How to Configure Windows DNS Log

V009

2025/08/18

Copyright Declaration

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

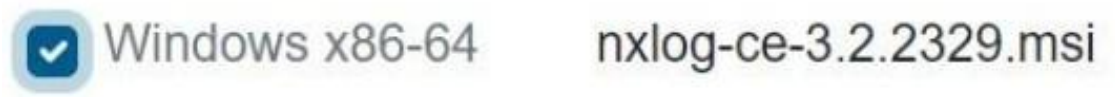
1.1 NXLog Installation

(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.

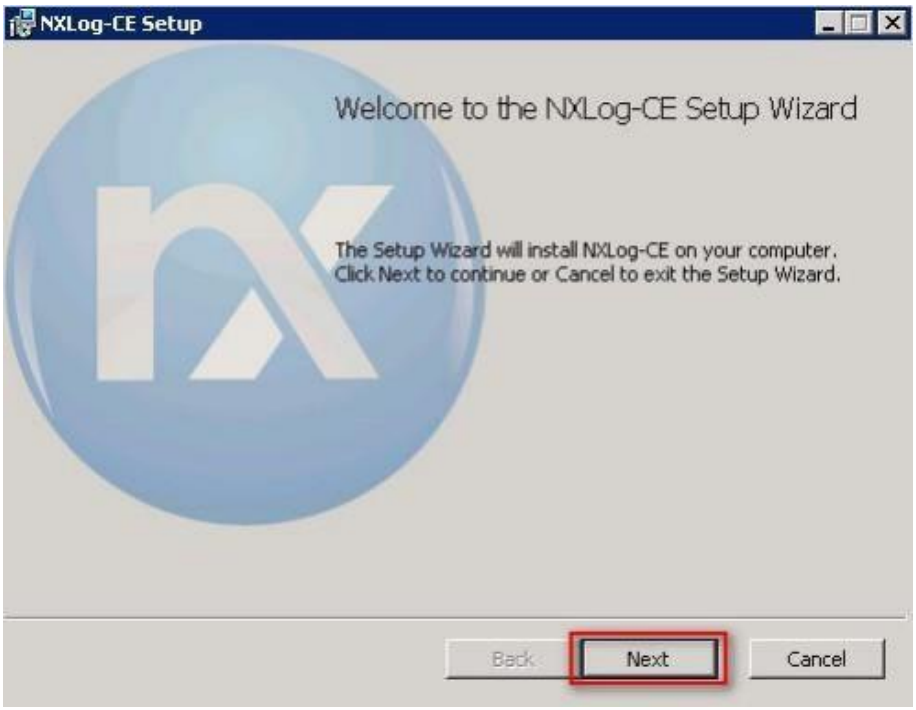
Example Here: **nxlog-ce-3.2.2329.msi**



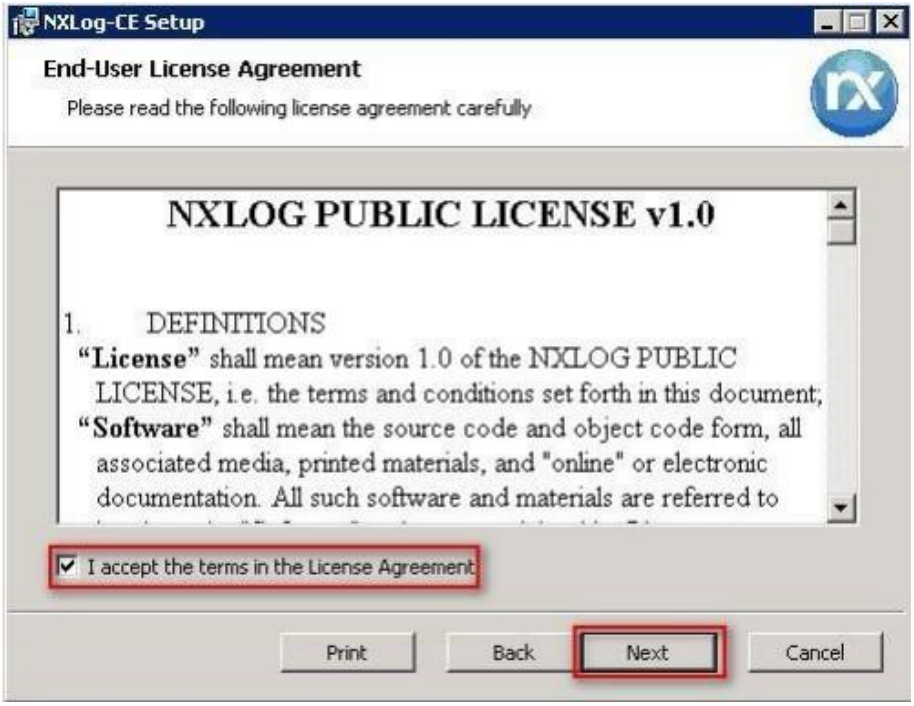
(2) Install NXLog

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

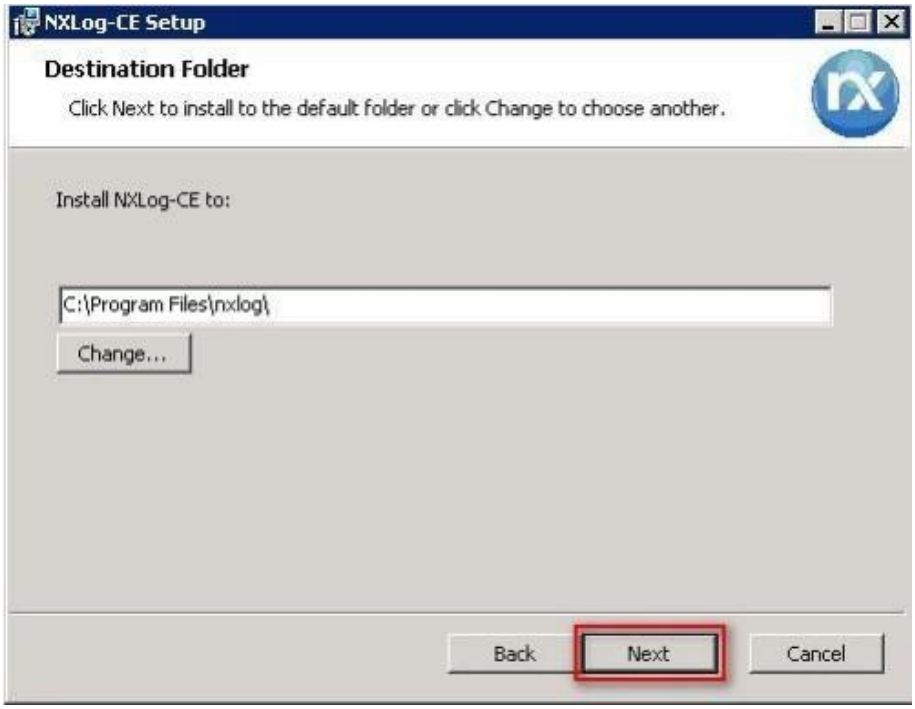
Double-click "**nxlog-ce-3.2.2329.msi.**"



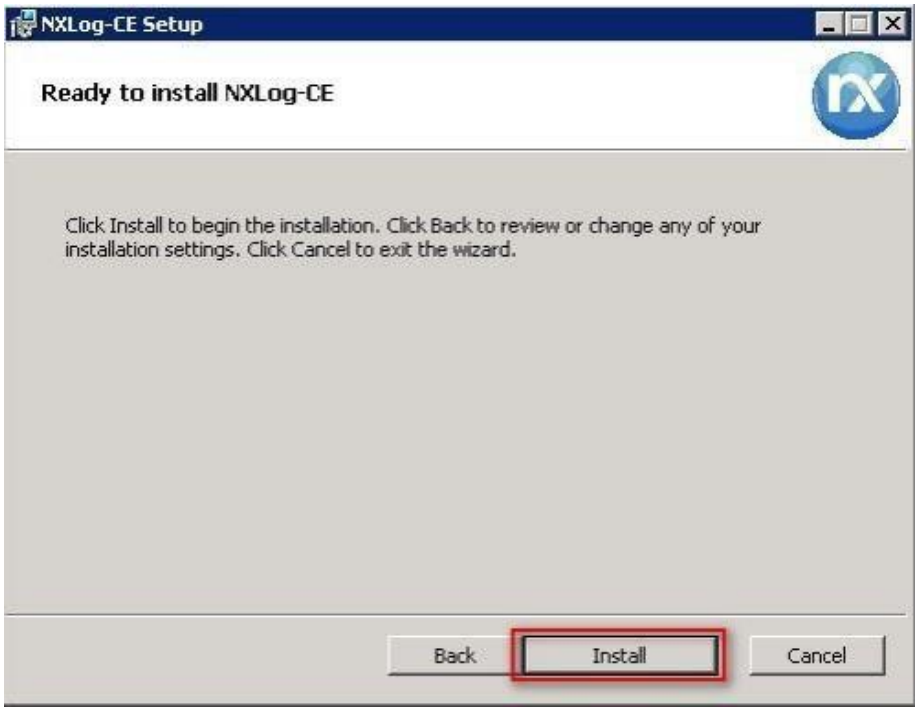
(3) Select “I accept the terms in the License Agreement,” then click “Next.”



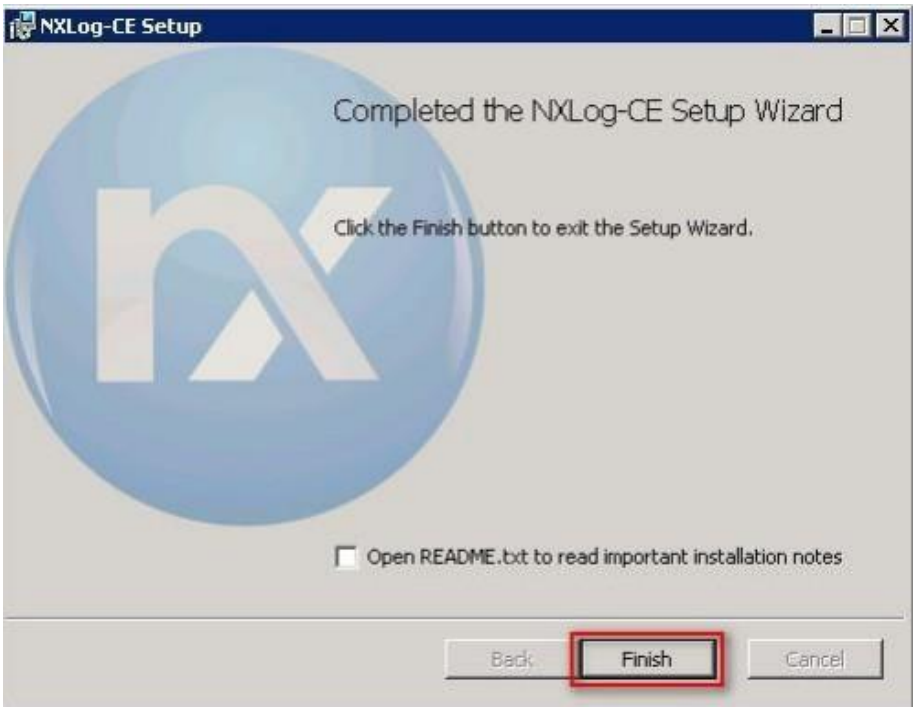
(4) Click “Next.” (The default installation path is (C:\Program Files\nxlog\).



(5) Click “Install.”

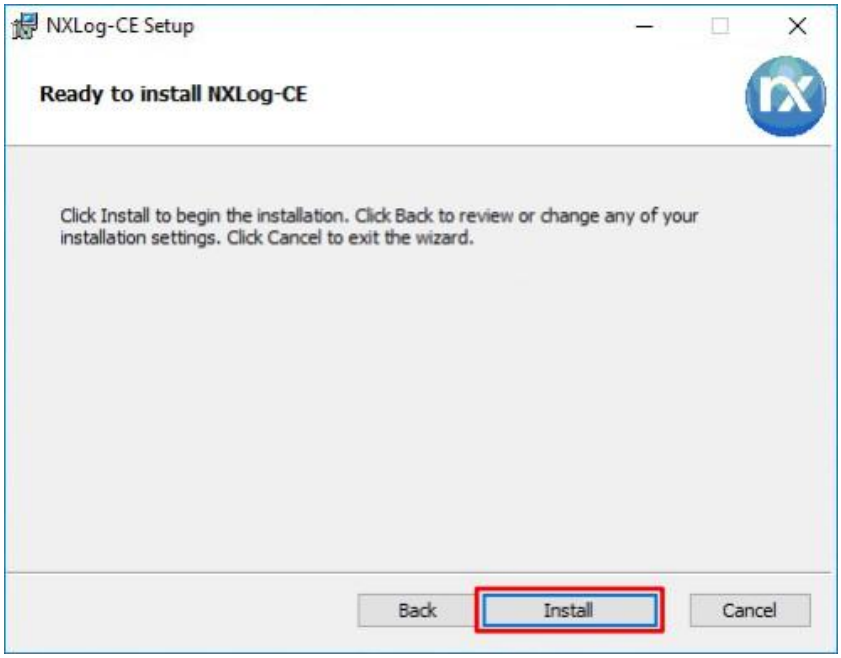


(6) Click “Finish.”



<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.

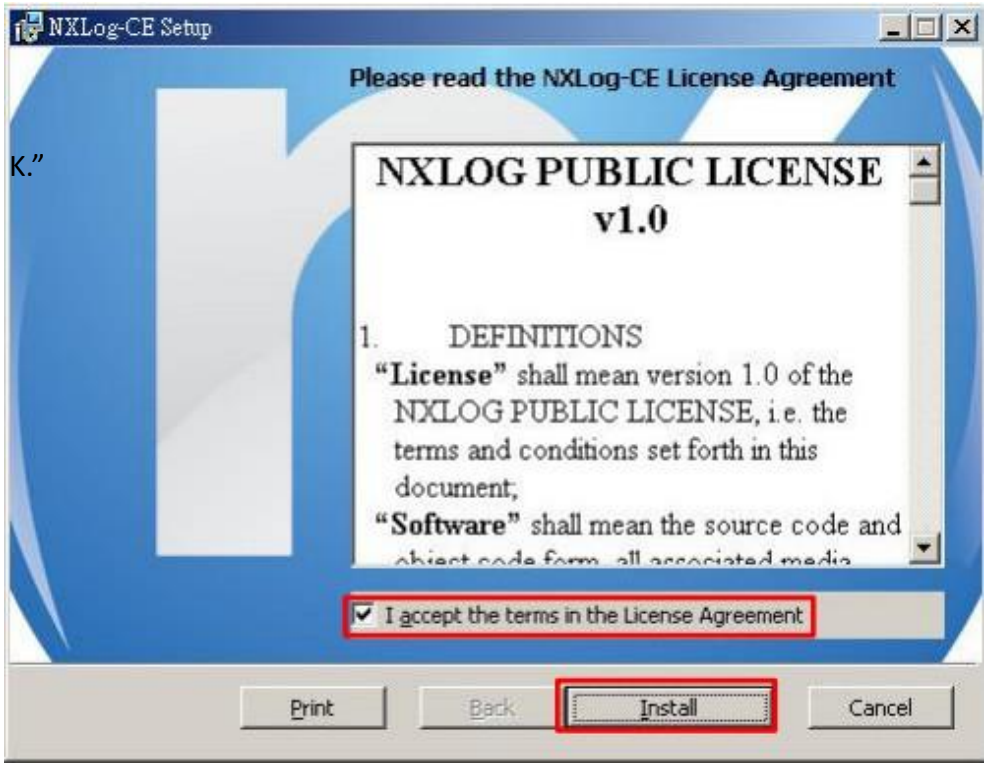


<2.3> For Windows **2000**:

(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**.”



K.”

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:

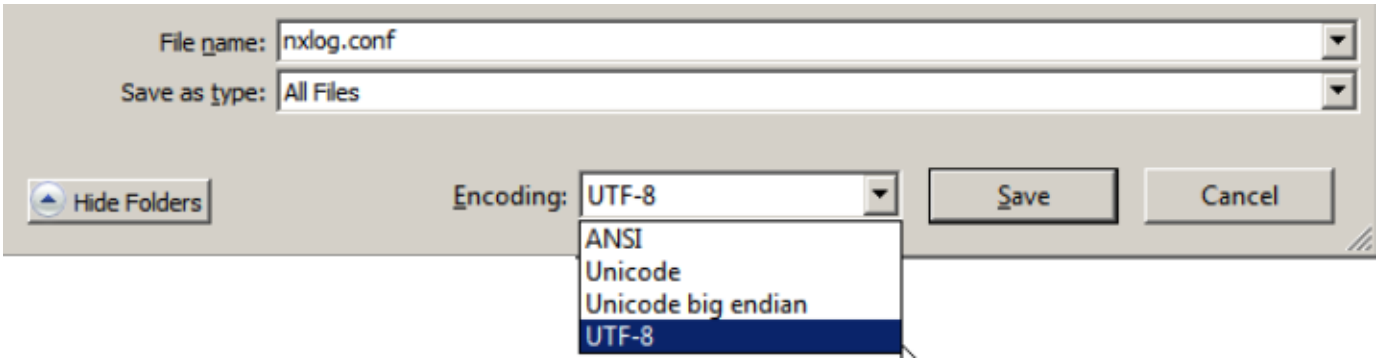
```
define ROOT C:\Program Files    (x86)\nxlog
```

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.

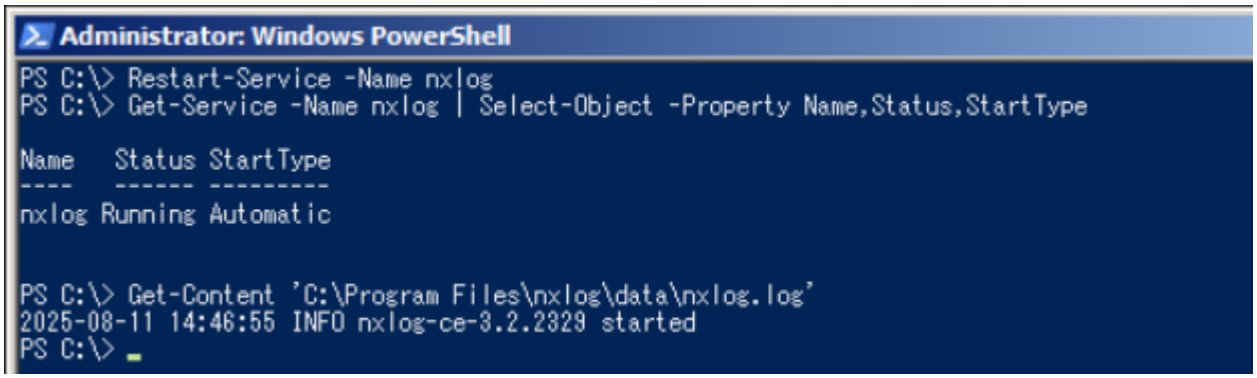


1.4 Starting the NXLog Service

(1) Open “Windows Powershell.”

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

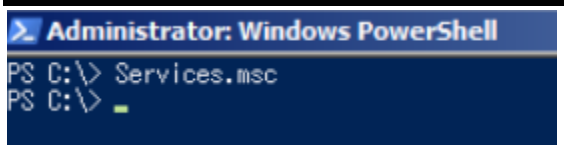
```
PS C:\> Restart-Service -Name nxlog
PS C:\> Get-Service -Name nxlog | Select-Object -Property Name,Status,StartType
PS C:\> Get-Content 'C:\ Program Files\ nxlog\data\nxlog.log'
```



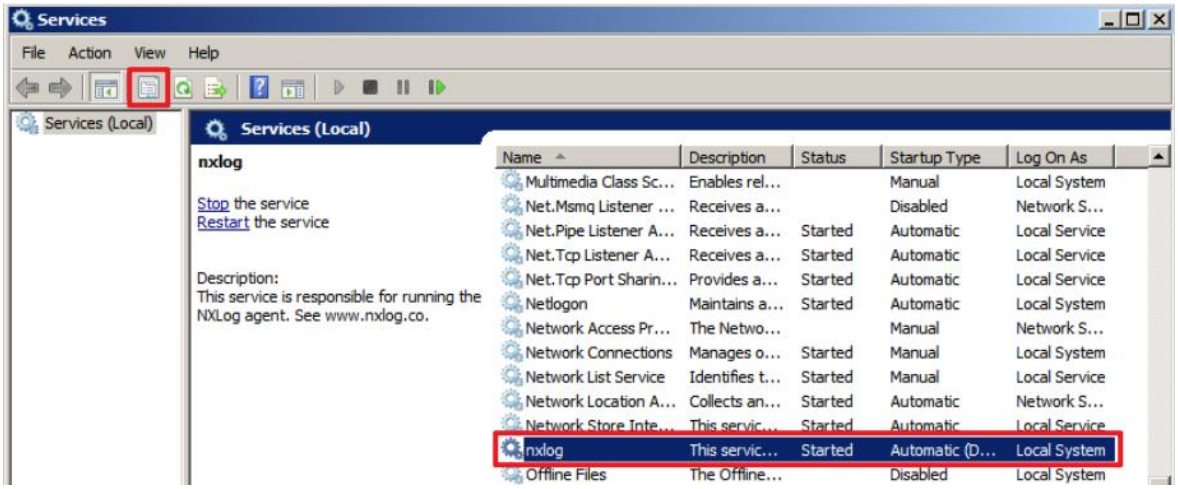
Note: This example is for a 64-bit operating system. For a 32-bit system, replace the highlighted text with: **'C:\Program Files(x86)\nxlog\conf\nxlog.conf'**

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

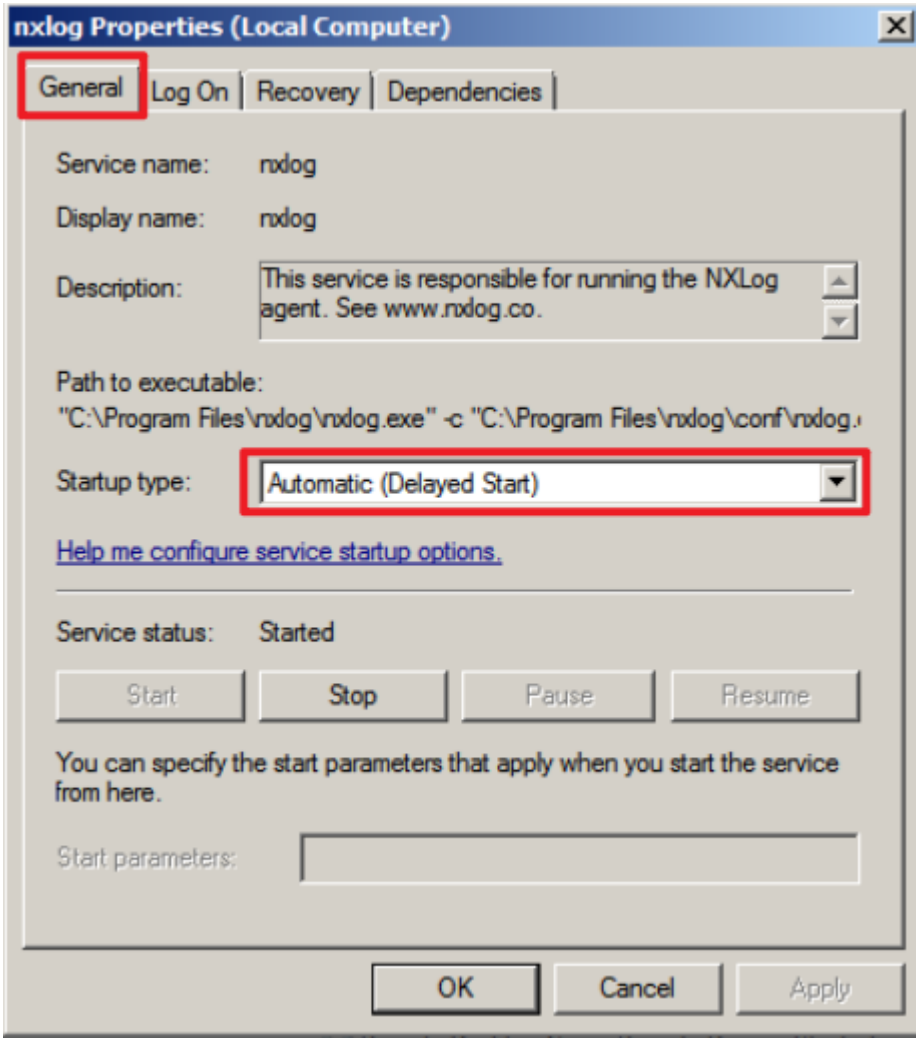
```
PS C:\> Services.msc
```



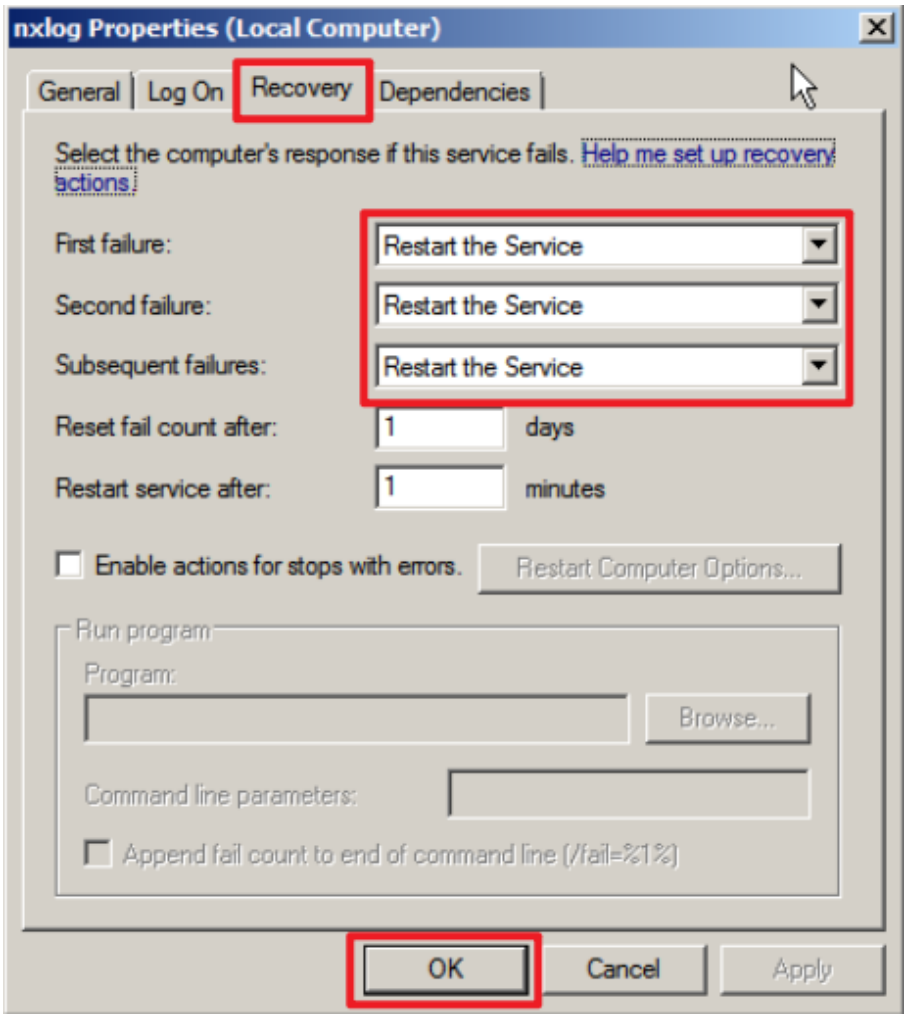
(4) Open the NXLog service properties: select “NXLog” → Click “Properties.”



(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."

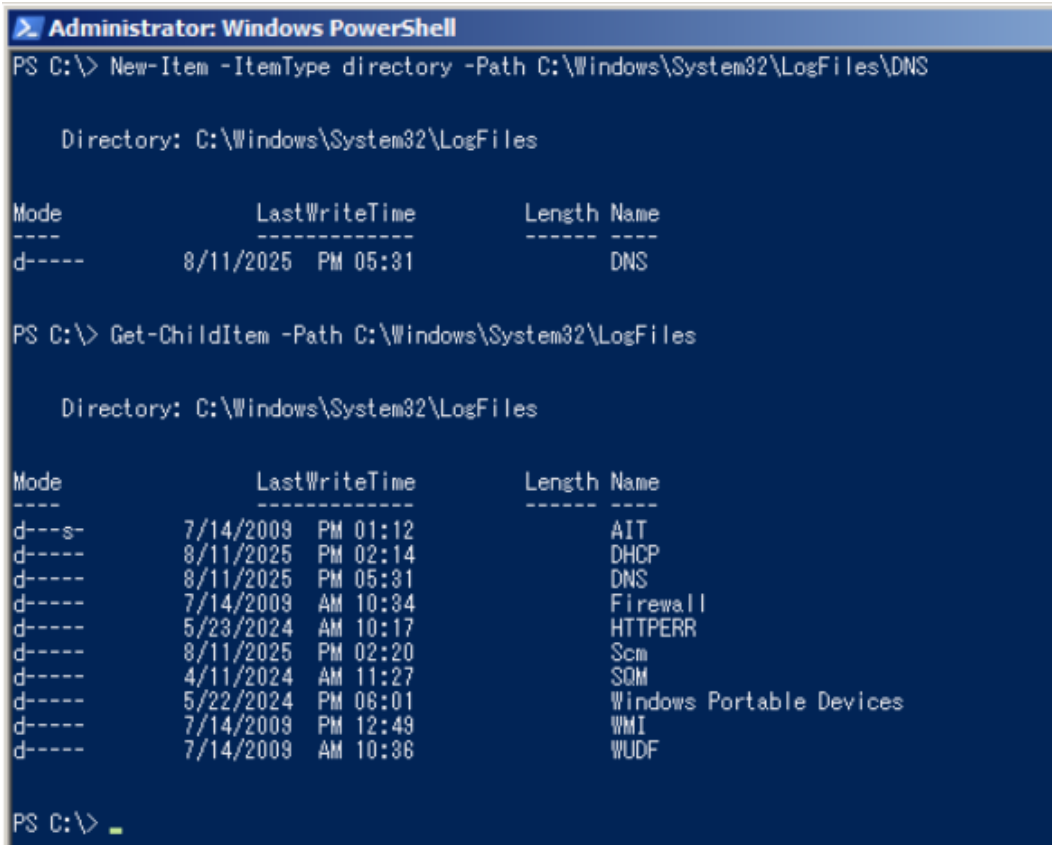


2. Windows Server 2008

(1) Open “Windows PowerShell.”

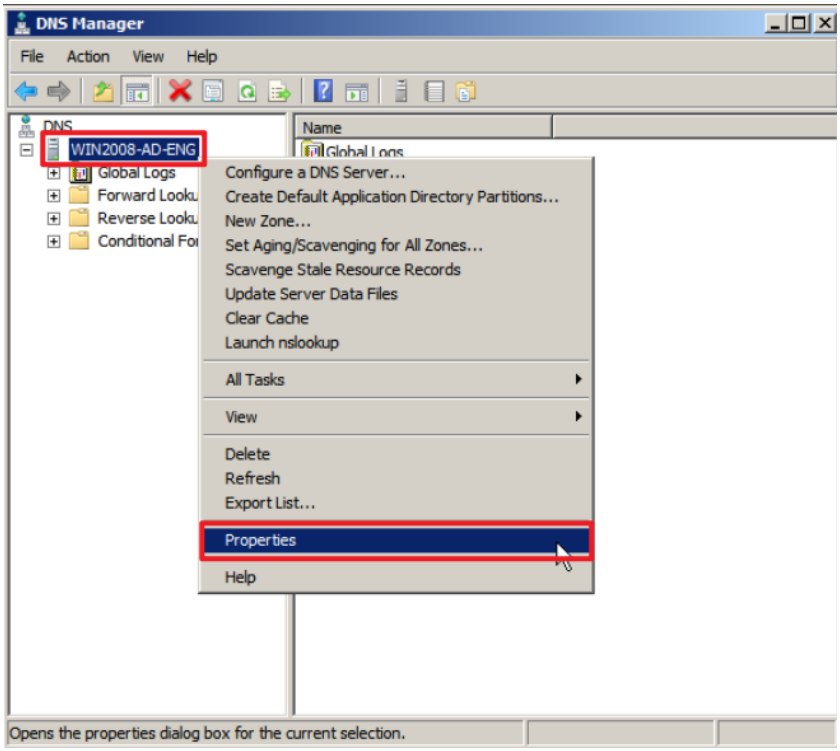
(2) Enter the command below to create the DNS log folder:

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

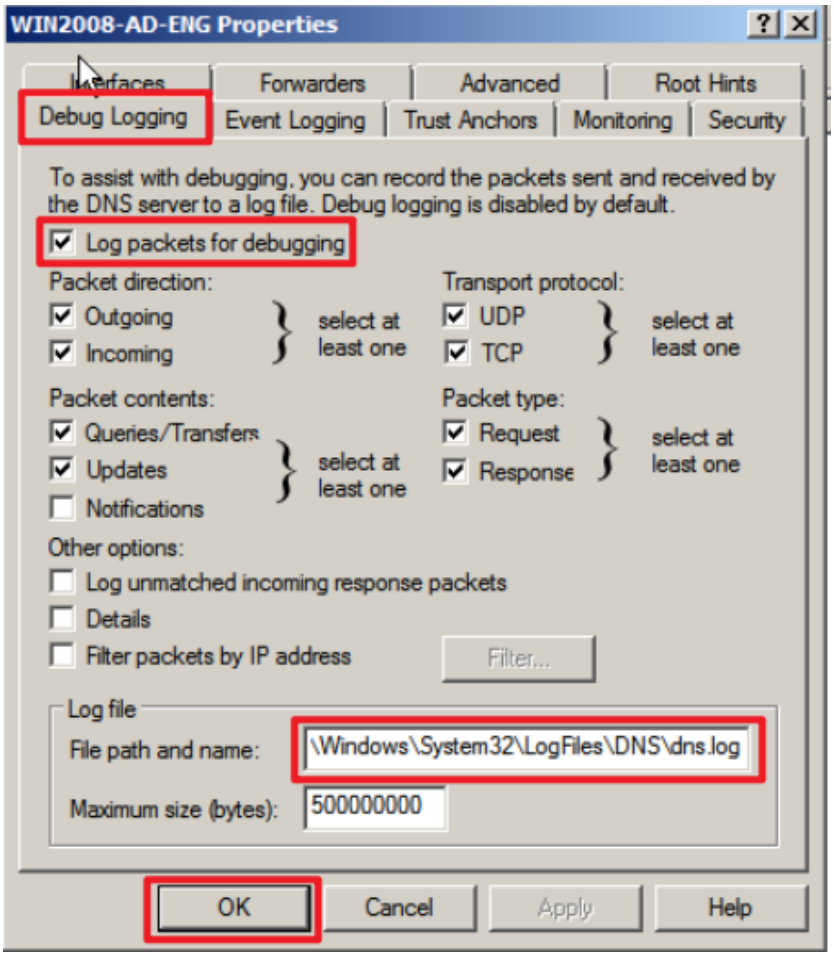


(3) Open DNS.

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



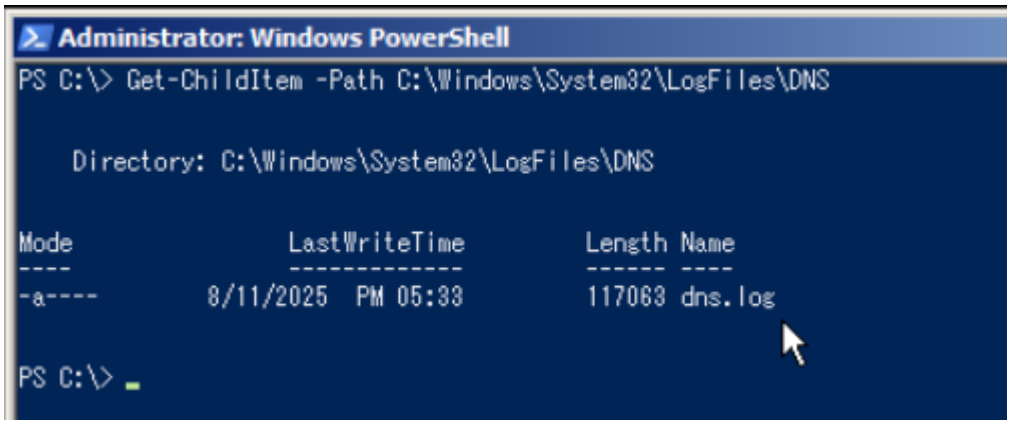
(5) On the “Debug Logging” tab → check “Log packets for debugging” → enter the “file path and name”: C:\Windows\System32\LogFiles\DNS\dns.log and click “OK.”



(6) Open “Windows PowerShell” again.

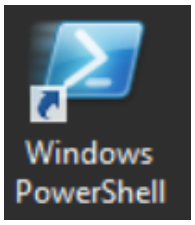
(7) Enter the command below to verify that the file dns.log has been created:

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



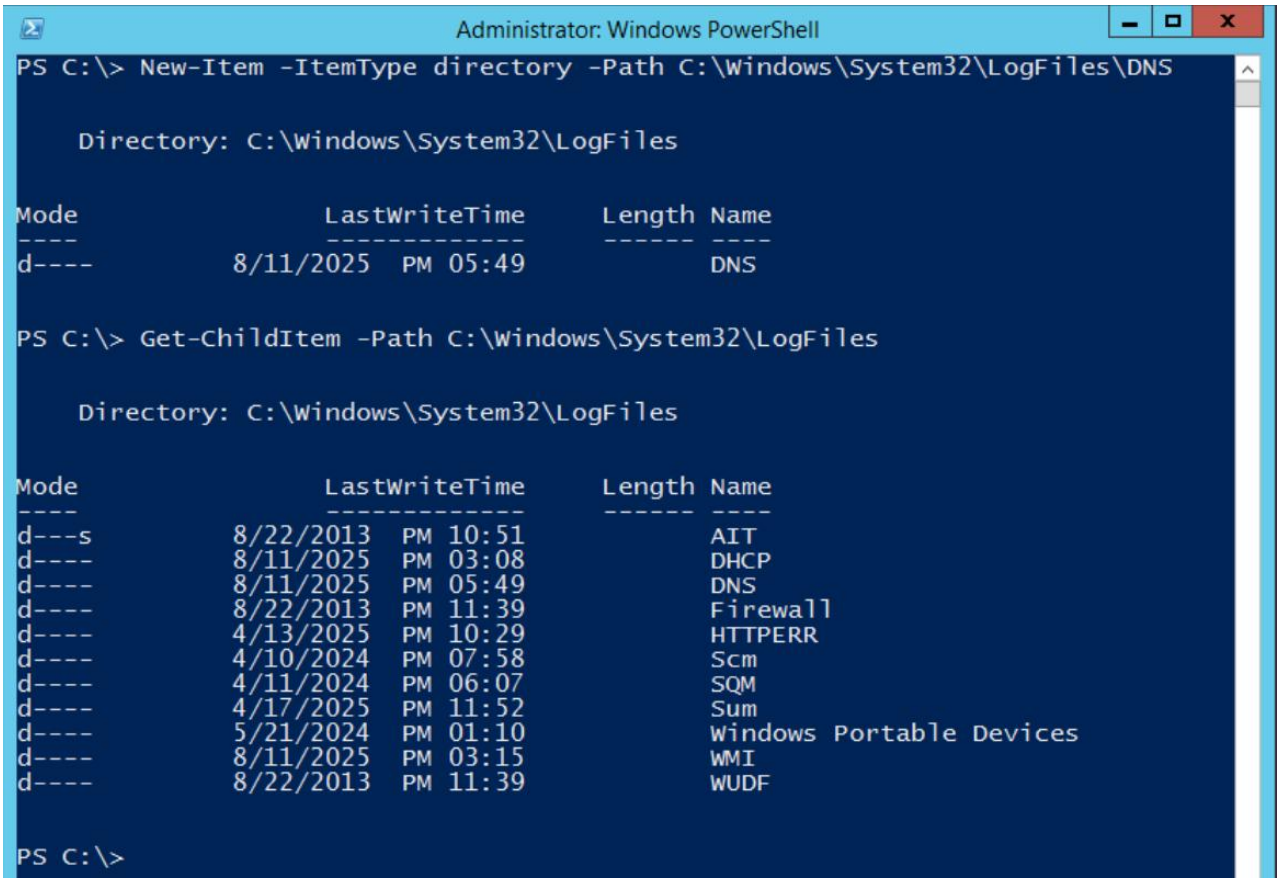
3. Windows Server 2012

(1) Open “Windows PowerShell.”



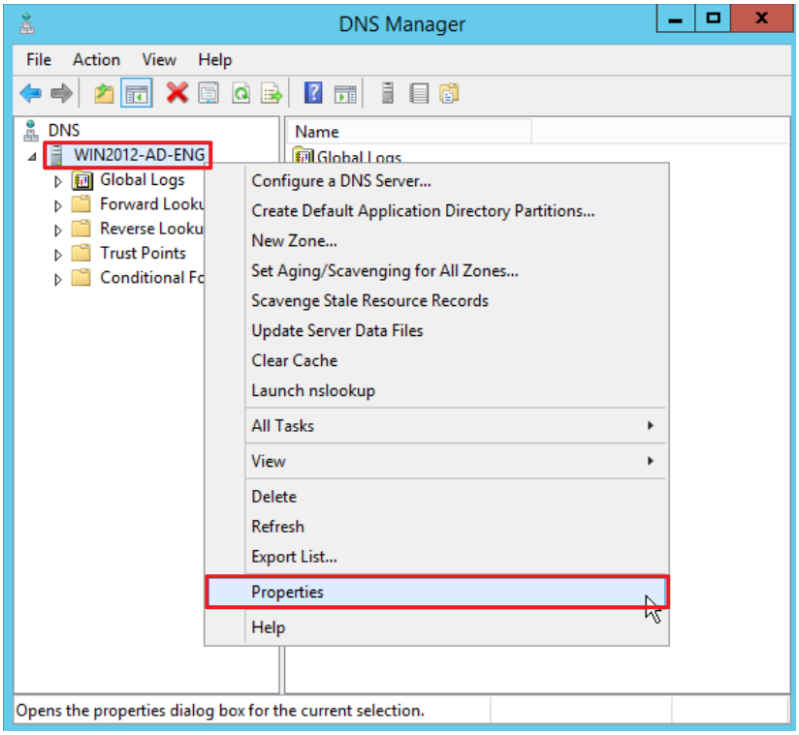
(2) Enter the command below to create the DNS log folder:

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

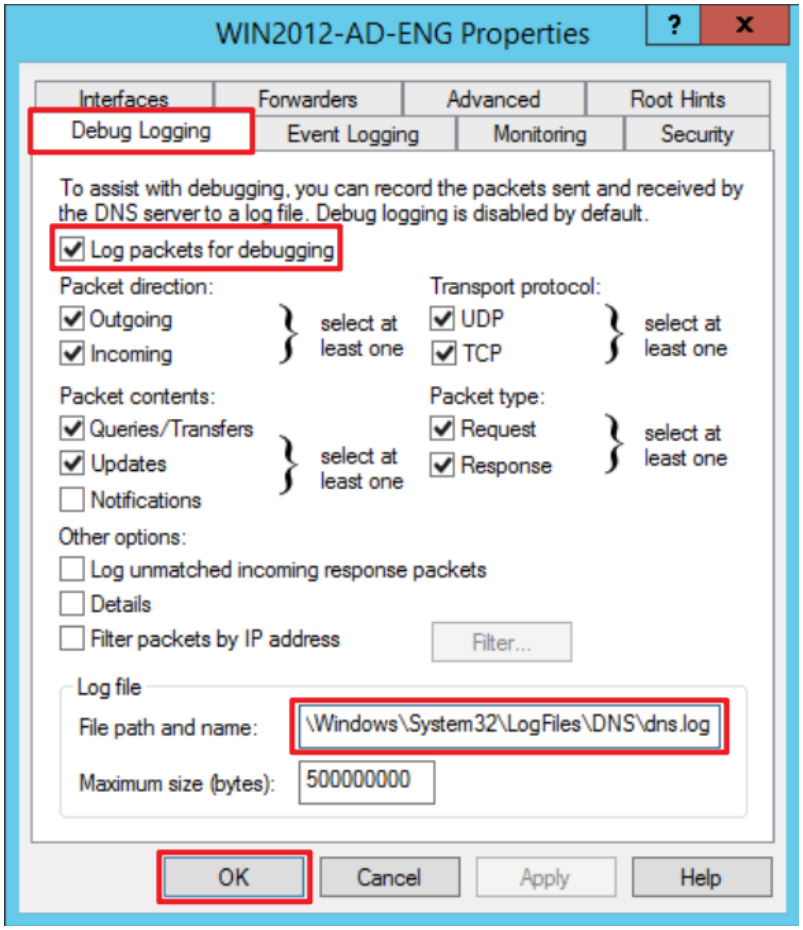


(3) Open DNS.

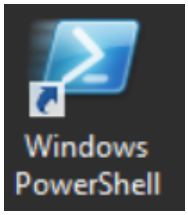
(4) Right-click the DNS server (the example here is Win2012-AD-ENG) → click “Properties.”



(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.”

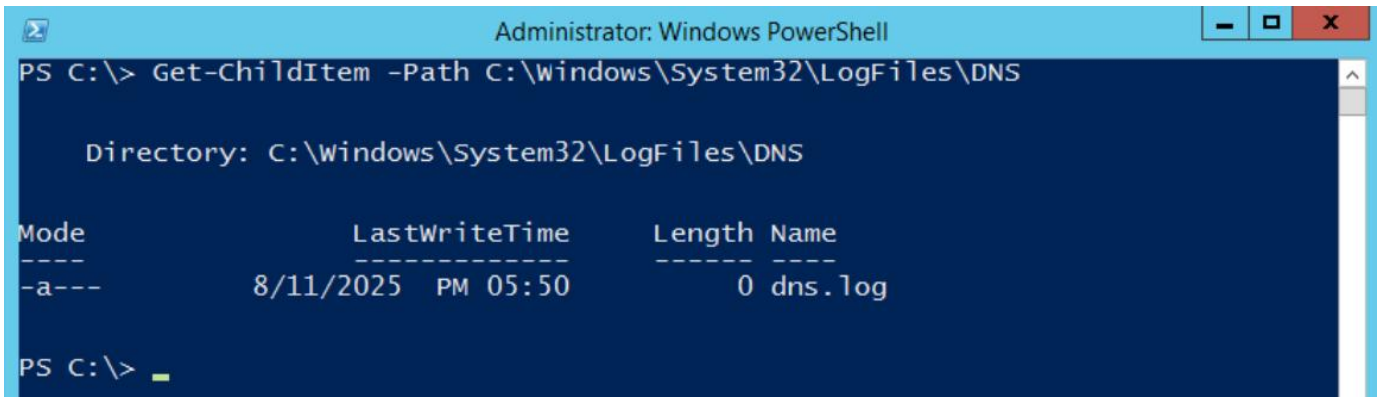


(6) Open “Windows PowerShell” again.



(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
```

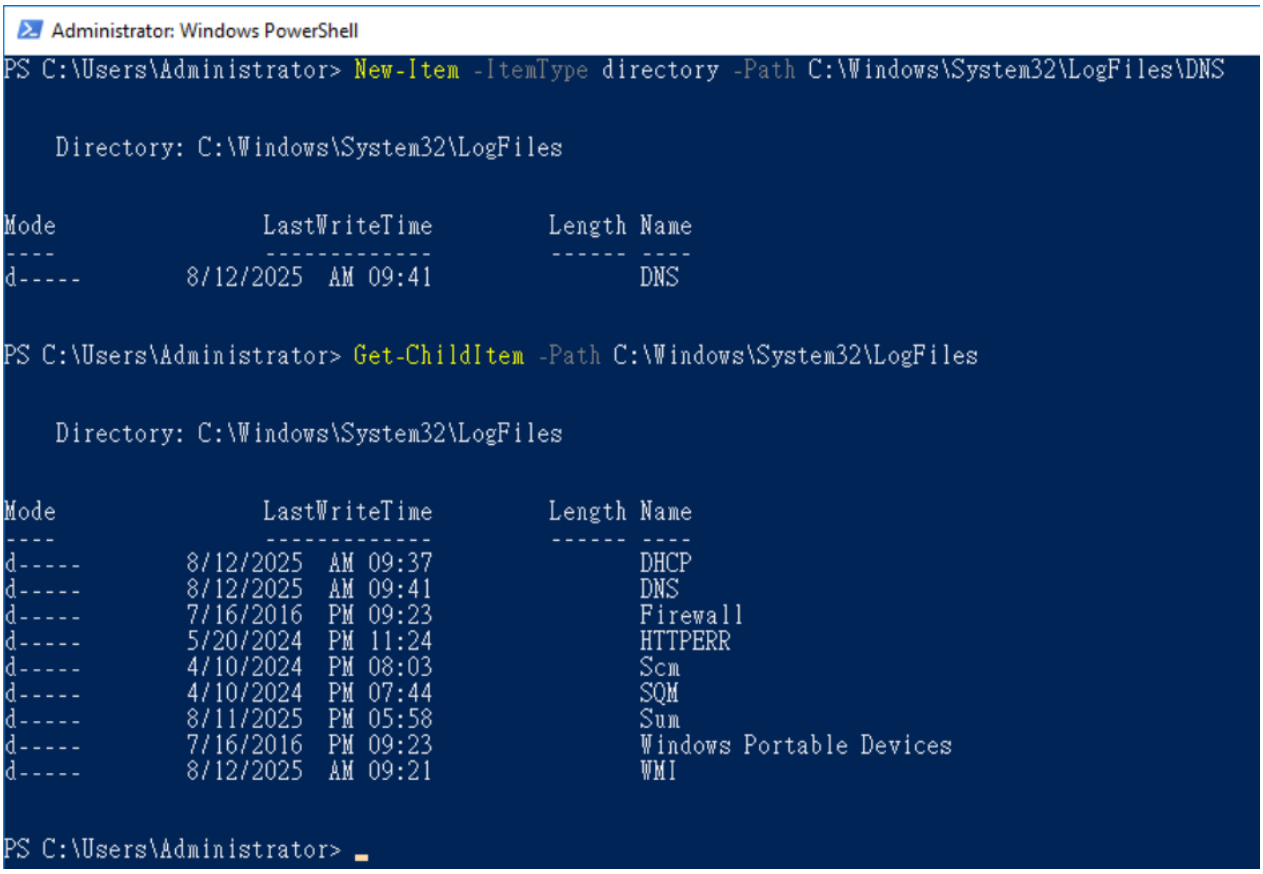


4. Windows Server 2016

(1) Open “Windows PowerShell.”

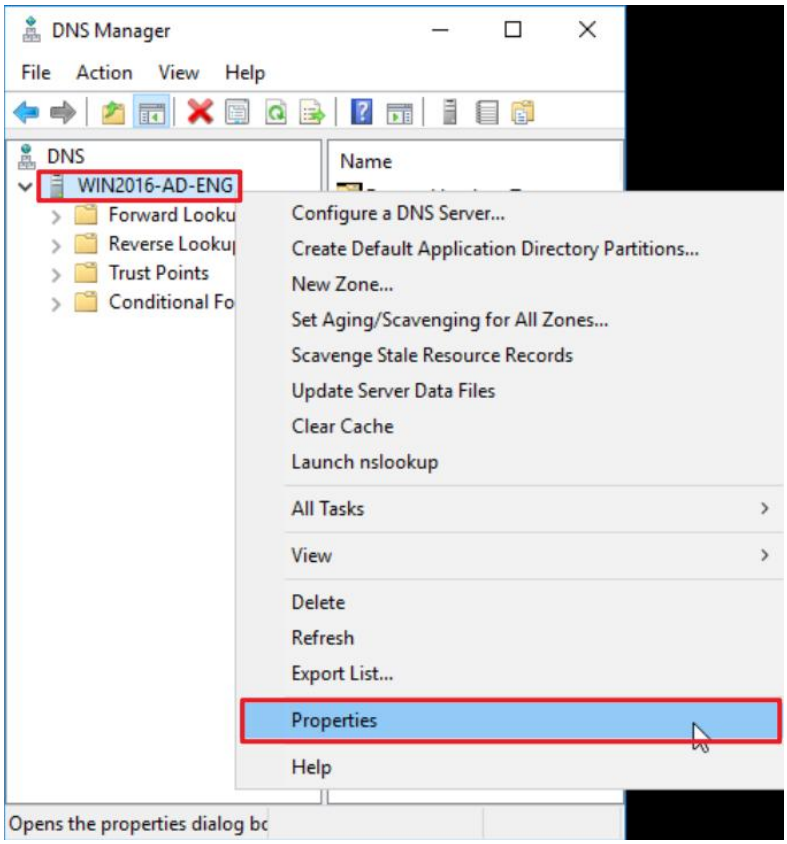
(2) Enter the command below to create the DNS log folder:

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

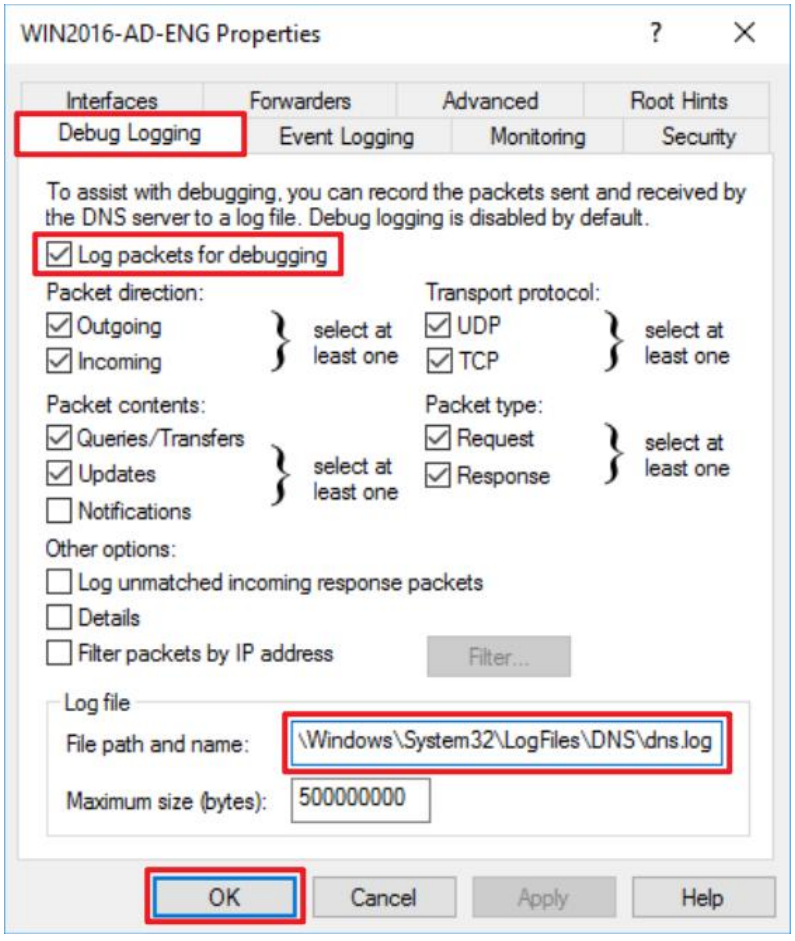


(3) Open DNS.

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



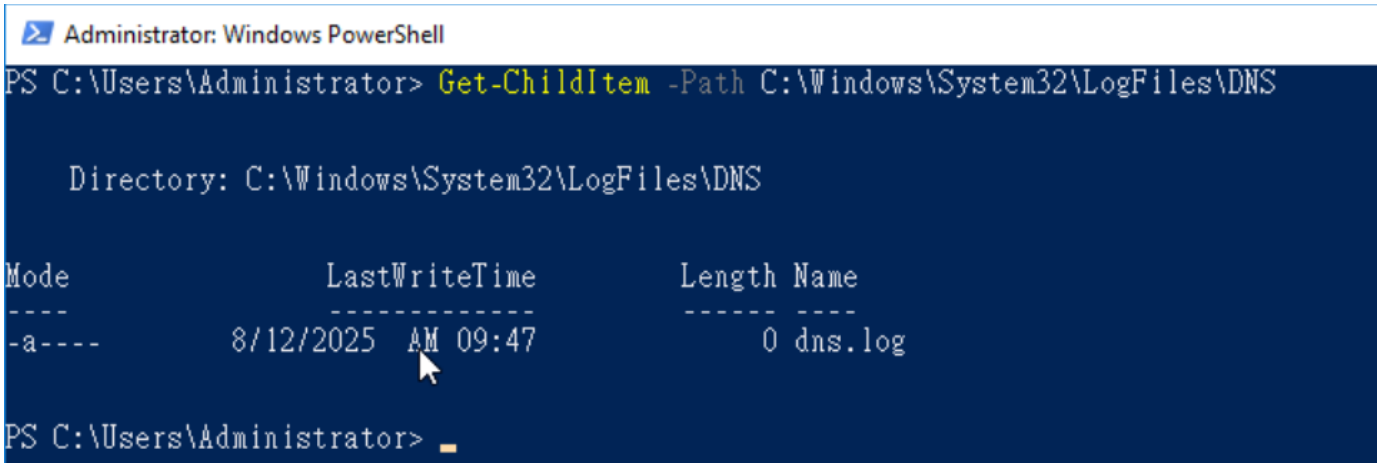
(5) On the “Debug Logging” tab → check “Log packets for debugging” → enter the “file path and name”: C:\Windows\System32\LogFiles\DNS\dns.log and click “OK.”



(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
```

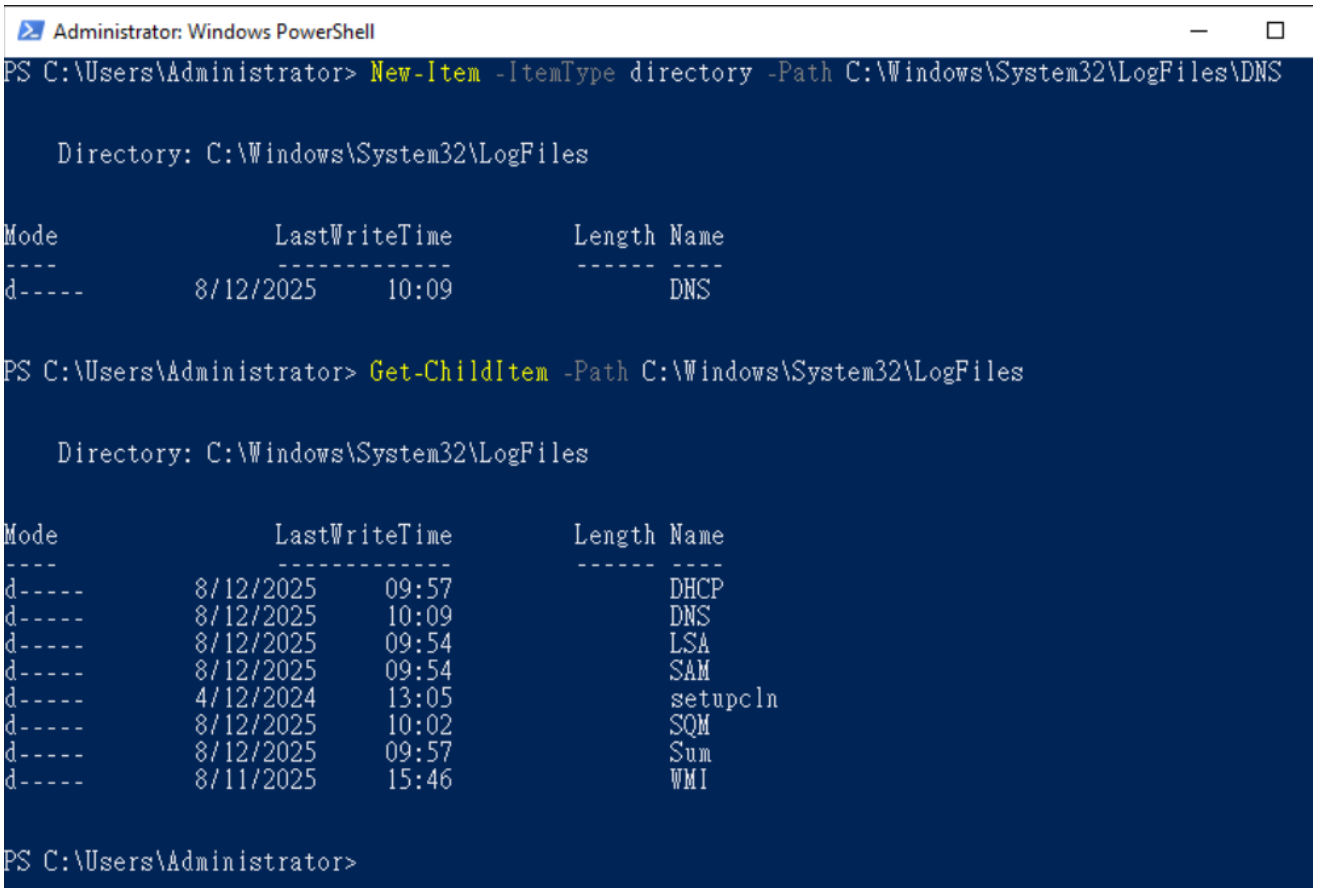


5. Windows Server 2019

(1) Open “Windows PowerShell.”

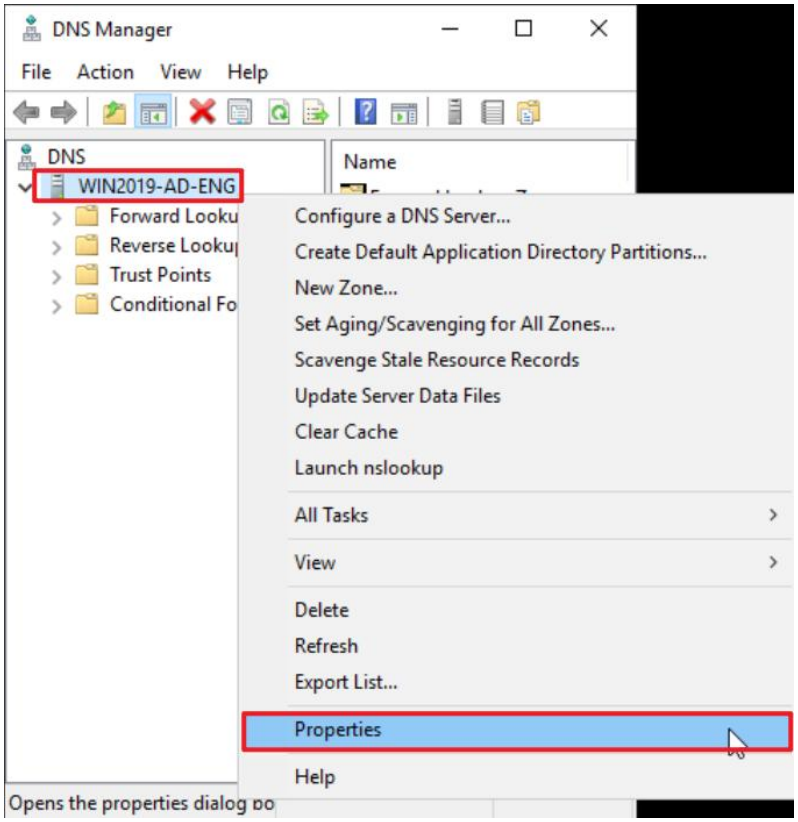
(2) Enter the command below to create the DNS log folder:

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

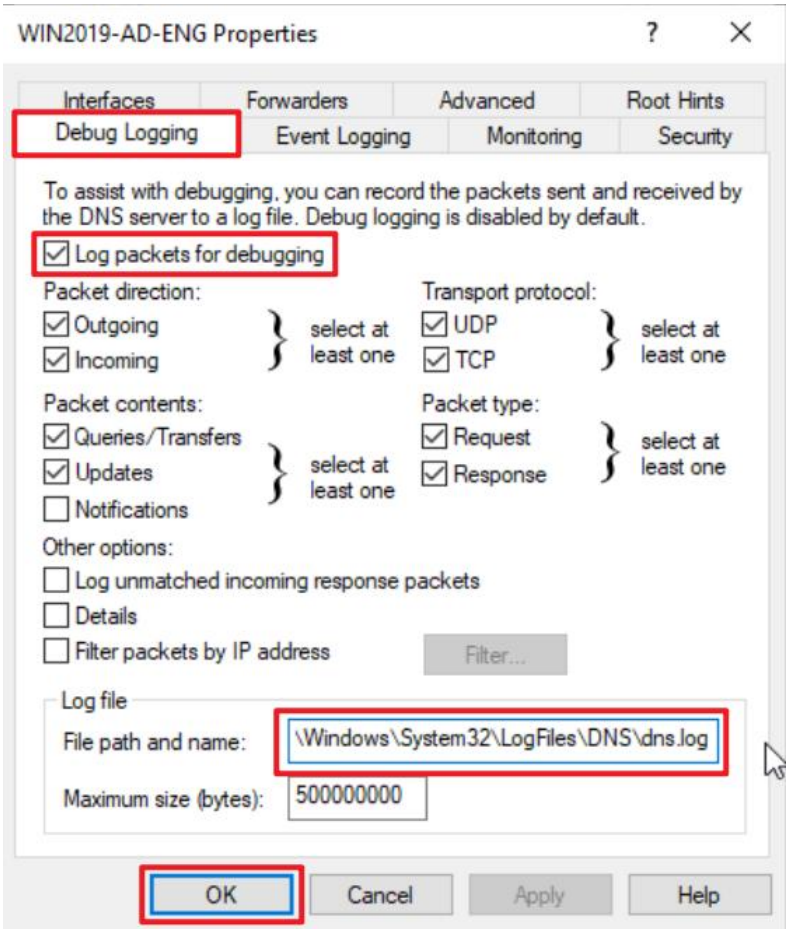


(3) Open DNS.

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



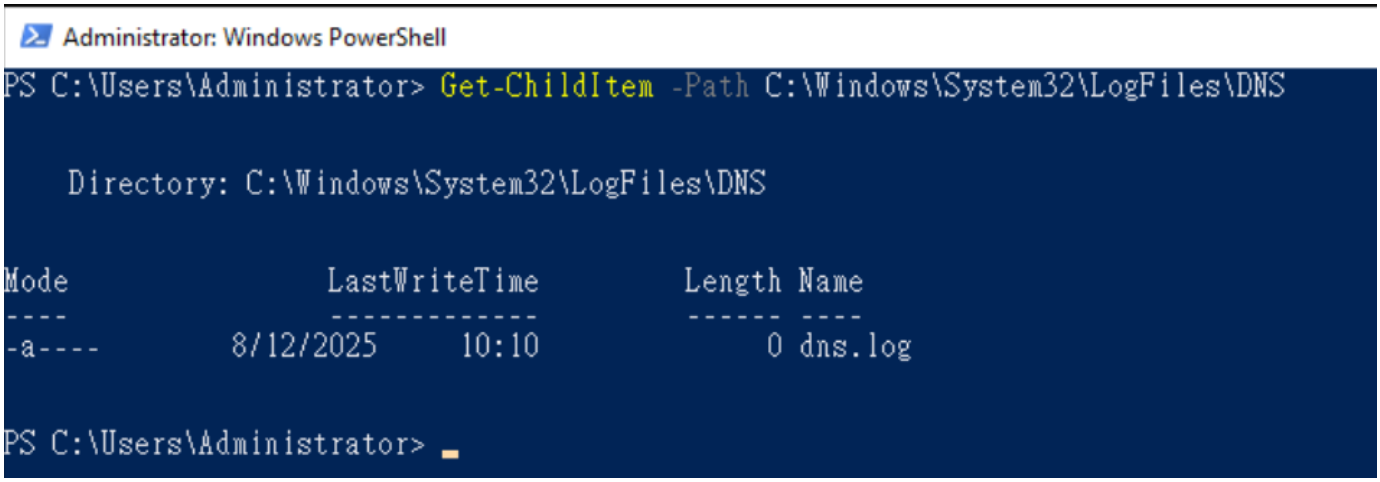
(5) On the “Debug Logging” tab → check “Log packets for debugging” → enter the “file path and name”: C:\Windows\System32\LogFiles\DNS\dns.log and click “OK.”



(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
```

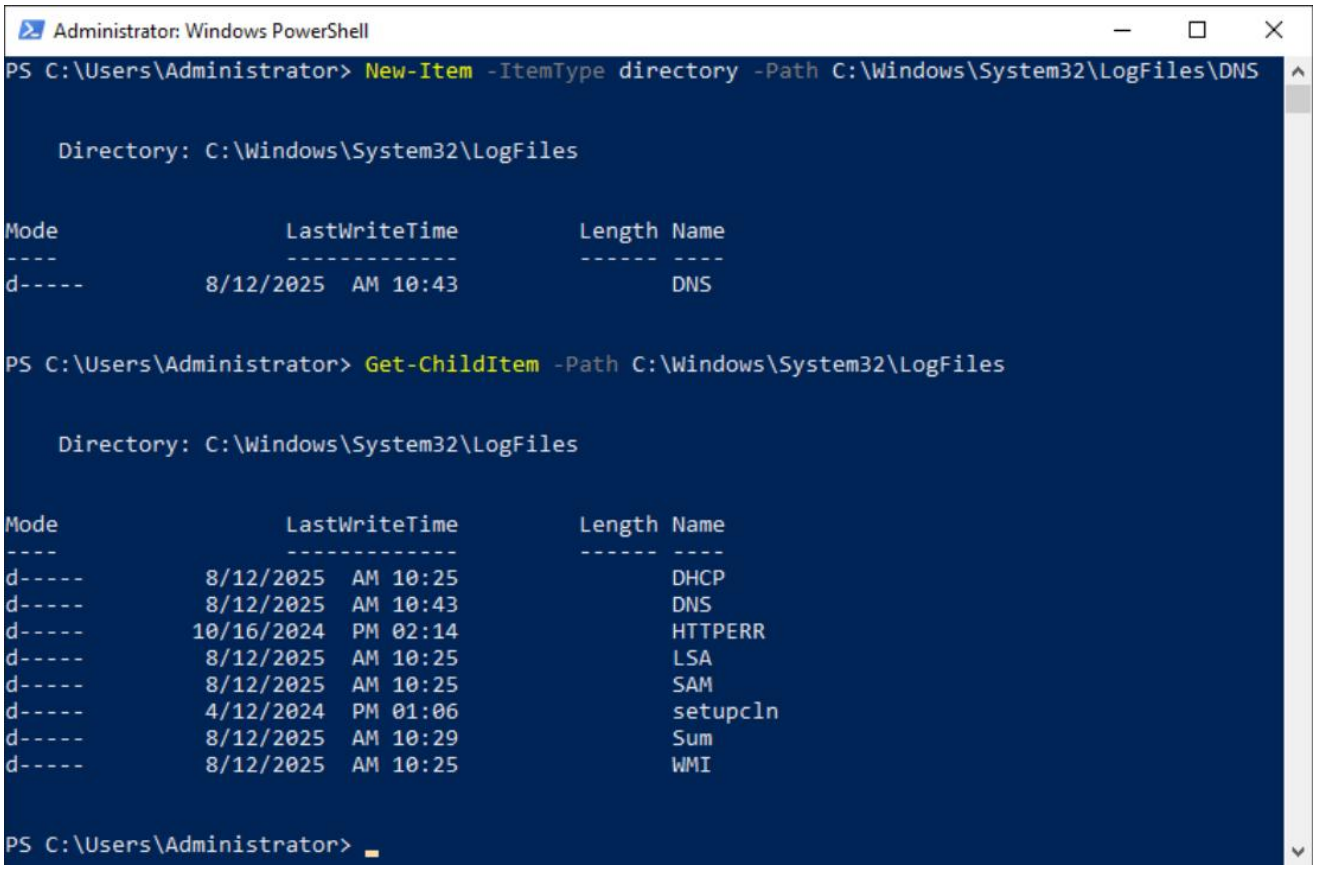


6. Windows Server 2022

(1) Open “Windows PowerShell.”

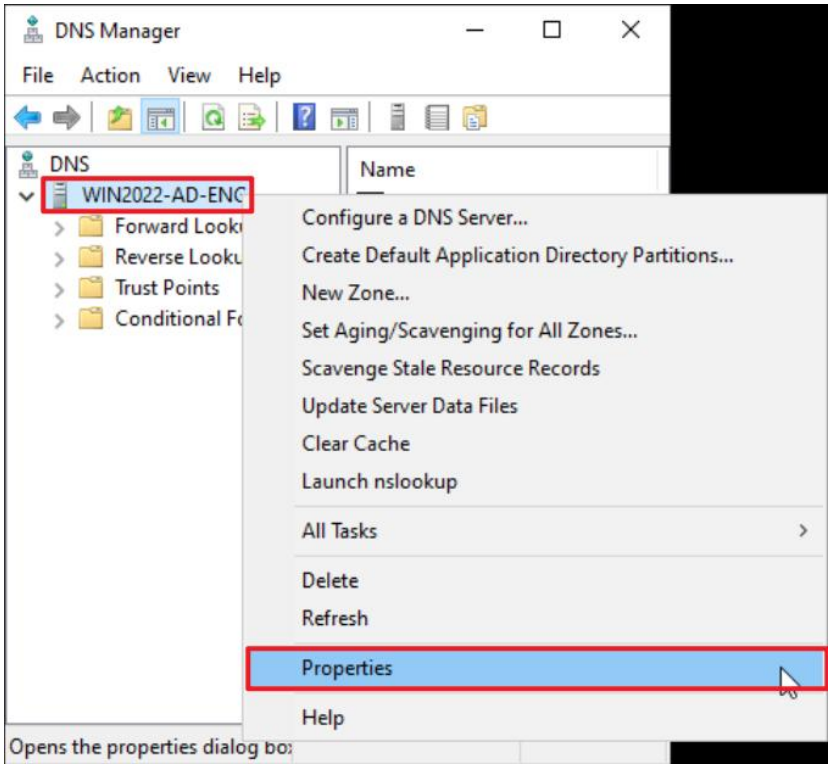
(2) Enter the command below to create the DNS log folder:

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

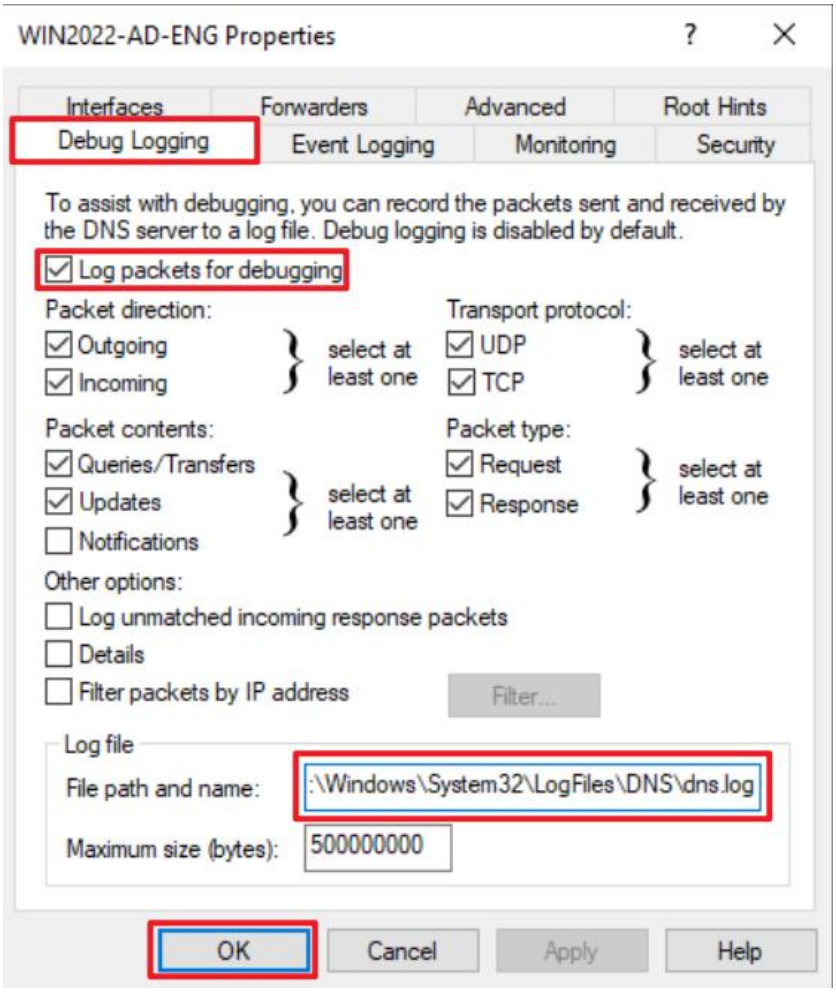


(3) Open DNS.

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



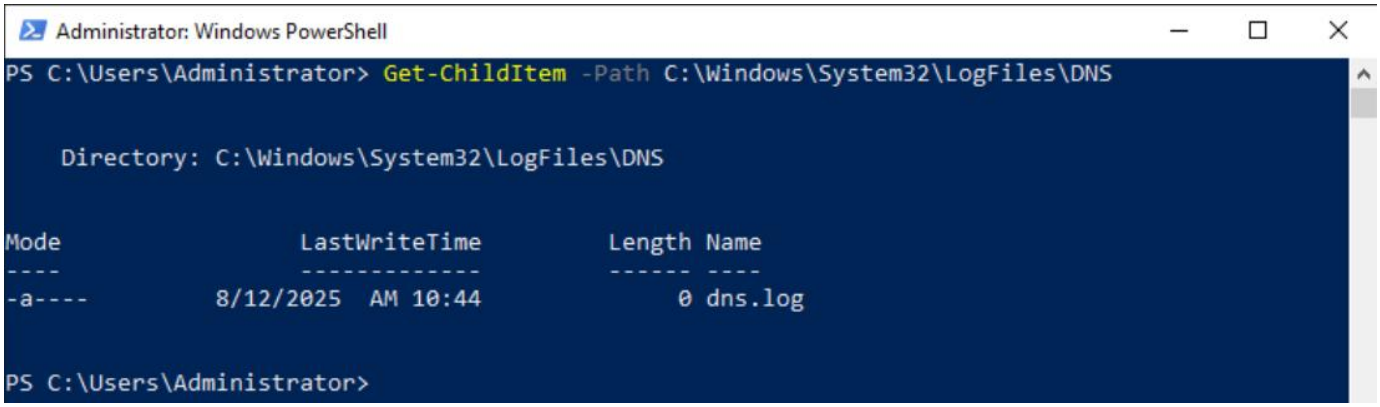
(5) On the “Debug Logging” tab → check “Log packets for debugging” → enter the “file path and name”: C:\Windows\System32\LogFiles\DNS\dns.log and click “OK.”



(6) Open “Windows PowerShell” again.

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

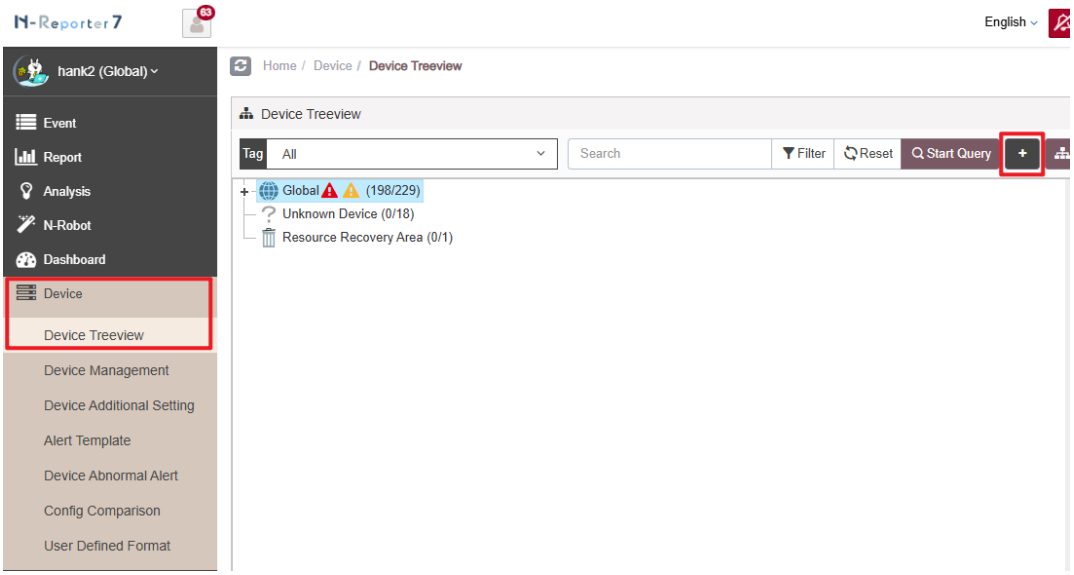
```
PS C:\> Get-ChildItem -Path C:\Windows\System32\LogFiles\DNS
```



7. N-Reporter

(1) Add a Windows DNS device:

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

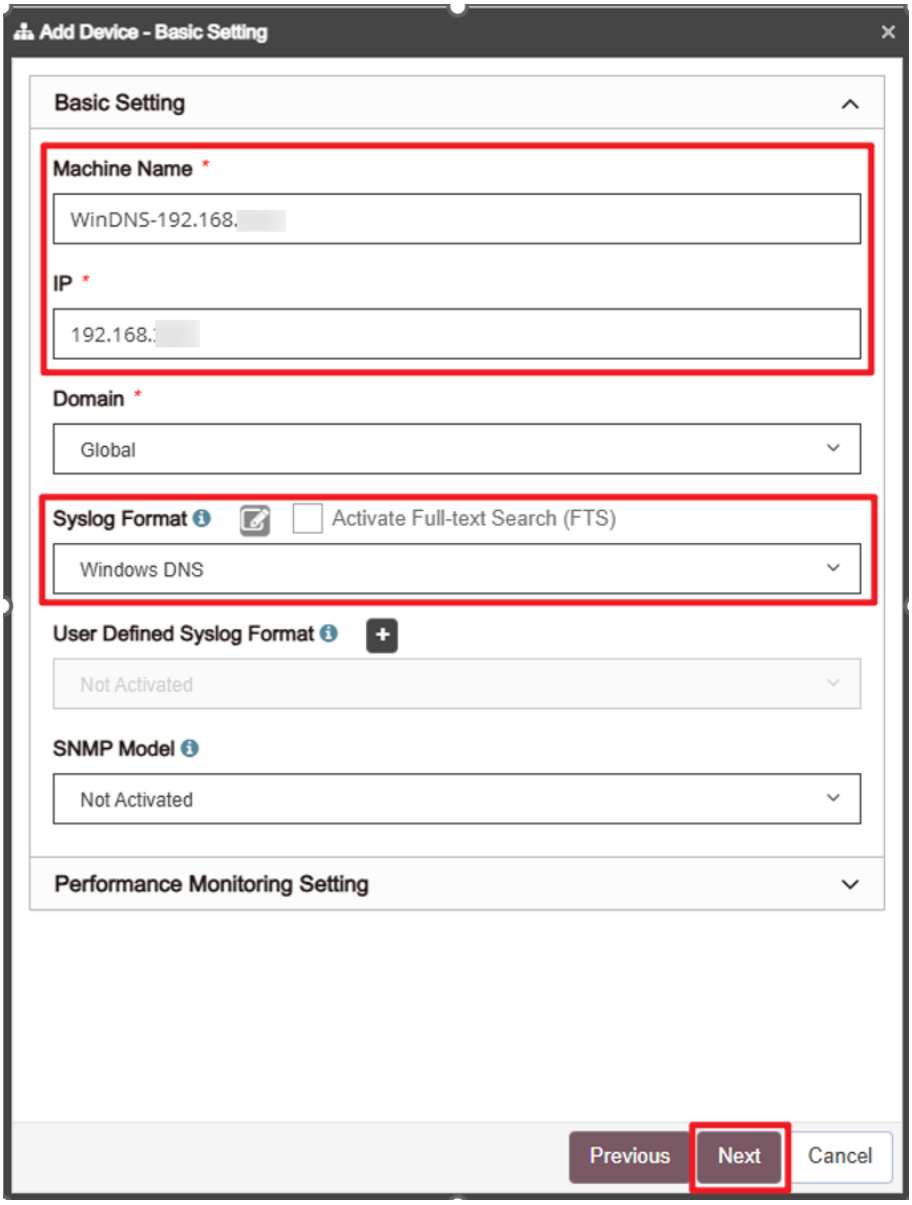


(2) Select the device type:

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

(3) Basic Device Settings:

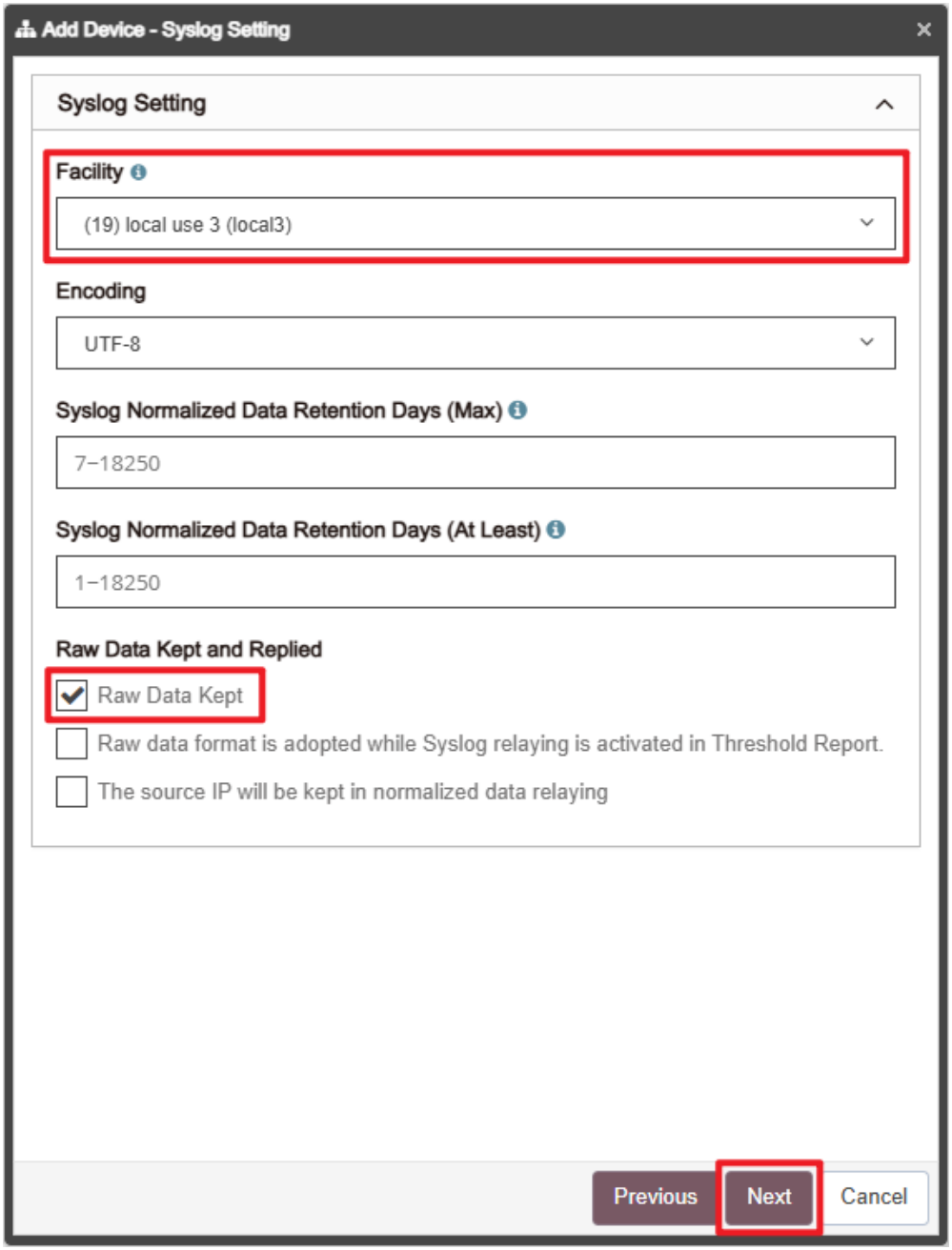
Enter the device name and IP address → For Syslog Data Format, select “Windows DNS” → click “Next.”



(4) Syslog Settings

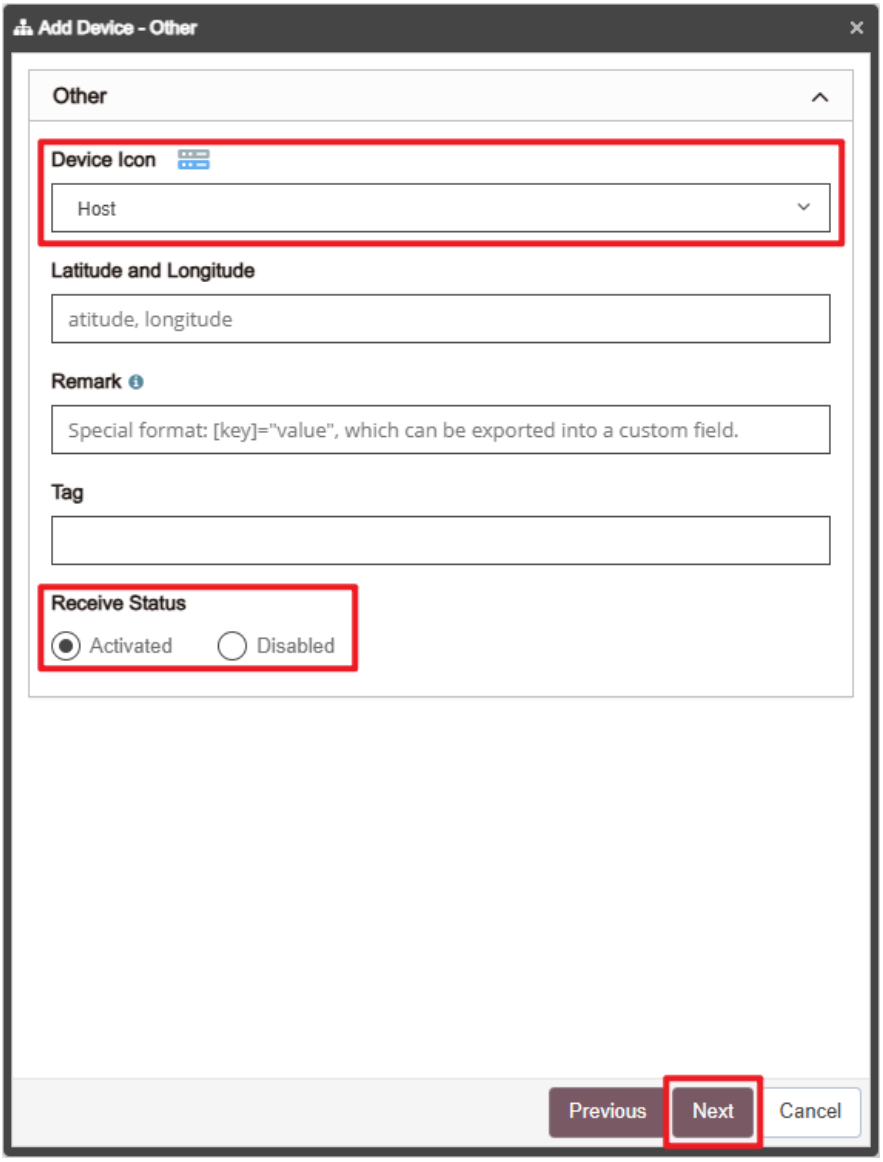
Set “Facility” to “(19) local use 3 (local3)” → click “Next.”

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

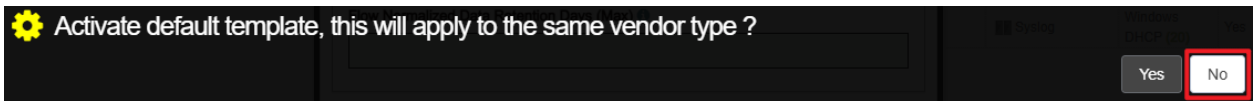


(5) Others

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



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



Tel：+886-4-23752865　Fax：+886-4-23757458
Sales Information：sales@npartner.com
Technical Support：support@npartner.com