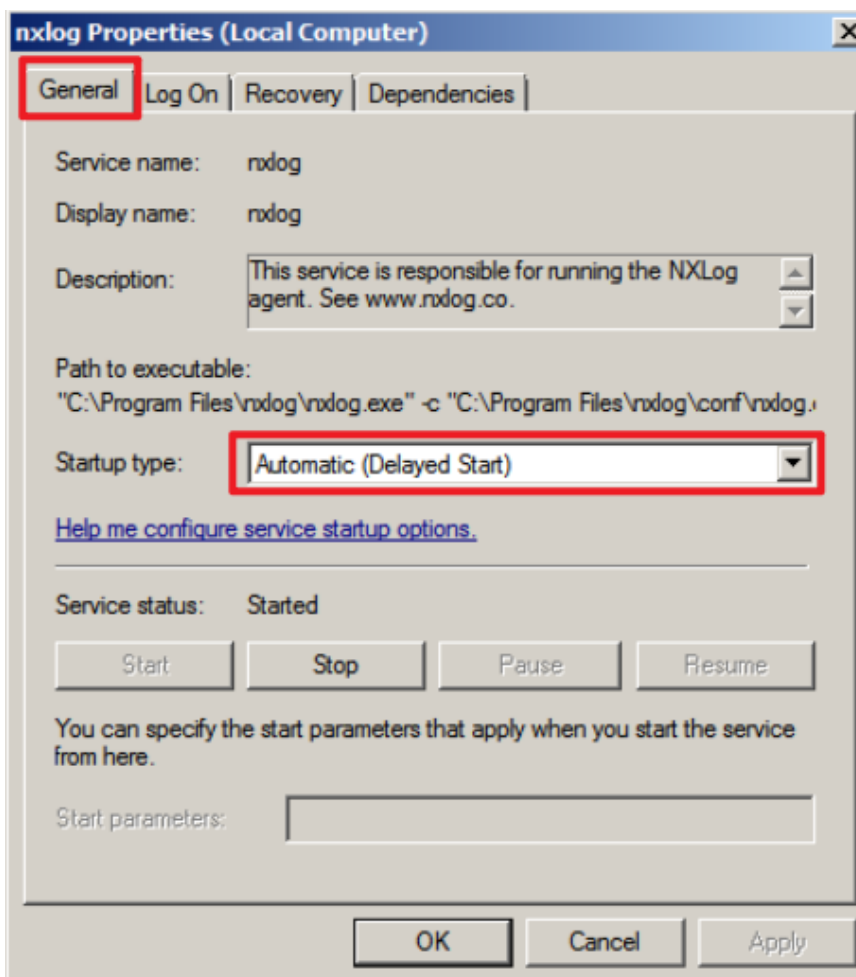
```
C:\> Services.msc
```



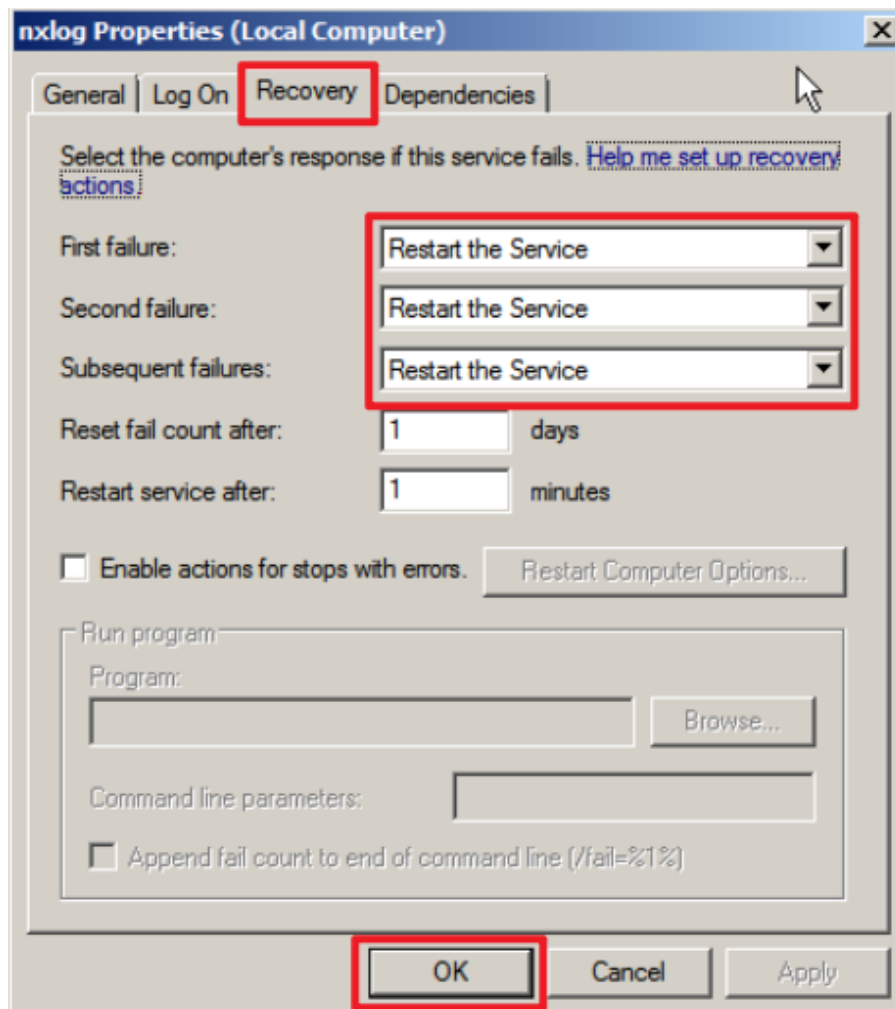
(4) Open the NXLog service properties: select “NXLog” →  Click “Properties.”



(5) On the General tab, verify that Startup type is set to Automatic (Delayed Start).



- (6) On the Recovery tab, verify that First failure, Second failure, and Subsequent failures are all set to “Restart the Service”, then click “OK.”



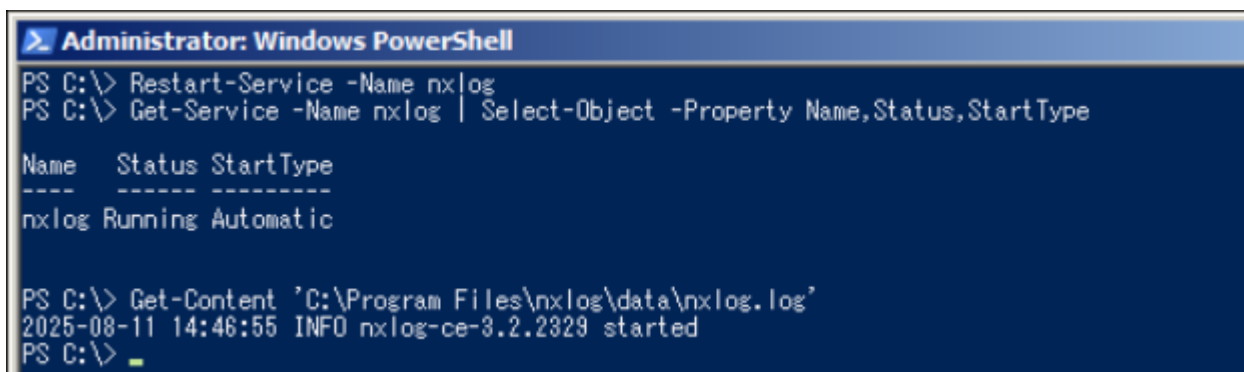
1.4.2 For Windows Server 2008 or later

(1) Open “Windows Powershell.”



(2) Restart the NXLog service, verify that it is running, and ensure there are no error messages:

```
PS C:\> Restart-Service -Name nxlog
PS C:\> Get-Service -Name nxlog | Select-Object -Property Name,Status,StartType
PS C:\> Get-Content 'C:\Program Files\ nxlog\data\nxlog.log'
```

A screenshot of a Windows PowerShell console window titled "Administrator: Windows PowerShell". The console shows the following commands and output:

```
PS C:\> Restart-Service -Name nxlog
PS C:\> Get-Service -Name nxlog | Select-Object -Property Name,Status,StartType

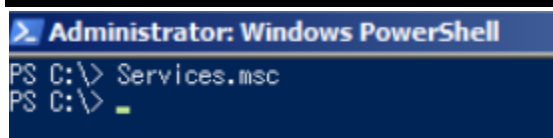
Name      Status StartType
-----
nxlog     Running Automatic

PS C:\> Get-Content 'C:\Program Files\nxlog\data\nxlog.log'
2025-08-11 14:46:55 INFO nxlog-ce-3.2.2329 started
PS C:\> _
```

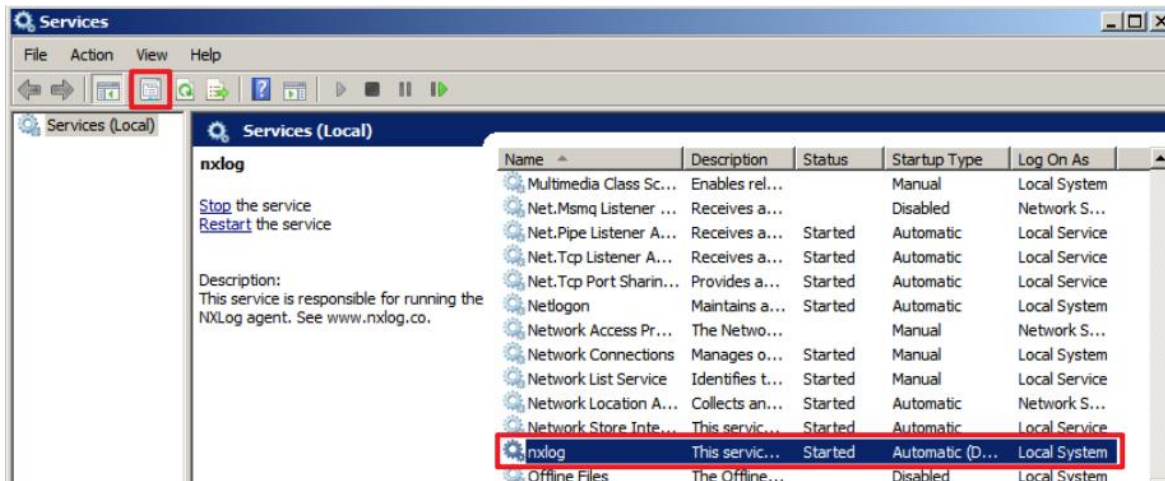
Note: This example is for a 64-bit operating system. For a 32-bit system, replace the highlighted text with: '**C:\Program Files(x86)\nxlog\conf\nxlog.conf**'

(3) Enter the command below to open the **Services** console:

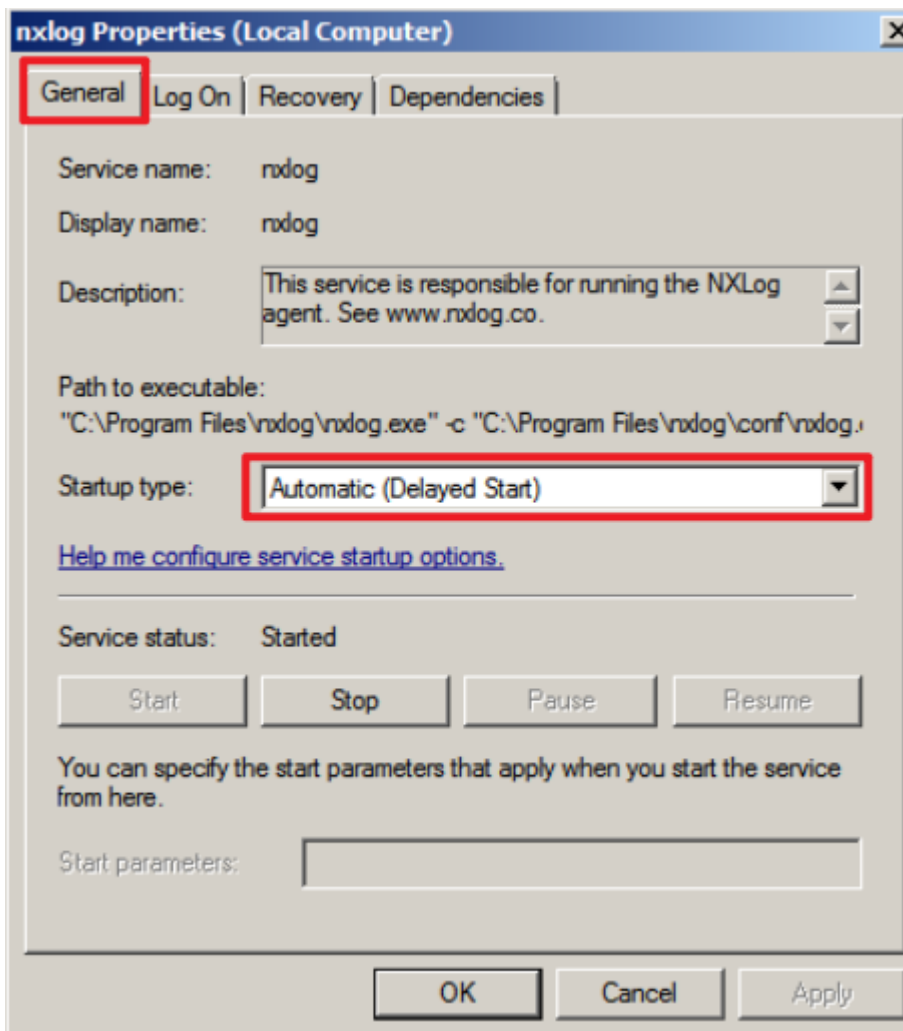
```
PS C:\> Services.msc
```



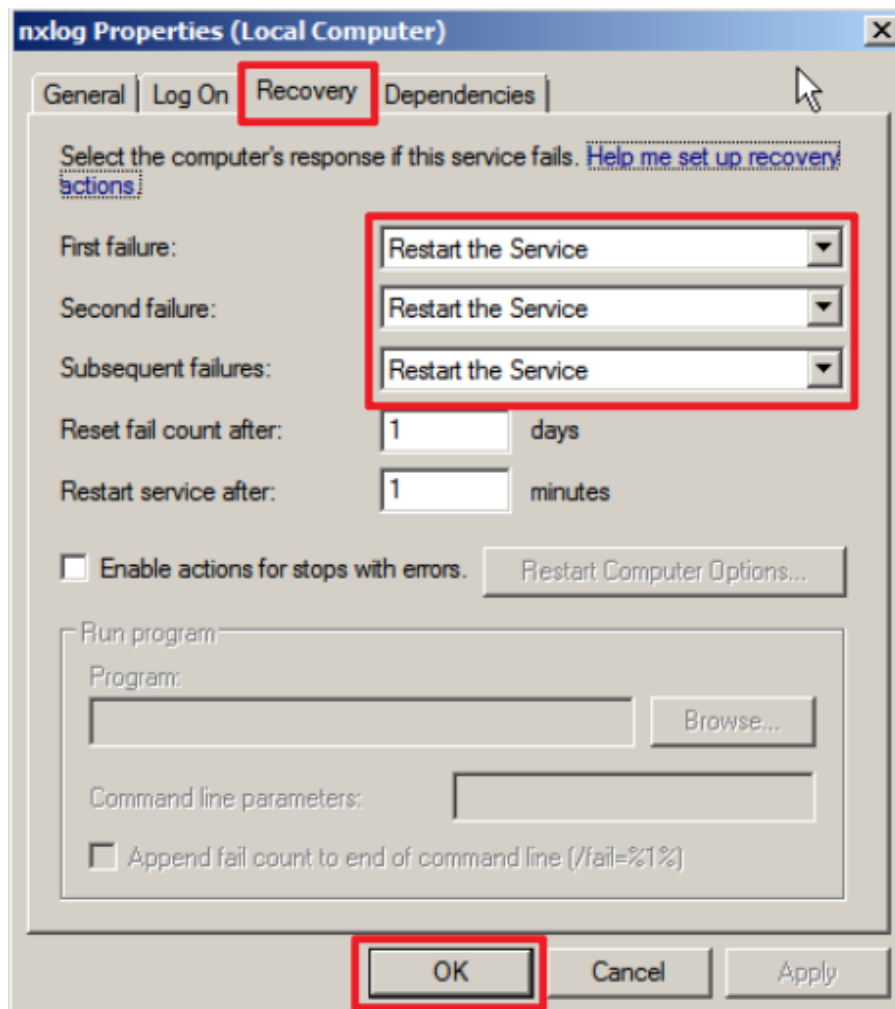
(4) Open the NXLog service properties: select “NXLog” →  Click “Properties.”



(5) On the General tab, verify that Startup type is set to Automatic (Delayed Start).



- (6) On the Recovery tab, verify that First failure, Second failure, and Subsequent failures are all set to “Restart the Service”, then click “OK.”



2. Windows Server 2003

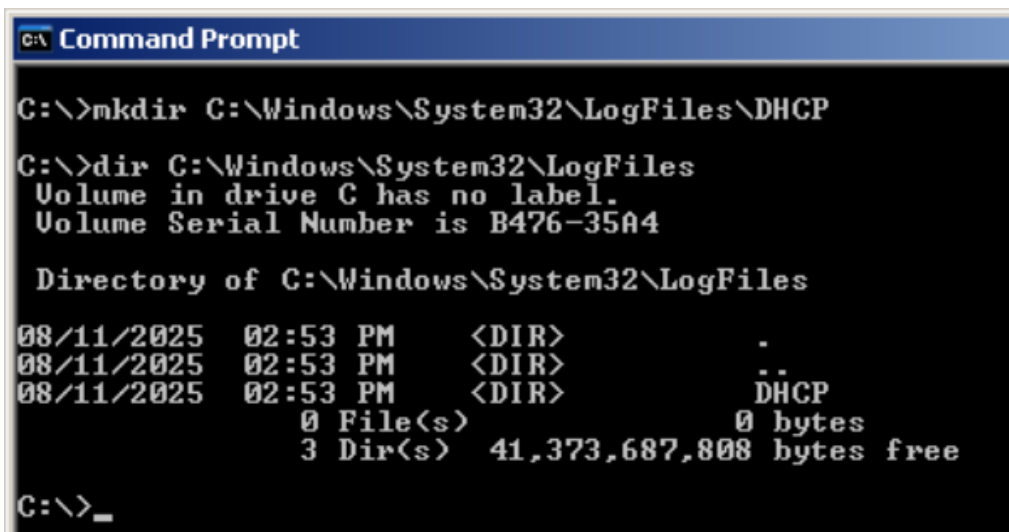
(1) Open "Command Prompt."



(2) Enter the command below to create the DHCP log folder:

```
C:\> mkdir C:\Windows\System32\LogFiles\DHCP
```

```
C:\> dir C:\Windows\System32\LogFiles
```

A screenshot of the Windows Command Prompt window. The title bar says 'C:\> Command Prompt'. The command prompt shows the execution of 'mkdir C:\Windows\System32\LogFiles\DHCP' and 'dir C:\Windows\System32\LogFiles'. The output shows the directory listing for C:\Windows\System32\LogFiles, including a new directory named 'DHCP' created on 08/11/2025 at 02:53 PM. The free space is 41,373,687,808 bytes.

```
C:\>mkdir C:\Windows\System32\LogFiles\DHCP

C:\>dir C:\Windows\System32\LogFiles
Volume in drive C has no label.
Volume Serial Number is B476-35A4

Directory of C:\Windows\System32\LogFiles

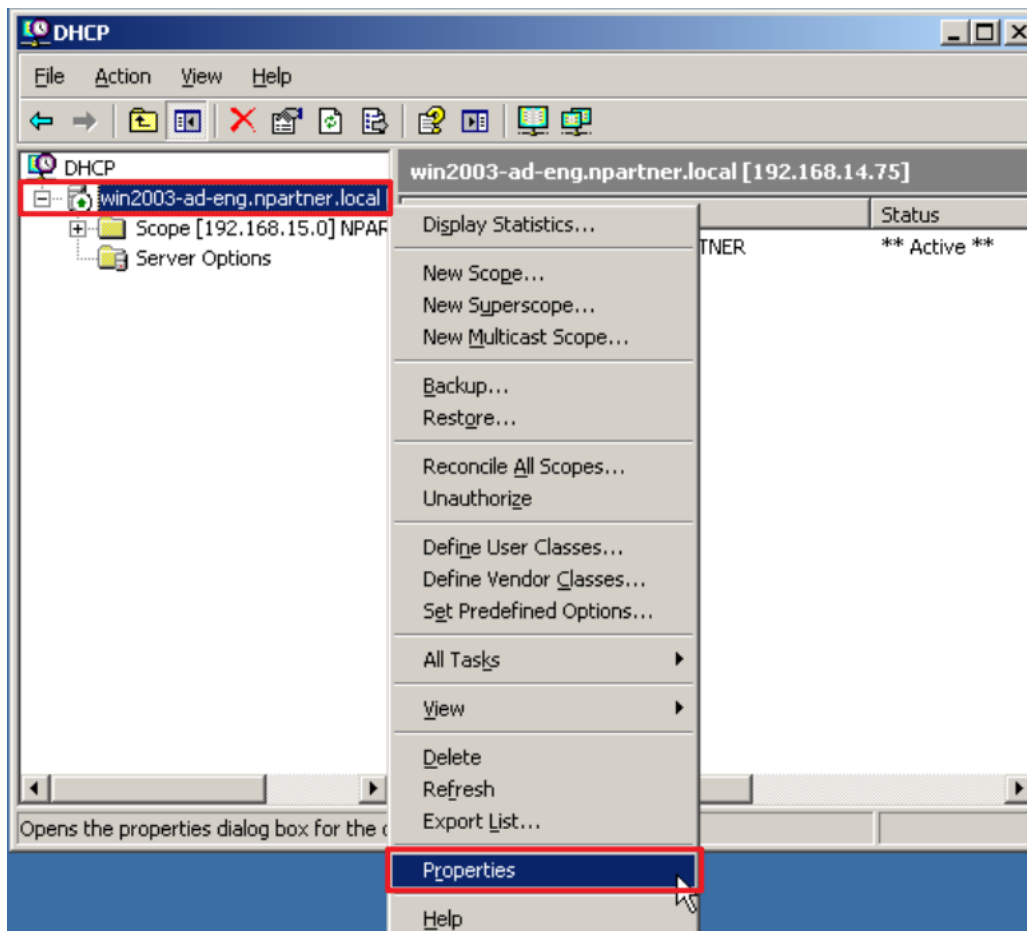
08/11/2025  02:53 PM    <DIR>          .
08/11/2025  02:53 PM    <DIR>          ..
08/11/2025  02:53 PM    <DIR>          DHCP
               0 File(s)                0 bytes
               3 Dir(s)  41,373,687,808 bytes free

C:\>_
```

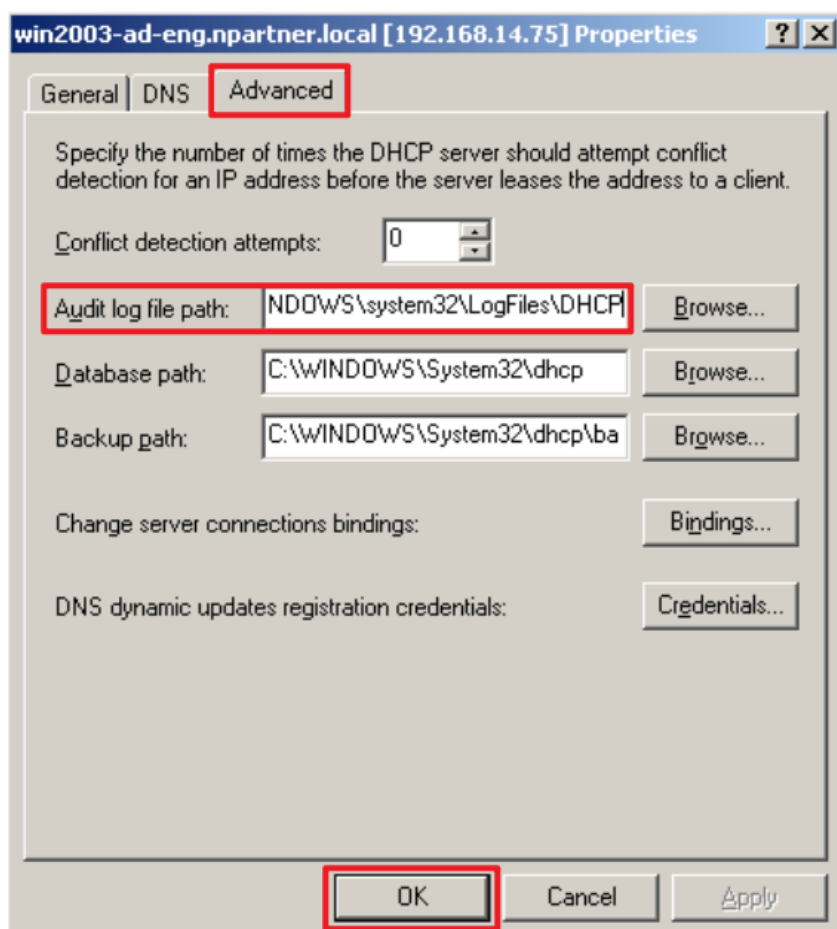
(3) Open DHCP.



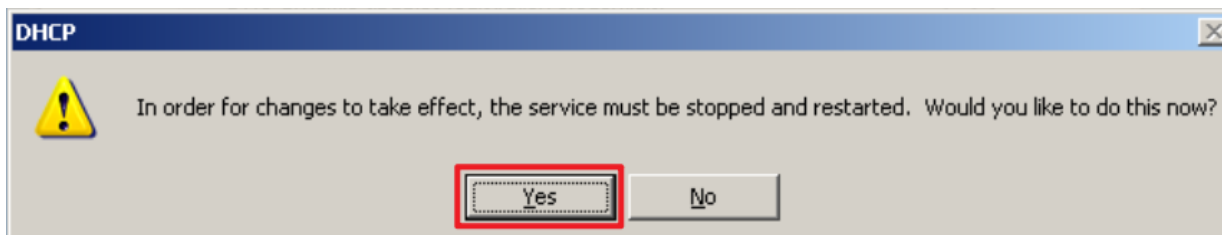
(4) Right-click “DHCP Server” (the example here is **win2003-ad-eng.npartner.local**) → select “Properties.”



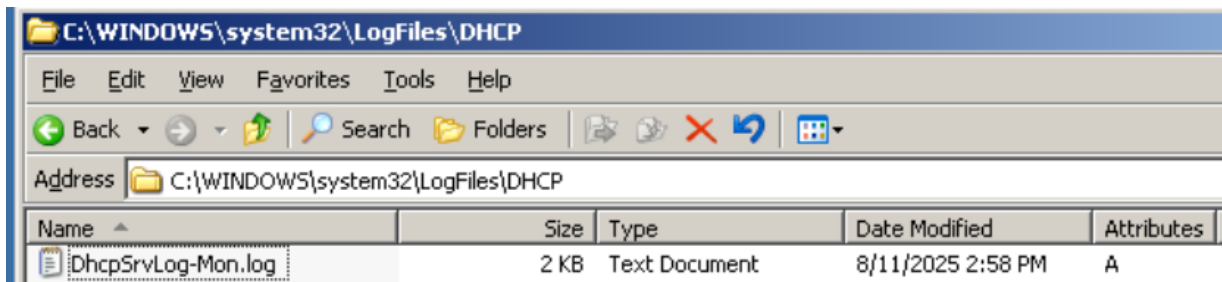
(5) On the Advanced tab, enter the audit log file path: **C:\Windows\System32\LogFiles\DHCP** and click “OK.”



(6) Click “Yes” to restart the DHCP Server service.



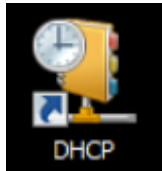
(7) Verify that the file Dhcp.log has been generated.



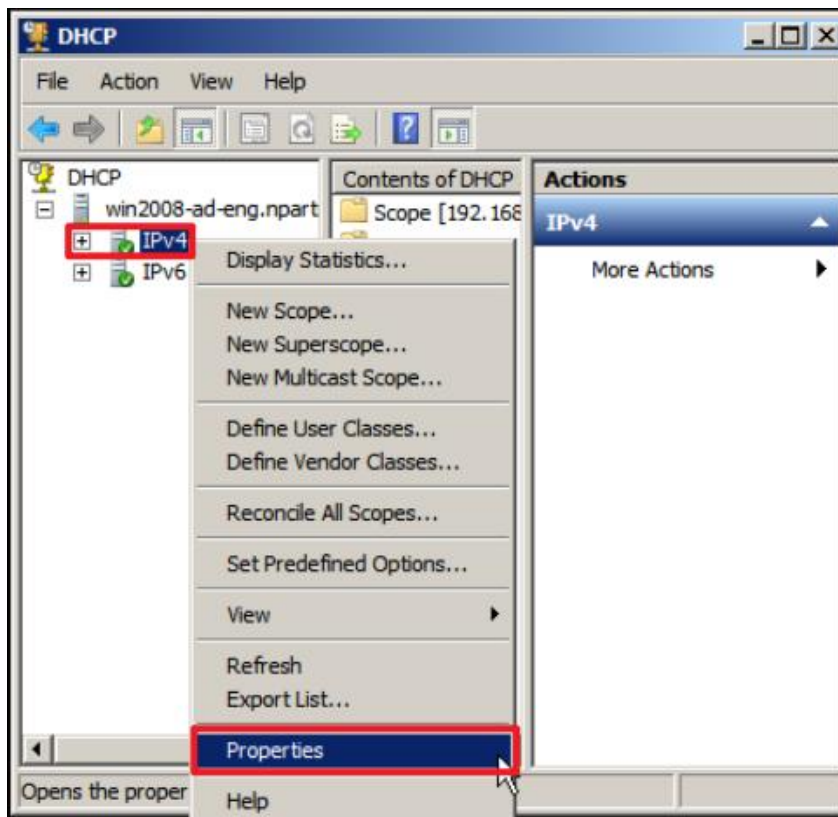
3. Windows Server 2008

3.1 DHCP IPv4

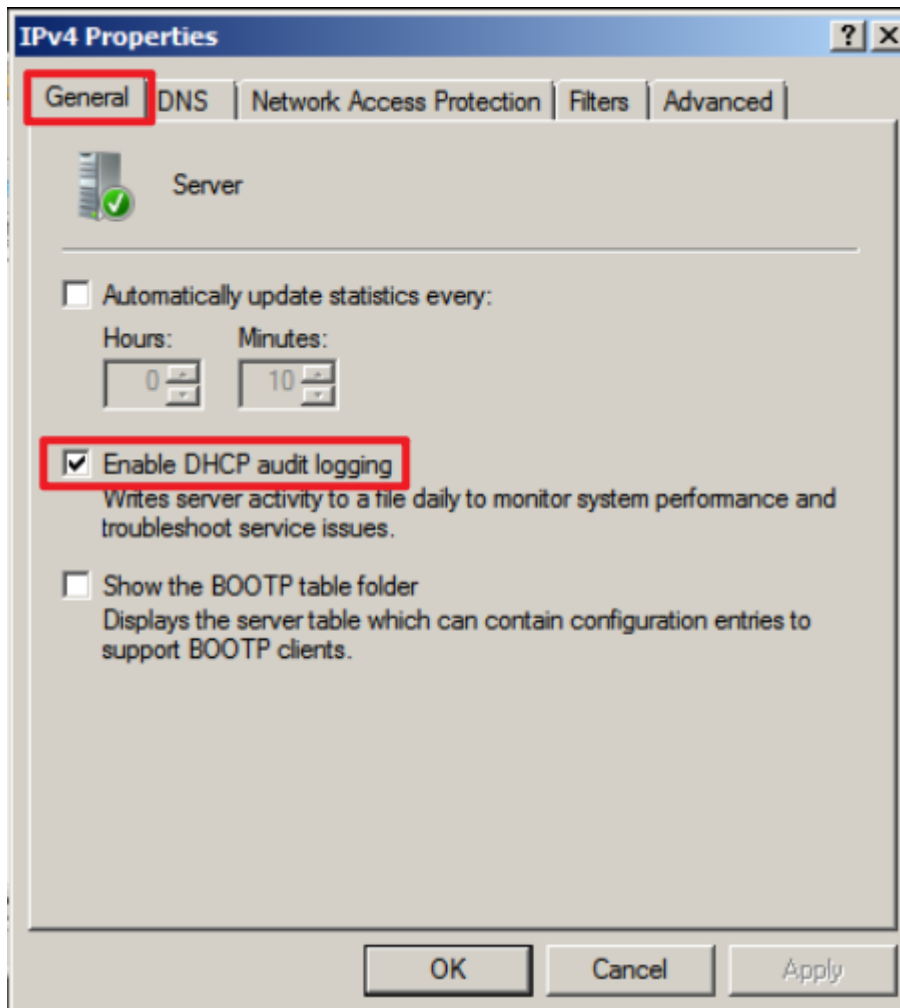
(1) Open **DHCP**.



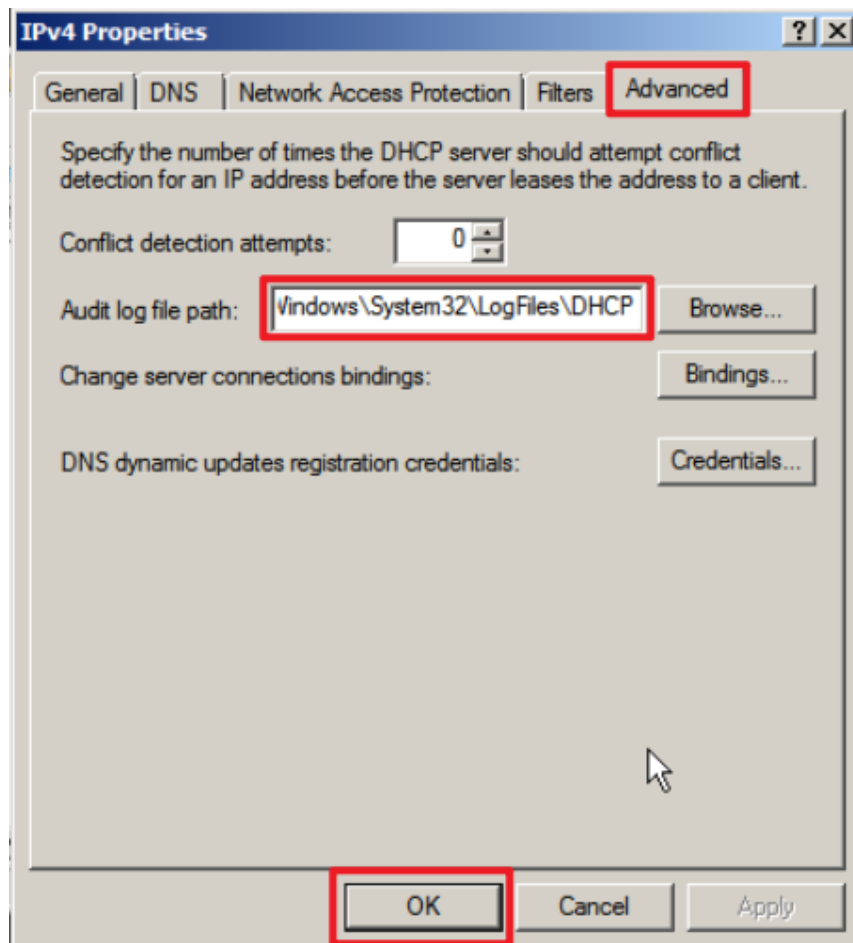
(2) Right-click "IPv4" → select "Properties."



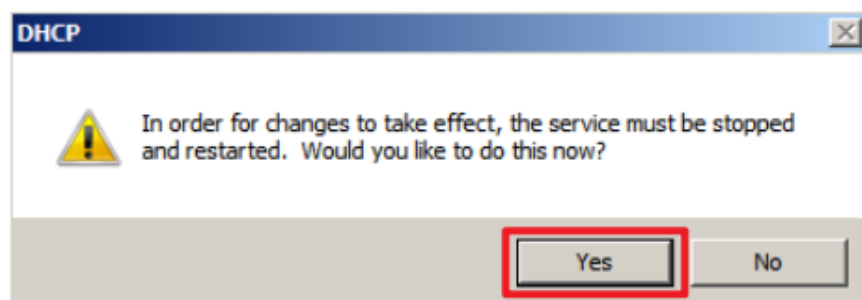
(3) On the General tab, verify that “Enable DHCP audit logging” is selected.



(4) On the Advanced tab, enter the audit log file path: **C:\Windows\System32\LogFiles\DHCP** and click “OK.”

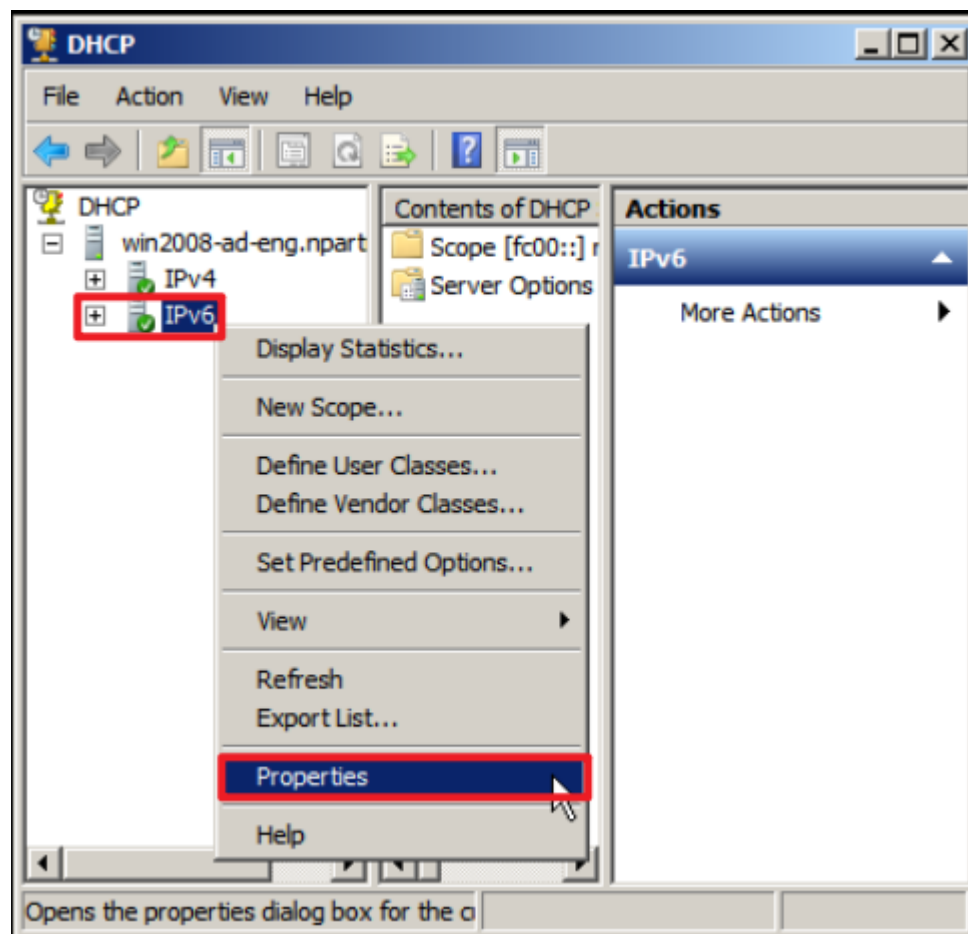


(5) Click “Yes” to restart the DHCP Server service.

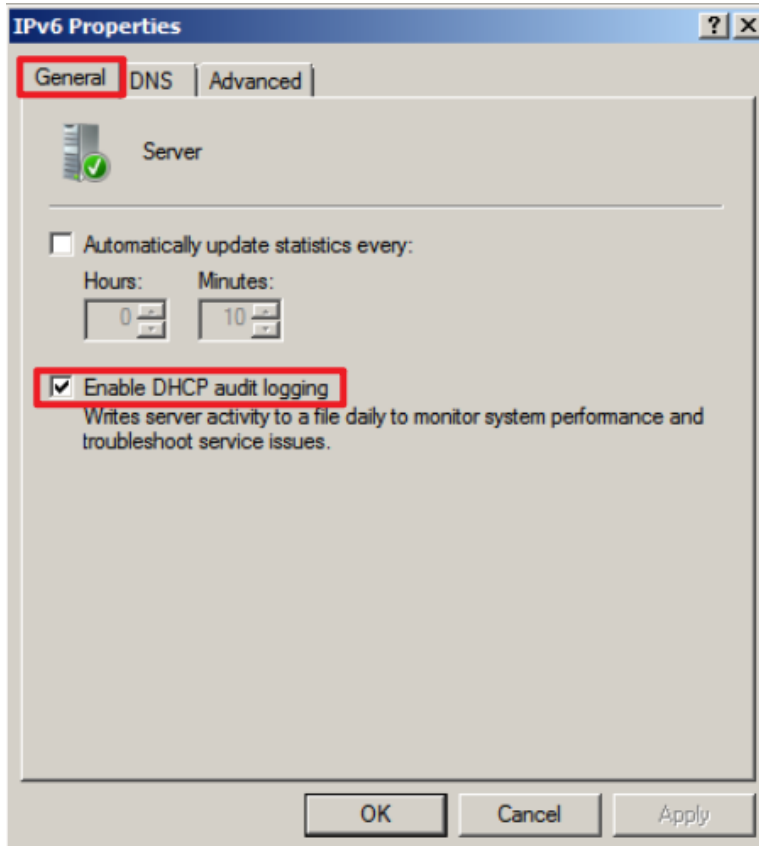


3.2 DHCP IPv6

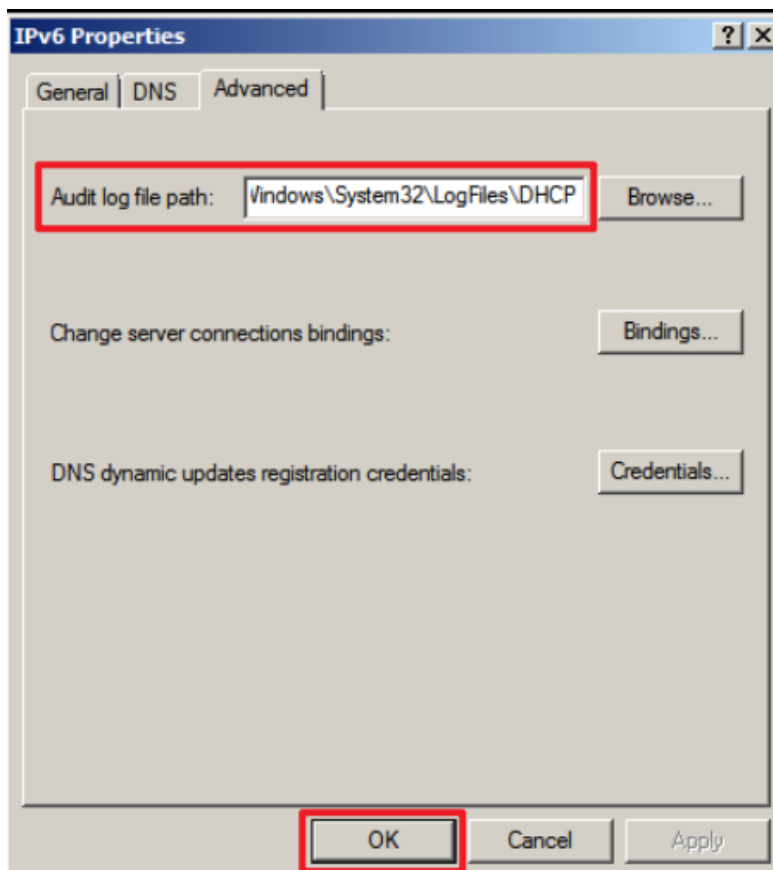
(1) Right-click “IPv6” → select “Properties.”



(2) On the General tab, verify that “Enable DHCP audit logging” is selected.



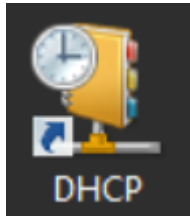
(3) On the Advanced tab, enter the audit log file path: **C:\Windows\System32\LogFiles\DHCP** and click “OK.”



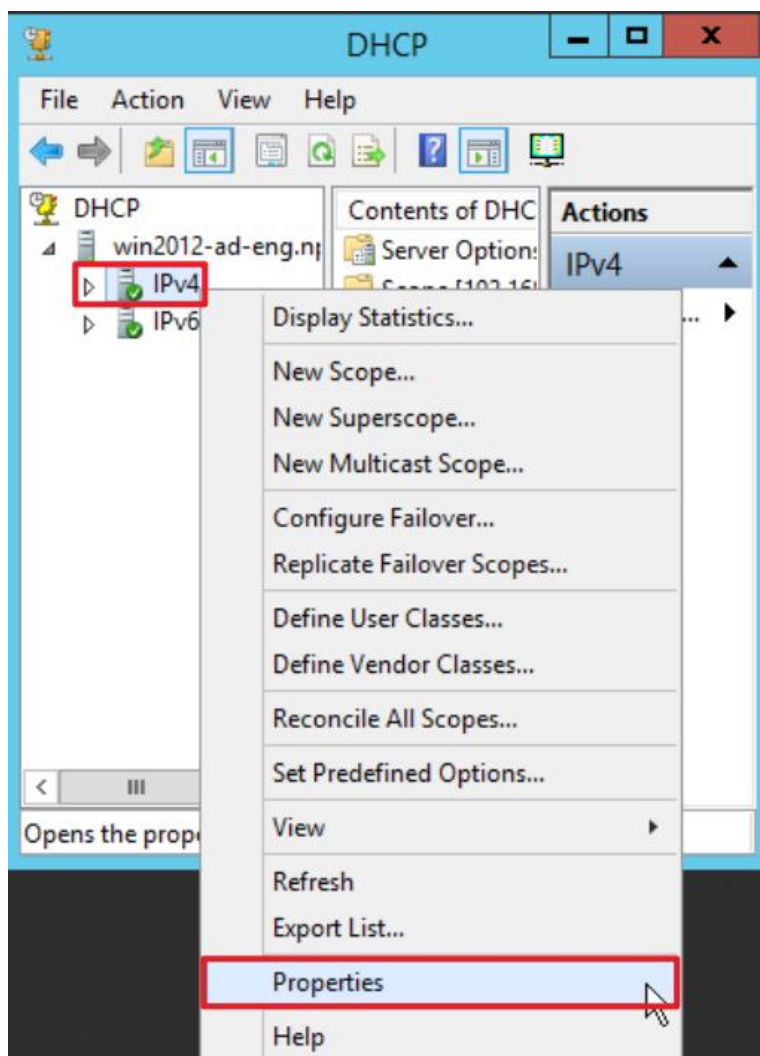
4. Windows Server 2012

4.1 DHCP IPv4

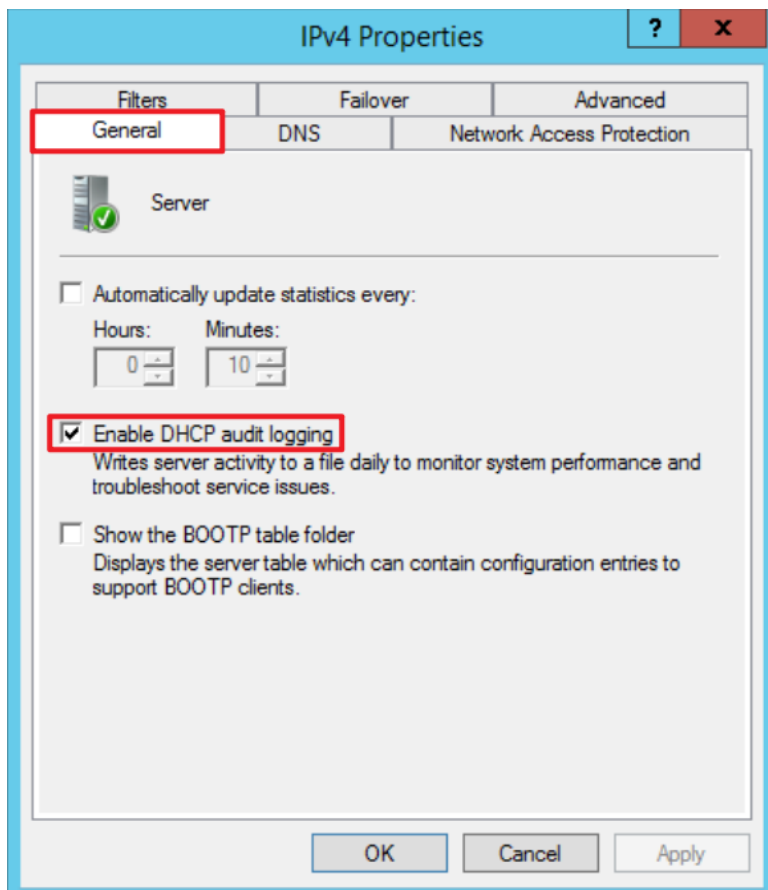
(1) Open DHCP.



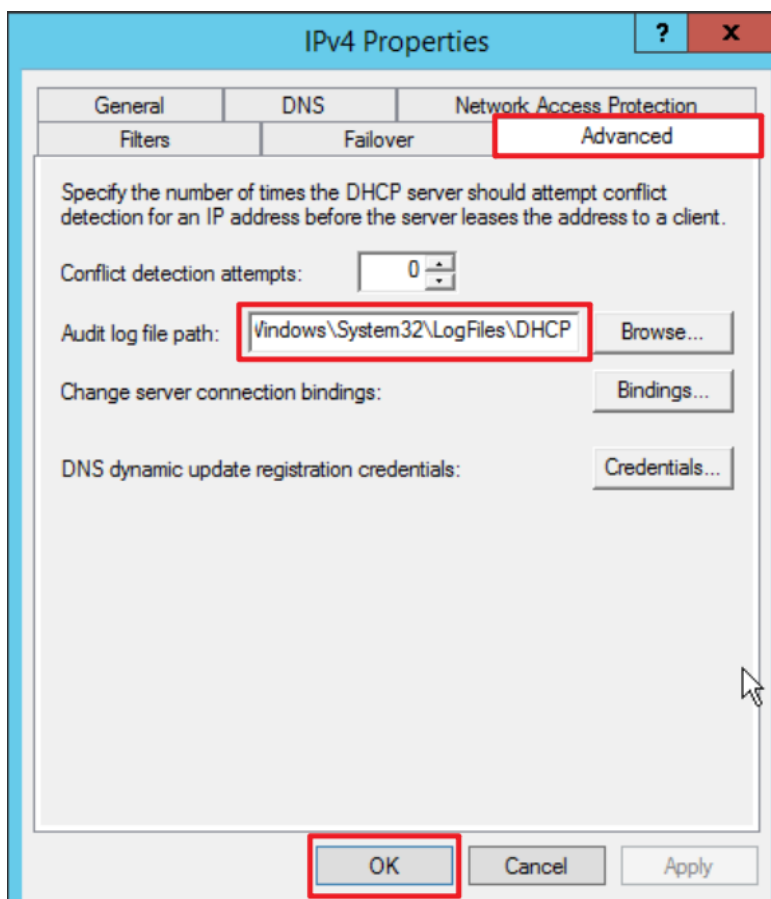
(2) Right-click "IPv4" → select "Properties."



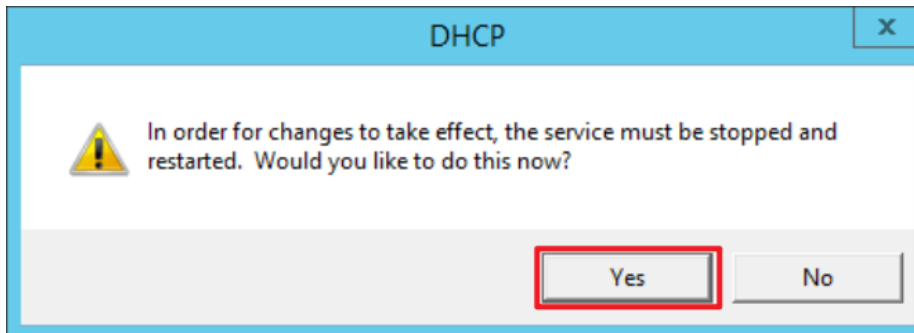
(3) On the General tab, verify that Enable “DHCP audit logging” is selected.



(4) On the Advanced tab, enter the audit log file path: **C:\Windows\System32\LogFiles\DHCP** and click “OK.”

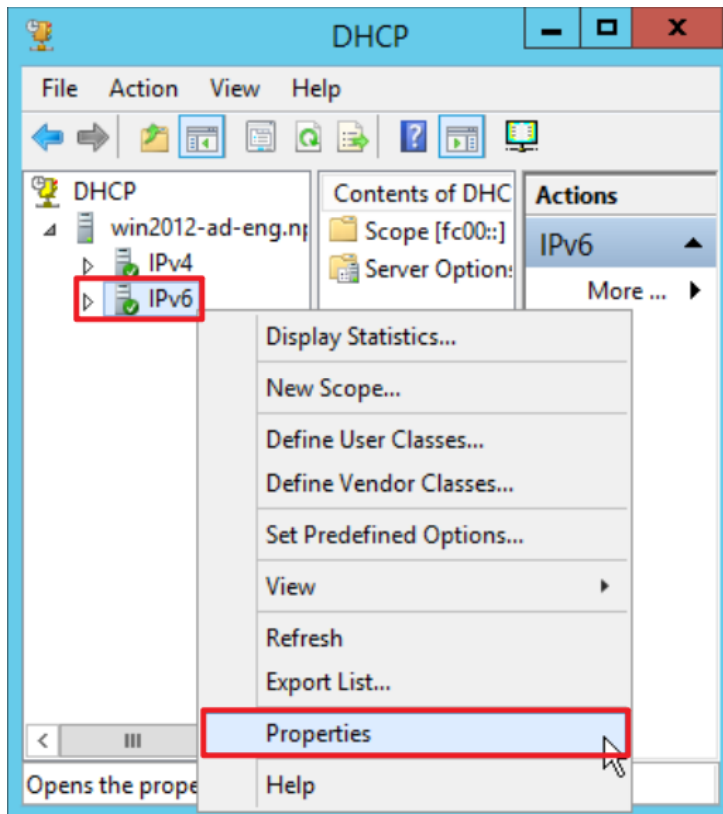


(5) Click Yes to restart the DHCP Server service.

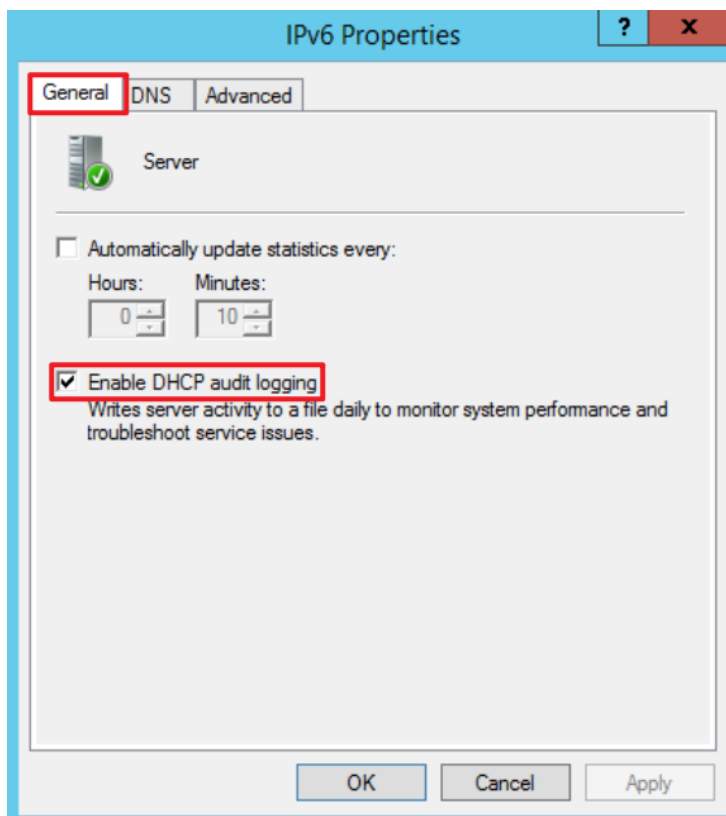


4.2 DHCP IPv6

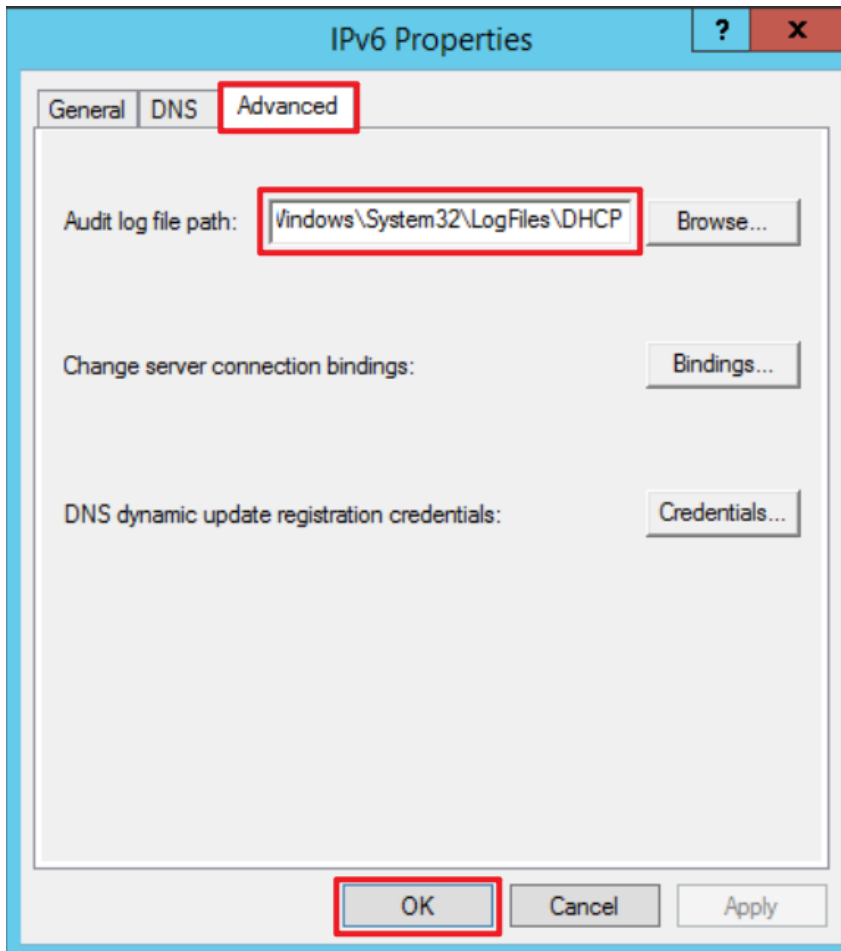
(1) Right-click “IPv6” → select “Properties.”



(2) On the General tab, verify that “Enable DHCP audit logging” is selected.



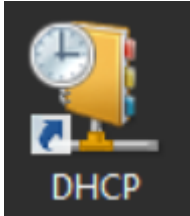
(3) On the Advanced tab, enter the audit log file path: **C:\Windows\System32\LogFiles\DHCP** and click “OK.”



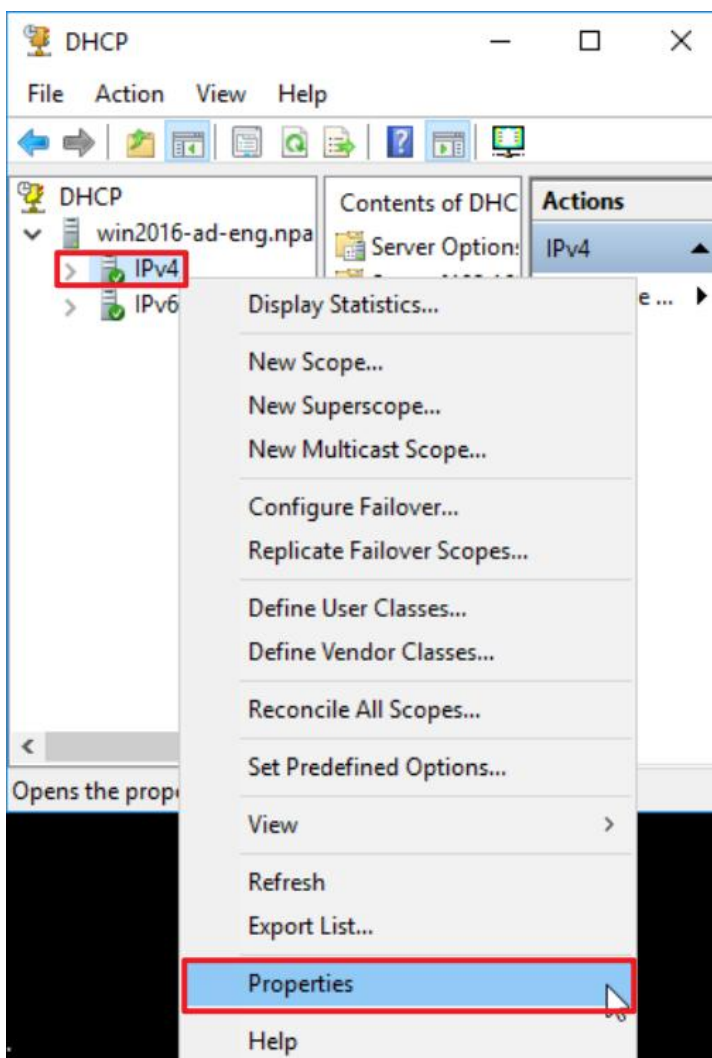
5. Windows Server 2016

5.1 DHCP IPv4

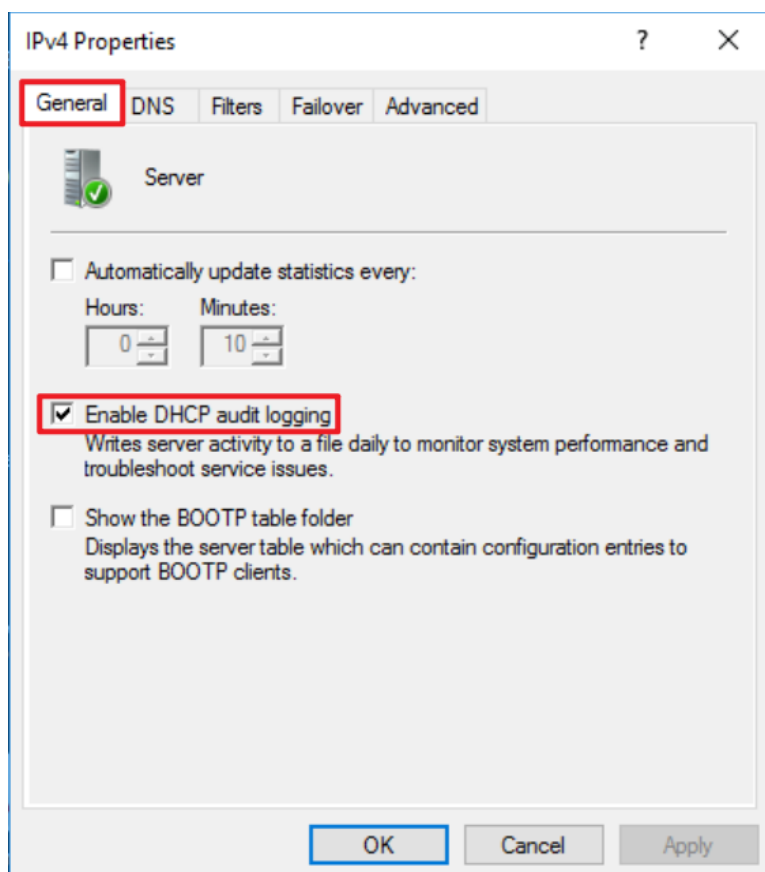
(1) Open DHCP.



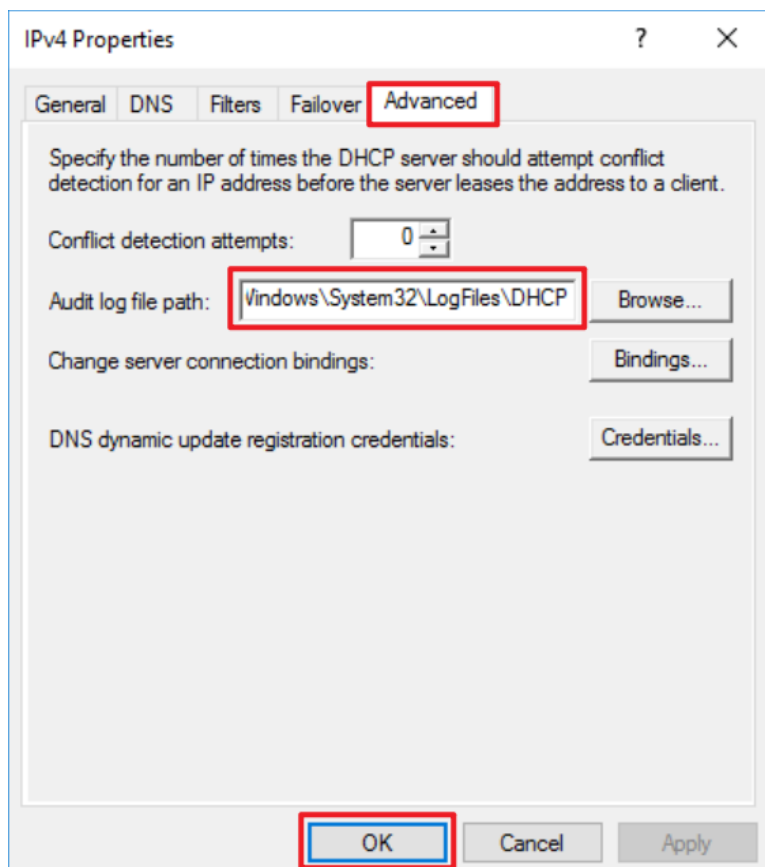
(2) Right-click "IPv4" → select "Properties."



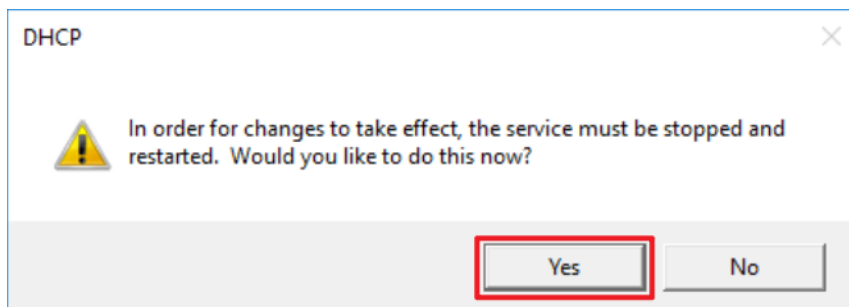
(3) On the General tab, verify that Enable “DHCP audit logging” is selected.



(4) On the Advanced tab, enter the audit log file path: **C:\Windows\System32\LogFiles\DHCP** and click “OK.”

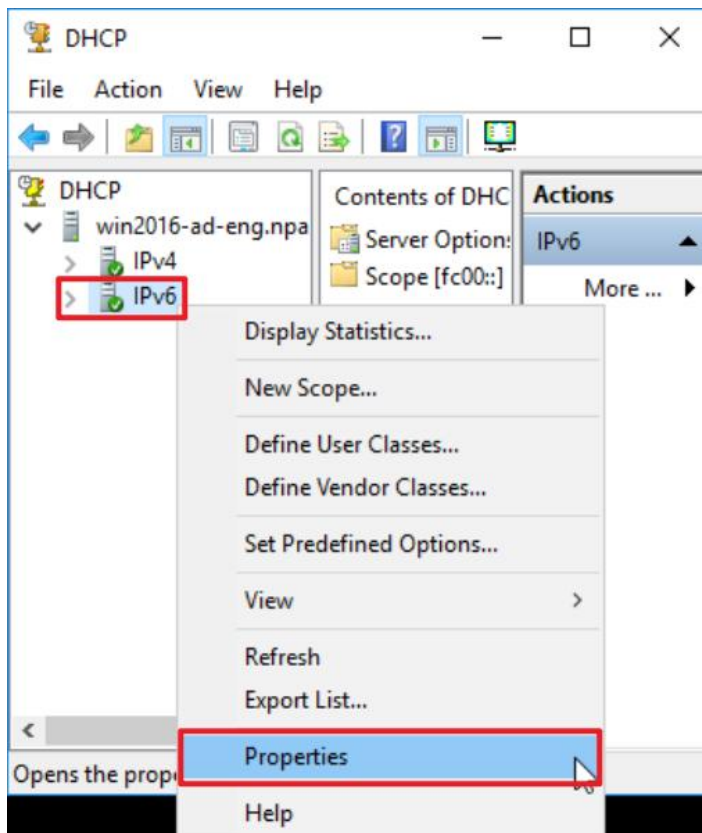


(5) Click Yes to restart the DHCP Server service.

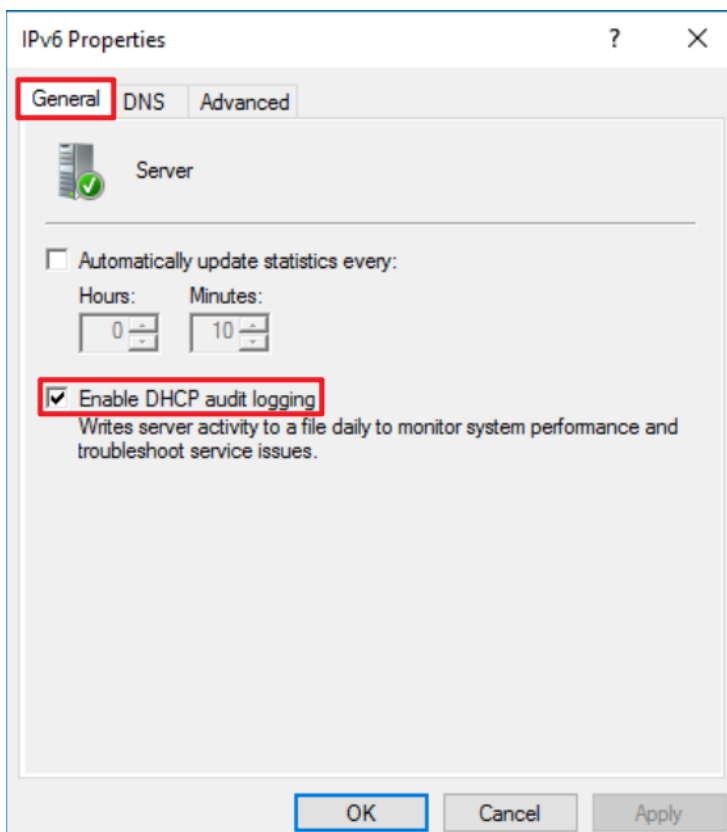


5.2 DHCP IPv6

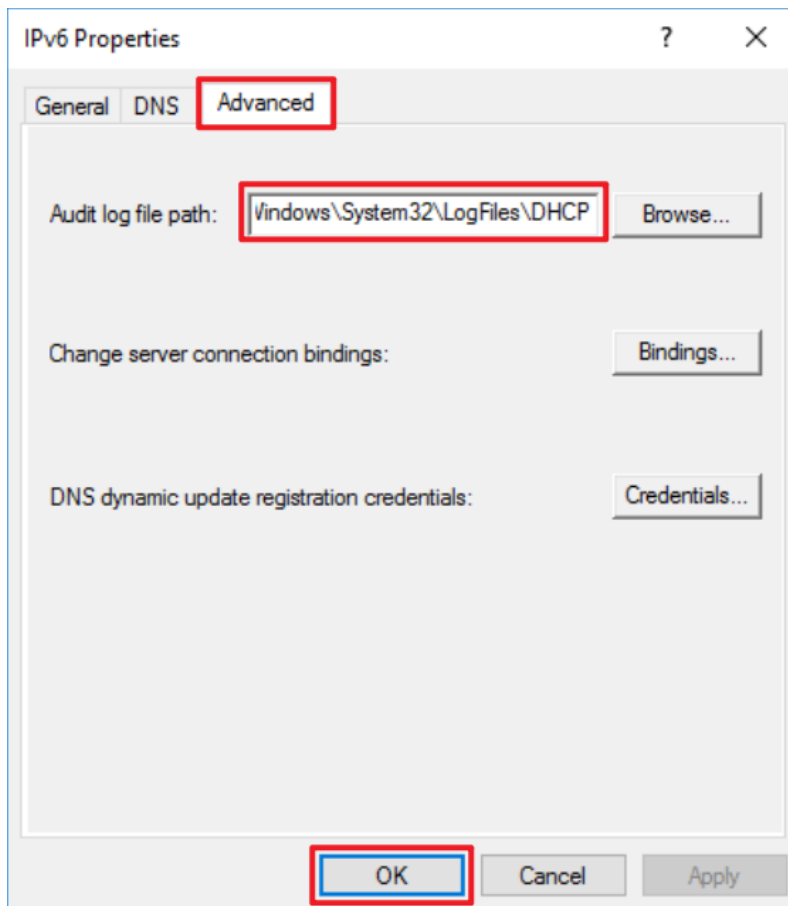
(1) Right-click “IPv6” → select “Properties.”



(2) On the General tab, verify that “Enable DHCP audit logging” is selected.



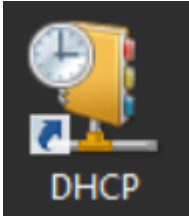
(3) On the Advanced tab, enter the audit log file path: **C:\Windows\System32\LogFiles\DHCP** and click “OK.”



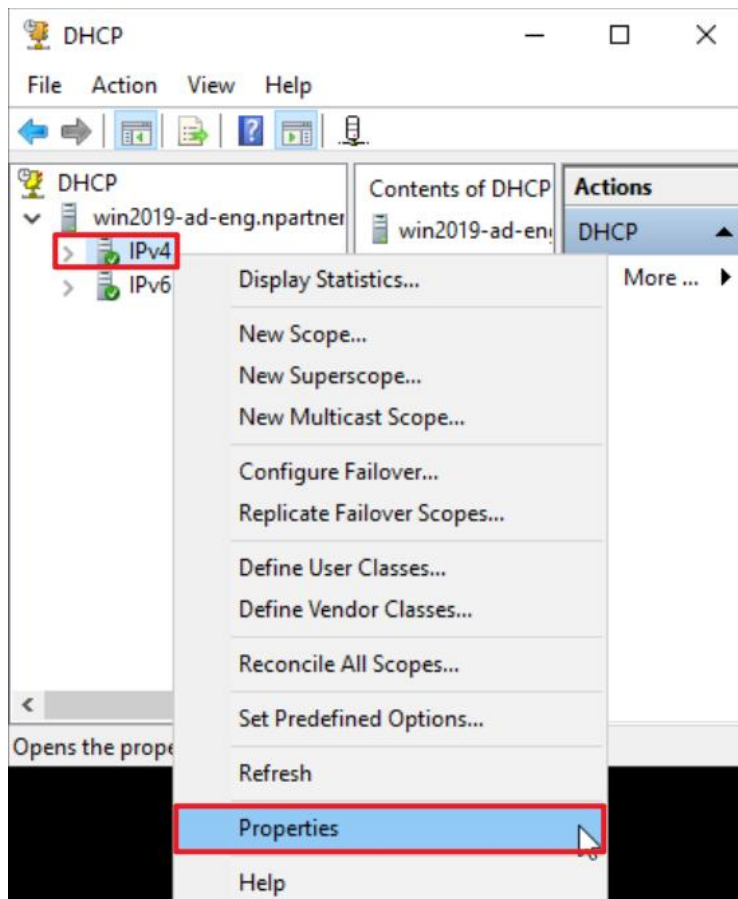
6. Windows Server 2019

6.1 DHCP IPv4

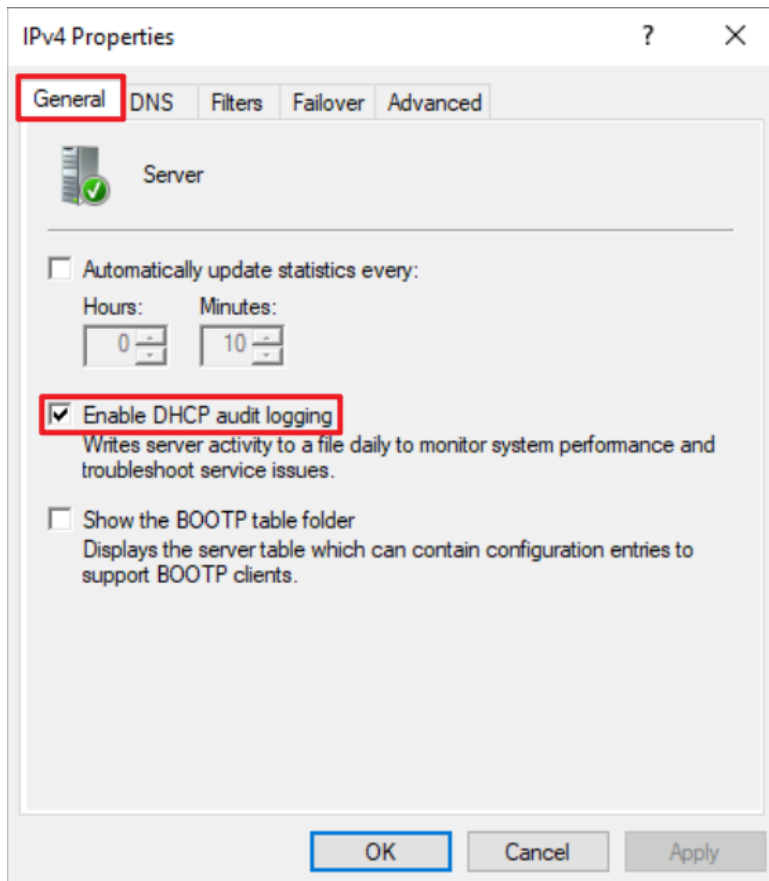
(1) Open DHCP.



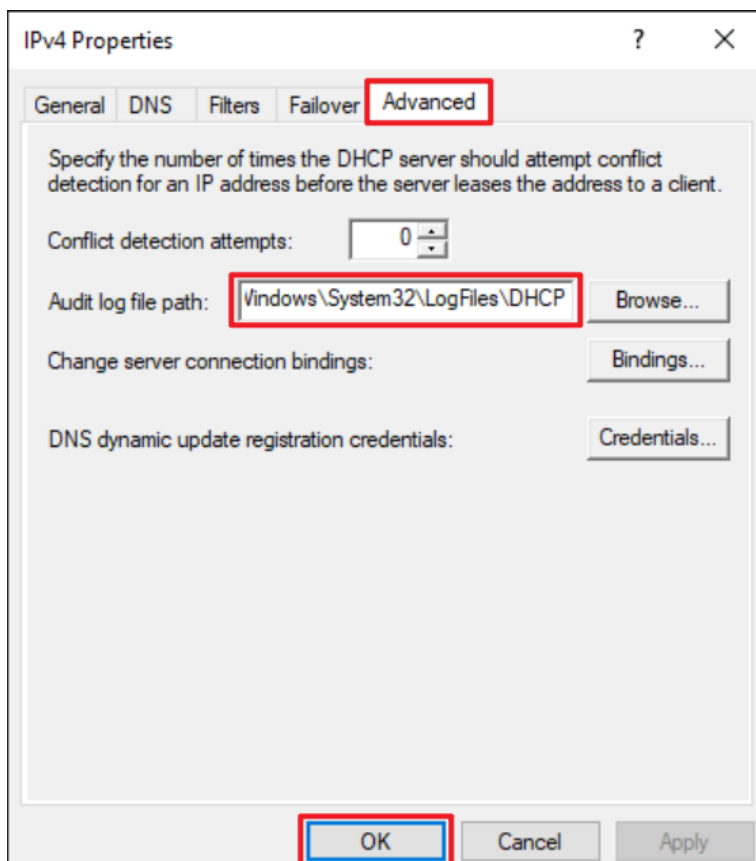
(2) Right-click "IPv4" → select "Properties."



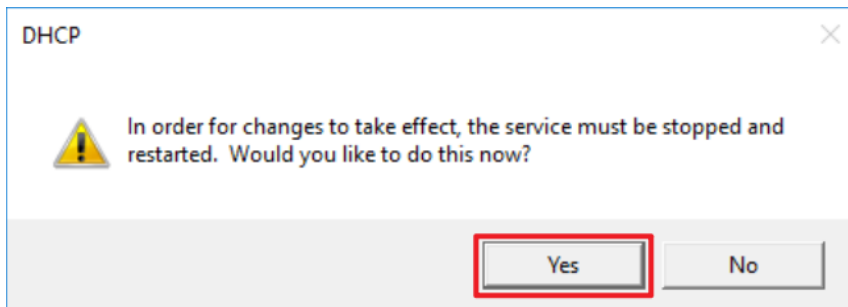
(3) On the General tab, verify that Enable “DHCP audit logging” is selected.



(4) On the Advanced tab, enter the audit log file path: **C:\Windows\System32\LogFiles\DHCP** and click “OK.”

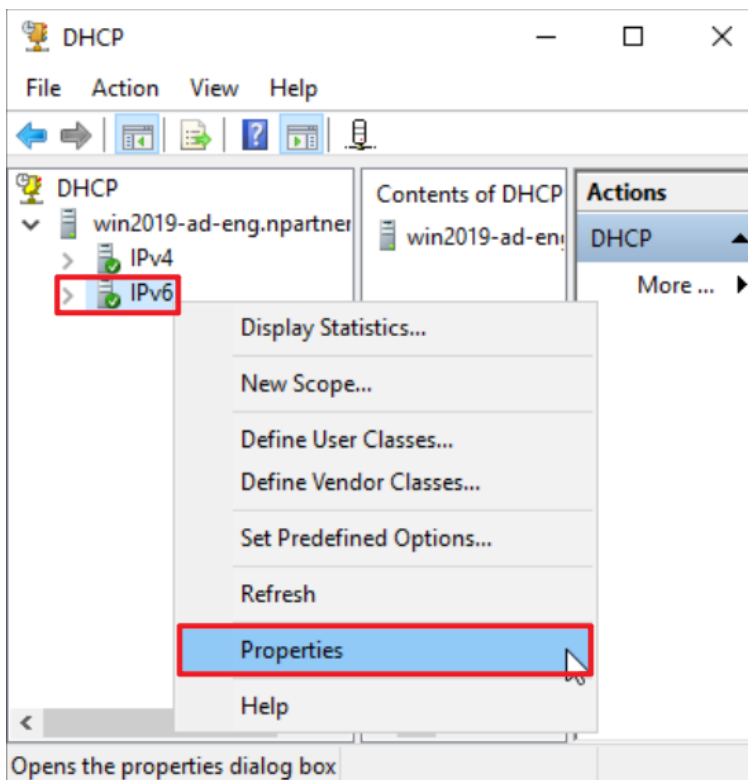


(5) Click Yes to restart the DHCP Server service.

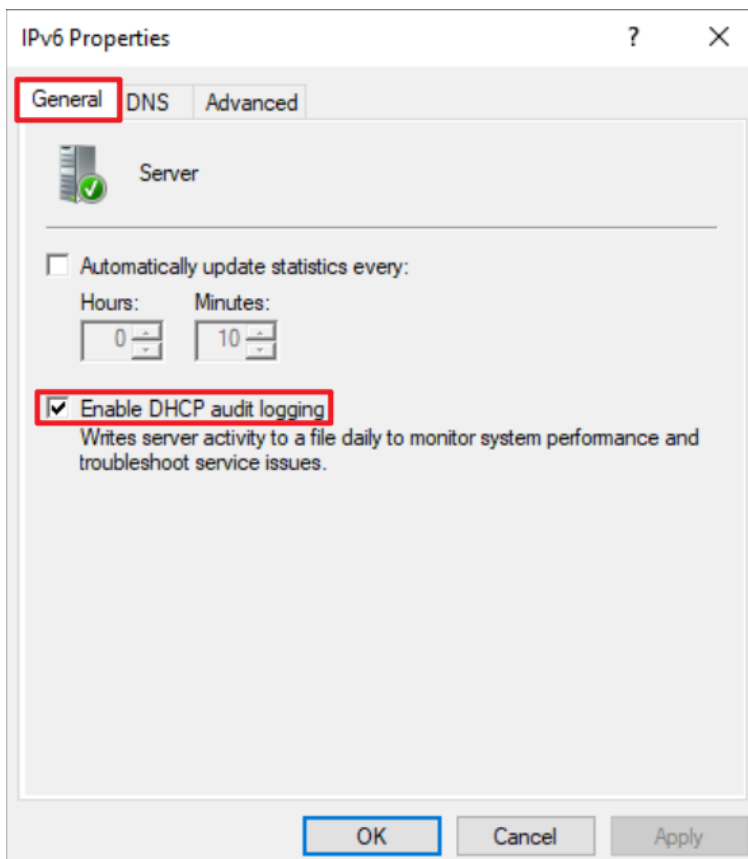


6.2 DHCP IPv6

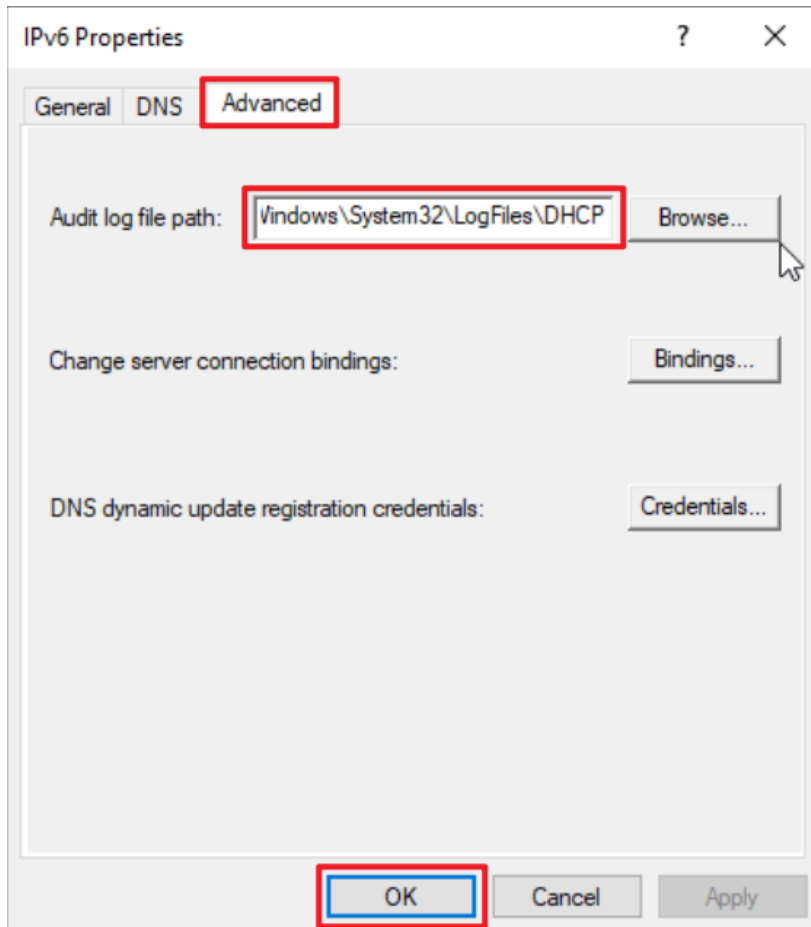
(1) Right-click “IPv6” → select “Properties.”



(2) On the General tab, verify that “Enable DHCP audit logging” is selected.



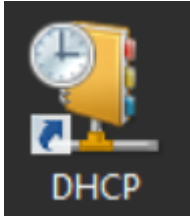
(3) On the Advanced tab, enter the audit log file path: **C:\Windows\System32\LogFiles\DHCP** and click “OK.”



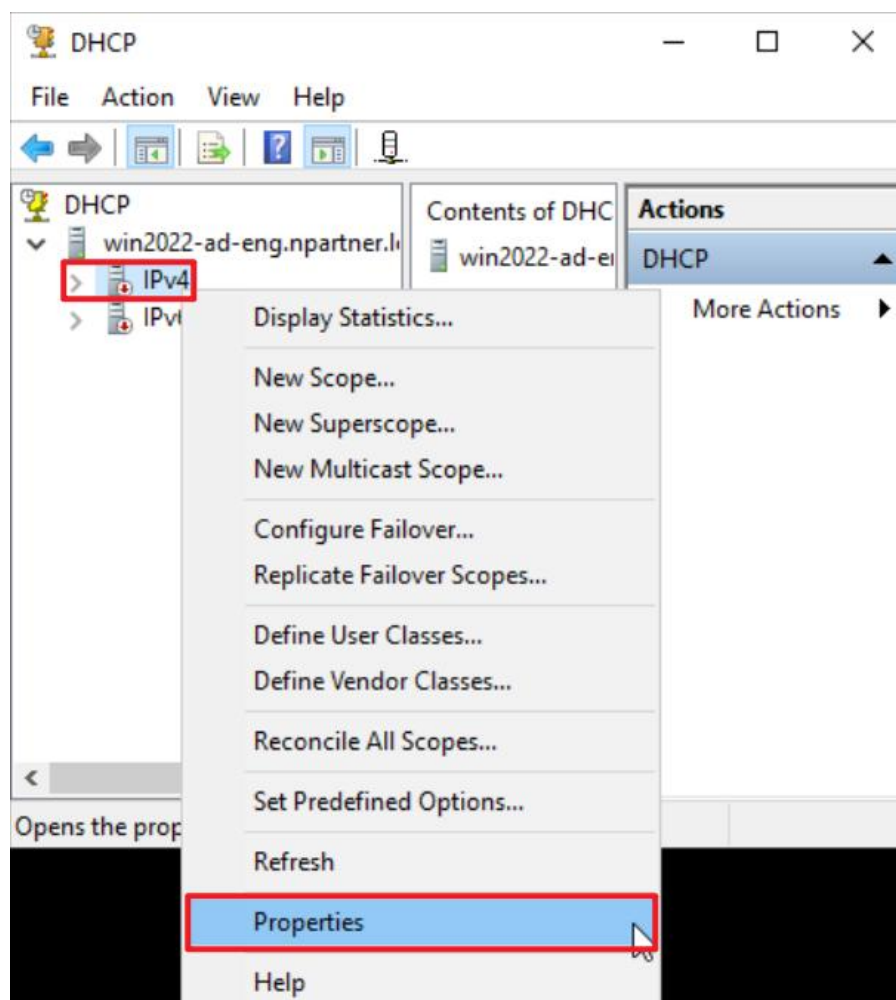
7. Windows Server 2022

7.1 DHCP IPv4

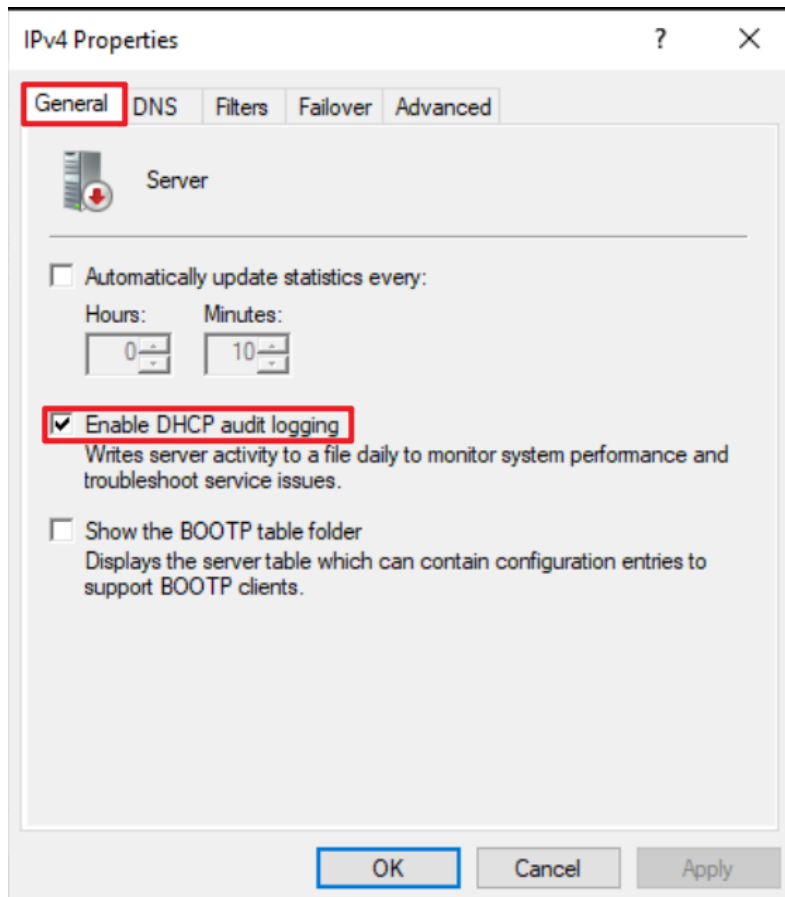
(1) Open DHCP.



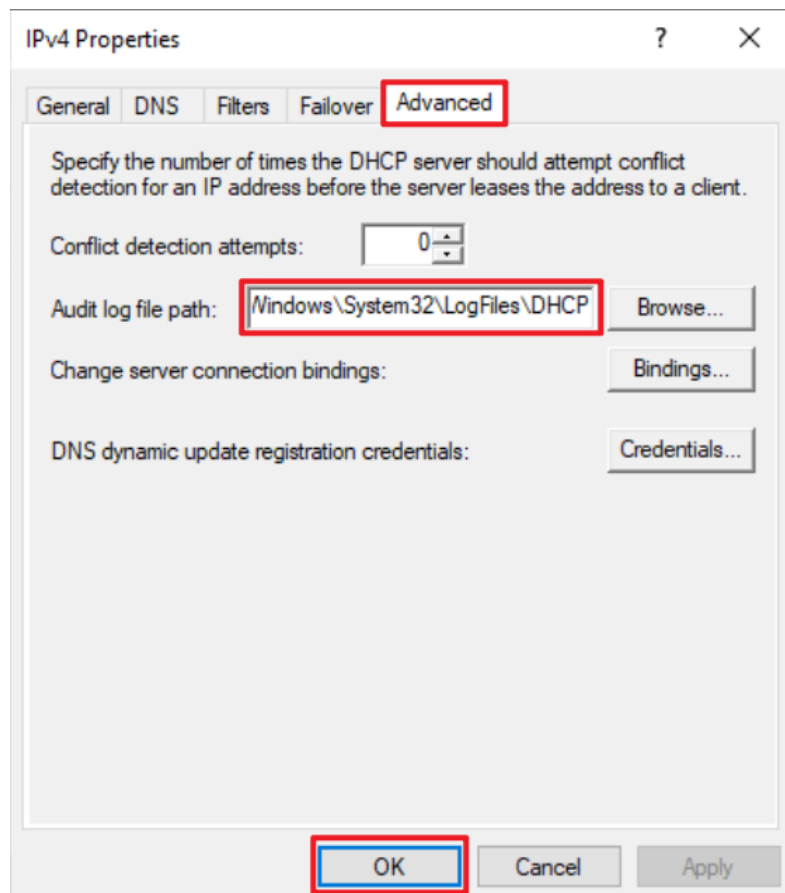
(2) Right-click "IPv4" → select "Properties."



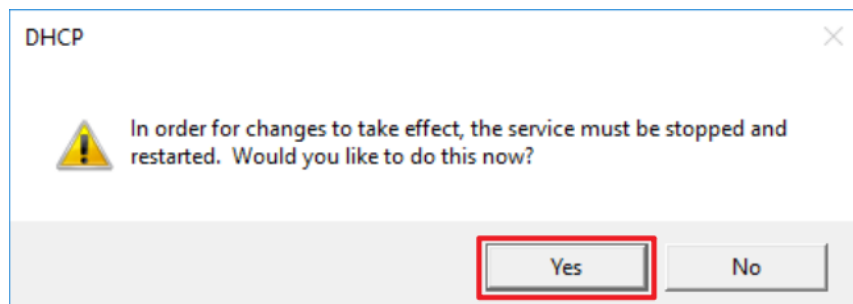
(3) On the General tab, verify that Enable “DHCP audit logging” is selected.



(4) On the Advanced tab, enter the audit log file path: **C:\Windows\System32\LogFiles\DHCP** and click “OK.”

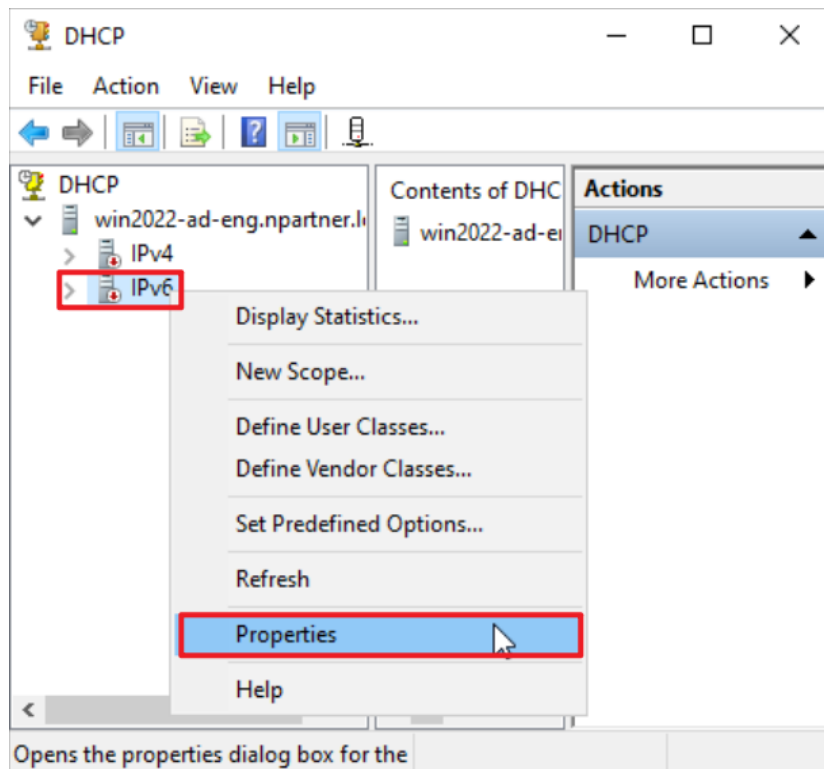


(5) Click Yes to restart the DHCP Server service.

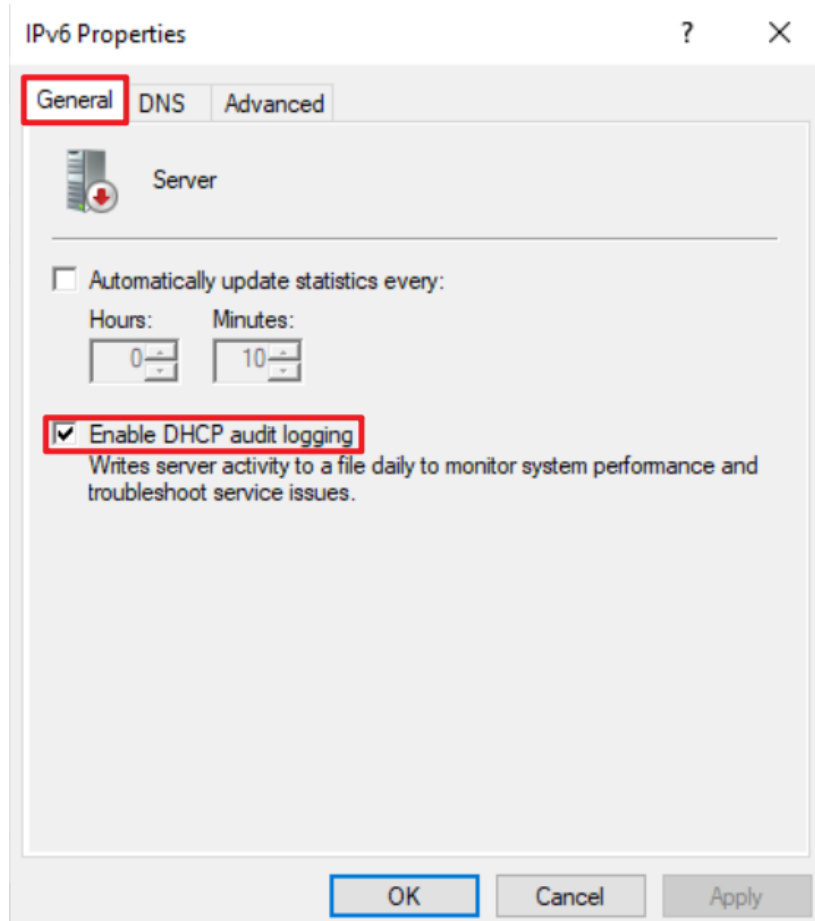


7.2 DHCP IPv6

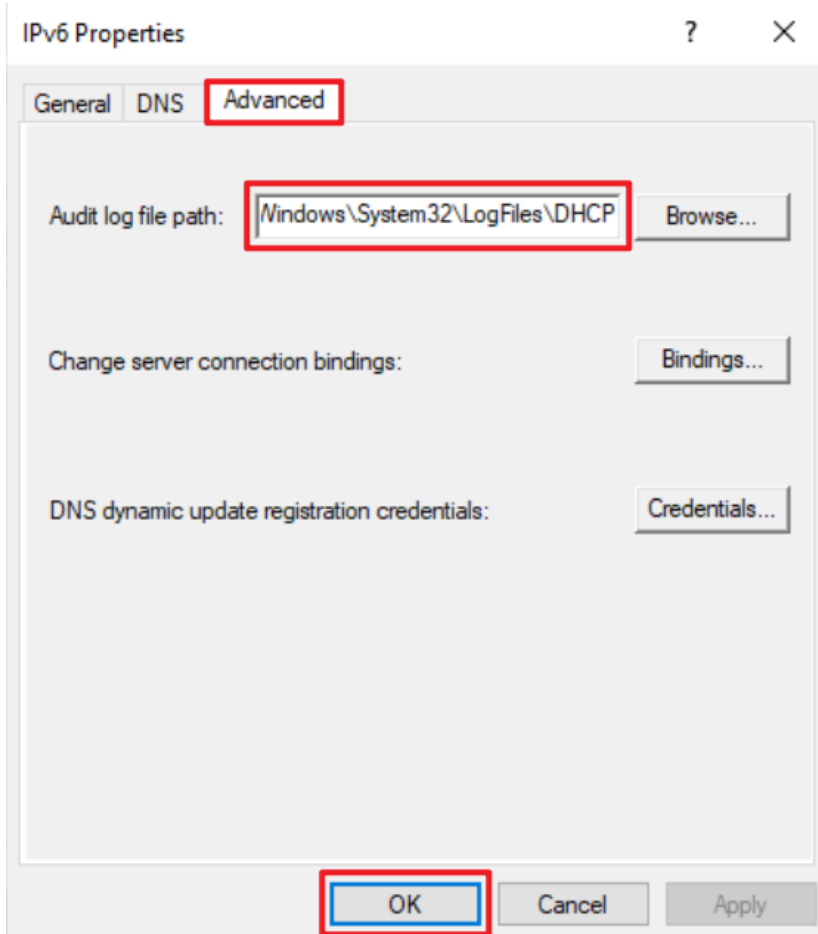
(1) Right-click “IPv6” → select “Properties.”



(2) On the General tab, verify that “Enable DHCP audit logging” is selected.



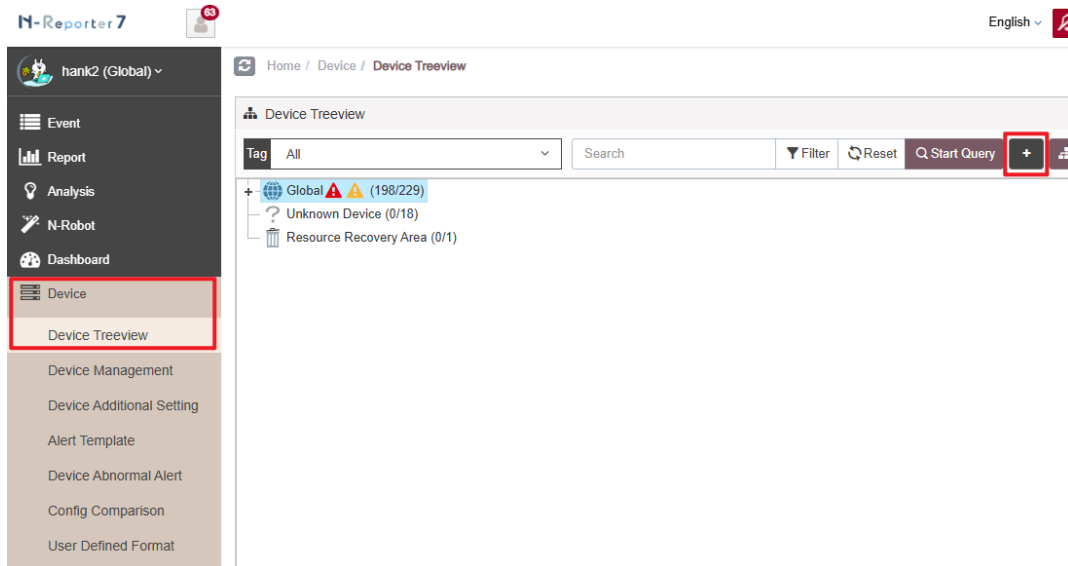
(3) On the Advanced tab, enter the audit log file path: **C:\Windows\System32\LogFiles\DHCP** and click “OK.”



8. N-Reporter

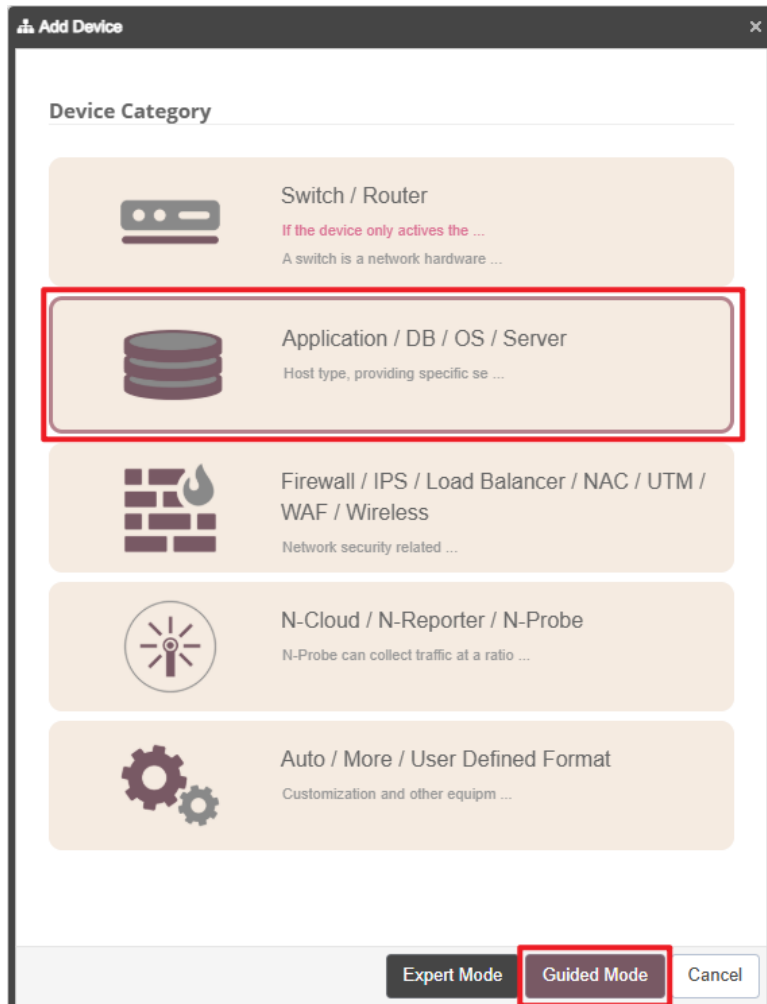
(1) Add a Windows DHCP device:

Go to “Device Management” → “Device Treeview” → click “Add.”



(2) Select the device type:

Choose “Application/DB/OS/Server” → click “Guided Mode.”



8.1 For Windows Server 2003 or earlier

(1) Basic Device Settings:

Enter the device name and IP address → For Syslog Data Format, select “Windows DHCP” → click “Next.”

Add Device - Basic Setting

Basic Setting

Machine Name *

WinDHCP-192.168.

IP *

192.168.

Domain *

Global

Syslog Format ⓘ ☐ Activate Full-text Search (FTS)

Windows DHCP

User Defined Syslog Format ⓘ +

Not Activated

SNMP Model ⓘ

Not Activated

Performance Monitoring Setting

Previous **Next** Cancel

(2) Syslog Settings

Set “Facility” to “(20) local use 4 (local4)” and “Encoding” to “BIG5” → click “Next.”

If “Raw Data Kept” is checked, the “Event Query” page will display raw data information.

Add Device - Syslog Setting

Syslog Setting

Facility ⓘ

(20) local use 4 (local4) ▼

Encoding

BIG5 ▼

Syslog Normalized Data Retention Days (Max) ⓘ

7-18250

Syslog Normalized Data Retention Days (At Least) ⓘ

1-18250

Raw Data Kept and Replied

☒ Raw Data Kept

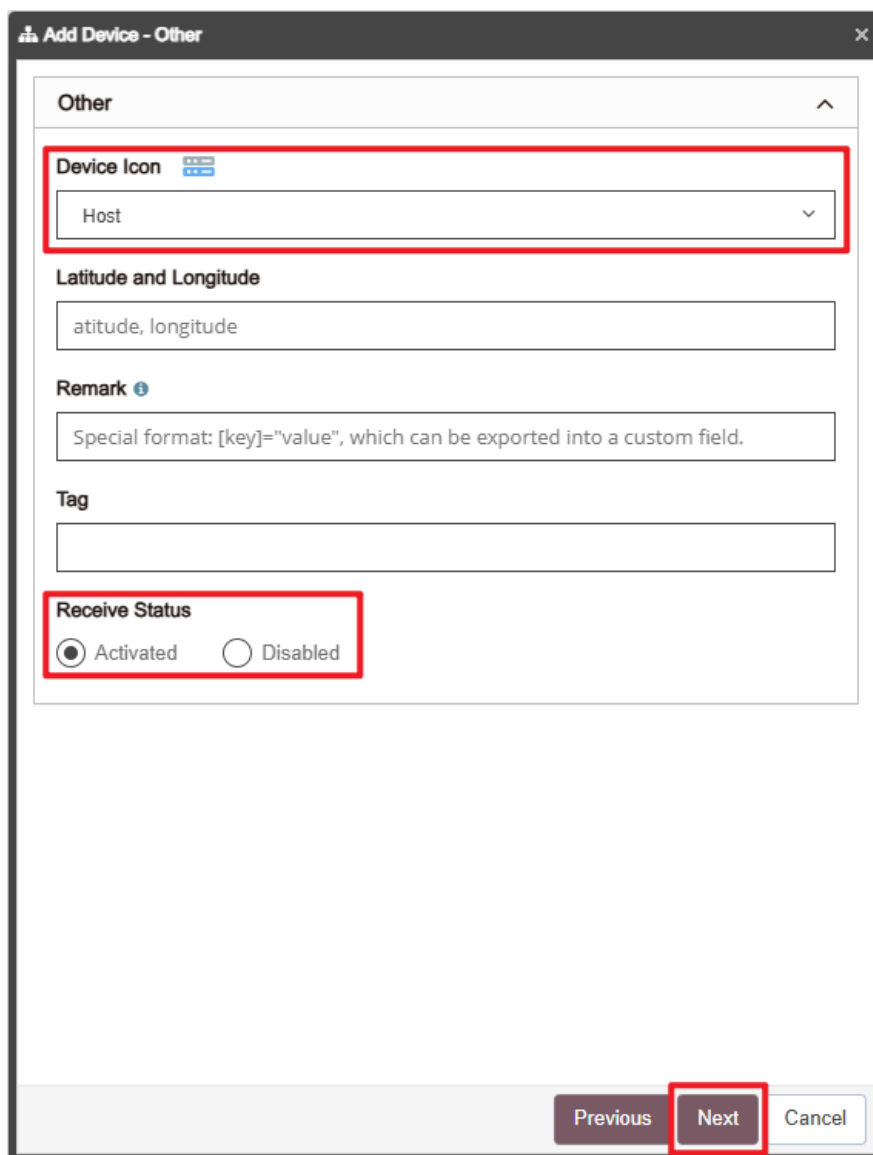
☐ Raw data format is adopted while Syslog relaying is activated in Threshold Report.

☐ The source IP will be kept in normalized data relaying

Previous **Next** Cancel

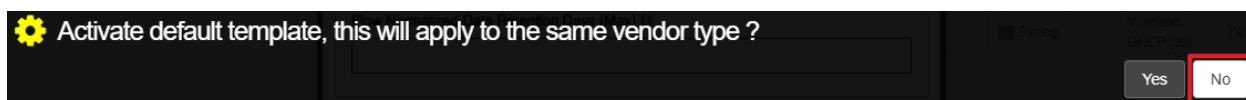
(3) Others

Set “Device Icon” to “Host” → Set “Receiving Status” to Activated” → click “Next” → Confirm.



The screenshot shows a dialog box titled "Add Device - Other". It contains several input fields: "Device Icon" (a dropdown menu with "Host" selected), "Latitude and Longitude" (a text field with placeholder "atitude, longitude"), "Remark" (a text field with placeholder "Special format: [key]='value', which can be exported into a custom field."), and "Tag" (an empty text field). Below these is the "Receive Status" section with two radio buttons: "Activated" (selected) and "Disabled". At the bottom right, there are three buttons: "Previous", "Next" (highlighted with a red box), and "Cancel".

Activate default templates for devices of the same vendor type, click “No.”



The screenshot shows a confirmation dialog box with a yellow gear icon and the text "Activate default template, this will apply to the same vendor type ?". There are two buttons at the bottom right: "Yes" and "No" (highlighted with a red box).

8.2 For Windows Server 2008 or later

(1) Basic Device Settings:

Enter the device name and IP address → For Syslog Data Format, select “Windows DHCP” → click “Next.”

Add Device - Basic Setting

Basic Setting

Machine Name *
WinDHCP-192.168.

IP *
192.168.

Domain *
Global

Syslog Format ⓘ ☐ Activate Full-text Search (FTS)
Windows DHCP

User Defined Syslog Format ⓘ
Not Activated

SNMP Model ⓘ
Not Activated

Performance Monitoring Setting ▼

Previous **Next** Cancel

(2) Syslog Settings

Set “Facility” to “(20) local use 4 (local4)” and “Encoding” to “UTF-8” → click “Next.”

If “Raw Data Kept” is checked, the “Event Query” page will display raw data information.

Add Device - Syslog Setting

Syslog Setting

Facility ⓘ

(20) local use 4 (local4) ▼

Encoding

UTF-8 ▼

Syslog Normalized Data Retention Days (Max) ⓘ

7-18250

Syslog Normalized Data Retention Days (At Least) ⓘ

1-18250

Raw Data Kept and Replied

☒ Raw Data Kept

☐ Raw data format is adopted while Syslog relaying is activated in Threshold Report.

☐ The source IP will be kept in normalized data relaying

Previous **Next** Cancel

(3) Others

Set “Device Icon” to “Host” → Set “Receiving Status” to Activated” → click “Next” → Confirm.

The screenshot shows a dialog box titled "Add Device - Other". It contains several input fields: "Device Icon" (a dropdown menu with "Host" selected), "Latitude and Longitude" (a text field with "atitude, longitude" entered), "Remark" (a text field with "Special format: [key]='value', which can be exported into a custom field." entered), and "Tag" (an empty text field). Below these fields is the "Receive Status" section, which has two radio buttons: "Activated" (selected) and "Disabled". At the bottom of the dialog, there are three buttons: "Previous", "Next" (highlighted with a red box), and "Cancel".

Activate default templates for devices of the same vendor type, click “No.”

The screenshot shows a confirmation dialog box with a yellow gear icon and the text "Activate default template, this will apply to the same vendor type ?". There are two buttons at the bottom: "Yes" and "No" (highlighted with a red box).

9. Troubleshooting

9.1 Adjusting the DHCP Log File Size

(1) Open “Windows PowerShell.”



(2) Enter the command below to view the DHCP Server audit log settings:

```
PS C:\> Get-DhcpServerAuditLog
```

A screenshot of a Windows PowerShell window titled 'Administrator: Windows PowerShell'. The command 'Get-DhcpServerAuditLog' has been executed, and the output is displayed as follows:

```
Path           : C:\Windows\System32\LogFiles\DHCP
Enable         : True
MaxMBFileSize   : 70
DiskCheckInterval : 50
MinMBDiskSpace  : 20
```

The prompt 'PS C:\>' is visible at the bottom.

(3) Enter the command below to set the DHCP log file size:

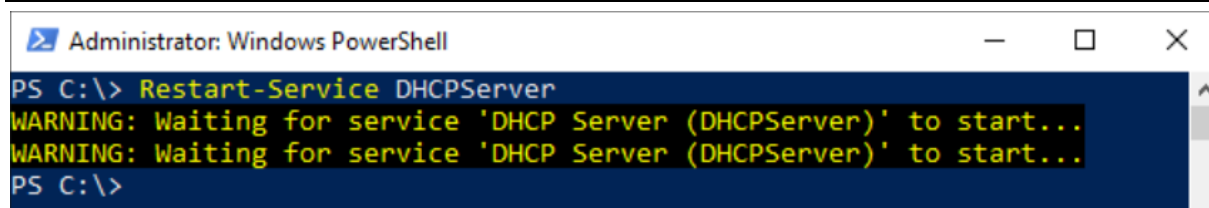
Parameter: -MaxMBFileSize 700

700 MB ÷ 7 days = maximum 100 MB per file

A screenshot of a Windows PowerShell window titled 'Administrator: Windows PowerShell'. The command 'Set-DhcpServerAuditLog -MaxMBFileSize 700' has been entered. Below the command, a yellow warning message is displayed: 'WARNING: Please restart the DHCP server service on WIN2022-AD-ENG for the new setting to take effect.' The prompt 'PS C:\>' is visible at the bottom.

(4) Enter the command below to restart the DHCP Server service:

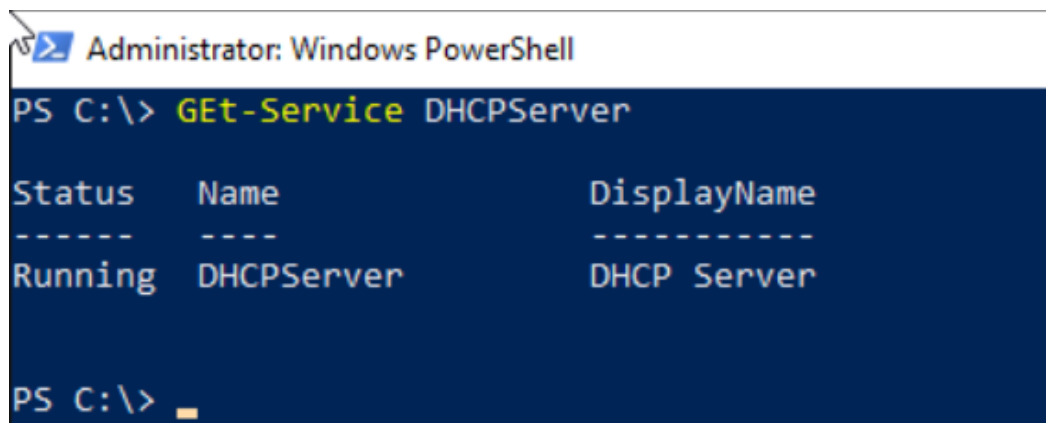
```
PS C:\> Restart-Service DHCPServer
```



```
Administrator: Windows PowerShell
PS C:\> Restart-Service DHCPServer
WARNING: Waiting for service 'DHCP Server (DHCPServer)' to start...
WARNING: Waiting for service 'DHCP Server (DHCPServer)' to start...
PS C:\>
```

(5) Enter the command below to check the DHCP Server service:

```
PS C:\> Get-Service DHCPServer
```



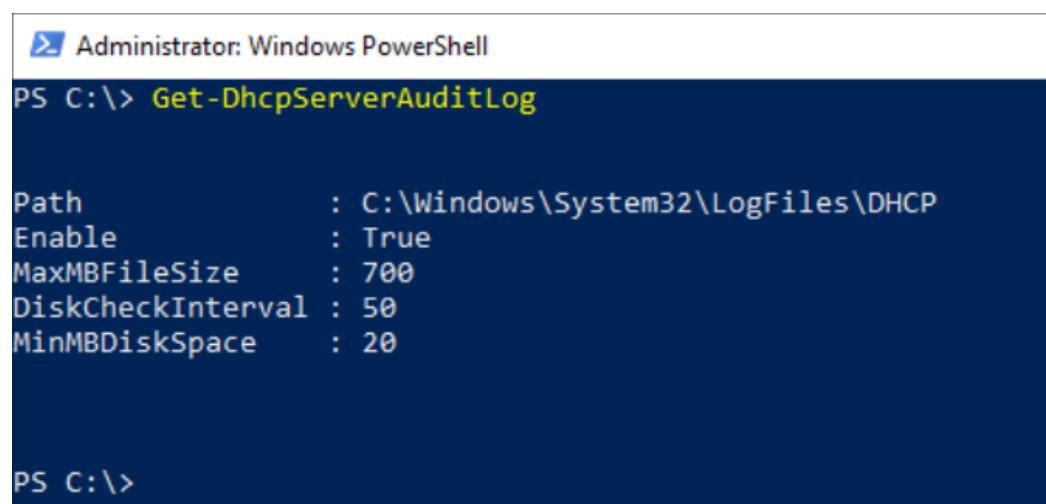
```
Administrator: Windows PowerShell
PS C:\> Get-Service DHCPServer

Status      Name            DisplayName
-----
Running     DHCPServer      DHCP Server

PS C:\>
```

(6) Enter the command below to view the DHCP Server audit log settings again:

```
PS C:\> Get-DhcpServerAuditLog
```



```
Administrator: Windows PowerShell
PS C:\> Get-DhcpServerAuditLog

Path           : C:\Windows\System32\LogFiles\DHCP
Enable         : True
MaxMBFileSize  : 700
DiskCheckInterval : 50
MinMBDiskSpace : 20

PS C:\>
```



Tel : +886-4-23752865 Fax : +886-4-23757458

Sales Information : sales@npartner.com

Technical Support : support@npartner.com