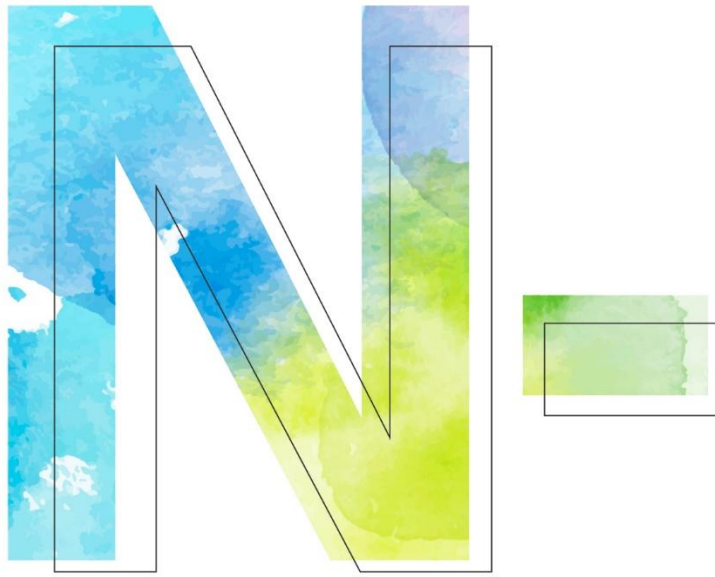




Partner

How to Configure Windows DNS Log

V009

2025/08/18





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 Group Policy Settings	5
1.2 Download NXLog Configuration File	7
1.3 NXLog Configuration	8
2. Windows Server 2008	14
3. Windows Server 2012	17
4. Windows Server 2016	20
5. Windows Server 2019	23
6. Windows Server 2022	26
7. N-Reporter	29
Contact	33

Preface

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

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

This document applies to Windows Server 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**



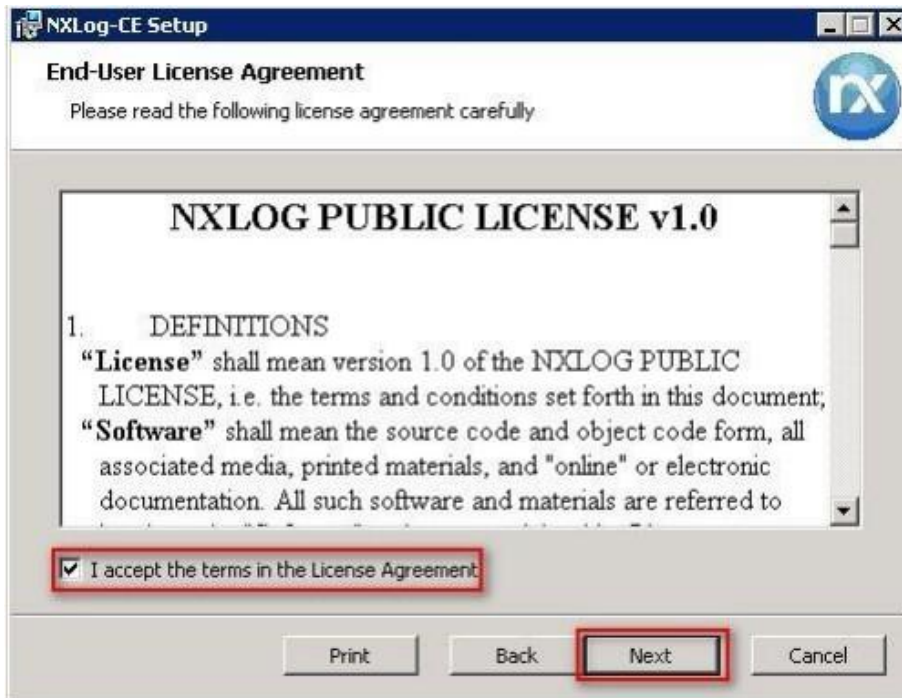
(2) Install NXLog

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

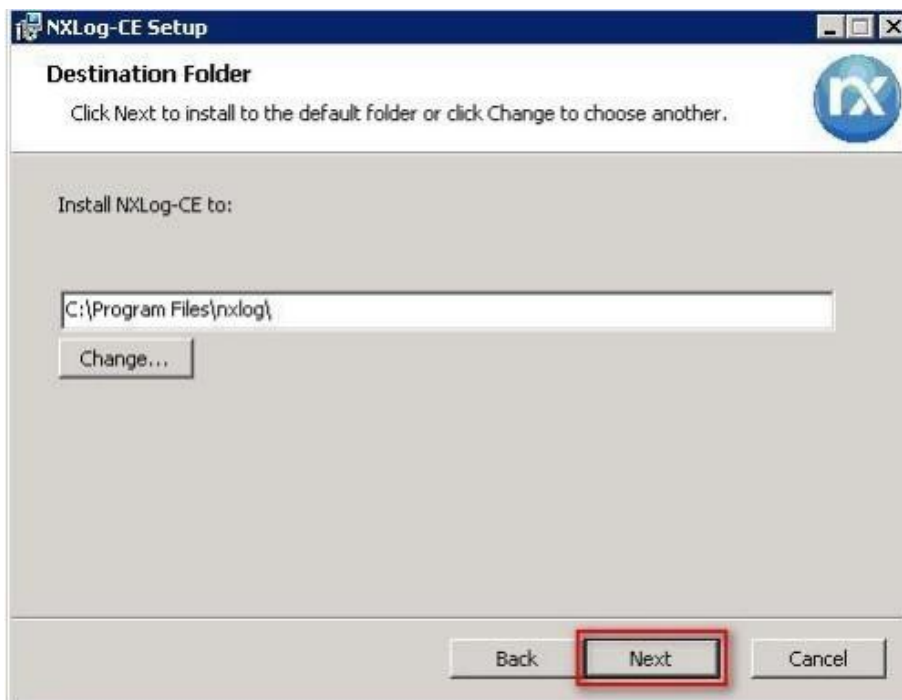
Double-click “**nxlog-ce-3.2.2329.msi.**”



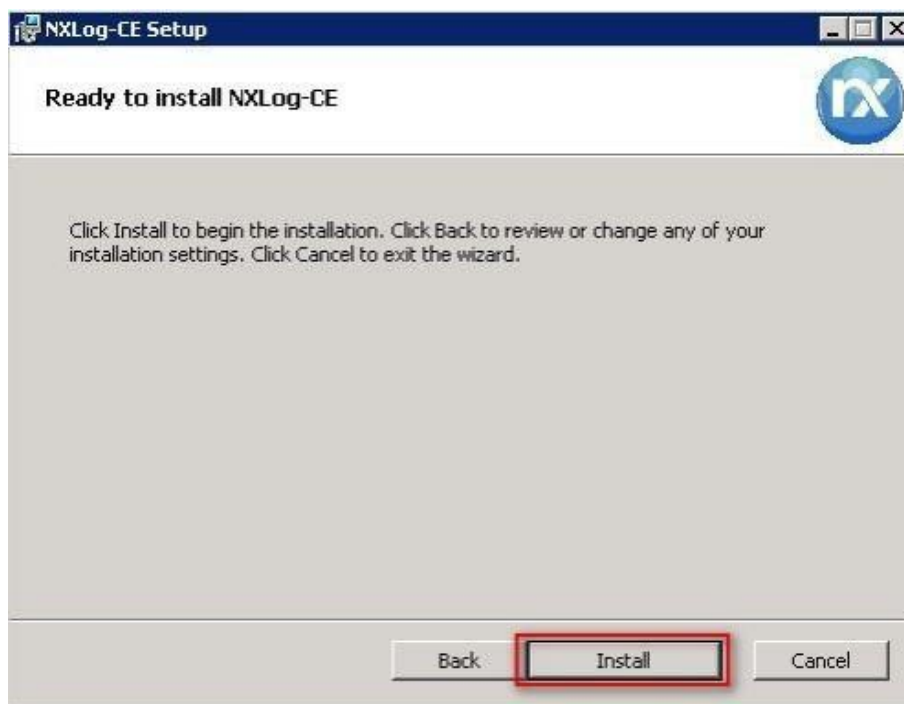
(3) Select "I accept the terms in the License Agreement," then click "Next."



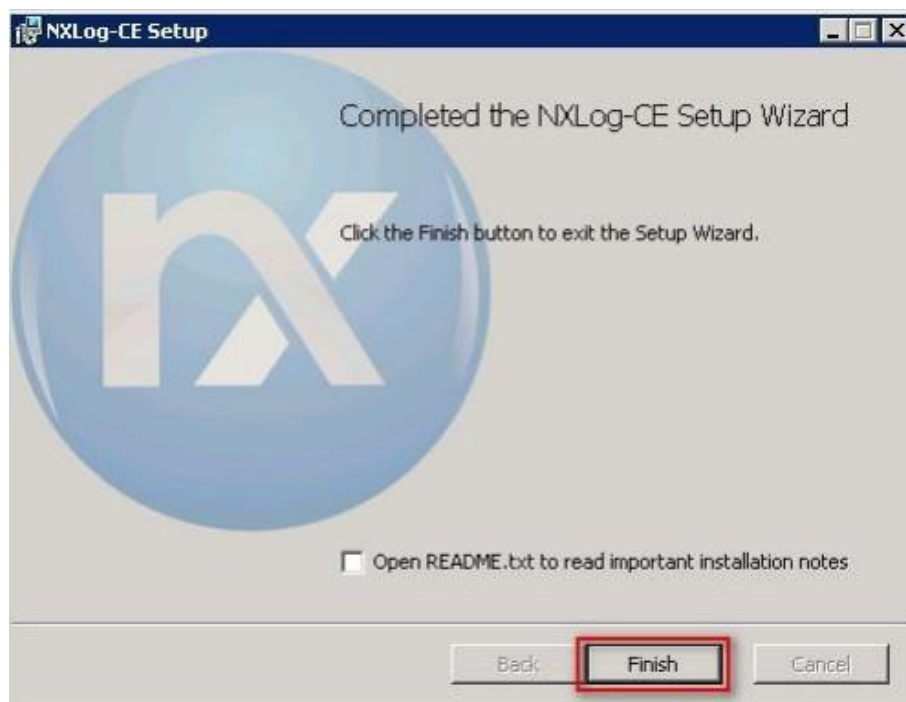
(4) Click "Next." (The default installation path is (C:\Program Files\nxlog\)).



(5) Click "Install."

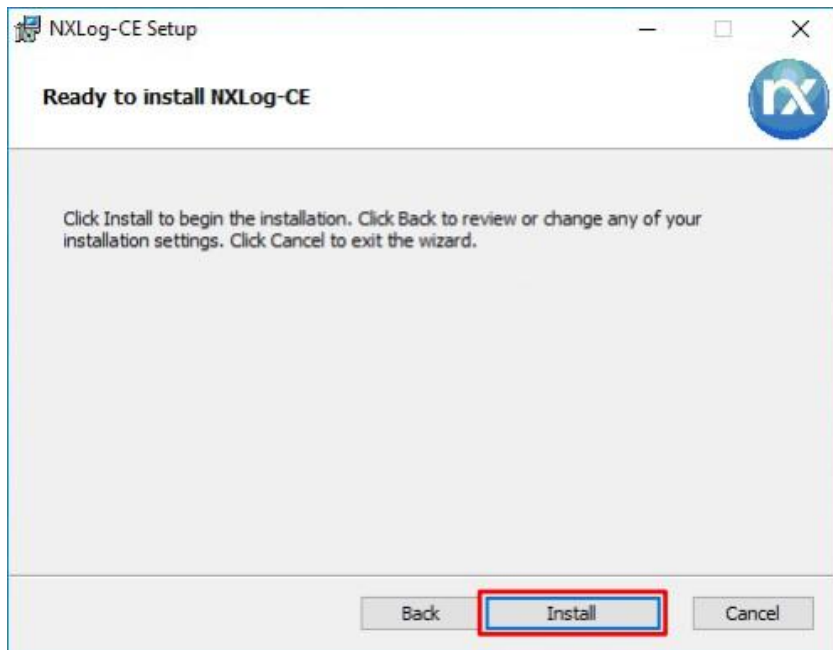


(6) Click "Finish."



<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.

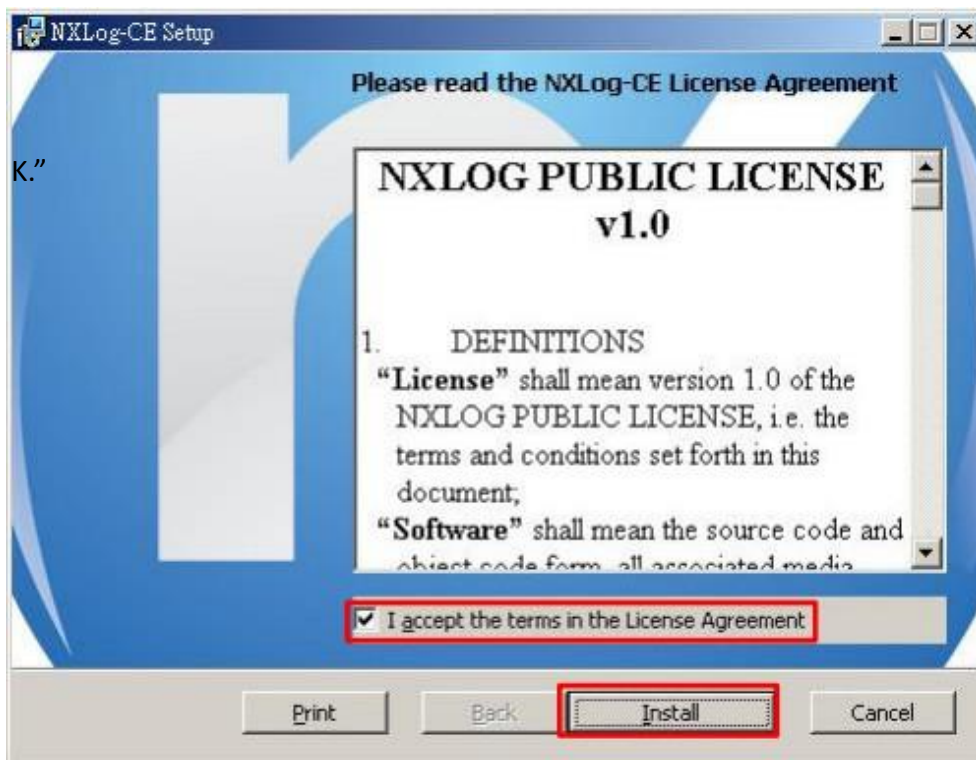


<2.3> For Windows 2000:

(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) Open “Windows PowerShell.”



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

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

```
PS C:\> Invoke-WebRequest -Uri`http://www.npartner.com/download/tech/nxlog_WinDNS.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 192.168.3.88
define DnsPath C:\windows\System32\LogFiles\DNS
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 DNS log file use the following:
<Input in_dnslog>
Module im_file
File '%DnsPath%\dns.log'
ReadFromLast TRUE
SavePos TRUE
Exec if $raw_event !~ /^\/d/ drop();
</Input>

<Output out_dnslog>
Module om_udp
Host %NCloud%
Port 514
Exec $syslogFacilityvalue = 19;
Exec if $raw_event =~ /^\/d+\/d+\/d+\s(上午\s)(\d+:\d+:\d+)\s(.+)/ $raw_event = $1 + ' ' + $3 + 'AM ' + $4;
Exec if $raw_event =~ /^\/d+\/d+\/d+\s(下午\s)(\d+:\d+:\d+)\s(.+)/ $raw_event = $1 + ' ' + $3 + 'PM ' + $4;
Exec $raw_event = "winDNS [Info]: " + $raw_event;
Exec to_syslog_bsd();
</Output>

<Route dnslog>
Path in_dnslog => out_dnslog
</Route>
```

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

```
define NCloud 192.168.8.4
define DnsPath C:\Windows\System32\LogFiles\DNS
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 DNS log file use the following:

```
<Input in_dnslog>
```

```

Module im_file
File '%DnsPath%\dns.log'
SavePos TRUE
ReadFromLast TRUE
</Input>

<Output out_dnslog>
Module om_udp
Host %NCloud%
Port 514
Exec $SyslogFacilityValue = 19;
Exec if $raw_event =~ /^(d+\d+\d+)\s(上午\s)(d+\.d+\.d+)\s)(.+)/ $raw_event = $1 + ' ' + $3 + 'AM ' + $4;
Exec if $raw_event =~ /^(d+\d+\d+)\s(下午\s)(d+\.d+\.d+)\s)(.+)/ $raw_event = $1 + ' ' + $3 + 'PM ' + $4;
Exec $raw_event = "WinDNS [Info]: " + $raw_event ;
Exec to_syslog_bsd();
</Output>

<Route dnslog>
Path in_dnslog => out_dnslog
</Route>

```

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

```
define NCloud 192.168.8.4
```

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

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

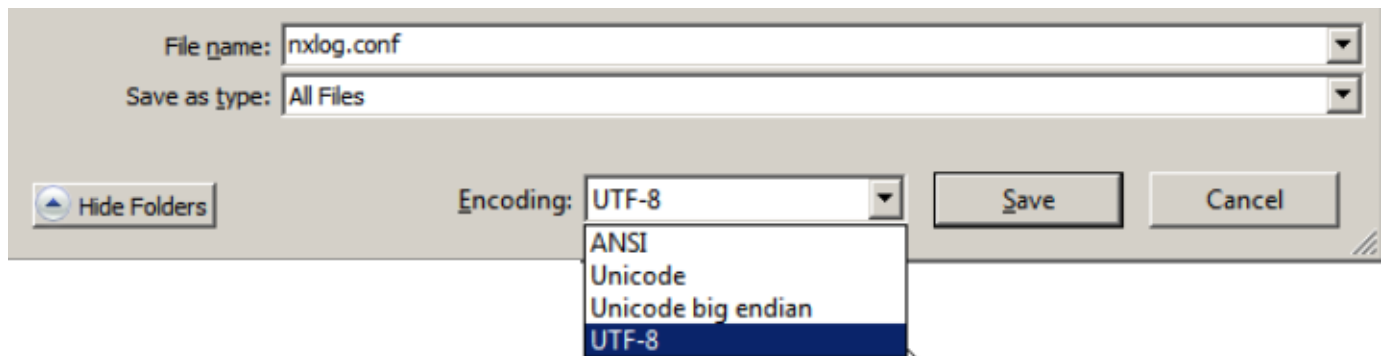
```
define ROOT C:\Program Files (x86)\nxlog
```

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

Sysnative is a redirected folder:

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

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.



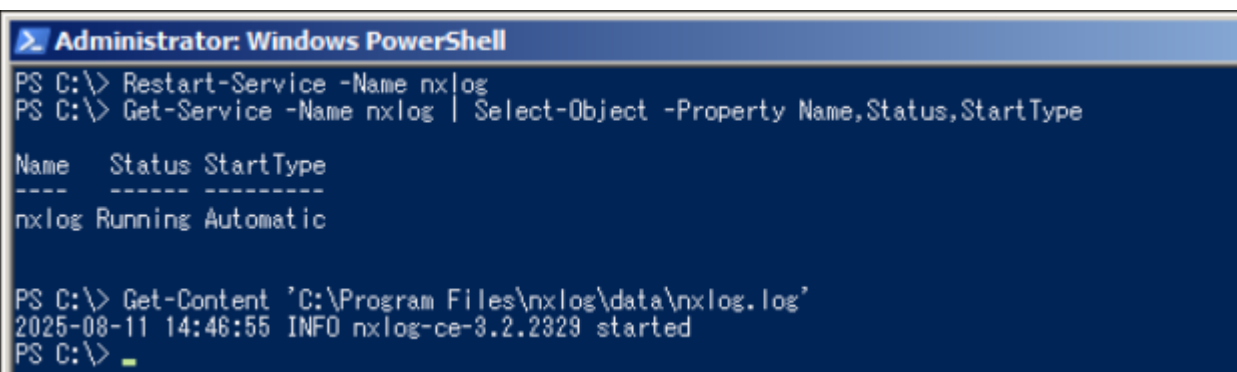
1.4 Starting the NXLog Service

(1) 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

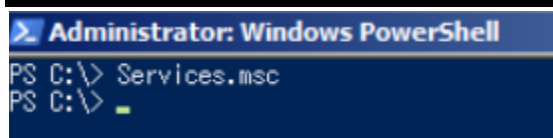
Name      Status StartType
-----
nxlog     Running Automatic

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:\> _
```

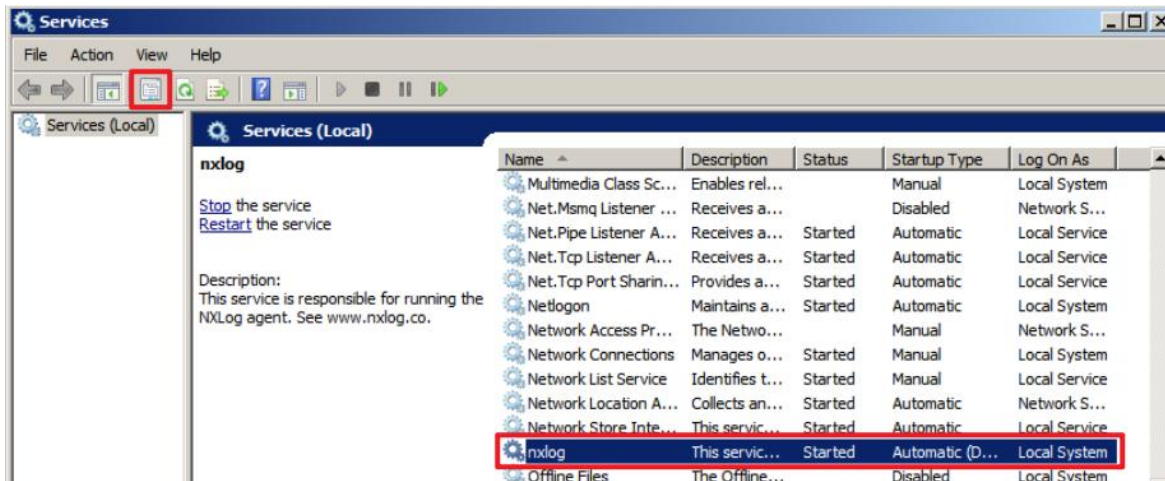
Note: This example is for a 64-bit operating system. For a 32-bit system, replace the highlighted text with: 'C:\Program Files(x86)\nxlog\conf\nxlog.conf'

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

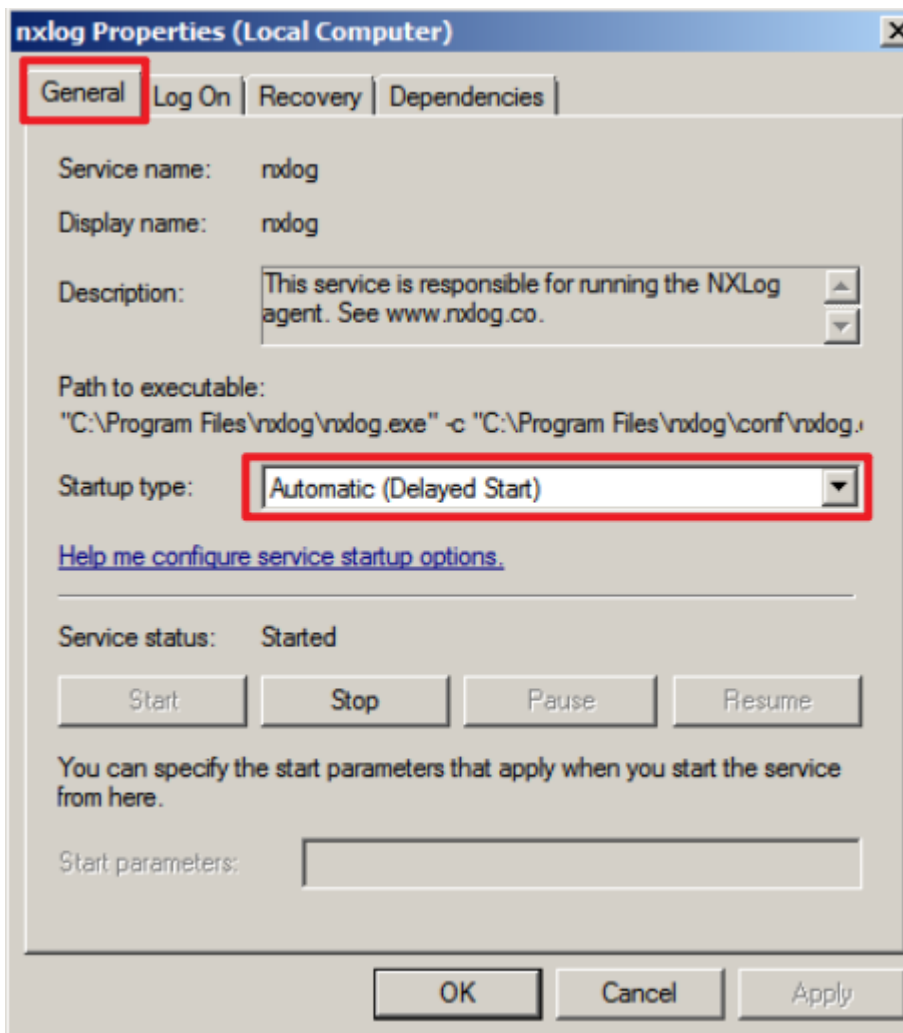
```
PS C:\> Services.msc
```



(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.”

The screenshot shows the 'nxlog Properties (Local Computer)' dialog box with the 'Recovery' tab selected. The 'Recovery' tab is highlighted with a red box. The 'First failure:', 'Second failure:', and 'Subsequent failures:' dropdown menus are all set to 'Restart the Service' and are also highlighted with a red box. The 'Reset fail count after:' is set to '1' days, and 'Restart service after:' is set to '1' minutes. The 'Enable actions for stops with errors.' checkbox is unchecked. The 'Run program:' section is empty. The 'OK' button at the bottom is highlighted with a red box.

nxlog Properties (Local Computer)

General | Log On | **Recovery** | Dependencies

Select the computer's response if this service fails. [Help me set up recovery actions.](#)

First failure: Restart the Service

Second failure: Restart the Service

Subsequent failures: Restart the Service

Reset fail count after: 1 days

Restart service after: 1 minutes

☐ Enable actions for stops with errors. Restart Computer Options...

Run program:

Program: Browse...

Command line parameters:

☐ Append fail count to end of command line (/fail=%1%)

OK Cancel Apply

2. Windows Server 2008

(1) Open “Windows PowerShell.”



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

```
PS C:\> New-Item -ItemType directory -Path C:\Windows\System32\LogFiles\DNS
```

```
PS C:\> Get-ChildItem -Path C:\Windows\System32\LogFiles
```

```
Administrator: Windows PowerShell
PS C:\> New-Item -ItemType directory -Path C:\Windows\System32\LogFiles\DNS

Directory: C:\Windows\System32\LogFiles

Mode                LastWriteTime         Length Name
----                -
d-----            8/11/2025   PM 05:31         DNS

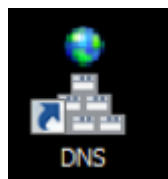
PS C:\> Get-ChildItem -Path C:\Windows\System32\LogFiles

Directory: C:\Windows\System32\LogFiles

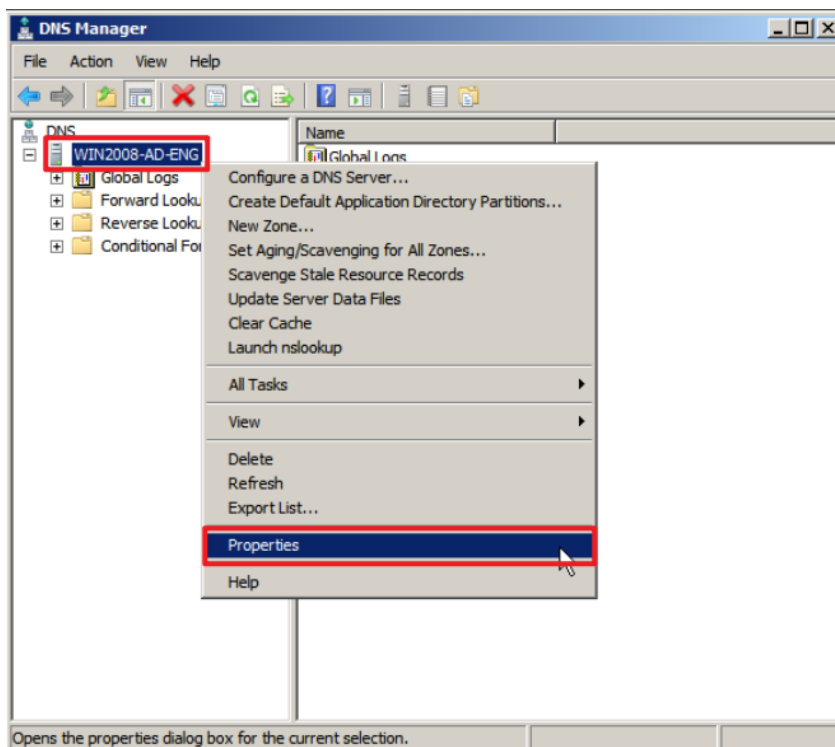
Mode                LastWriteTime         Length Name
----                -
d---s-             7/14/2009   PM 01:12         AIT
d-----            8/11/2025   PM 02:14        DHCP
d-----            8/11/2025   PM 05:31        DNS
d-----            7/14/2009   AM 10:34      Firewall
d-----            5/23/2024   AM 10:17      HTTPERR
d-----            8/11/2025   PM 02:20        Scm
d-----            4/11/2024   AM 11:27        SDM
d-----            5/22/2024   PM 06:01  Windows Portable Devices
d-----            7/14/2009   PM 12:49        WMI
d-----            7/14/2009   AM 10:36       WUDF

PS C:\> _
```

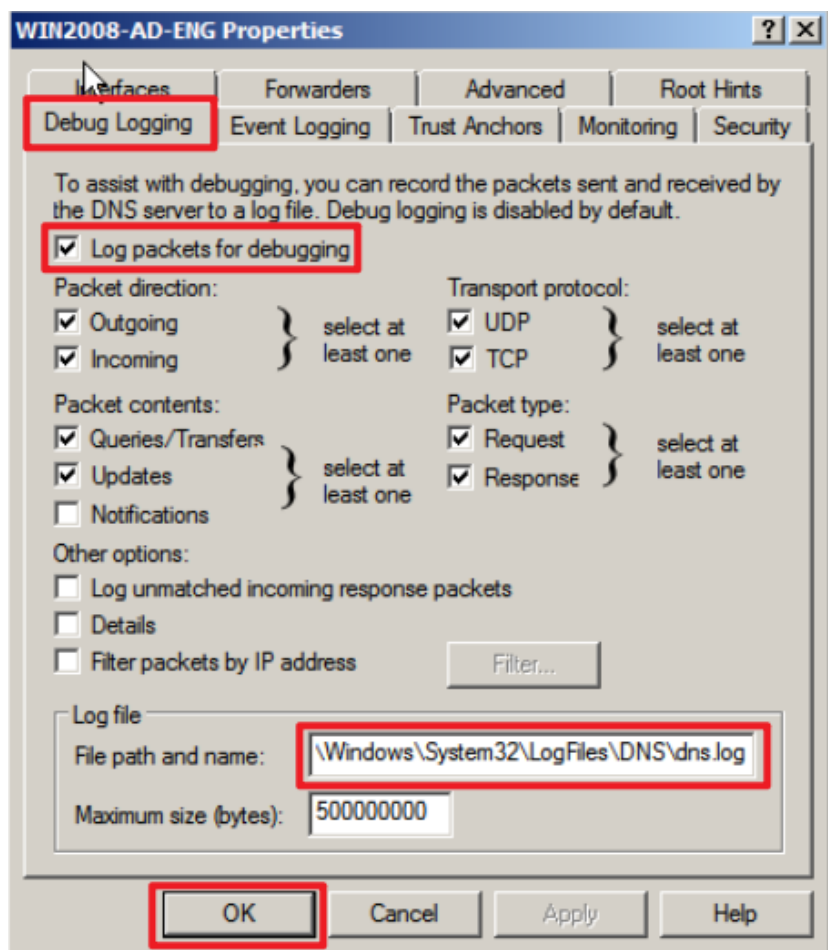
(3) Open DNS.



(4) Right-click the DNS server (the example here is **Win2008-AD-ENG**) → click “Properties.”



(5) On the “Debug Logging” tab → check “Log packets for debugging” → enter the “file path and name”:
C:\Windows\System32\LogFiles\DNS\dns.log and click “OK.”

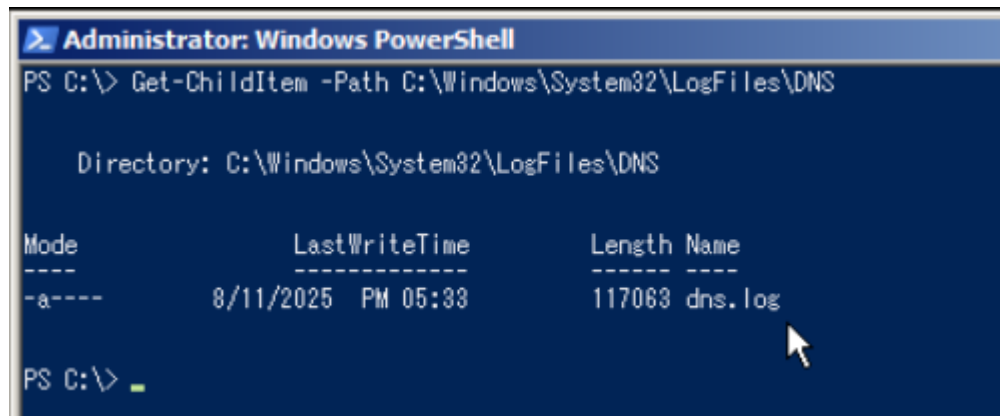


(6) Open “Windows PowerShell” again.



(7) Enter the command below to verify that the file **dns.log** has been created:

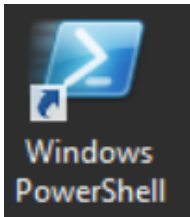
```
PS C:\> Get-ChildItem -Path C:\Windows\System32\LogFiles\DNS
```

The image shows a screenshot of an Administrator: Windows PowerShell terminal window. The command 'Get-ChildItem -Path C:\Windows\System32\LogFiles\DNS' has been executed. The output shows the directory 'C:\Windows\System32\LogFiles\DNS' and a table of files. The table has columns for Mode, LastWriteTime, Length, and Name. A single file 'dns.log' is listed with a length of 117068 bytes and a last write time of 8/11/2025 PM 05:33. A mouse cursor is pointing at the 'dns.log' file name.

Mode	LastWriteTime	Length	Name
-a----	8/11/2025 PM 05:33	117068	dns.log

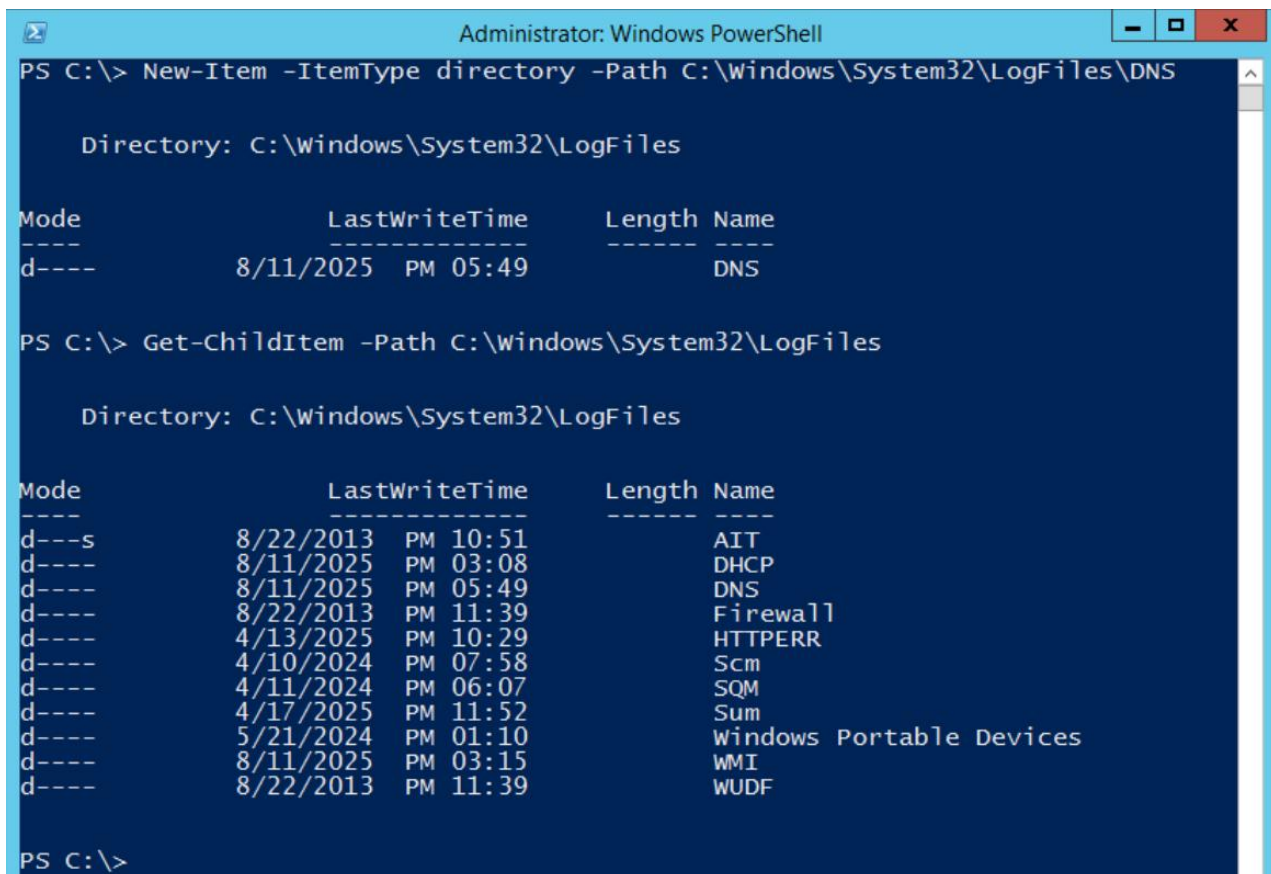
3. Windows Server 2012

(1) Open “Windows PowerShell.”



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

```
PS C:\> New-Item -ItemType directory -Path C:\Windows\System32\LogFiles\DNS
PS C:\> Get-ChildItem -Path C:\Windows\System32\LogFiles
```

A screenshot of a Windows PowerShell console window titled "Administrator: Windows PowerShell". The window shows the execution of two commands. The first command, "New-Item -ItemType directory -Path C:\Windows\System32\LogFiles\DNS", creates a new directory named "DNS" in the "C:\Windows\System32\LogFiles" path. The second command, "Get-ChildItem -Path C:\Windows\System32\LogFiles", lists the contents of the "C:\Windows\System32\LogFiles" directory. The output shows a table of files and directories, including "AIT", "DHCP", "DNS", "Firewall", "HTTPERR", "Scm", "SQM", "Sum", "Windows Portable Devices", "WMI", and "WUDF".

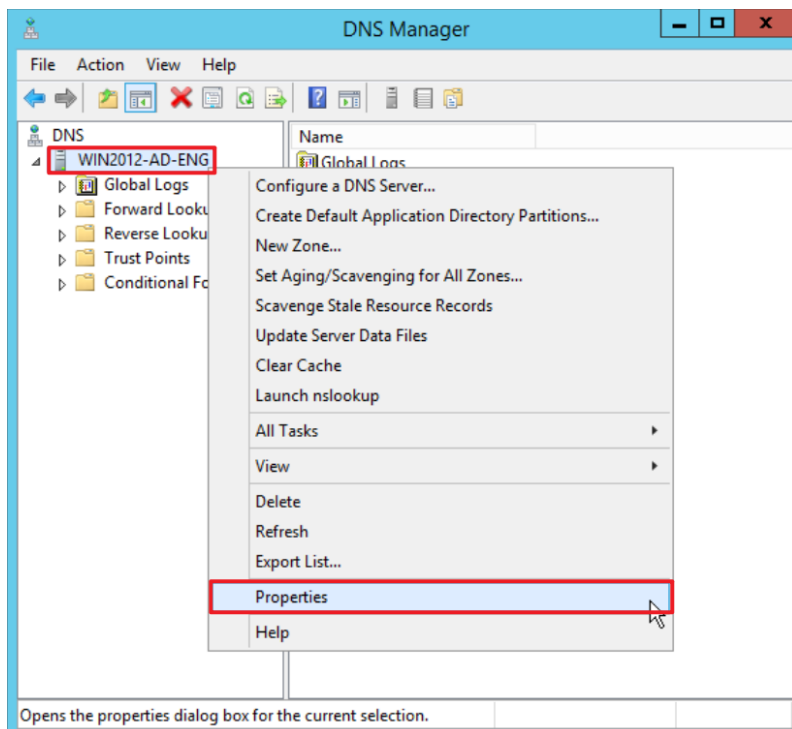
Mode	LastWriteTime	Length	Name
d----	8/11/2025 PM 05:49		DNS

Mode	LastWriteTime	Length	Name
d---s	8/22/2013 PM 10:51		AIT
d----	8/11/2025 PM 03:08		DHCP
d----	8/11/2025 PM 05:49		DNS
d----	8/22/2013 PM 11:39		Firewall
d----	4/13/2025 PM 10:29		HTTPERR
d----	4/10/2024 PM 07:58		Scm
d----	4/11/2024 PM 06:07		SQM
d----	4/17/2025 PM 11:52		Sum
d----	5/21/2024 PM 01:10		Windows Portable Devices
d----	8/11/2025 PM 03:15		WMI
d----	8/22/2013 PM 11:39		WUDF

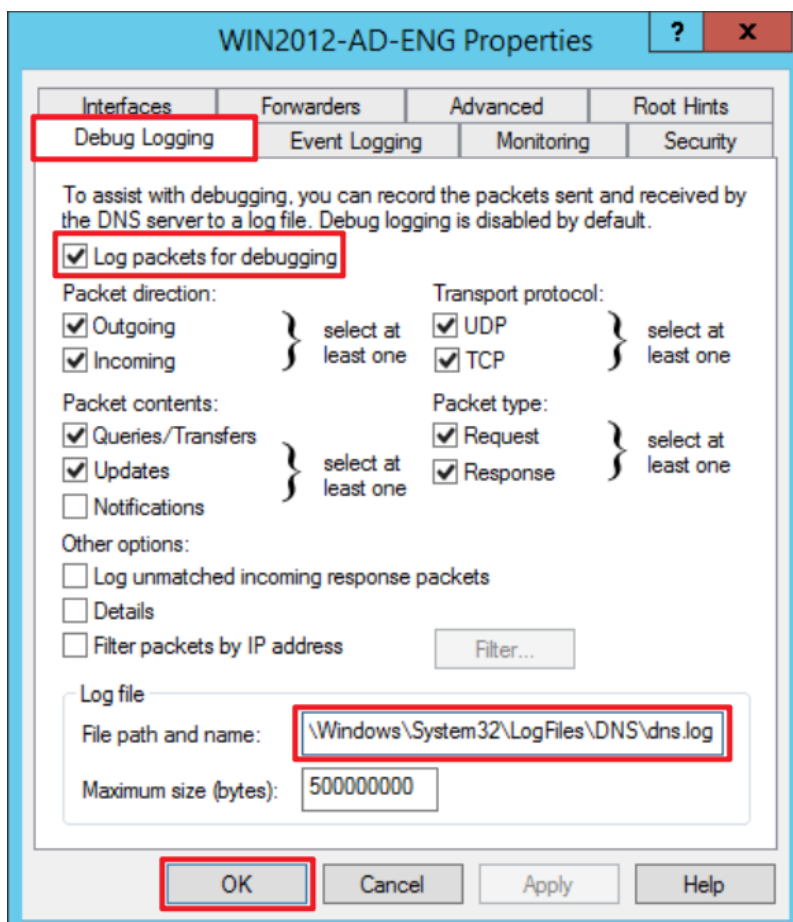
(3) Open DNS.



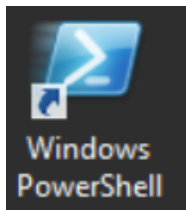
(4) Right-click the DNS server (the example here is **Win2012-AD-ENG**) → click “Properties.”



(5) On the “Debug Logging” tab → check “Log packets for debugging” → enter the “file path and name”:
C:\Windows\System32\LogFiles\DNS\dns.log and click “OK.”



(6) Open “Windows PowerShell” again.



(7) Enter the command below to verify that the file **dns.log** has been created:

```
PS C:\> Get-ChildItem -Path C:\Windows\System32\LogFiles\DNS
```

A screenshot of a Windows PowerShell window titled "Administrator: Windows PowerShell". The command entered is "PS C:\> Get-ChildItem -Path C:\Windows\System32\LogFiles\DNS". The output shows the directory "C:\Windows\System32\LogFiles\DNS" and a table of files. The table has columns for Mode, LastWriteTime, Length, and Name. The file "dns.log" is listed with a length of 0 and a last write time of 8/11/2025 PM 05:50.

```
Administrator: Windows PowerShell
PS C:\> Get-ChildItem -Path C:\Windows\System32\LogFiles\DNS

Directory: C:\Windows\System32\LogFiles\DNS

Mode                LastWriteTime         Length Name
----                -
-a---            8/11/2025   PM 05:50             0 dns.log

PS C:\> _
```

4. Windows Server 2016

(1) Open “Windows PowerShell.”



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

```
PS C:\> New-Item -ItemType directory -Path C:\Windows\System32\LogFiles\DNS
PS C:\> Get-ChildItem -Path C:\Windows\System32\LogFiles
```

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> New-Item -ItemType directory -Path C:\Windows\System32\LogFiles\DNS

Directory: C:\Windows\System32\LogFiles

Mode                LastWriteTime         Length Name
----                -
d-----            8/12/2025   AM 09:41             DNS

PS C:\Users\Administrator> Get-ChildItem -Path C:\Windows\System32\LogFiles

Directory: C:\Windows\System32\LogFiles

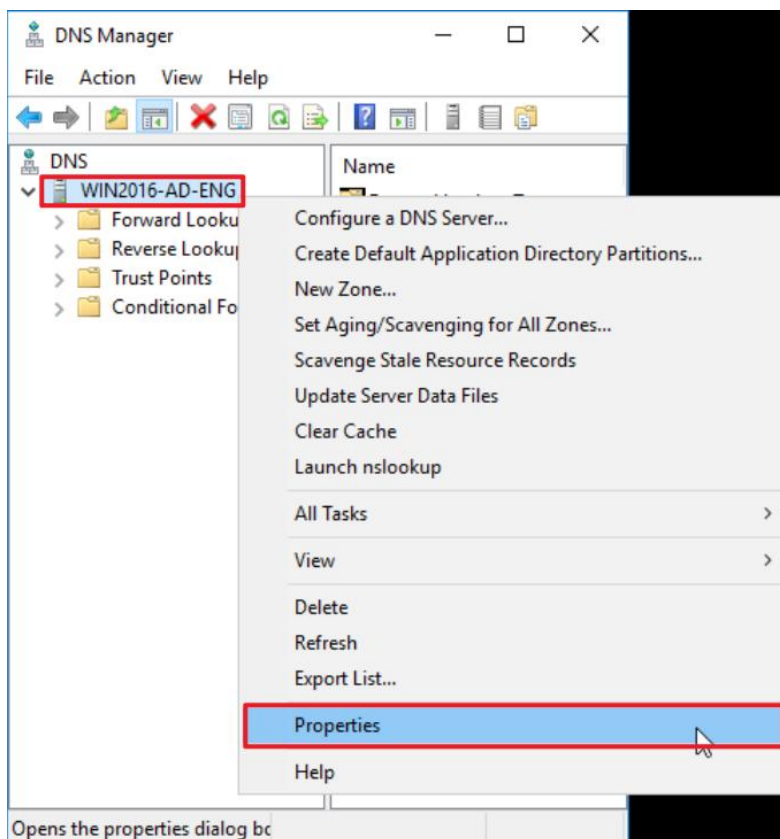
Mode                LastWriteTime         Length Name
----                -
d-----            8/12/2025   AM 09:37             DHCP
d-----            8/12/2025   AM 09:41             DNS
d-----            7/16/2016   PM 09:23             Firewall
d-----            5/20/2024   PM 11:24             HTTPERR
d-----            4/10/2024   PM 08:03             Scm
d-----            4/10/2024   PM 07:44             SQM
d-----            8/11/2025   PM 05:58             Sum
d-----            7/16/2016   PM 09:23             Windows Portable Devices
d-----            8/12/2025   AM 09:21             WMI

PS C:\Users\Administrator> _
```

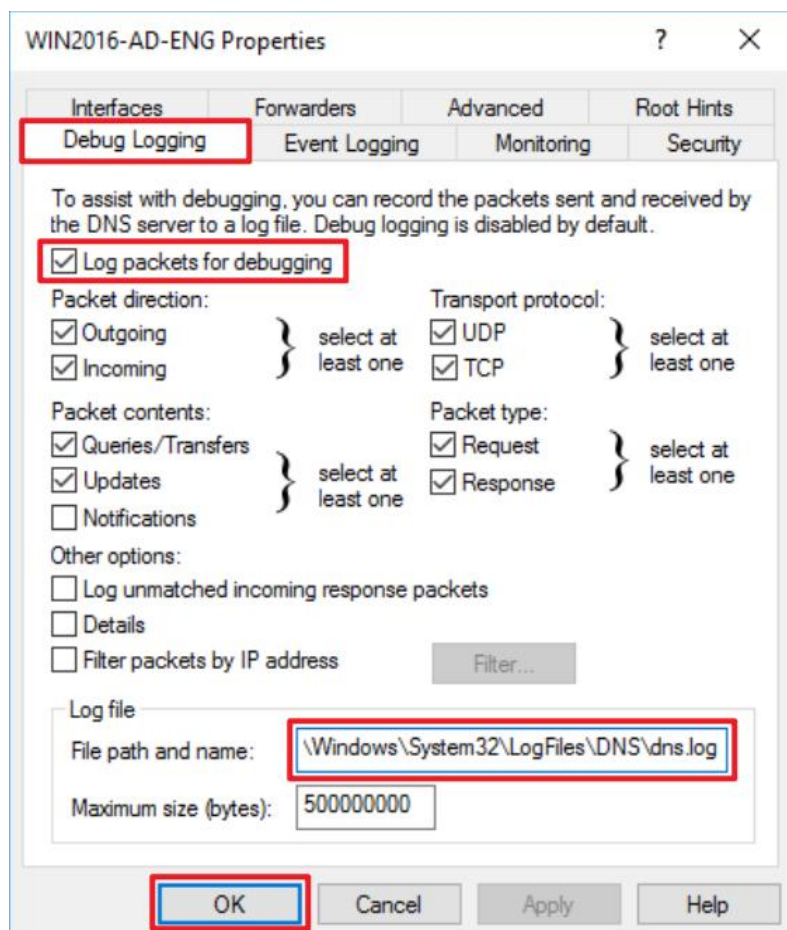
(3) Open DNS.



(4) Right-click the DNS server (the example here is **Win2016-AD-ENG**) → click “Properties.”



(5) On the “Debug Logging” tab → check “Log packets for debugging” → enter the “file path and name”:
C:\Windows\System32\LogFiles\DNS\dns.log and click “OK.”



(6) Open “Windows PowerShell” again.



(7) Enter the command below to verify that the file **dns.log** has been created:

```
PS C:\> Get-ChildItem -Path C:\Windows\System32\LogFiles\DNS
```

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-ChildItem -Path C:\Windows\System32\LogFiles\DNS

Directory: C:\Windows\System32\LogFiles\DNS

Mode                LastWriteTime         Length Name
----                -
-a----           8/12/2025  AM 09:47             0 dns.log

PS C:\Users\Administrator>
```

5. Windows Server 2019

(1) Open “Windows PowerShell.”



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

```
PS C:\> New-Item -ItemType directory -Path C:\Windows\System32\LogFiles\DNS
```

```
PS C:\> Get-ChildItem -Path C:\Windows\System32\LogFiles
```

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> New-Item -ItemType directory -Path C:\Windows\System32\LogFiles\DNS

Directory: C:\Windows\System32\LogFiles

Mode                LastWriteTime         Length Name
----                -
d-----            8/12/2025    10:09             DNS

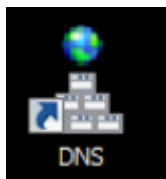
PS C:\Users\Administrator> Get-ChildItem -Path C:\Windows\System32\LogFiles

Directory: C:\Windows\System32\LogFiles

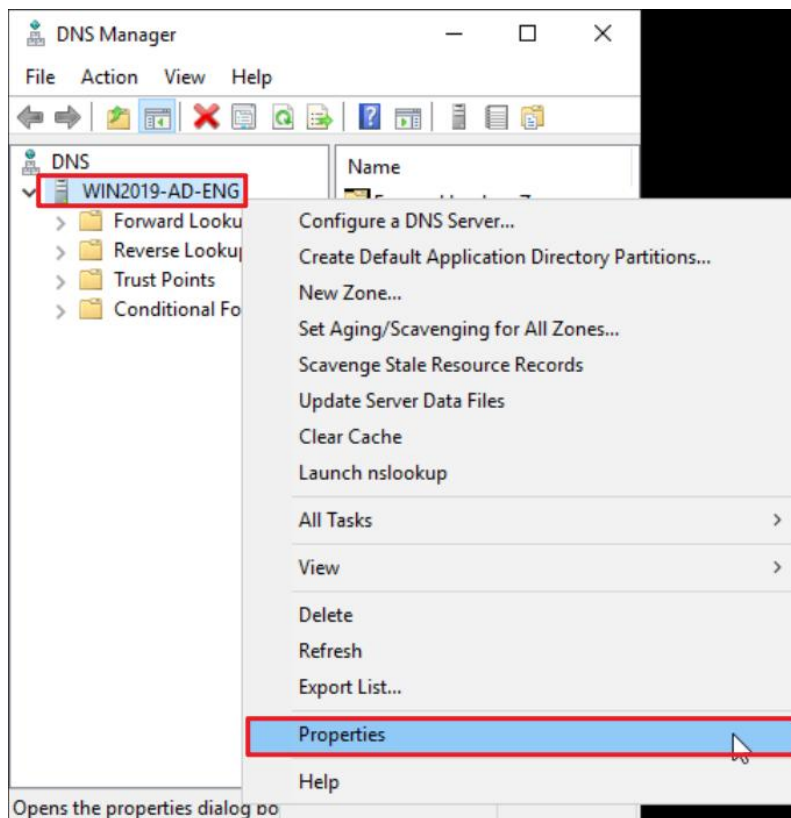
Mode                LastWriteTime         Length Name
----                -
d-----            8/12/2025    09:57             DHCP
d-----            8/12/2025    10:09             DNS
d-----            8/12/2025    09:54             LSA
d-----            8/12/2025    09:54             SAM
d-----            4/12/2024    13:05      setupcln
d-----            8/12/2025    10:02             SQM
d-----            8/12/2025    09:57             Sum
d-----            8/11/2025    15:46             WMI

PS C:\Users\Administrator>
```

(3) Open DNS.

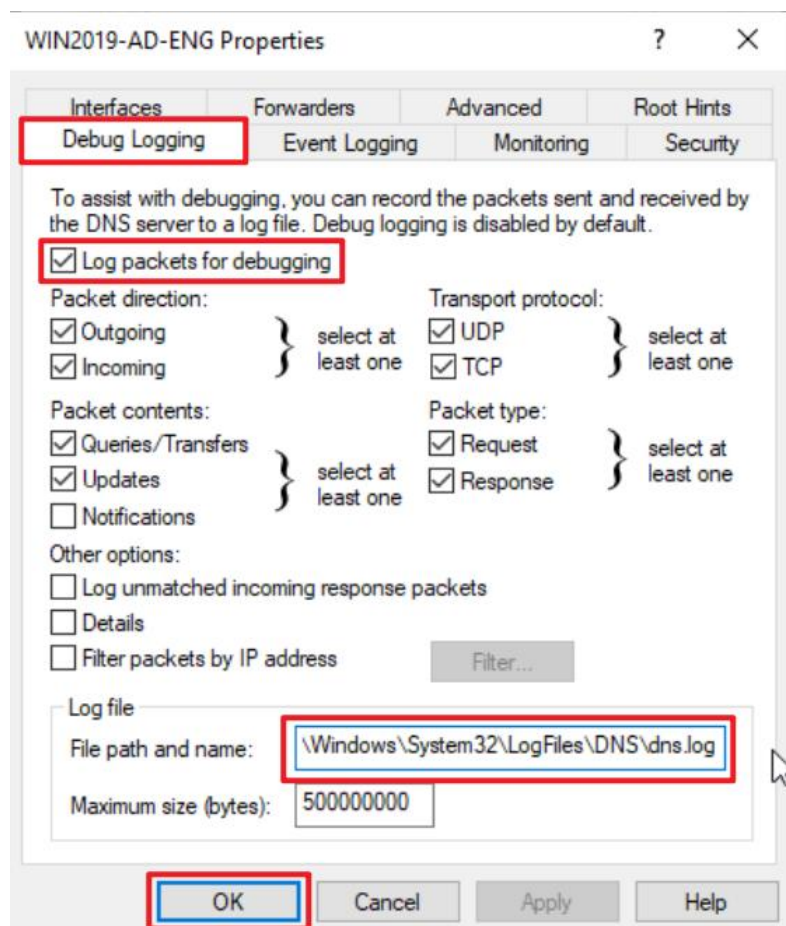


(4) Right-click the DNS server (the example here is **Win2019-AD-ENG**) → click “Properties.”



(5) On the “Debug Logging” tab → check “Log packets for debugging” → enter the “file path and name”:

C:\Windows\System32\LogFiles\DNS\dns.log and click “OK.”



(6) Open “Windows PowerShell” again.



(7) Enter the command below to verify that the file **dns.log** has been created:

```
PS C:\> Get-ChildItem -Path C:\Windows\System32\LogFiles\DNS
```

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-ChildItem -Path C:\Windows\System32\LogFiles\DNS

Directory: C:\Windows\System32\LogFiles\DNS

Mode                LastWriteTime         Length Name
----                -
-a-----         8/12/2025   10:10             0 dns.log

PS C:\Users\Administrator> _
```

6. Windows Server 2022

(1) Open “Windows PowerShell.”



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

```
PS C:\> New-Item -ItemType directory -Path C:\Windows\System32\LogFiles\DNS
PS C:\> Get-ChildItem -Path C:\Windows\System32\LogFiles
```

A screenshot of a Windows PowerShell console window titled "Administrator: Windows PowerShell". The window shows the execution of two commands. The first command, `New-Item -ItemType directory -Path C:\Windows\System32\LogFiles\DNS`, successfully creates the directory. The second command, `Get-ChildItem -Path C:\Windows\System32\LogFiles`, lists the contents of the LogFiles directory, showing several subdirectories including DHCP, DNS, HTTPERR, LSA, SAM, setupcln, Sum, and WMI.

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> New-Item -ItemType directory -Path C:\Windows\System32\LogFiles\DNS

Directory: C:\Windows\System32\LogFiles

Mode                LastWriteTime         Length Name
----                -
d-----            8/12/2025  AM 10:43             DNS

PS C:\Users\Administrator> Get-ChildItem -Path C:\Windows\System32\LogFiles

Directory: C:\Windows\System32\LogFiles

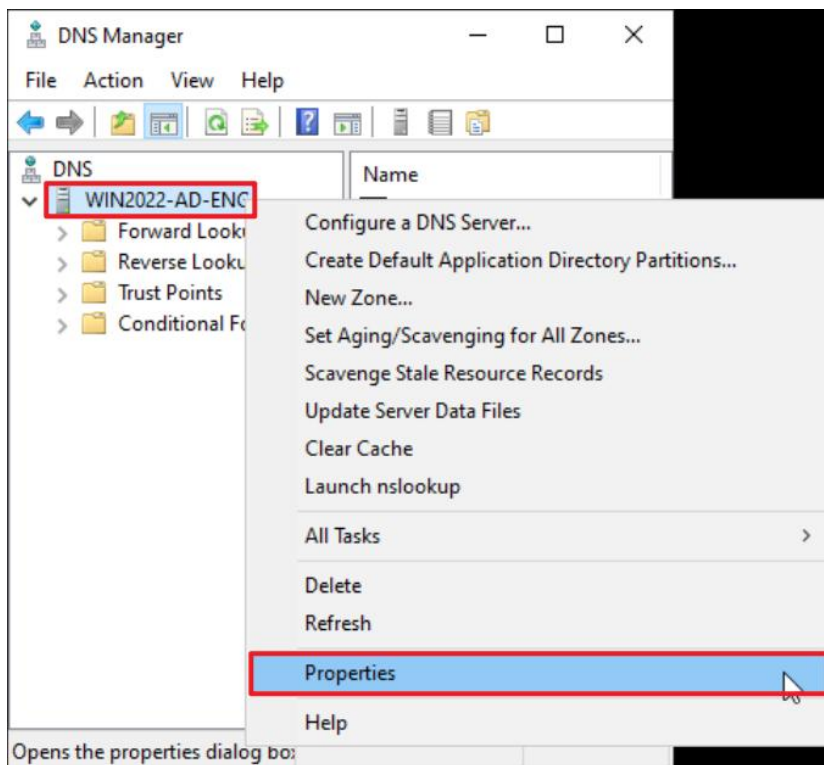
Mode                LastWriteTime         Length Name
----                -
d-----            8/12/2025  AM 10:25             DHCP
d-----            8/12/2025  AM 10:43             DNS
d-----           10/16/2024  PM 02:14            HTTPERR
d-----            8/12/2025  AM 10:25             LSA
d-----            8/12/2025  AM 10:25             SAM
d-----            4/12/2024  PM 01:06          setupcln
d-----            8/12/2025  AM 10:29             Sum
d-----            8/12/2025  AM 10:25             WMI

PS C:\Users\Administrator>
```

(3) Open DNS.

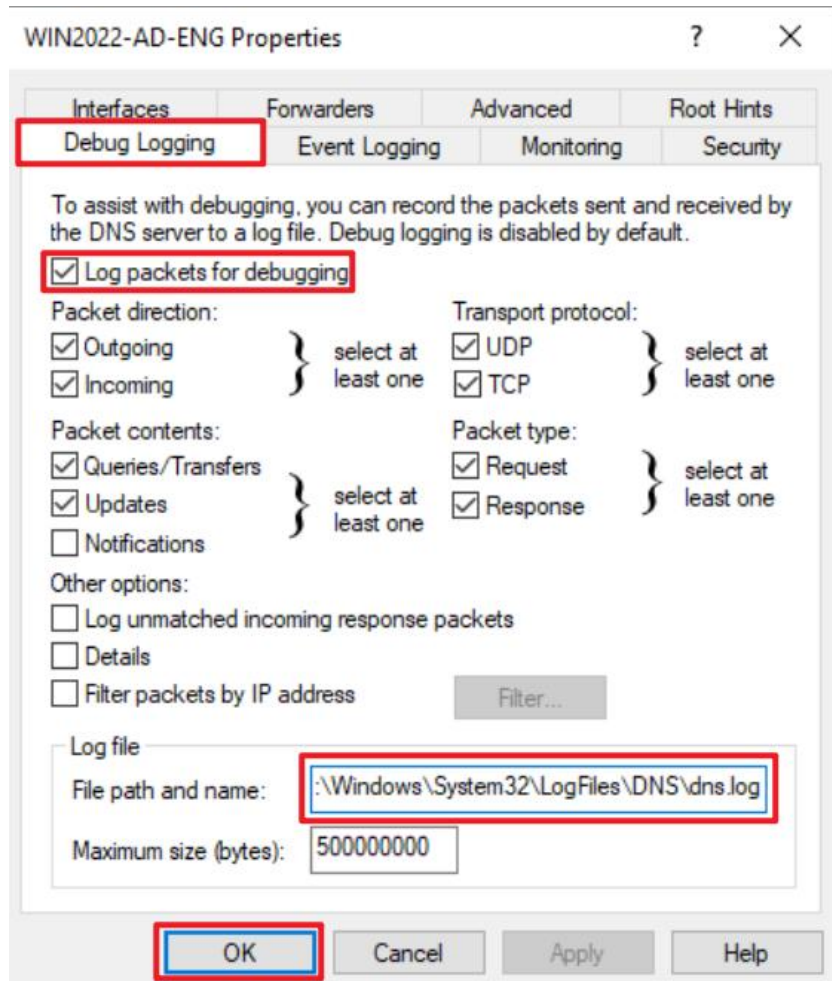


(4) Right-click the DNS server (the example here is **Win2022-AD-ENG**) → click “Properties.”



(5) On the “Debug Logging” tab → check “Log packets for debugging” → enter the “file path and name”:

C:\Windows\System32\LogFiles\DNS\dns.log and click “OK.”

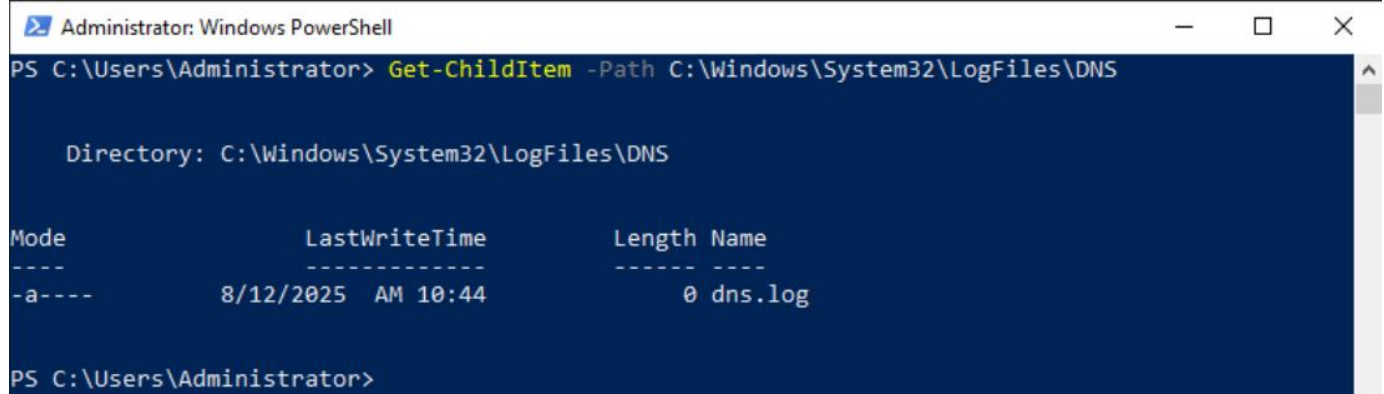


(6) Open “Windows PowerShell” again.



(7) Enter the command below to verify that the file **dns.log** has been created:

```
PS C:\> Get-ChildItem -Path C:\Windows\System32\LogFiles\DNS
```

A screenshot of a Windows PowerShell window titled "Administrator: Windows PowerShell". The window shows the command `Get-ChildItem -Path C:\Windows\System32\LogFiles\DNS` being executed. The output shows the directory `C:\Windows\System32\LogFiles\DNS` and a table of files. The table has columns for Mode, LastWriteTime, Length, and Name. A single file, `dns.log`, is listed with a mode of `-a----`, a last write time of `8/12/2025 AM 10:44`, and a length of `0`.

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-ChildItem -Path C:\Windows\System32\LogFiles\DNS

Directory: C:\Windows\System32\LogFiles\DNS

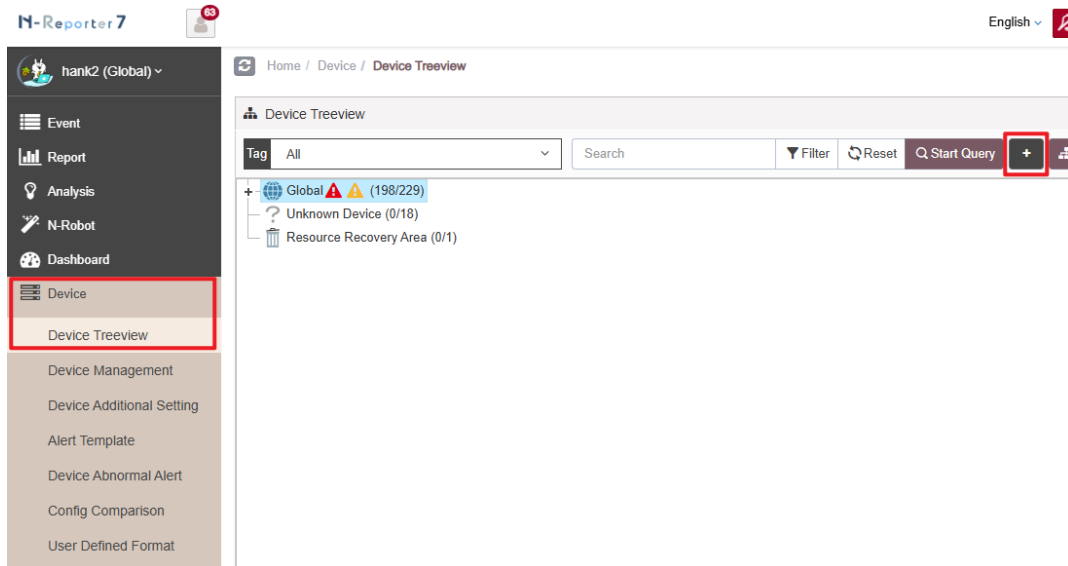
Mode                LastWriteTime         Length Name
----                -
-a-----         8/12/2025  AM 10:44             0 dns.log

PS C:\Users\Administrator>
```

7. N-Reporter

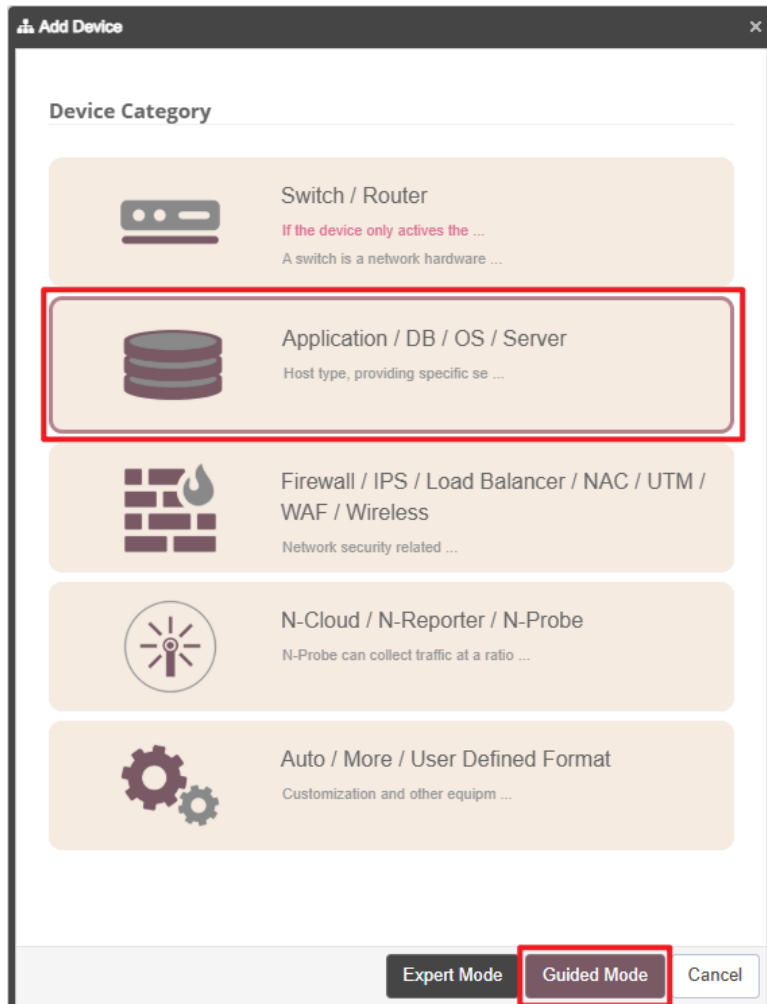
(1) Add a Windows DNS device:

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



(2) Select the device type:

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



(3) Basic Device Settings:

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

Add Device - Basic Setting

Basic Setting

Machine Name *
WinDNS-192.168.

IP *
192.168.

Domain *
Global

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

User Defined Syslog Format ⓘ +
Not Activated

SNMP Model ⓘ
Not Activated

Performance Monitoring Setting

Previous **Next** Cancel

(4) Syslog Settings

Set “Facility” to “(19) local use 3 (local3)” → click “Next.”

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

Add Device - Syslog Setting

Syslog Setting

Facility ⓘ

(19) local use 3 (local3)

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

(5) 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 "atitute, longitude"), "Remark" (a text field with a 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: "Yes" and "No" (highlighted with a red box).



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

Sales Information : sales@npartner.com

Technical Support : support@npartner.com