N-Partner

How to Configure MS SQL Audit Event Log

V021

2025/08/26

N-Reporter N-Cloud N-Probe N-Robot

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

This document describes how N-Reporter users can configure MS SQL event logging using the open-source tool NXLog.

NXLog converts MS SQL event 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.

References

sqlcmd Utility:

https://docs.microsoft.com/sql/tools/sqlcmd-utility?view=sql-server-ver15

Common Criteria Compliance (replaces C2 Audit Mode):

https://learn.microsoft.com/sql/database-engine/configure-windows/c2-audit-mode-server-configuration-option?view=sql-server-ver15

sys.dm_exec_sessions (Dynamic Management View):

https://docs.microsoft.com/sql/relational-databases/system-dynamic-management-views/sys-dm-exec-sessions-transact-sql?view=sql-server-ver15

sys.traces (System Catalog View):

https://docs.microsoft.com/sql/relational-databases/system-catalog-views/sys-traces-transact-sql?view=sql-server-ver15

Enable Common Criteria Compliance Server Configuration Option:

https://docs.microsoft.com/sql/database-engine/configure-windows/common-criteria-compliance-enabled-server-configuration-option?view=sql-server-ver15

Configure Login Auditing:

https://docs.microsoft.com/sql/ssms/configure-login-auditing-sql-server-management-studio?view=sql-server-ver15#SSMSProcedure

Server Audit and Server Audit Specification:

https://docs.microsoft.com/sql/relational-databases/security/auditing/create-a-server-audit-and-server-audit-specification?view=sql-server-ver15

Database Audit Specification:

https://docs.microsoft.com/sql/relational-databases/security/auditing/create-a-server-audit-and-database-audit-specification?view=sql-server-ver15

SQL Server Audit Action Groups and Actions:

https://docs.microsoft.com/sql/relational-databases/security/auditing/sql-server-audit-action-groups-and-actions?view=sql-server-ver15

Supported MS SQL Server Versions for Audit Logging

SQLServer/Version	Enterprise Edition	Developer Edition	Standard Edition	Web Edition	Express Edition
SQL Server **2008**	Server- and database-level audit	Server- and database-level audit	**Not supported**	**Not supported**	**Not supported**
SQL Server **2012 / 2014**	Server- and database-level audit	Server- and database-level audit	Server-level audit only	Server-level audit only	Server-level audit only
SQL Server **2016 / 2019 /2022**	Server- and database-level audit	Server- and database-level audit	Server- and database-level audit	Server- and database-level audit	Server- and database-level audit

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

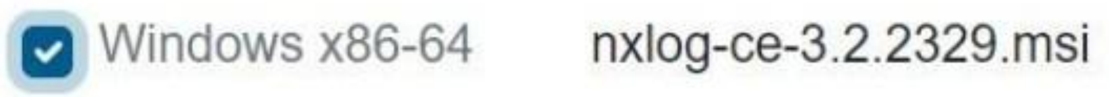
1.1 NXLog Installation

(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**

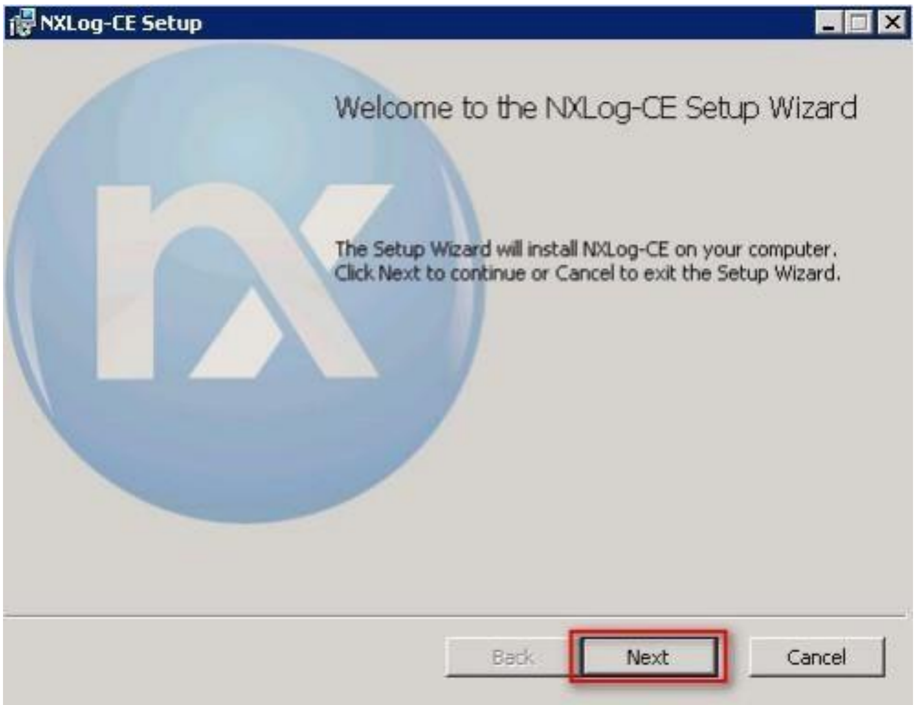


☑ Windows x86-64 nxlog-ce-3.2.2329.msi

(2) Install NXLog

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

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

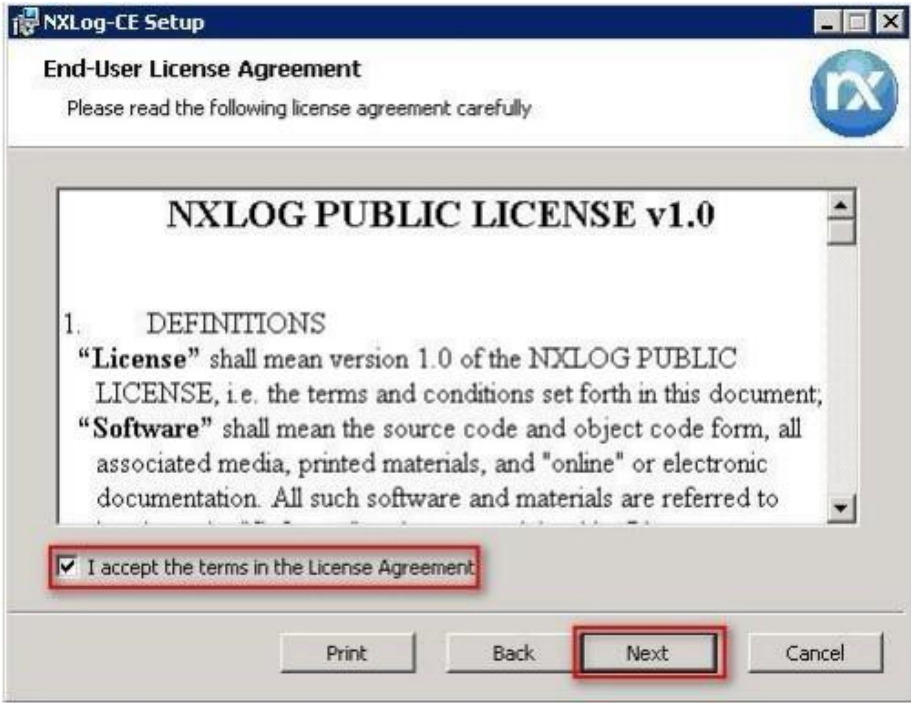


NXLog-CE Setup

Welcome to the NXLog-CE Setup Wizard

The Setup Wizard will install NXLog-CE on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

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



NXLog-CE Setup

End-User License Agreement

Please read the following license agreement carefully

NXLOG PUBLIC LICENSE v1.0

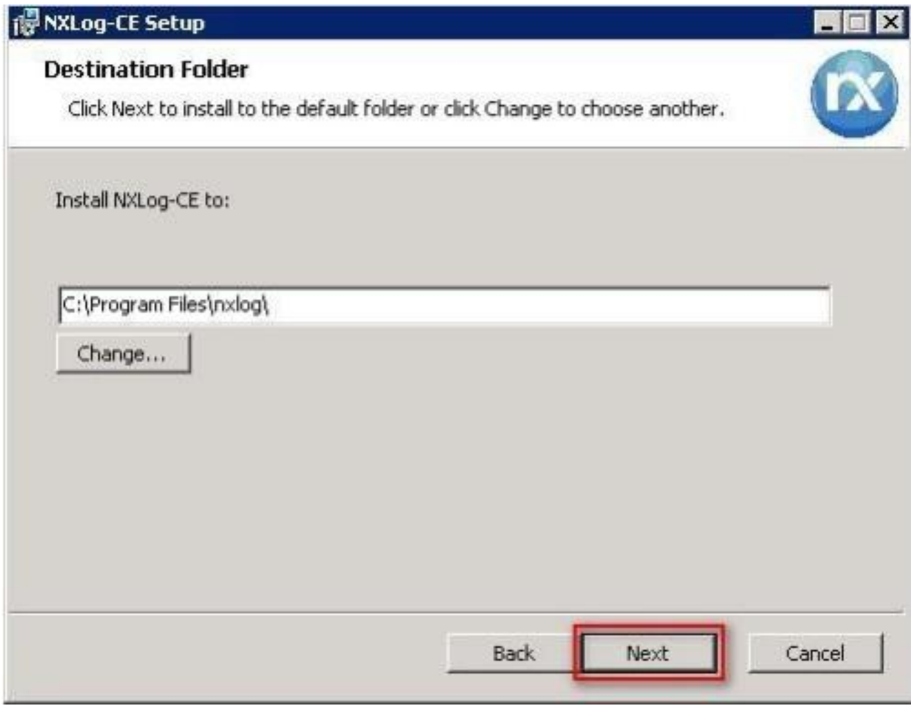
1. DEFINITIONS

“License” shall mean version 1.0 of the NXLOG PUBLIC LICENSE, i.e. the terms and conditions set forth in this document;

“Software” shall mean the source code and object code form, all associated media, printed materials, and "online" or electronic documentation. All such software and materials are referred to

☑ I accept the terms in the License Agreement

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



NXLog-CE Setup

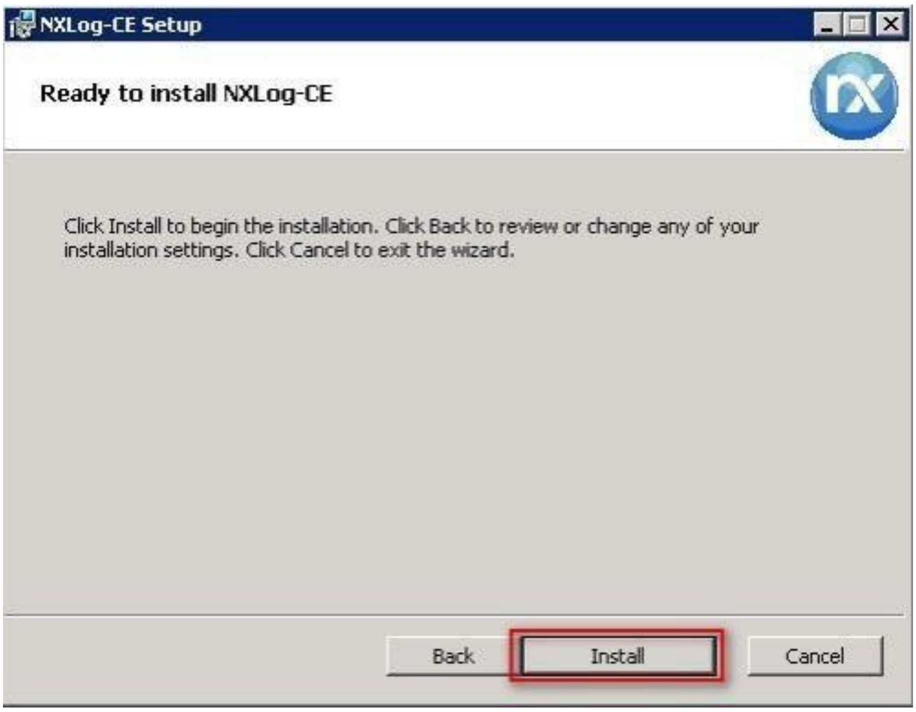
Destination Folder

Click Next to install to the default folder or click Change to choose another.

Install NXLog-CE to:

C:\Program Files\nxlog\

(5) Click "Install."

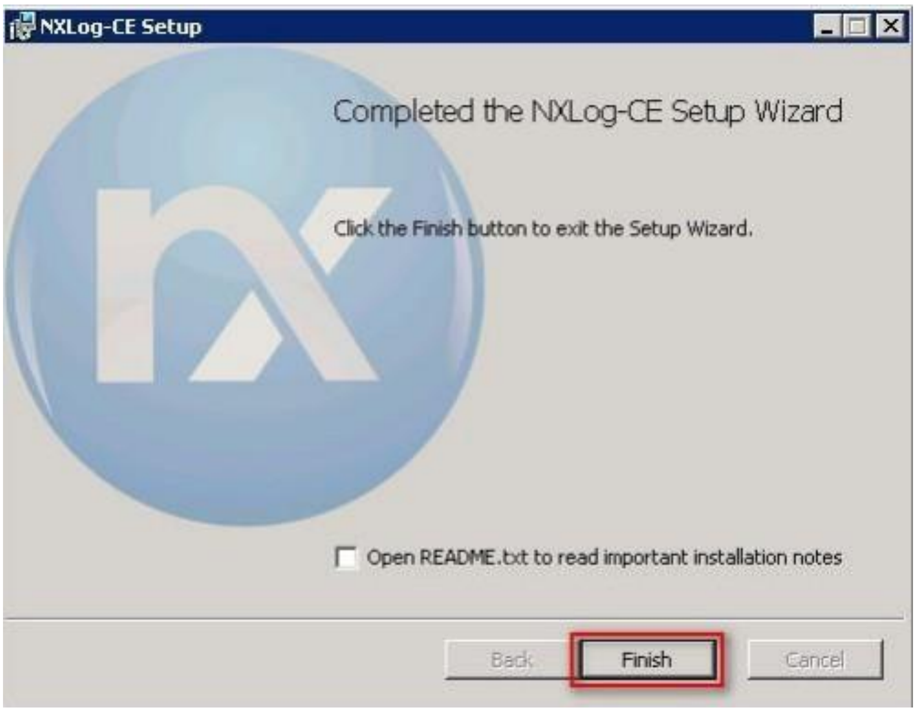


NXLog-CE Setup

Ready to install NXLog-CE

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

(6) Click "Finish."



NXLog-CE Setup

Completed the NXLog-CE Setup Wizard

Click the Finish button to exit the Setup Wizard.

□ Open README.txt to read important installation notes

1.2 Download NXLog Configuration File

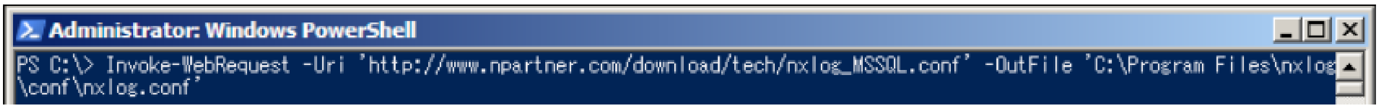
1.2.1 MS SQL Standalone (Non-Clustered) Configuration File

(1) Open “Windows PowerShell.”

(2) Download the “NXLog MS SQL standalone template configuration file” and overwrite the existing NXLog configuration file in the Windows system.

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

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



```
PS C:\> Invoke-WebRequest -Uri 'http://www.npartner.com/download/tech/nxlog_MSSQL.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'

1.2.2 MS SQL Cluster Configuration File

(1) Open “Windows PowerShell.”

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

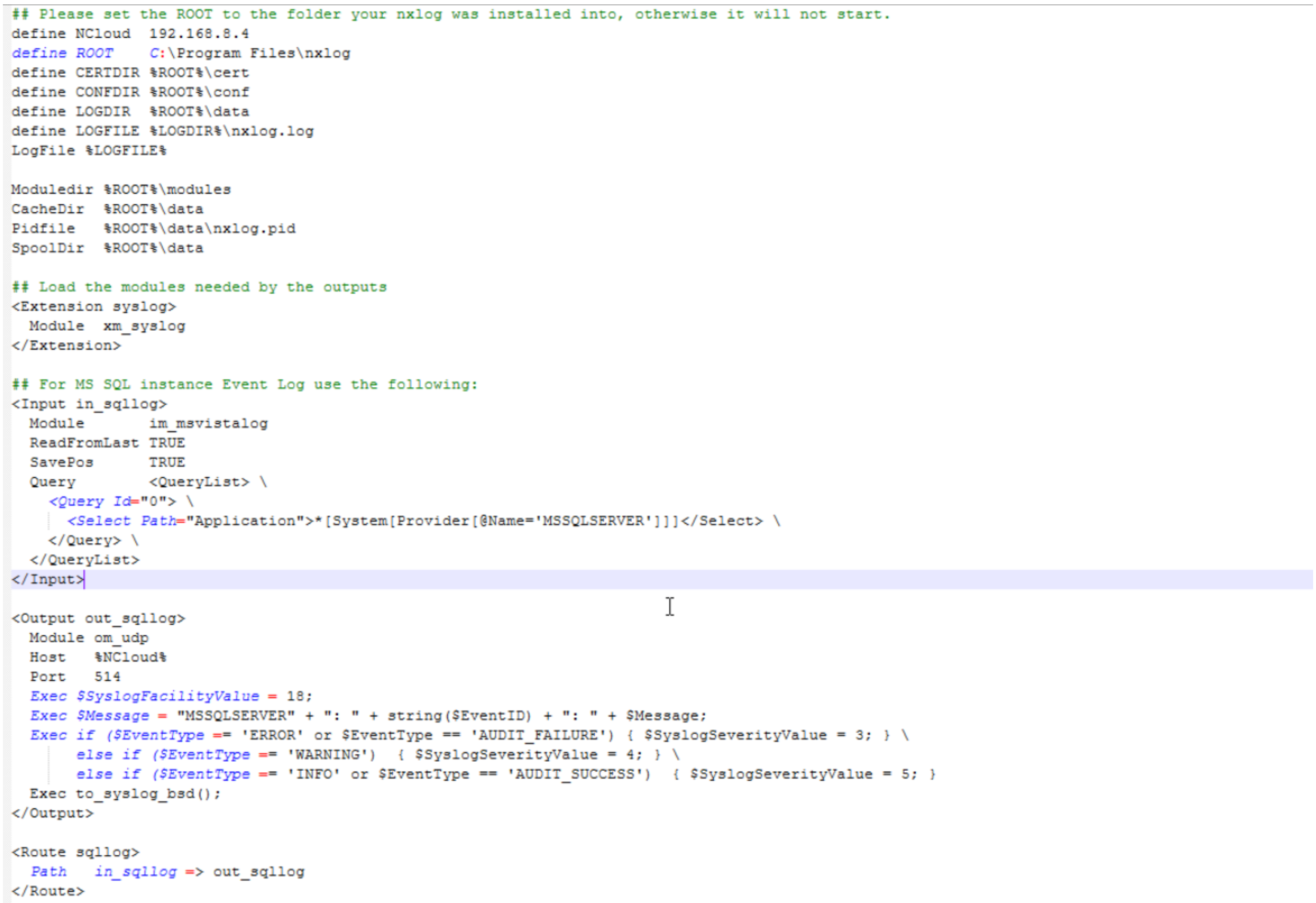
Download link: http://www.npartner.com/download/tech/nxlog_MSSQLcluster.conf

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

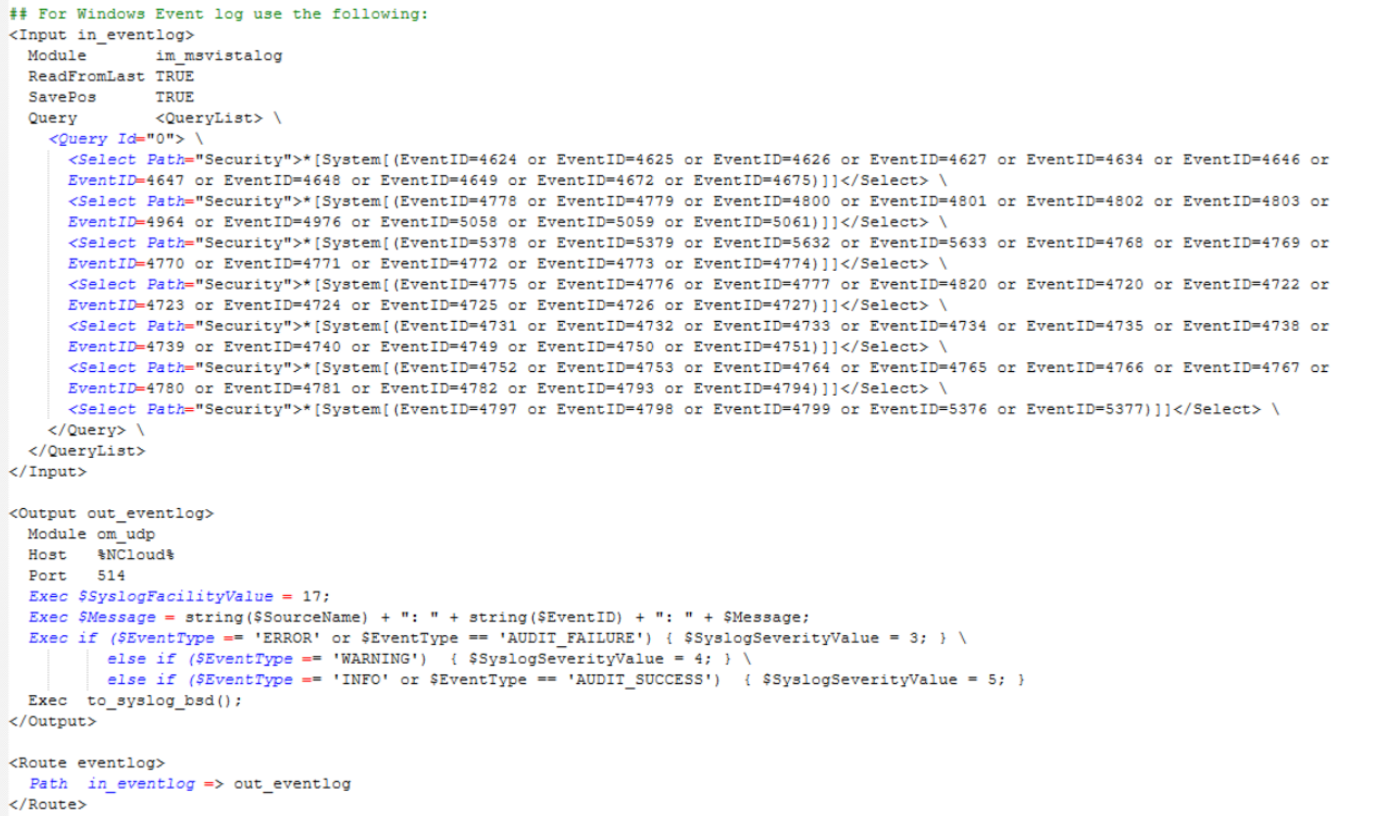
Note: This example is for a 64-bit operating system. For a 32-bit system, replace the highlighted text with: 'C:\ **Program Files(x86)**\nxlog\conf\nxlog.conf'

1.3 NXLog Configuration

1.3.1 MS SQL Standalone (Non-Clustered) Configuration File



```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud  192.168.8.4
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
SpoolDir  %ROOT%\data

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

## For MS SQL instance Event Log use the following:
<Input in_sqllog>
  Module       im_msvistalog
  ReadFromLast TRUE
  SavePos      TRUE
  Query        <QueryList> \
    <Query Id="0"> \
      <Select Path="Application">*[System[Provider[@Name='MSSQLSERVER']]]</Select> \
    </Query> \
  </QueryList>
</Input>

<Output out_sqllog>
  Module om_udp
  Host   %NCloud%
  Port   514
  Exec $SyslogFacilityValue = 18;
  Exec $Message = "MSSQLSERVER" + ": " + string($EventID) + ": " + $Message;
  Exec if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') { $SyslogSeverityValue = 3; } \
       else if ($EventType == 'WARNING')  { $SyslogSeverityValue = 4; } \
       else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS')  { $SyslogSeverityValue = 5; }
  Exec to_syslog_bsd();
</Output>

<Route sqllog>
  Path   in_sqllog => out_sqllog
</Route>
```



```
## For Windows Event log use the following:
<Input in_eventlog>
  Module       im_msvistalog
  ReadFromLast TRUE
  SavePos      TRUE
  Query        <QueryList> \
    <Query Id="0"> \
      <Select Path="Security">*[System[(EventID=4624 or EventID=4625 or EventID=4626 or EventID=4627 or EventID=4634 or EventID=4646 or
      EventID=4647 or EventID=4648 or EventID=4649 or EventID=4672 or EventID=4675)]]</Select> \
      <Select Path="Security">*[System[(EventID=4778 or EventID=4779 or EventID=4800 or EventID=4801 or EventID=4802 or EventID=4803 or
      EventID=4964 or EventID=4976 or EventID=5058 or EventID=5059 or EventID=5061)]]</Select> \
      <Select Path="Security">*[System[(EventID=5378 or EventID=5379 or EventID=5632 or EventID=5633 or EventID=4768 or EventID=4769 or
      EventID=4770 or EventID=4771 or EventID=4772 or EventID=4773 or EventID=4774)]]</Select> \
      <Select Path="Security">*[System[(EventID=4775 or EventID=4776 or EventID=4777 or EventID=4820 or EventID=4720 or EventID=4722 or
      EventID=4723 or EventID=4724 or EventID=4725 or EventID=4726 or EventID=4727)]]</Select> \
      <Select Path="Security">*[System[(EventID=4731 or EventID=4732 or EventID=4733 or EventID=4734 or EventID=4735 or EventID=4738 or
      EventID=4739 or EventID=4740 or EventID=4749 or EventID=4750 or EventID=4751)]]</Select> \
      <Select Path="Security">*[System[(EventID=4752 or EventID=4753 or EventID=4764 or EventID=4765 or EventID=4766 or EventID=4767 or
      EventID=4780 or EventID=4781 or EventID=4782 or EventID=4793 or EventID=4794)]]</Select> \
      <Select Path="Security">*[System[(EventID=4797 or EventID=4798 or EventID=4799 or EventID=5376 or EventID=5377)]]</Select> \
    </Query> \
  </QueryList>
</Input>

<Output out_eventlog>
  Module om_udp
  Host   %NCloud%
  Port   514
  Exec $SyslogFacilityValue = 17;
  Exec $Message = string($SourceName) + ": " + string($EventID) + ": " + $Message;
  Exec if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') { $SyslogSeverityValue = 3; } \
         else if ($EventType == 'WARNING')  { $SyslogSeverityValue = 4; } \
         else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS')  { $SyslogSeverityValue = 5; }
  Exec  to_syslog_bsd();
</Output>

<Route eventlog>
  Path  in_eventlog => out_eventlog
</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 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
SpoolDir %ROOT%\data

## Load the modules needed by the outputs
<Extension syslog>
Module xm_syslog
</Extension>
## For MS SQL instance Event Log use the following:
<Input im_sqllog>
Module im_msvistalog
ReadFromLast TRUE
SavePos TRUE
Query <QueryList> \
<Query Id="0"> \
<Select Path="Application">*[System[(Provider[@Name='MSSQLSERVER']]]</Select> \
</Query> \
</QueryList>
</Input>

<Output out_sqllog>
Module om_udp
Host %NCloud%
Port 514
Exec $SyslogFacilityValue = 18;
Exec $Message = "MSSQLSERVER" + ": " + string($EventID) + ": " + $Message;
Exec if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') {$SyslogSeverityValue = 3;}\
else if ($EventType == 'WARNING') {$SyslogSeverityValue = 4;}\
else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS') {$SyslogSeverityValue = 5;}
Exec to_syslog_bsd();
</Output>

<Route sqllog>
Path in_sqllog => out_sqllog
</Route>

## For Windows Event log use the following:
<Input in_eventlog>
Module im_msvistalog
ReadFromLast TRUE
SavePos TRUE
Query <QueryList> \
<Query Id="0"> \
<Select Path="Security">*[System[(EventID=4624 or EventID=4625 or EventID=4626
or EventID=4627 or EventID=4634 or EventID=4646 or EventID=4647 or EventID=4648 or EventID=4649 or
EventID=4672 or EventID=4675)]]</Select> \
<Select Path="Security">*[System[(EventID=4778 or EventID=4779 or EventID=4800
or EventID=4801 or EventID=4802 or EventID=4803 or EventID=4964 or EventID=4976 or EventID=5058 or
EventID=5059 or EventID=4061)]]</Select> \
<Select Path="Security">*[System[(EventID=5378 or EventID=5379 or EventID=5632
or EventID=5633 or EventID=4768 or EventID=4769 or EventID=4770 or EventID=4771 or EventID=4772 or
EventID=4773 or EventID=4774)]]</Select> \
<Select Path="Security">*[System[(EventID=4775 or EventID=4776 or EventID=4777
or EventID=4820 or EventID=4720 or EventID=4722 or EventID=4723 or EventID=4724 or EventID=4725 or
EventID=4726 or EventID=4727)]]</Select> \
<Select Path="Security">*[System[(EventID=4731 or EventID=4732 or EventID=4733
or EventID=4734 or EventID=4735 or EventID=4738 or EventID=4739 or EventID=4740 or EventID=4749 or
EventID=4750 or EventID=4751)]]</Select> \
<Select Path="Security">*[System[(EventID=4752 or EventID=4753 or EventID=4764
or EventID=4765 or EventID=4766 or EventID=4767 or EventID=4780 or EventID=4781 or EventID=4782 or
EventID=4793 or EventID=4794)]]</Select> \
<Select Path="Security">*[System[(EventID=4797 or EventID=4798 or EventID=4799 or
EventID=5376 or EventID=5377)]]</Select> \
</Query> \
</QueryList>
</Input>

<Output out_eventlog>
Module om_udp
Host %NCloud%
Port 514
Exec $SyslogFacilityValue = 17;
Exec $Message = string($SourceName) + ": " + string($EventID) + ": " + $Message;
Exec if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') {$SyslogSeverityValue = 3;}\
else if ($EventType == 'WARNING') {$SyslogSeverityValue = 4;}\
else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS') {$SyslogSeverityValue = 5;}
Exec to_syslog_bsd();
</Output>

<Route eventlog>
Path in_eventlog => out_eventlog
</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.

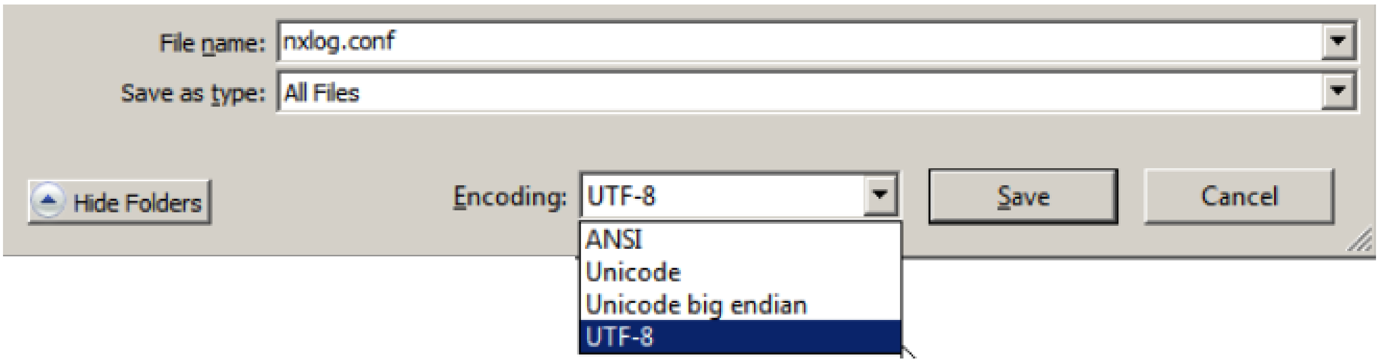
For a 32-bit operating system, use the following setting instead:

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

Replace the text shown in blue with the MS SQL instance name.

```
<Select Path=”Application”>*[System[(Provider[@Name='MSSQLSERVER']]] \
```

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.

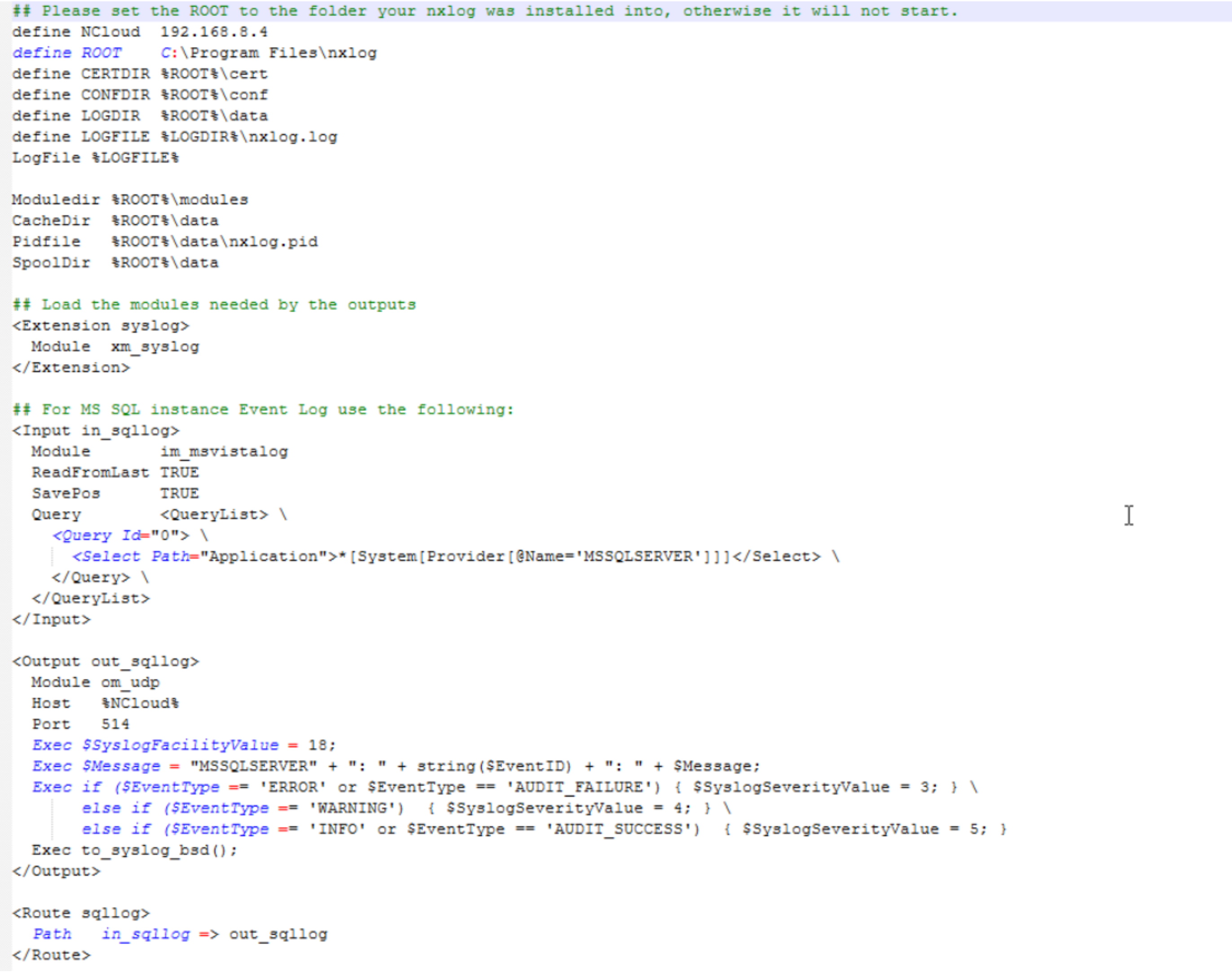


File name: nxlog.conf

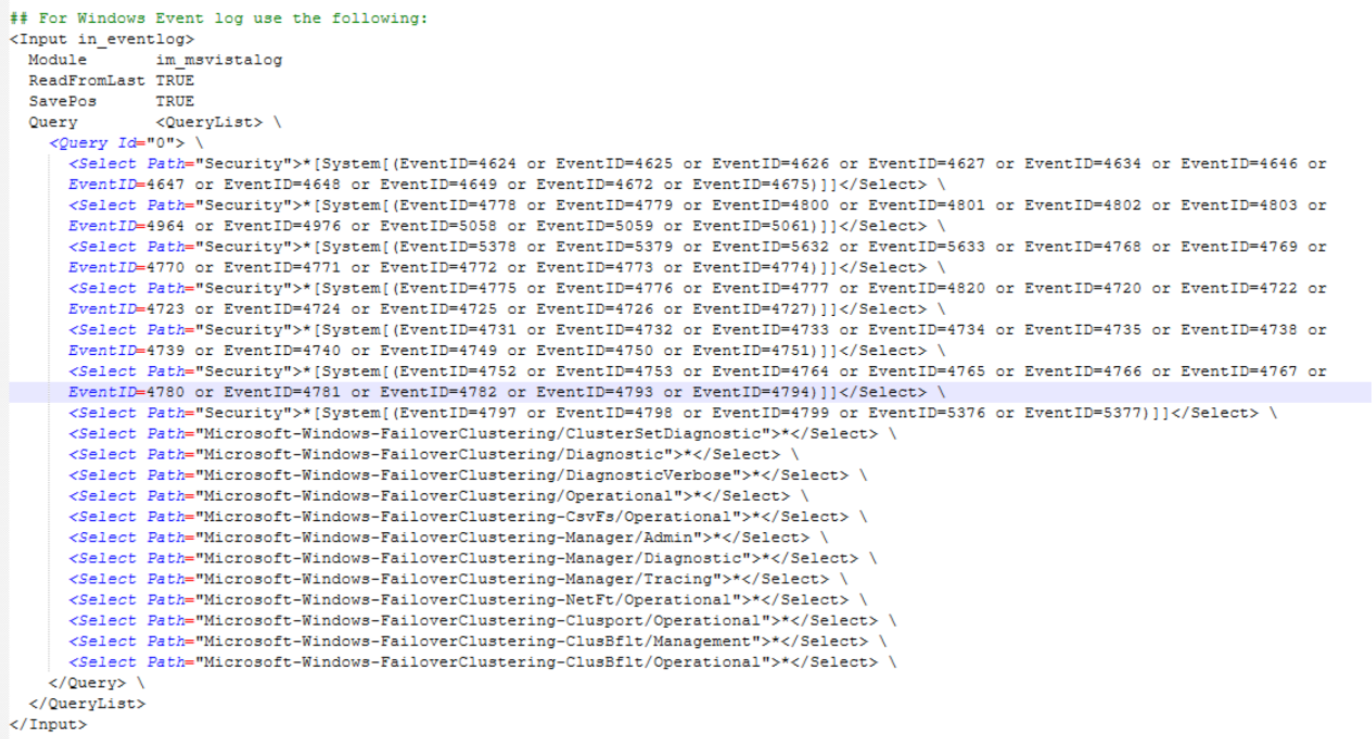
Save as type: All Files

Encoding: UTF-8

1.3.2 MS SQL Cluster Configuration File



```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud  192.168.8.4
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
SpoolDir  %ROOT%\data

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

## For MS SQL instance Event Log use the following:
<Input in_sqllog>
  Module       im_msvistalog
  ReadFromLast TRUE
  SavePos      TRUE
  Query        <QueryList> \
    <Query Id="0"> \
      <Select Path="Application">*[System[Provider[@Name='MSSQLSERVER']]]</Select> \
    </Query> \
  </QueryList>
</Input>

<Output out_sqllog>
  Module om_udp
  Host   %NCloud%
  Port   514
  Exec $SyslogFacilityValue = 18;
  Exec $Message = "MSSQLSERVER" + ": " + string($EventID) + ": " + $Message;
  Exec if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') { $SyslogSeverityValue = 3; } \
       else if ($EventType == 'WARNING')  { $SyslogSeverityValue = 4; } \
       else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS')  { $SyslogSeverityValue = 5; }
  Exec to_syslog_bsd();
</Output>

<Route sqllog>
  Path   in_sqllog => out_sqllog
</Route>
```



```
## For Windows Event log use the following:
<Input in_eventlog>
  Module       im_msvistalog
  ReadFromLast TRUE
  SavePos      TRUE
  Query        <QueryList> \
    <Query Id="0"> \
      <Select Path="Security">*[System[(EventID=4624 or EventID=4625 or EventID=4626 or EventID=4627 or EventID=4634 or EventID=4646 or
      EventID=4647 or EventID=4648 or EventID=4649 or EventID=4672 or EventID=4675)]]</Select> \
      <Select Path="Security">*[System[(EventID=4778 or EventID=4779 or EventID=4800 or EventID=4801 or EventID=4802 or EventID=4803 or
      EventID=4964 or EventID=4976 or EventID=5058 or EventID=5059 or EventID=5061)]]</Select> \
      <Select Path="Security">*[System[(EventID=5378 or EventID=5379 or EventID=5632 or EventID=5633 or EventID=4768 or EventID=4769 or
      EventID=4770 or EventID=4771 or EventID=4772 or EventID=4773 or EventID=4774)]]</Select> \
      <Select Path="Security">*[System[(EventID=4775 or EventID=4776 or EventID=4777 or EventID=4820 or EventID=4720 or EventID=4722 or
      EventID=4723 or EventID=4724 or EventID=4725 or EventID=4726 or EventID=4727)]]</Select> \
      <Select Path="Security">*[System[(EventID=4731 or EventID=4732 or EventID=4733 or EventID=4734 or EventID=4735 or EventID=4738 or
      EventID=4739 or EventID=4740 or EventID=4749 or EventID=4750 or EventID=4751)]]</Select> \
      <Select Path="Security">*[System[(EventID=4752 or EventID=4753 or EventID=4764 or EventID=4765 or EventID=4766 or EventID=4767 or
      EventID=4780 or EventID=4781 or EventID=4782 or EventID=4793 or EventID=4794)]]</Select> \
      <Select Path="Security">*[System[(EventID=4797 or EventID=4798 or EventID=4799 or EventID=5376 or EventID=5377)]]</Select> \
      <Select Path="Microsoft-Windows-FailoverClustering/ClusterSetDiagnostic">*</Select> \
      <Select Path="Microsoft-Windows-FailoverClustering/Diagnostic">*</Select> \
      <Select Path="Microsoft-Windows-FailoverClustering/DiagnosticVerbose">*</Select> \
      <Select Path="Microsoft-Windows-FailoverClustering/Operational">*</Select> \
      <Select Path="Microsoft-Windows-FailoverClustering-CsvFs/Operational">*</Select> \
      <Select Path="Microsoft-Windows-FailoverClustering-Manager/Admin">*</Select> \
      <Select Path="Microsoft-Windows-FailoverClustering-Manager/Diagnostic">*</Select> \
      <Select Path="Microsoft-Windows-FailoverClustering-Manager/Tracing">*</Select> \
      <Select Path="Microsoft-Windows-FailoverClustering-NetFt/Operational">*</Select> \
      <Select Path="Microsoft-Windows-FailoverClustering-Clusport/Operational">*</Select> \
      <Select Path="Microsoft-Windows-FailoverClustering-ClusBflt/Management">*</Select> \
      <Select Path="Microsoft-Windows-FailoverClustering-ClusBflt/Operational">*</Select> \
    </Query> \
  </QueryList>
</Input>
```

```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud 192.168.8.4
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
SpoolDir %ROOT%\data

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

## For MS SQL instance Event Log use the following:
<Input im_sqllog>
Module im_msvistalog
ReadFromLast TRUE
SavePos TRUE
Query <QueryList> \
<Query Id="0"> \
<Select Path="Application">*[System[(Provider[@Name='MSSQLSERVER']]]</Select> \
</Query> \
</QueryList>
</Input>

<Output out_sqllog>
Module om_udp
Host %NCloud%
Port 514
Exec $SyslogFacilityValue = 18;
```

```
    Exec $Message = "MSSQLSERVER" + ": " + string($EventID) + ": " + $Message;
    Exec if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') {$SyslogSeverityValue = 3;}\
    else if ($EventType == 'WARNING') {$SyslogSeverityValue = 4;}\
    else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS') {$SyslogSeverityValue = 5;}
    Exec to_syslog_bsd();
    </Output>

    <Route sqllog>
    Path in_sqllog => out_sqllog
    </Route>
    ## For Windows Event log use the following:
    <Input in_eventlog>
    Module im_msvistalog
    ReadFromLast TRUE
    SavePos TRUE
    Query <QueryList> \
    <Query Id="0"> \
    <Select Path="Security">*[System[(EventID=4624 or EventID=4625 or EventID=4626
    or EventID=4627 or EventID=4634 or EventID=4646 or EventID=4647 or EventID=4648 or
EventID=4649 or
    EventID=4672 or EventID=4675)]]</Select> \
    <Select Path="Security">*[System[(EventID=4778 or EventID=4779 or EventID=4800
    or EventID=4801 or EventID=4802 or EventID=4803 or EventID=4964 or EventID=4976 or
EventID=5058 or
    EventID=5059 or EventID=4061)]]</Select> \
    <Select Path="Security">*[System[(EventID=5378 or EventID=5379 or EventID=5632
    or EventID=5633 or EventID=4768 or EventID=4769 or EventID=4770 or EventID=4771 or
EventID=4772 or
    EventID=4773 or EventID=4774)]]</Select> \
    <Select Path="Security">*[System[(EventID=4775 or EventID=4776 or EventID=4777
    or EventID=4820 or EventID=4720 or EventID=4722 or EventID=4723 or EventID=4724 or
EventID=4725 or
    EventID=4726 or EventID=4727)]]</Select> \
    <Select Path="Security">*[System[(EventID=4731 or EventID=4732 or EventID=4733
    or EventID=4734 or EventID=4735 or EventID=4738 or EventID=4739 or EventID=4740 or
EventID=4749 or
```

```
    EventID=4750 or EventID=4751)]]</Select> \
    <Select Path="Security">*[System[(EventID=4752 or EventID=4753 or EventID=4764
    or EventID=4765 or EventID=4766 or EventID=4767 or EventID=4780 or EventID=4781 or
EventID=4782 or
    EventID=4793 or EventID=4794)]]</Select> \
    <Select Path="Security">*[System[(EventID=4797 or EventID=4798 or EventID=4799 or
    EventID=5376 or EventID=5377)]]</Select> \
    <Select Path="Microsoft-Windows-FailoverClustering/ClusterSetDiagnostic">*</Select> \
    <Select Path="Microsoft-Windows-FailoverClustering/Diagnostic">*</Select> \
    <Select Path="Microsoft-Windows-FailoverClustering/DiagnosticVerbose">*</Select> \
    <Select Path="Microsoft-Windows-FailoverClustering/Operational">*</Select> \
    <Select Path="Microsoft-Windows-FailoverClustering-CsvFs/Operational">*</Select> \
    <Select Path="Microsoft-Windows-FailoverClustering-Manager/Admin">*</Select> \
    <Select Path="Microsoft-Windows-FailoverClustering-Manager/Diagnostic">*</Select> \
    <Select Path="Microsoft-Windows-FailoverClustering-Manager/Tracing">*</Select> \
    <Select Path="Microsoft-Windows-FailoverClustering-NetFt/Operational">*</Select> \
    <Select Path="Microsoft-Windows-FailoverClustering-Clusport/Operational">*</Select> \
    <Select Path="Microsoft-Windows-FailoverClustering-ClusBflt/Management">*</Select> \
    <Select Path="Microsoft-Windows-FailoverClustering-ClusBflt/Operational">*</Select> \
    </Query> \
    </QueryList>
    </Input>

    <Output out_eventlog>
    Module om_udp
    Host %NCloud%
    Port 514
    Exec $SyslogFacilityValue = 17;
    Exec $Message = string($SourceName) + ": " + string($EventID) + ": " + $Message;
    Exec if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') {$SyslogSeverityValue = 3;}\
    else if ($EventType == 'WARNING') {$SyslogSeverityValue = 4;}\
    else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS') {$SyslogSeverityValue = 5;}
    Exec to_syslog_bsd();
    </Output>

    <Route eventlog>
    Path in_eventlog => out_eventlog
    </Route>
```

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

```
define NCloud 192.168.8.4
```

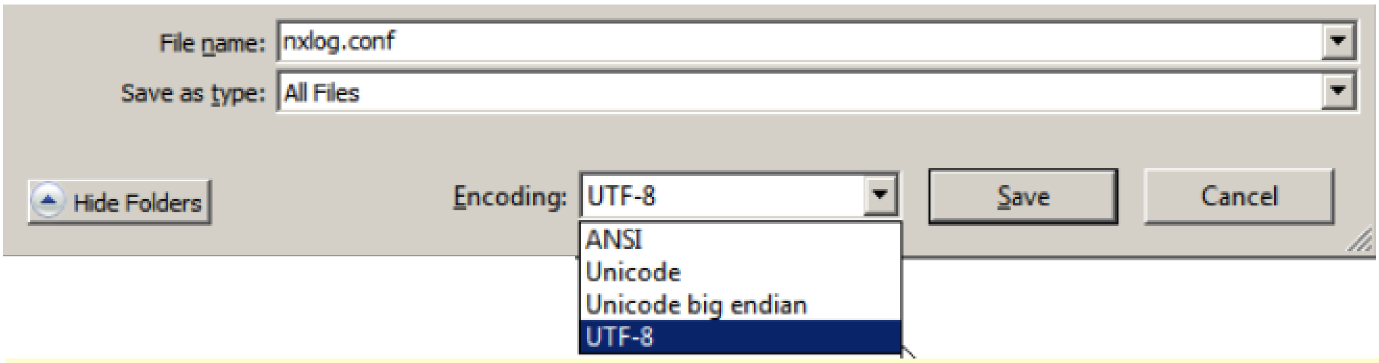
This example is based on a 64-bit operating system.

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

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

Replace the text shown in blue with the MS SQL instance name.

```
<Select Path=”Application”>*[System[(Provider[@Name='MSSQLSERVER']]] \
```



File name: nxlog.conf

Save as type: All Files

Encoding: UTF-8

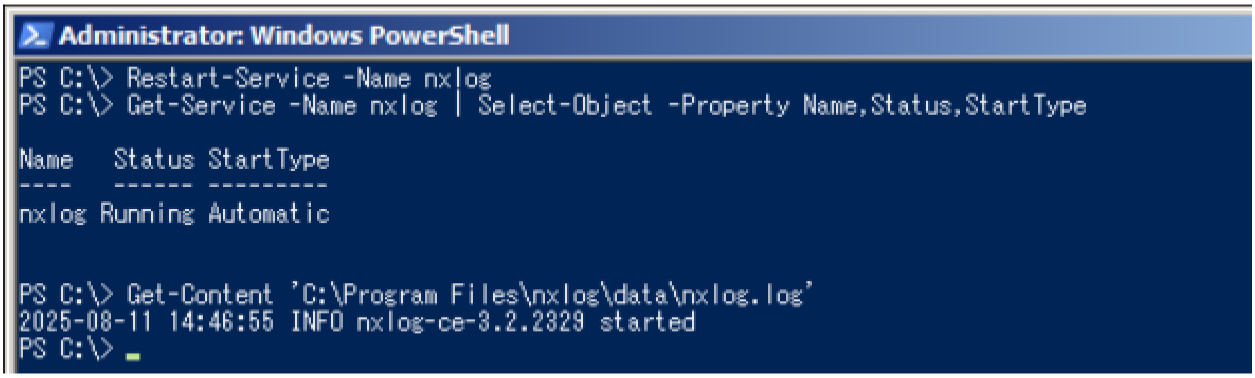
Note: After modifying the configuration file, save it as a new file to overwrite the original. For Save as type, select “All Files (*.*)”. For Encoding, select UTF-8 to avoid encoding errors that could prevent the service from starting.

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'
```

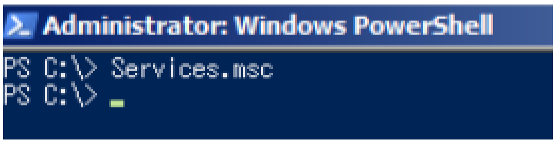


```
PS C:\> Restart-Service -Name nxlog
PS C:\> Get-Service -Name nxlog | Select-Object -Property Name,Status,StartType

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'

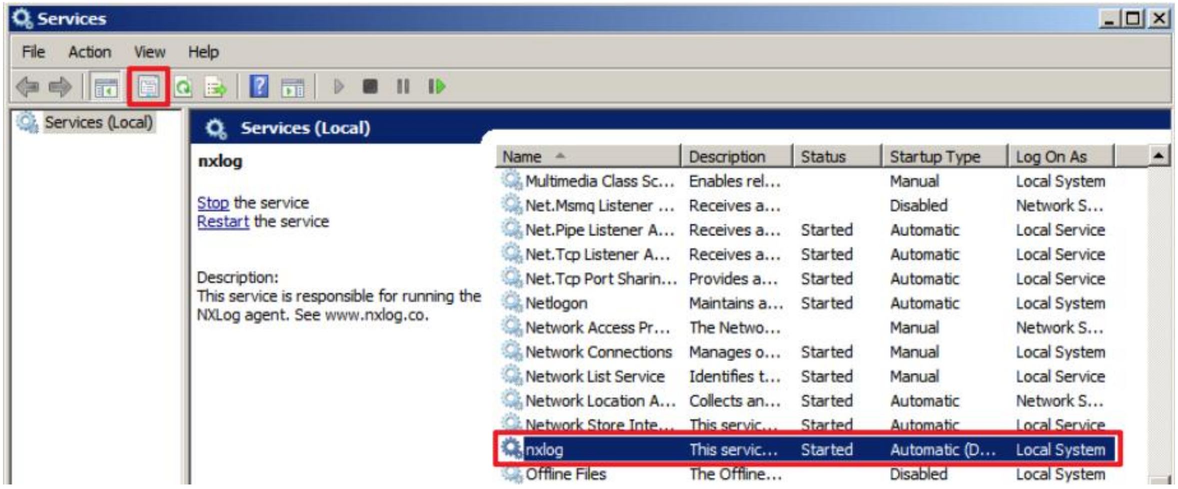
(3) Enter the command below to open the **Services** console:

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



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

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



Services (Local)

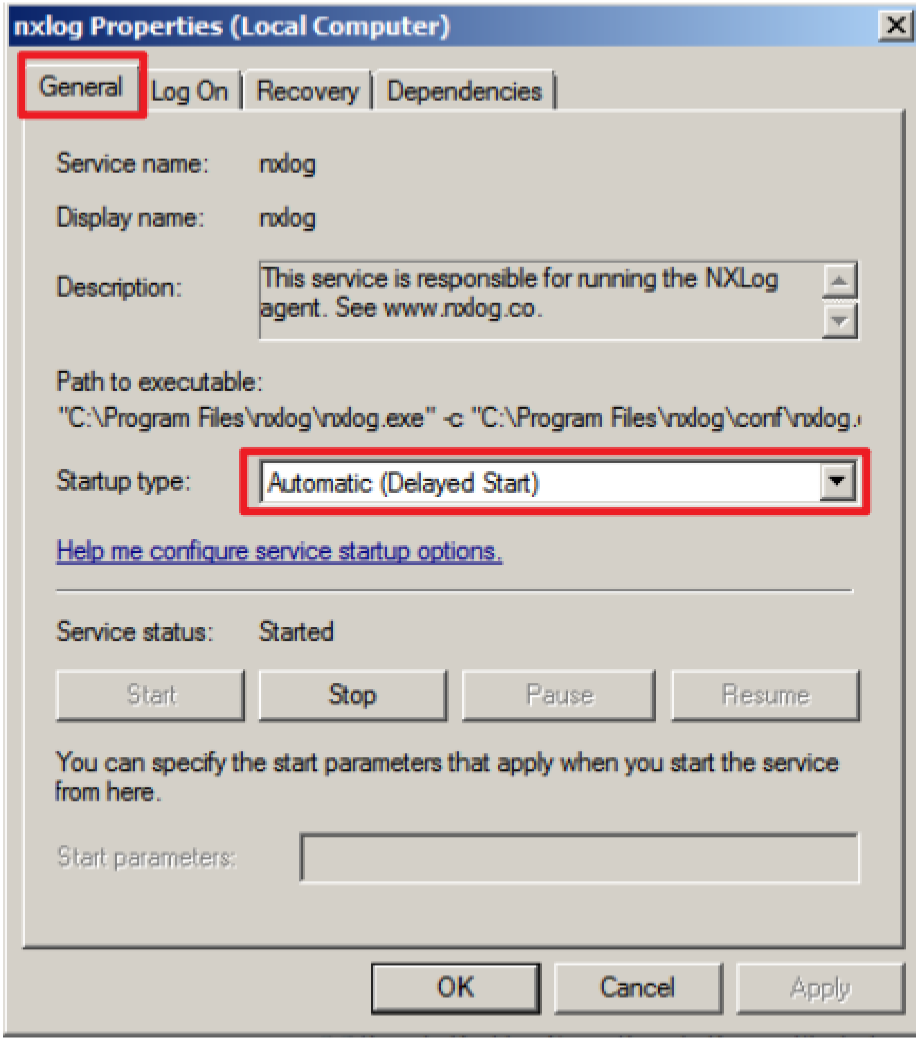
nxlog

Stop the service
Restart the service

Description:
This service is responsible for running the NXLog agent. See www.nxlog.co.

Name	Description	Status	Startup Type	Log On As
Multimedia Class Sc...	Enables rel...		Manual	Local System
Net.Msmq Listener ...	Receives a...		Disabled	Network S...
Net.Pipe Listener A...	Receives a...	Started	Automatic	Local Service
Net.Tcp Listener A...	Receives a...	Started	Automatic	Local Service
Net.Tcp Port Sharin...	Provides a...	Started	Automatic	Local Service
Netlogon	Maintains a...	Started	Automatic	Local System
Network Access Pr...	The Netwo...		Manual	Network S...
Network Connections	Manages o...	Started	Manual	Local System
Network List Service	Identifies t...	Started	Manual	Local Service
Network Location A...	Collects an...	Started	Automatic	Network S...
Network Store Inte...	This servic...	Started	Automatic	Local Service
nxlog	This servic...	Started	Automatic (D...	Local System
Offline Files	The Offline...		Disabled	Local System

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


nxlog Properties (Local Computer)
General
Log On
Recovery
Dependencies
Help me configure service startup options.
Start
Stop
Pause
Resume
OK
Cancel
Apply

Service name: nxlog

Display name: nxlog

Description: This service is responsible for running the NXLog agent. See www.nxlog.co.

Path to executable:
"C:\Program Files\nxlog\nxlog.exe" -c "C:\Program Files\nxlog\conf\nxlog.

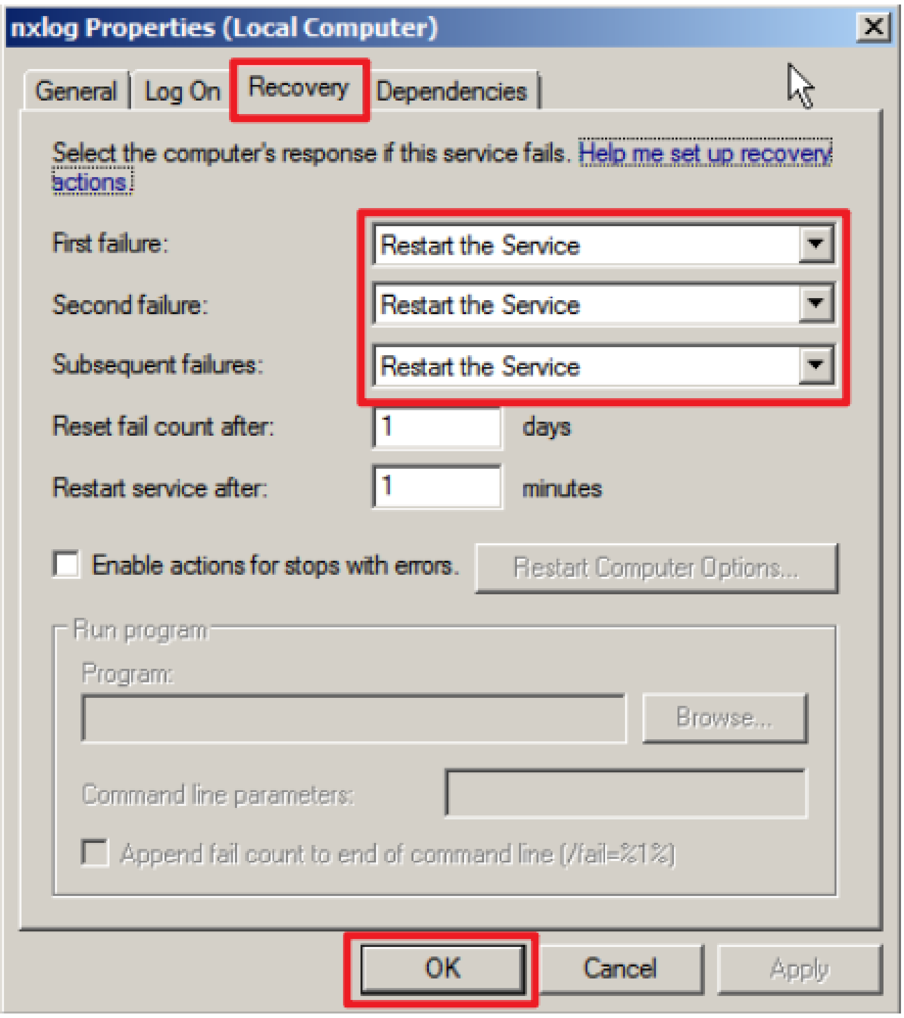
Startup type: Automatic (Delayed Start)

Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

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



nxlog Properties (Local Computer)

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. SQL Server 2008

2.1 Login Auditing

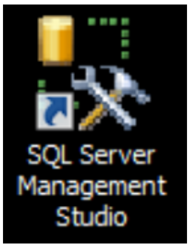
Enable login auditing to monitor SQL Server Database Engine login activities.

After configuration, the MS SQL Server service must be **restarted**.

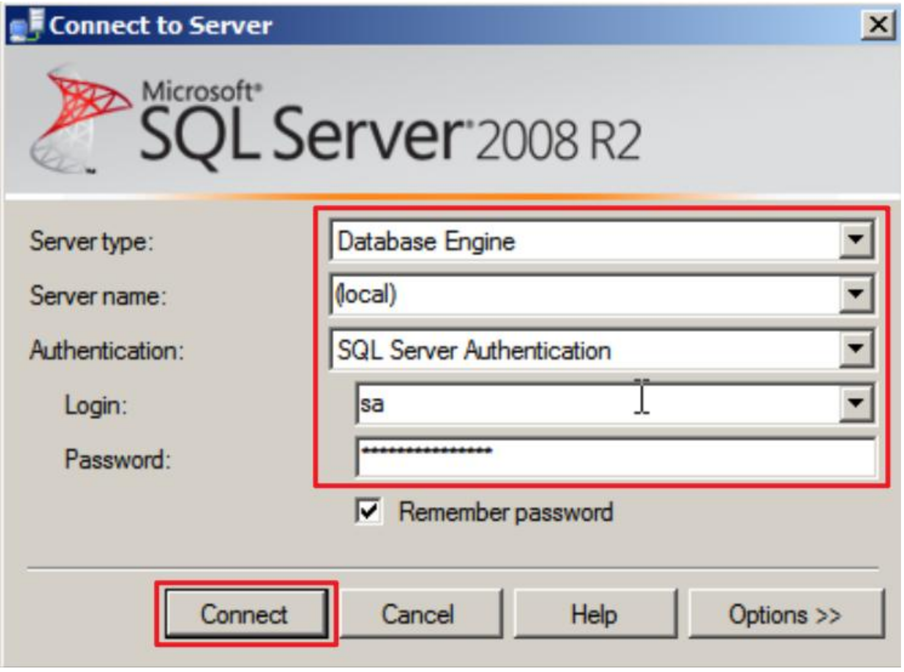
The following sections describe how to configure login auditing using both the graphical user interface (GUI) and command-line interface (CLI).

2.1.1 Configuring via Graphical User Interface (GUI)

(1) Open "SQL Server Management Studio (SSMS)."



(2) Enter the server's name → select the authentication method → click "Connect."



Server type: Database Engine

Server name: (local)

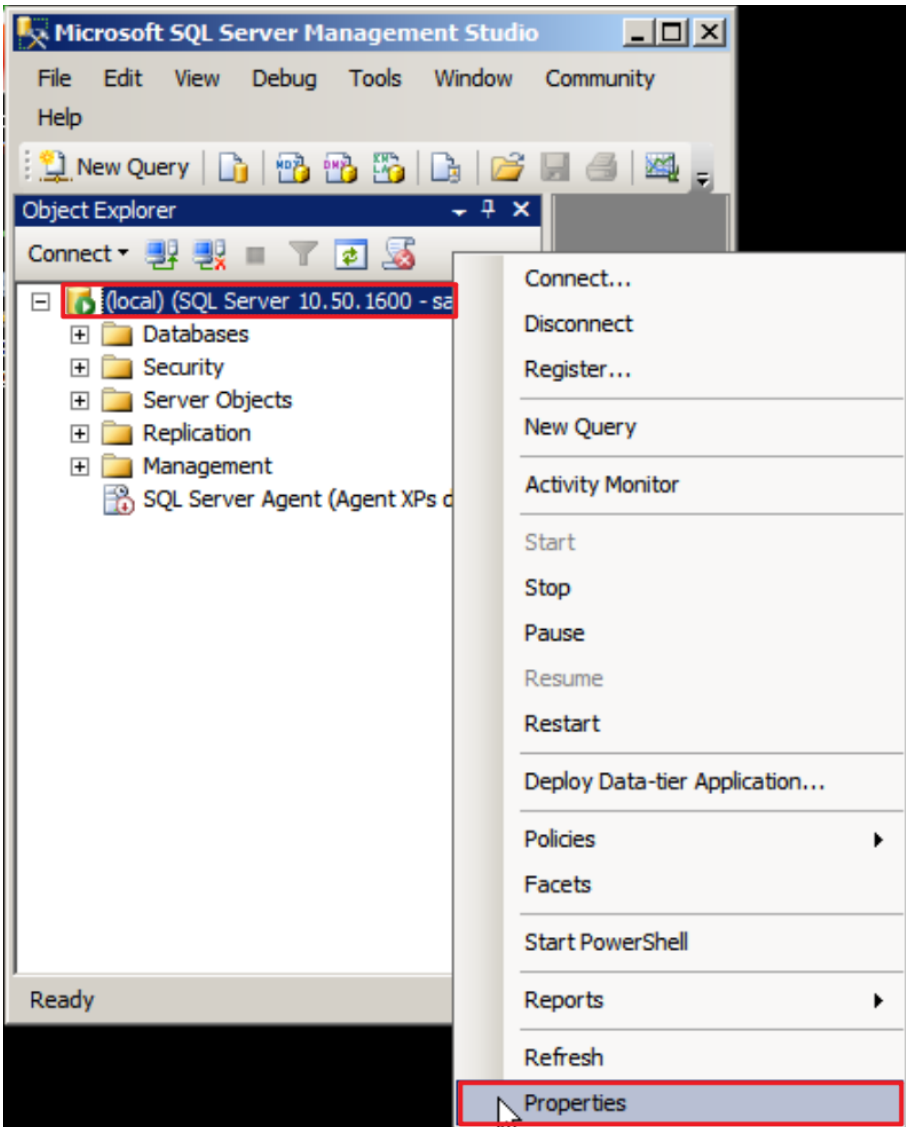
Authentication: SQL Server Authentication

Login: sa

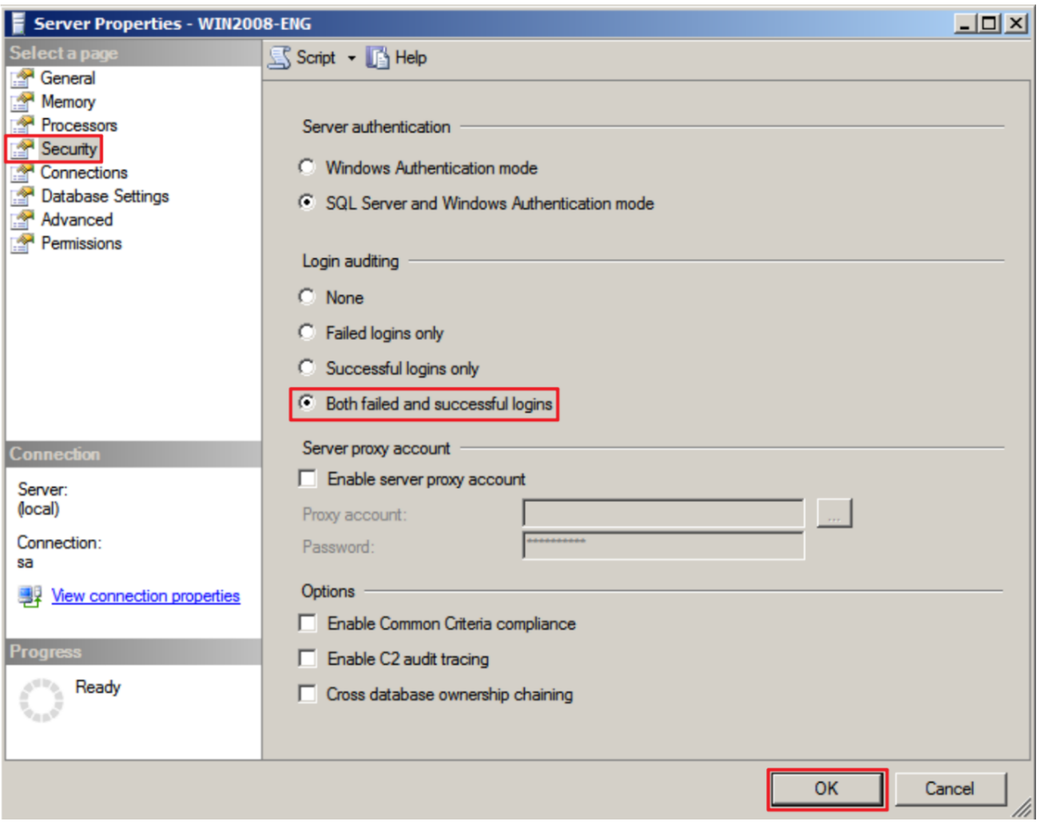
Password: ****************

☑ Remember password

(3) In [Server Name] (the example here is SQL Server 10.50.1600), right-click and select “Properties.”



(4) On the Security page, under Login auditing, select “Both failed and successful logins” → click “OK”.



Server Properties - WIN2008-ENG

Select a page: General, Memory, Processors, Security, Connections, Database Settings, Advanced, Permissions

Server authentication

○ Windows Authentication mode

● SQL Server and Windows Authentication mode

Login auditing

○ None

○ Failed logins only

○ Successful logins only

● Both failed and successful logins

Server proxy account

□ Enable server proxy account

Proxy account:

Password: ***********

Options

□ Enable Common Criteria compliance

□ Enable C2 audit tracing

□ Cross database ownership chaining

Connection

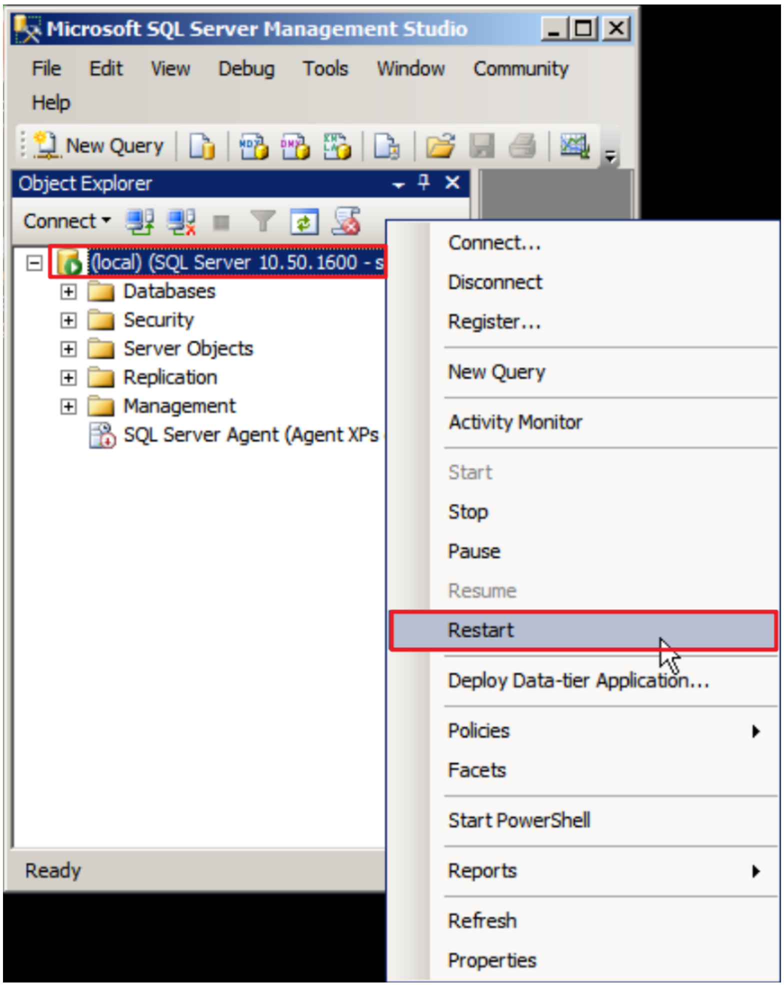
Server:
(local)

Connection:
sa

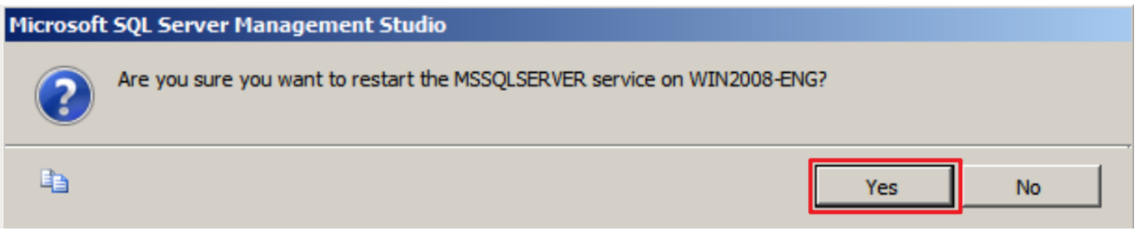
Progress

Ready

(5) Restart the MS SQL Server service: right-click [Server Name] (the example here is SQL Server 10.50.1600) → select “Restart.”



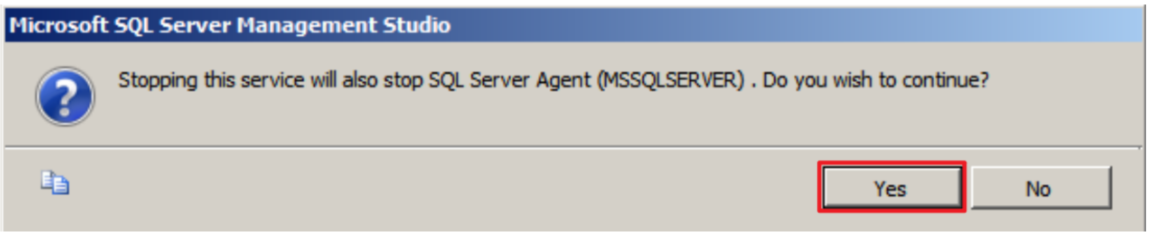
(6) Click “Yes” to restart the MS SQL Server service.



Microsoft SQL Server Management Studio

Are you sure you want to restart the MSSQLSERVER service on WIN2008-ENG?

(7) Click “Yes” again to stop the SQL Server Agent service.

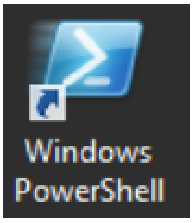


Microsoft SQL Server Management Studio

Stopping this service will also stop SQL Server Agent (MSSQLSERVER) . Do you wish to continue?

2.1.2 Configuring via Command-Line Interface (CLI)

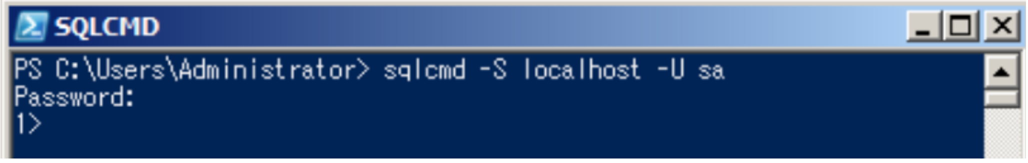
(1) Open “Windows PowerShell.”



(2) Enter the command below to log in using sa:

<2.1>Using sa account:

```
PS C:\> sqlcmd -S localhost -U sa
```



```
PS C:\Users\Administrator> sqlcmd -S localhost -U sa
Password:
1>
```

Options:

-S [protocol:]server[instance_name][,port]

-U login_id

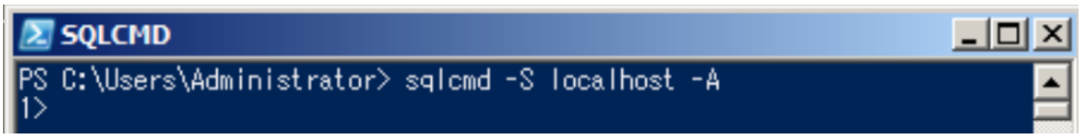
-P password

-A dedicated administrator connection

<2.2> Using Windows account:

Enter the command below to log in using Windows account:

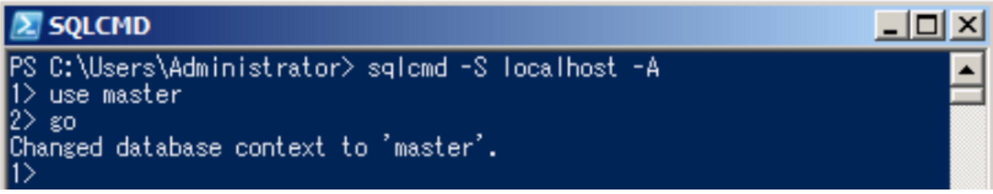
```
PS C:\> sqlcmd -S localhost -A
```



```
PS C:\Users\Administrator> sqlcmd -S localhost -A
1>
```

(3) Enter the command below to switch to the **master** database:

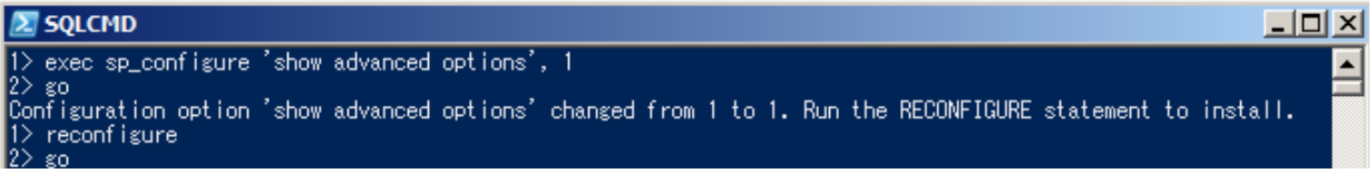
```
1 > use master
2 > go
```



```
PS C:\Users\Administrator> sqlcmd -S localhost -A
1> use master
2> go
Changed database context to 'master'.
1>
```

(4) Enter the command below to enable advanced options:

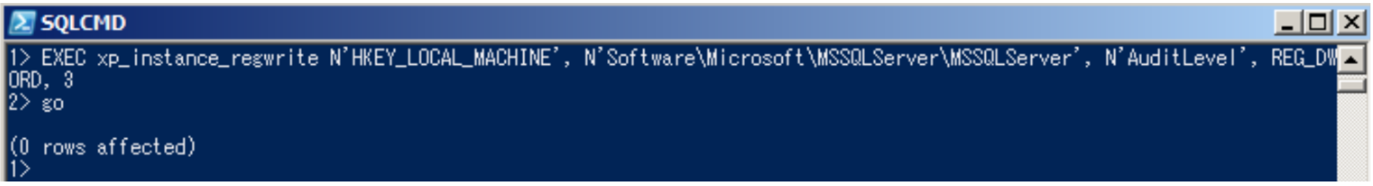
```
1 > exec sp_configure 'show advanced options', 1
2 > go
1 > reconfigure
2 > go
```



```
1> exec sp_configure 'show advanced options', 1
2> go
Configuration option 'show advanced options' changed from 1 to 1. Run the RECONFIGURE statement to install.
1> reconfigure
2> go
```

(5) Enter the command below to enable auditing for both failed and successful logins:

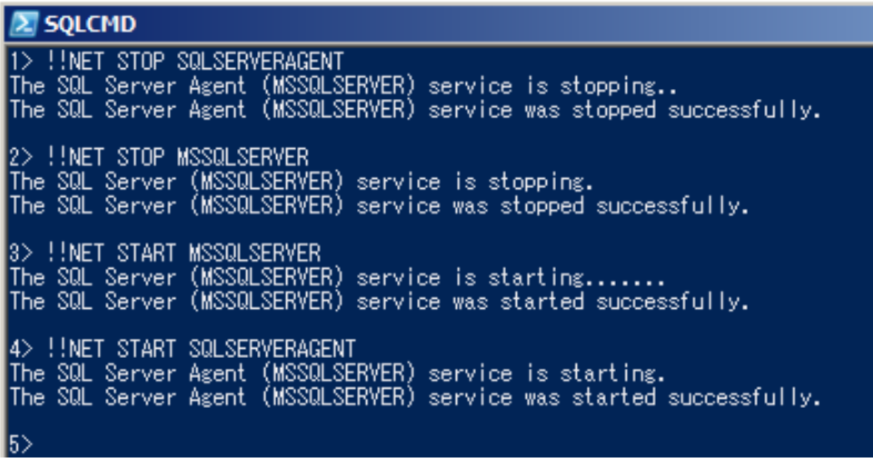
```
1 > EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE',
N'Software\Microsoft\MSSQLServer\MSSQLServer', N'AuditLevel', REG_DWORD, 3
2 > go
```



```
1> EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'Software\Microsoft\MSSQLServer\MSSQLServer', N'AuditLevel', REG_DW
ORD, 3
2> go

(0 rows affected)
1>
```

(6) Enter the command below to restart the MS SQL Server services:

```
1 > !!NET STOP SQLSERVERAGENT
2 > !!NET STOP MSSQLSERVER
3 > !!NET START MSSQLSERVER
4 > !!NET START SQLSERVERAGENT
```



```
1> !!NET STOP SQLSERVERAGENT
The SQL Server Agent (MSSQLSERVER) service is stopping..
The SQL Server Agent (MSSQLSERVER) service was stopped successfully.

2> !!NET STOP MSSQLSERVER
The SQL Server (MSSQLSERVER) service is stopping.
The SQL Server (MSSQLSERVER) service was stopped successfully.

3> !!NET START MSSQLSERVER
The SQL Server (MSSQLSERVER) service is starting.......
The SQL Server (MSSQLSERVER) service was started successfully.

4> !!NET START SQLSERVERAGENT
The SQL Server Agent (MSSQLSERVER) service is starting.
The SQL Server Agent (MSSQLSERVER) service was started successfully.

5>
```

2.2 Configuring Auditing

2.2.1 Server-Level Audit

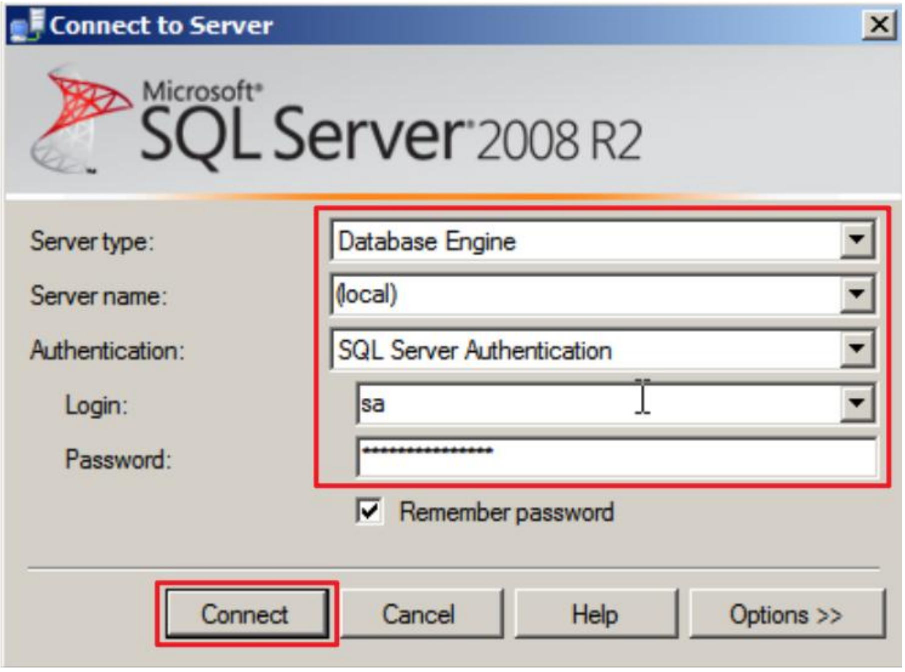
Enabling a server-level audit covers server operations such as administrative changes, login, and logout activities.

The following sections describe how to configure a server-level audit using the graphical user interface (GUI) and the command-line interface (CLI).

2.2.1.1 Configuring via Graphical User Interface (GUI)

(1) Open “SQL Server Management Studio (SSMS).”

(2) Enter the server’s name → select the authentication method → click “Connect.”



Connect to Server

Microsoft® SQL Server® 2008 R2

Server type: Database Engine

Server name: (local)

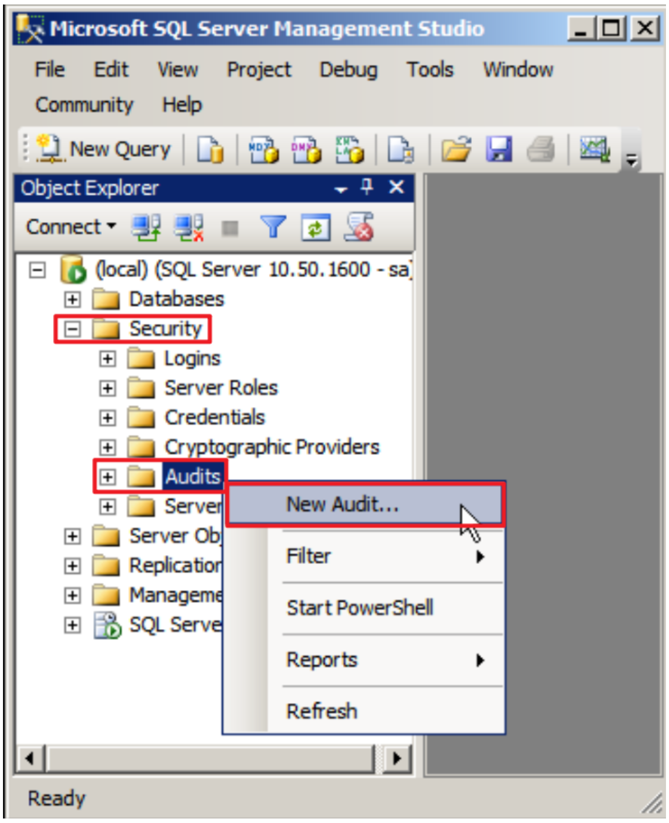
Authentication: SQL Server Authentication

Login: sa

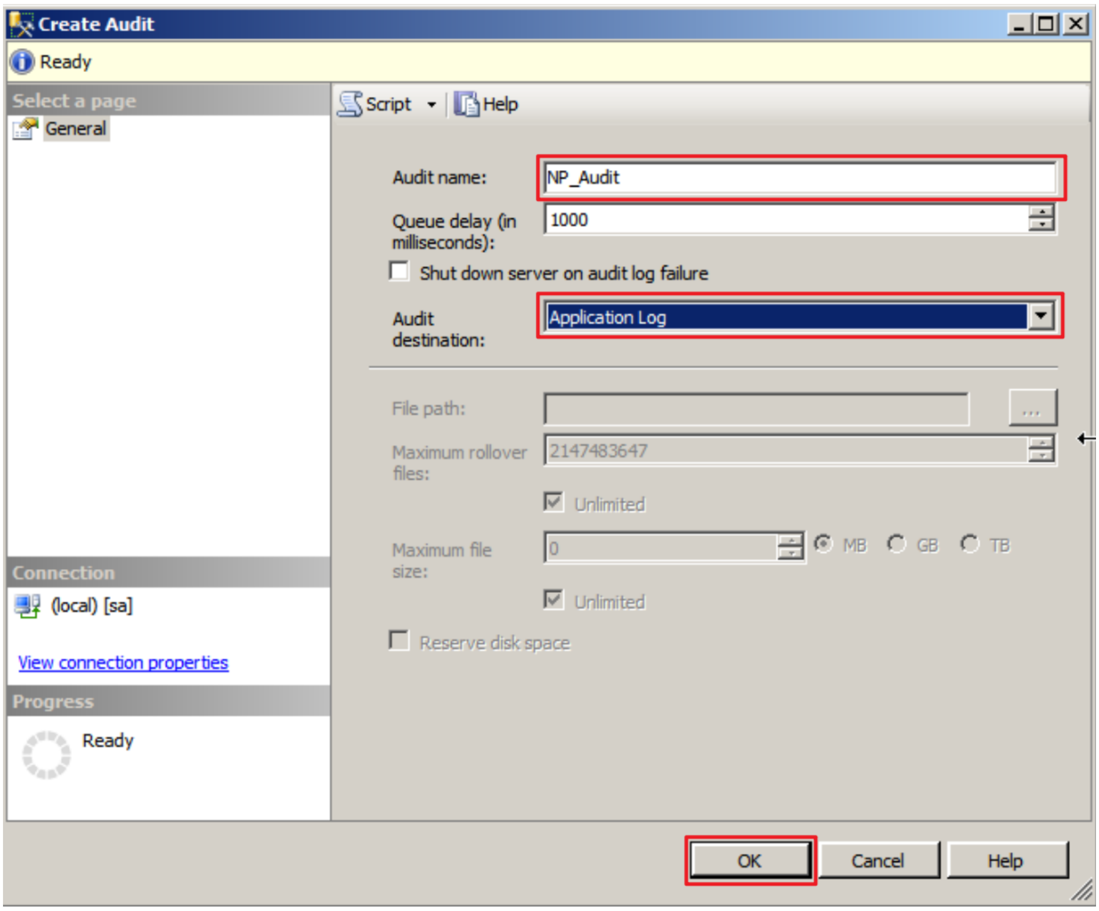
Password: ****************

☑ Remember password

(3) Expand “Security” → right-click “Audits” → select “New Audit...”



(4) Enter the audit name: (the example here is NP_Audit) → select audit destination: Application Log (this stores MS SQL audit logs in the Windows Event Viewer Application Log) → click “OK.”



Audit name: NP_Audit

Queue delay (in milliseconds): 1000

☐ Shut down server on audit log failure

Audit destination: Application Log

File path:

Maximum rollover files: 2147483647

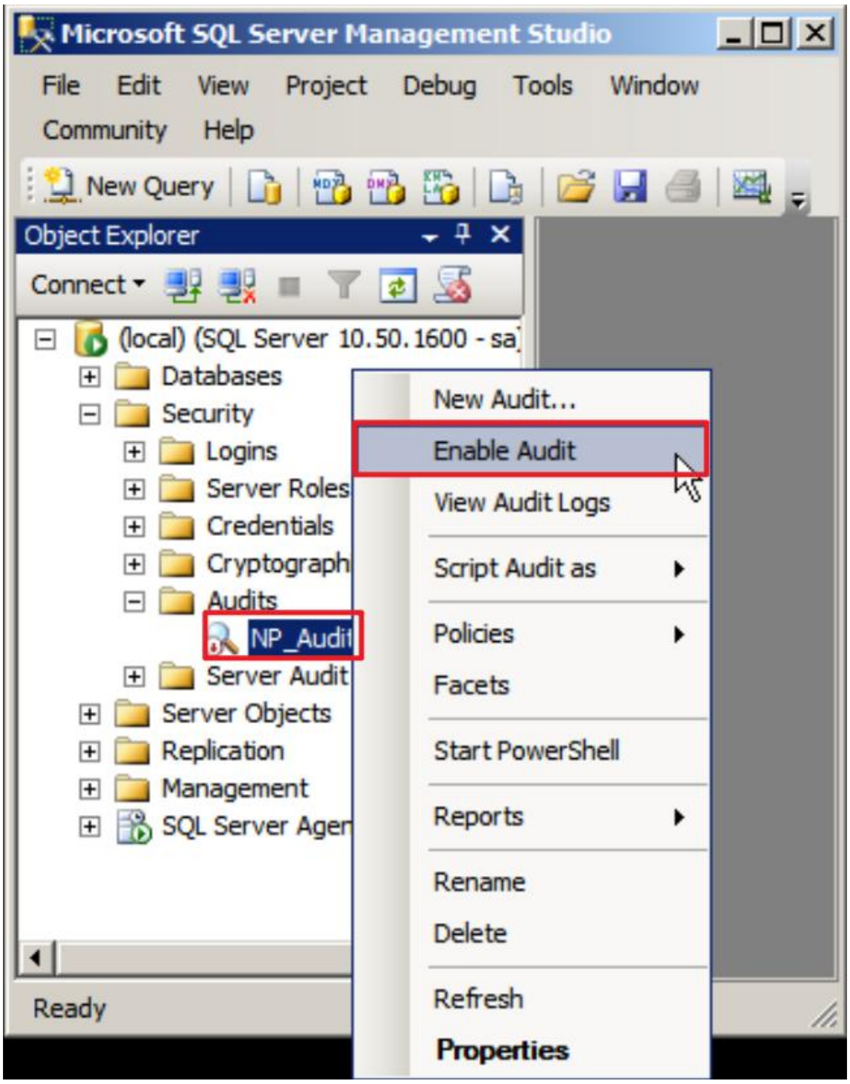
☑ Unlimited

Maximum file size: 0 ● MB ○ GB ○ TB

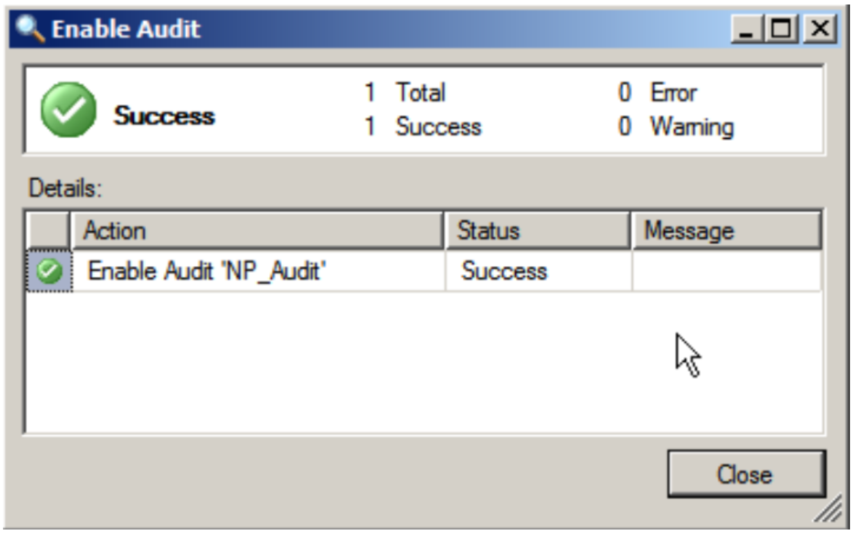
☑ Unlimited

☐ Reserve disk space

(5) In the audit list, right-click “NP_Audit” → select “Enable Audit.”



(6) Click “Close.”



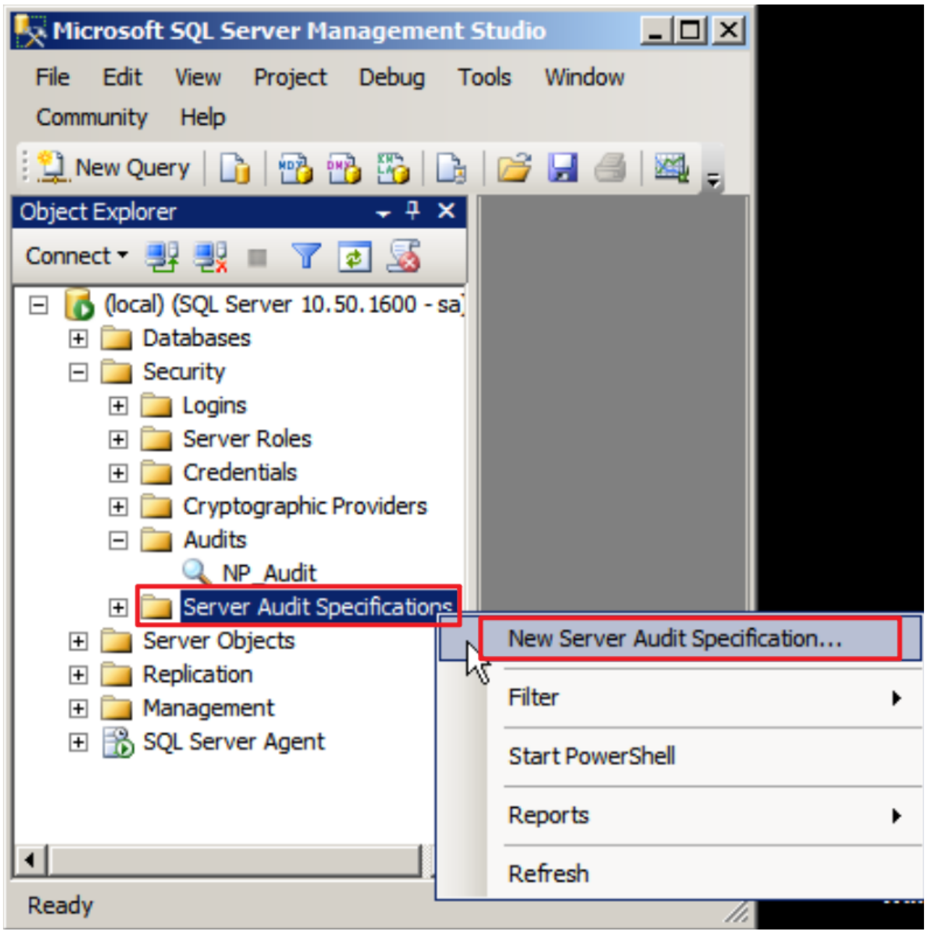
Success

1 Total
1 Success
0 Error
0 Warning

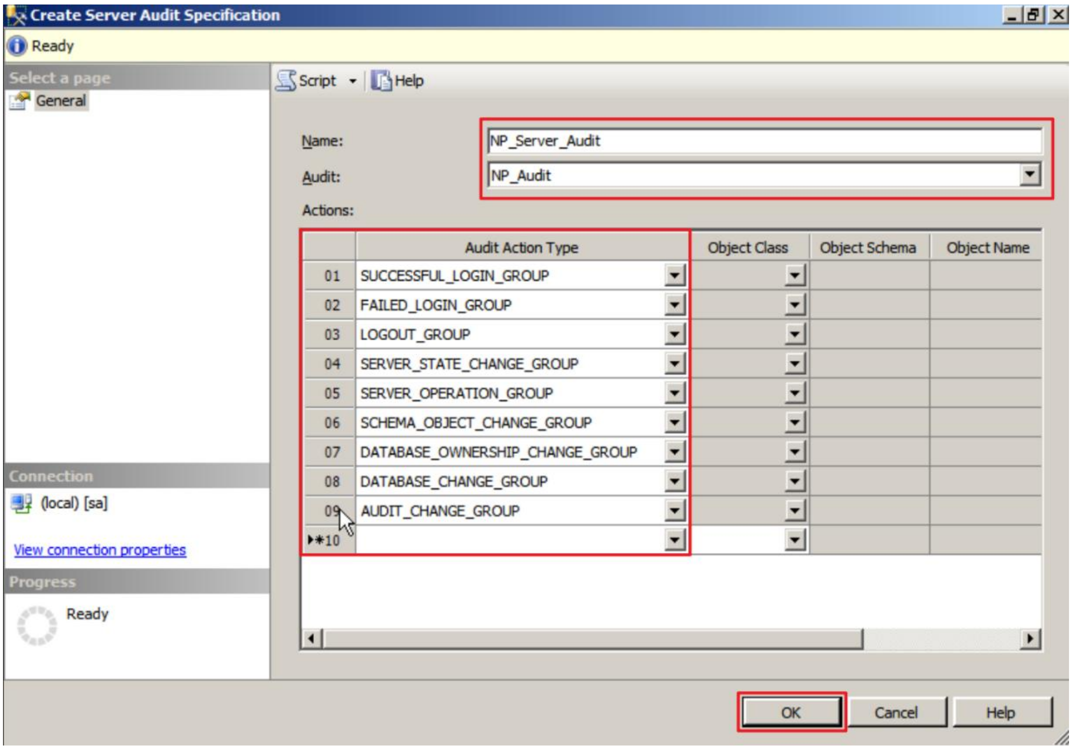
Details:

Action	Status	Message
Enable Audit 'NP_Audit'	Success	

(7) Right-click “Server Audit Specifications,” → select “New Server Audit Specification...”



(8) Enter the specification name: (the example here is NP_Server_Audit) → select audit: NP_Audit → select action(s) (refer to the **SQL Server Audit Action Groups and Actions** in the references for details) → click “OK.”



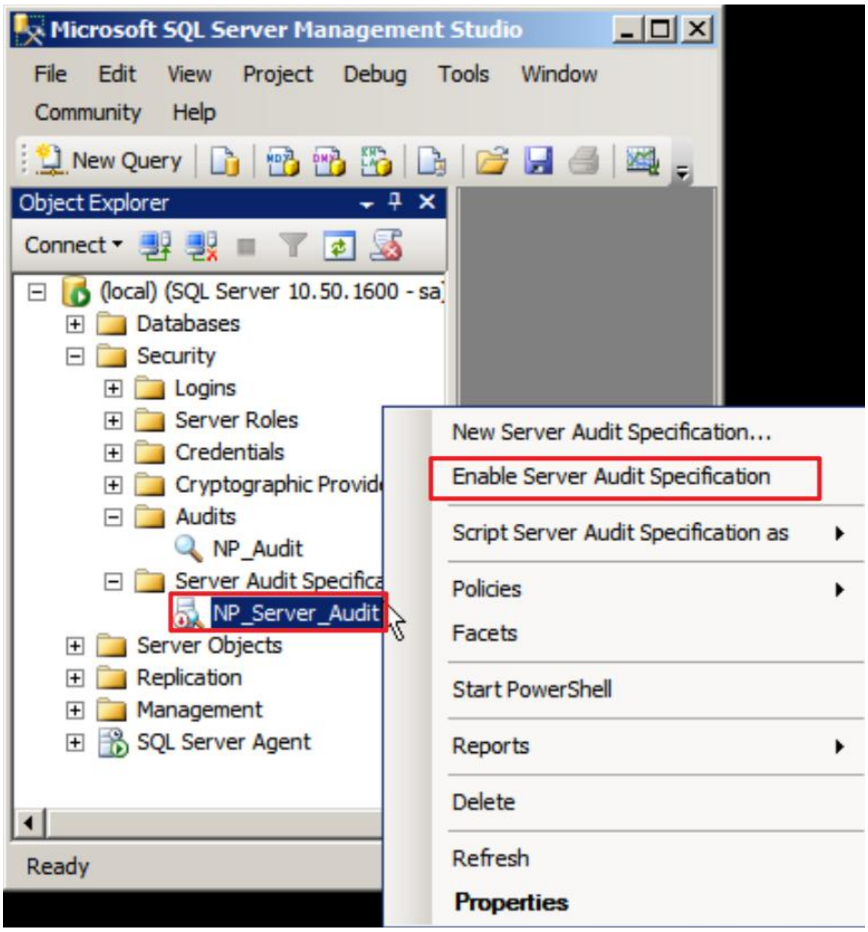
Name: NP_Server_Audit

Audit: NP_Audit

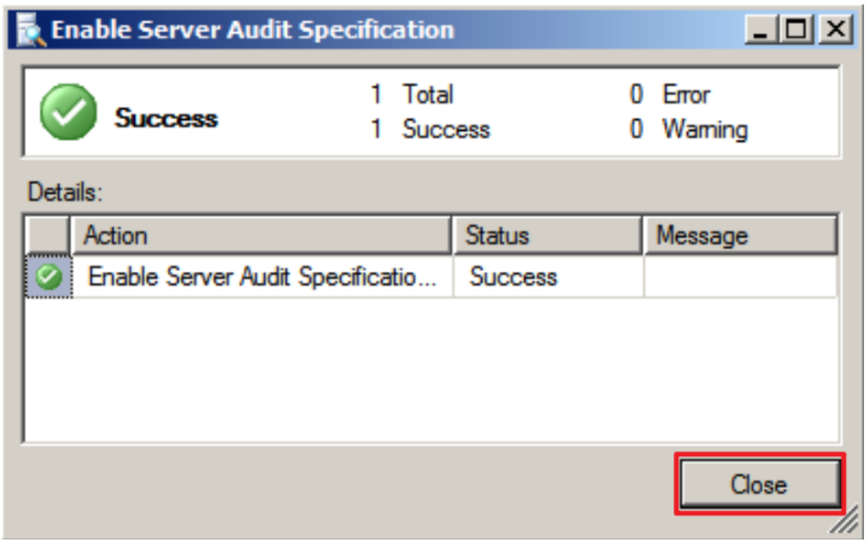
Actions:

	Audit Action Type	Object Class	Object Schema	Object Name
01	SUCCESSFUL_LOGIN_GROUP			
02	FAILED_LOGIN_GROUP			
03	LOGOUT_GROUP			
04	SERVER_STATE_CHANGE_GROUP			
05	SERVER_OPERATION_GROUP			
06	SCHEMA_OBJECT_CHANGE_GROUP			
07	DATABASE_OWNERSHIP_CHANGE_GROUP			
08	DATABASE_CHANGE_GROUP			
09	AUDIT_CHANGE_GROUP			
*10				

(9) In the server audit specification list, right-click “NP_Server_Audit” → select “Enable Server Audit Specification.”



(10) Click “Close.”



Success

1 Total	0 Error
1 Success	0 Warning

Details:

Action	Status	Message
Enable Server Audit Specificatio...	Success	

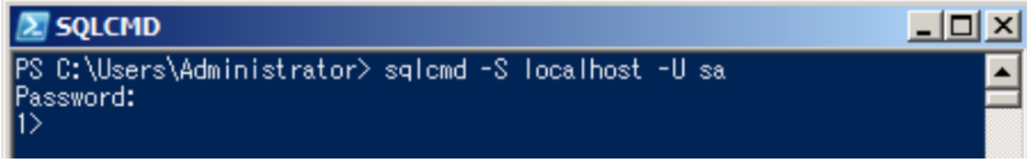
2.2.1.2 Configuring via Graphical User Interface (GUI)

(1) Open “Windows PowerShell.”

(2) Enter the command below to log in using either sa account:

<2.1>Using sa account:

```
PS C:\> sqlcmd -S localhost -U sa
```



```
PS C:\Users\Administrator> sqlcmd -S localhost -U sa
Password:
1>
```

Options:

-S [protocol:]server[instance_name][,port]

-U login_id

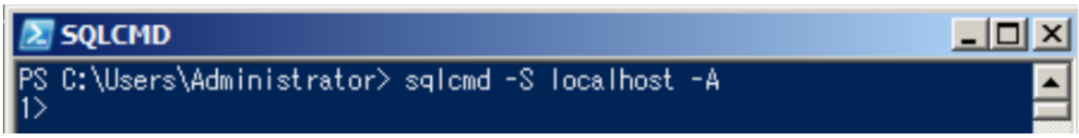
-P password

-A dedicated administrator connection

<2.2> Using Windows account:

Enter the command below to log in using Windows account:

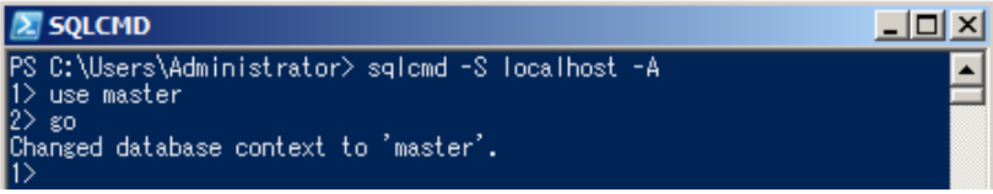
```
PS C:\> sqlcmd -S localhost -A
```



```
PS C:\Users\Administrator> sqlcmd -S localhost -A
1>
```

(3) Enter the command below to switch to the **master** database:

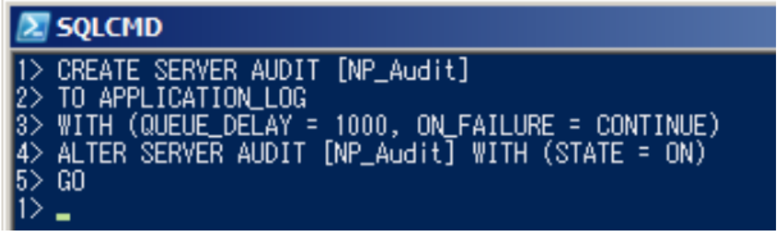
```
1 > use master
2 > go
```



```
PS C:\Users\Administrator> sqlcmd -S localhost -A
1> use master
2> go
Changed database context to 'master'.
1>
```

(4) Enter the audit name: NP_Audit → select audit destination: Application Log (this stores MS SQL audit logs in the Windows Event Viewer Application Log) → click “OK.”

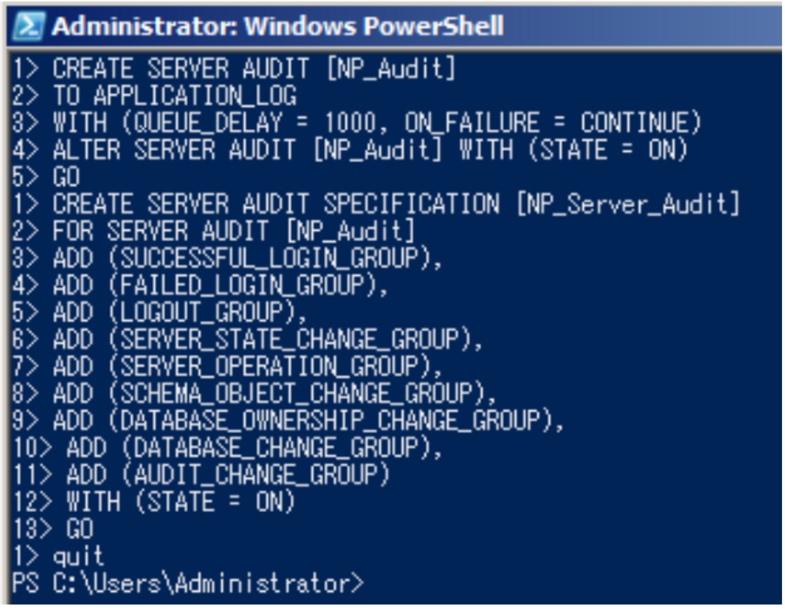
```
1 > CREATE SERVER AUDIT [ NP_Audit ]
2 > TO APPLICATION_LOG
3 > WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4 > ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5 > GO
```



```
1> CREATE SERVER AUDIT [NP_Audit]
2> TO APPLICATION_LOG
3> WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4> ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5> GO
1> _
```

(5) Enter the command below to configure the server audit and add actions. For detailed information, refer to the **SQL Server Audit Action Groups and Actions** in the references.

```
1 > CREATE SERVER AUDIT SPECIFICATION [ NP_Server_Audit ]
2 > FOR SERVER AUDIT [NP_Audit]
3 > ADD (SUCCESSFUL_LOGIN_GROUP),
4 > ADD (FAILED_LOGIN_GROUP),
5 > ADD (LOGOUT_GROUP),
6 > ADD (SERVER_STATE_CHANGE_GROUP),
7 > ADD (SERVER_OPERATION_GROUP),
8 > ADD (SCHEMA_OBJECT_CHANGE_GROUP),
9 > ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
10 > ADD (DATABASE_CHANGE_GROUP),
11 > ADD (AUDIT_CHANGE_GROUP)
12 > WITH (STATE = ON)
13 > GO
1 > quit
```



```
1> CREATE SERVER AUDIT [NP_Audit]
2> TO APPLICATION_LOG
3> WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4> ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5> GO
1> CREATE SERVER AUDIT SPECIFICATION [NP_Server_Audit]
2> FOR SERVER AUDIT [NP_Audit]
3> ADD (SUCCESSFUL_LOGIN_GROUP),
4> ADD (FAILED_LOGIN_GROUP),
5> ADD (LOGOUT_GROUP),
6> ADD (SERVER_STATE_CHANGE_GROUP),
7> ADD (SERVER_OPERATION_GROUP),
8> ADD (SCHEMA_OBJECT_CHANGE_GROUP),
9> ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
10> ADD (DATABASE_CHANGE_GROUP),
11> ADD (AUDIT_CHANGE_GROUP)
12> WITH (STATE = ON)
13> GO
1> quit
PS C:\Users\Administrator>
```

Replace the text shown in red with the server audit specification name.

2.2.2 Database-Level Audit

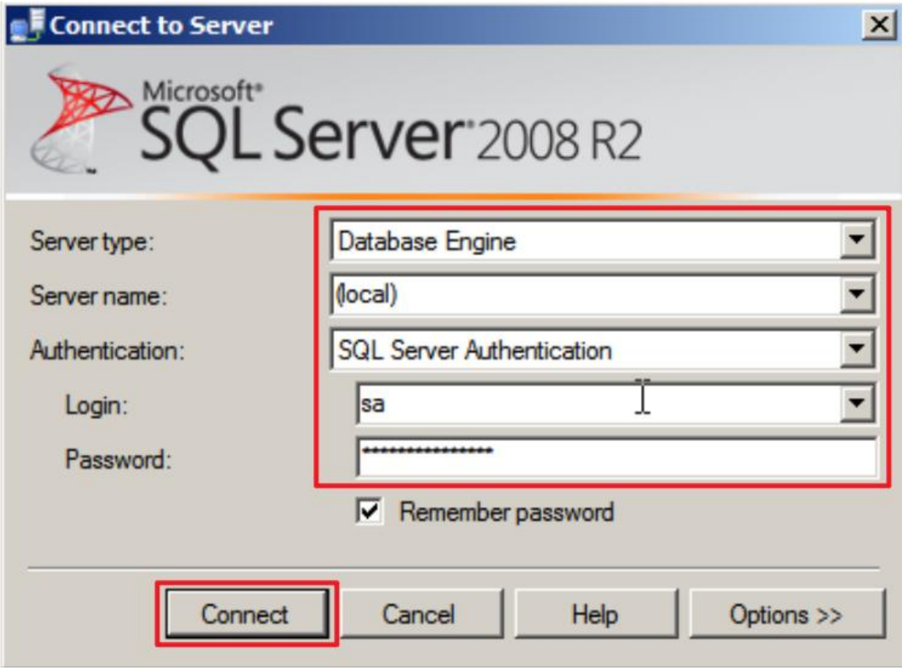
Enabling a database-level audit covers operations involving Data Manipulation Language (DML) and Data Definition Language (DDL) statements.

The following sections describe how to configure a database-level audit using the graphical user interface (GUI) and the command-line interface (CLI).

2.2.2.1 Configuring via Graphical User Interface (GUI)

(1) Open “SQL Server Management Studio (SSMS).”

(2) Enter the server’s name → select the authentication method → click “Connect.”



Server type: Database Engine

Server name: (local)

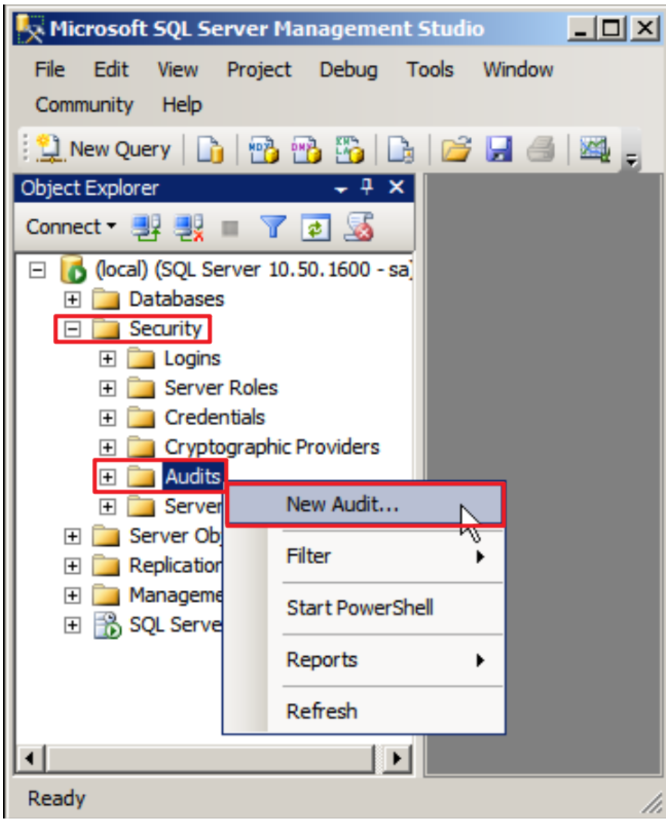
Authentication: SQL Server Authentication

Login: sa

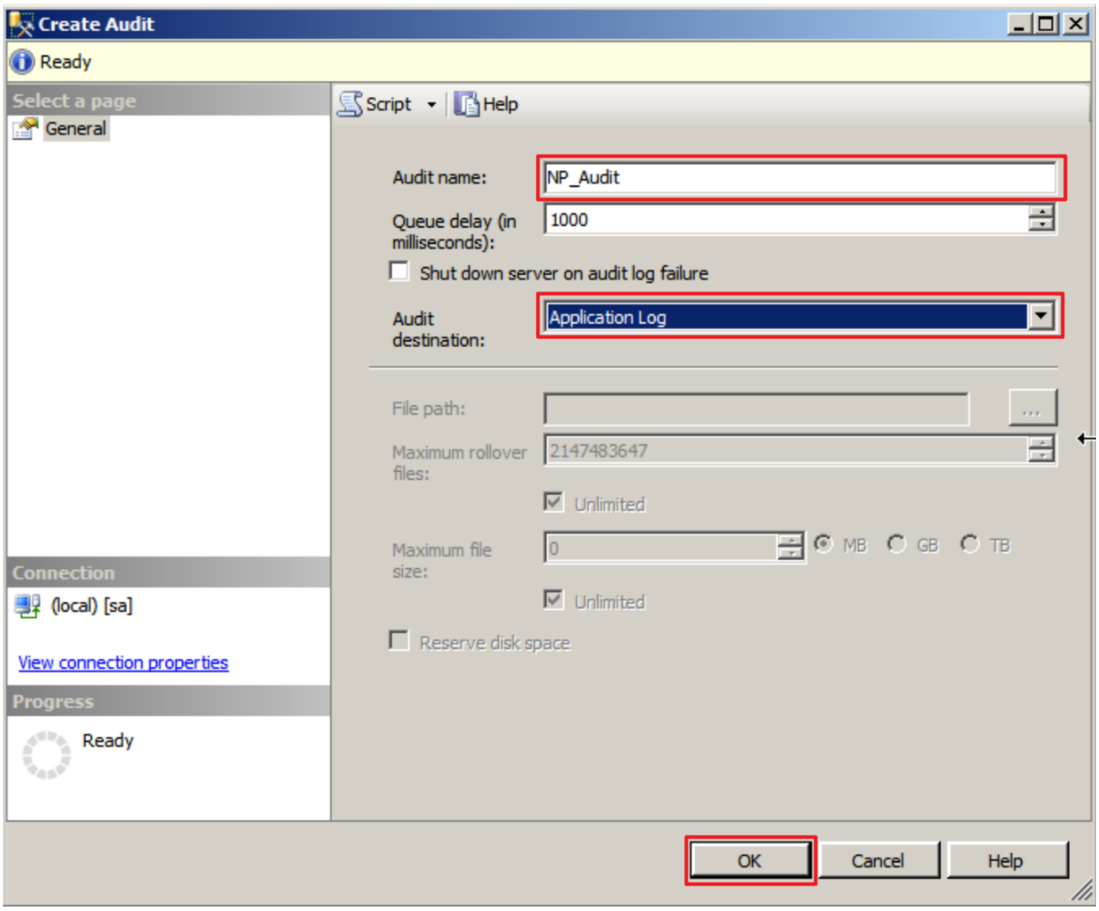
Password: ****************

☑ Remember password

(3) Expand “Security” → right-click “Audits” → select “New Audit...”



(4) Enter the audit name: (the example here is NP_Audit) → select audit destination: Application Log (this stores MS SQL audit logs in the Windows Event Viewer Application Log) → click “OK.”



Audit name: NP_Audit

Queue delay (in milliseconds): 1000

□ Shut down server on audit log failure

Audit destination: Application Log

File path:

Maximum rollover files: 2147483647

☑ Unlimited

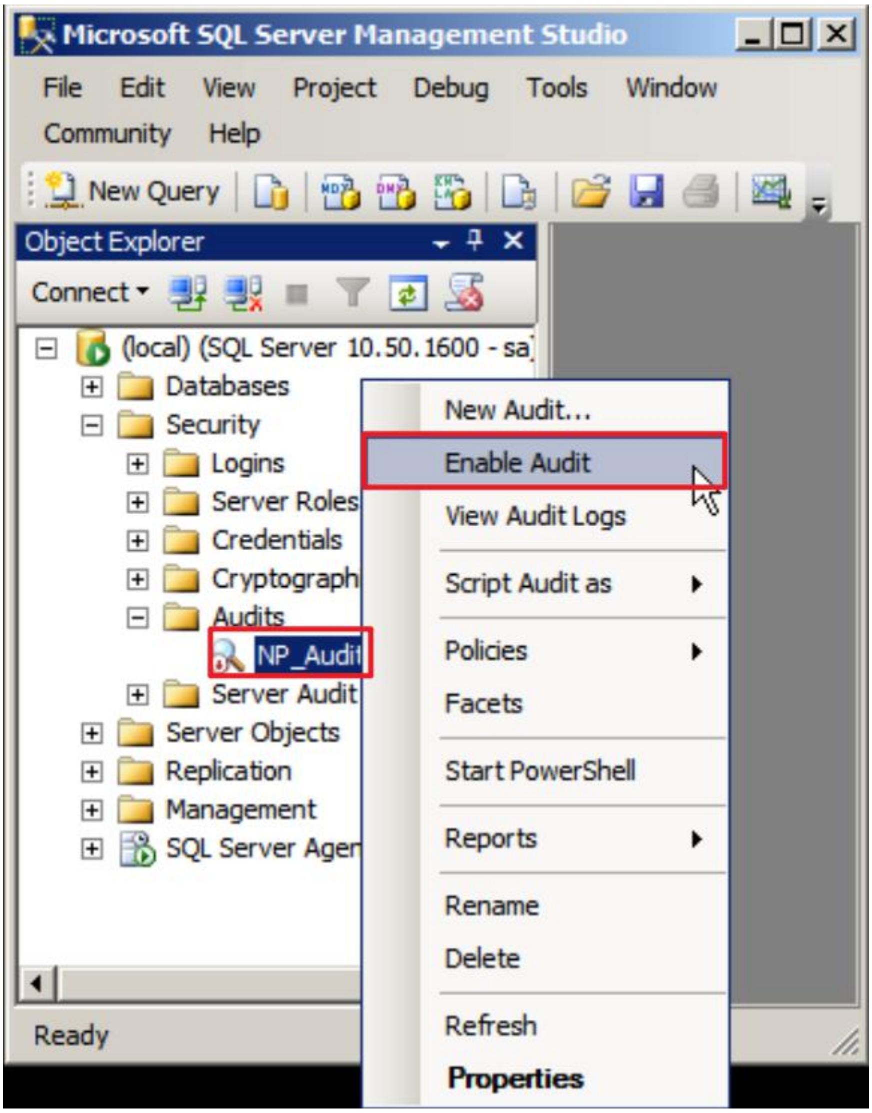
Maximum file size: 0 ● MB ○ GB ○ TB

☑ Unlimited

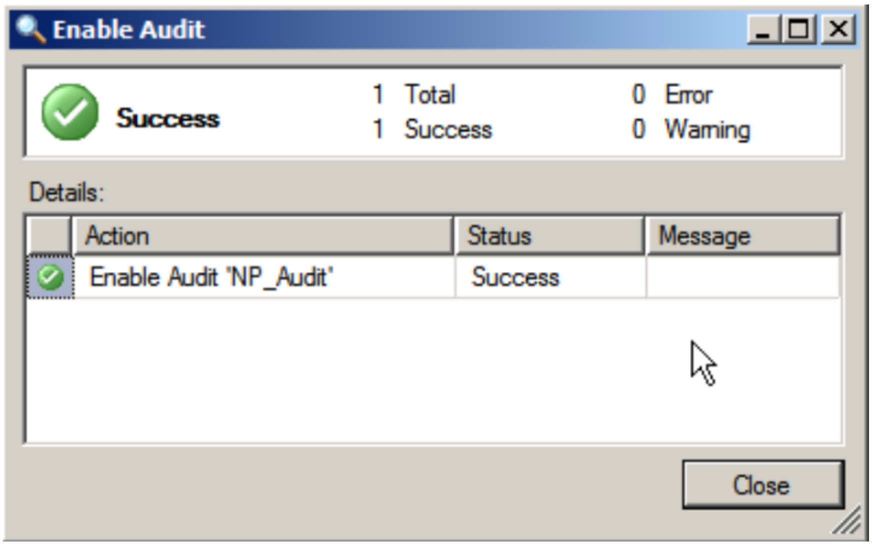
□ Reserve disk space

(local) [sa]

(5) In the audit list, right-click "NP_Audit" → select "Enable Audit."



(6) Click "Close."


Enable Audit

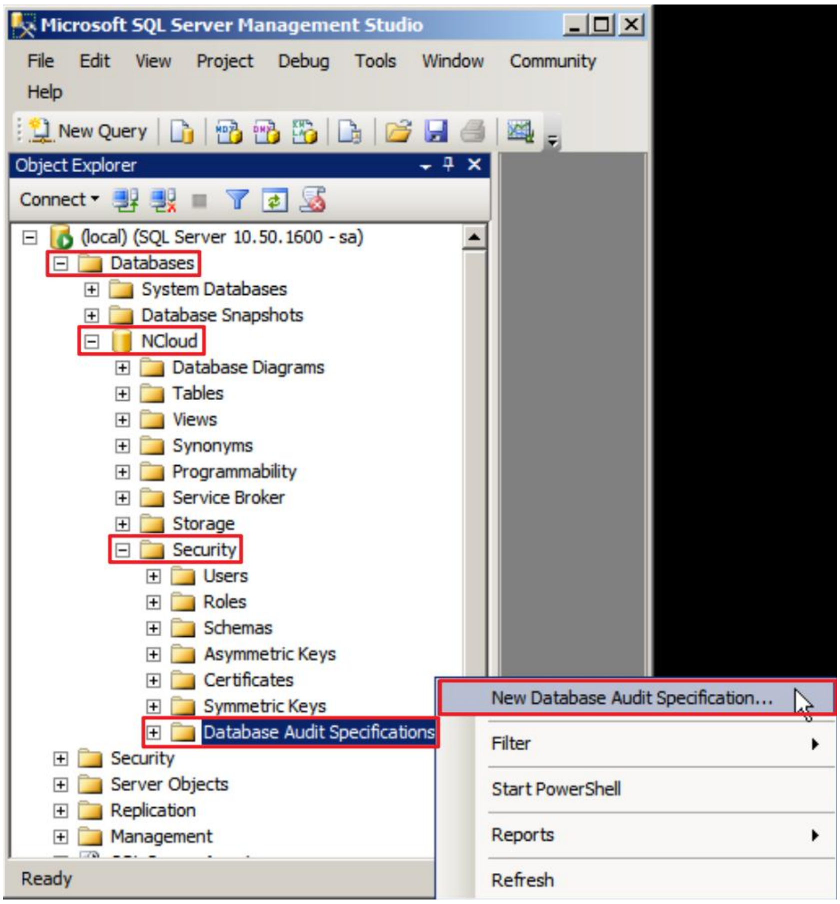
Success

1	Total
1	Success
0	Error
0	Warning

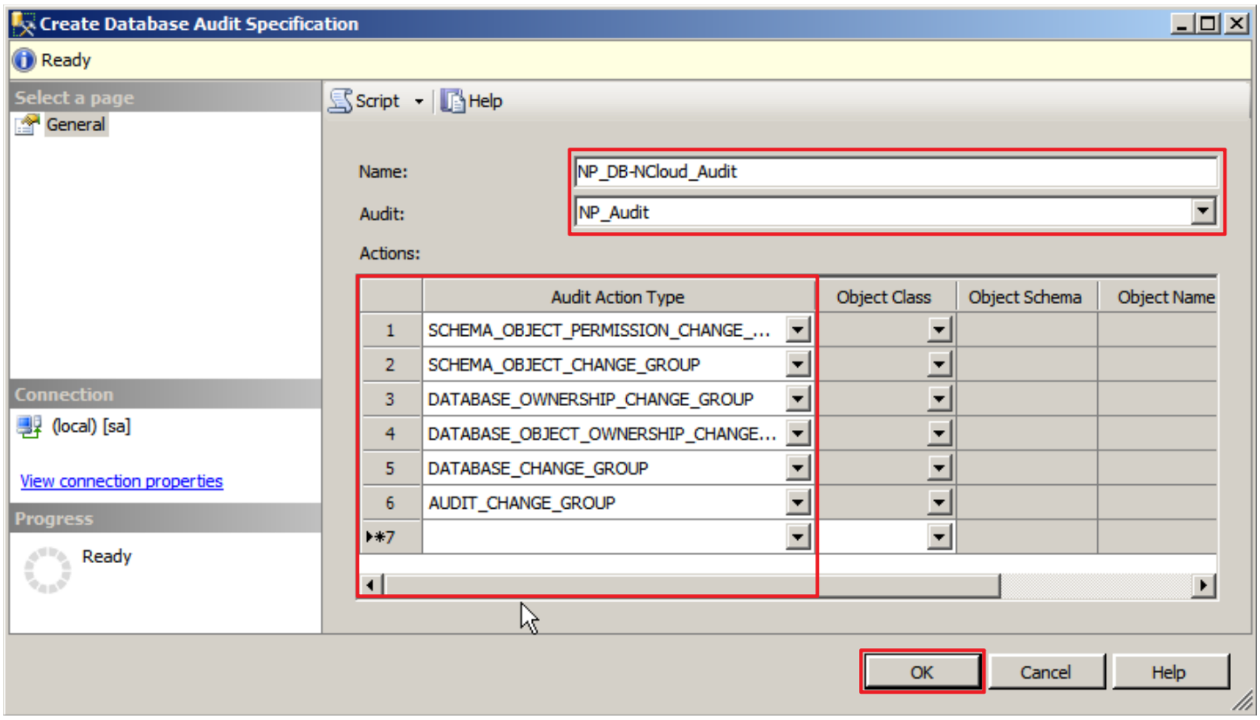
Details:

Action	Status	Message
Enable Audit 'NP_Audit'	Success	

(7) In “Databases,” select the target database (the example here is : NCloud) → expand “Security” → right-click “Database Audit Specifications” → select "New Database Audit Specification...”



(8) Enter the specification name: (the example here is NP_DB-NCloud_Audit) → select audit: NP_Audit and action(s) → select action(s) (refer to the **SQL Server Audit Action Groups and Actions** in the references for details) → click “OK.”



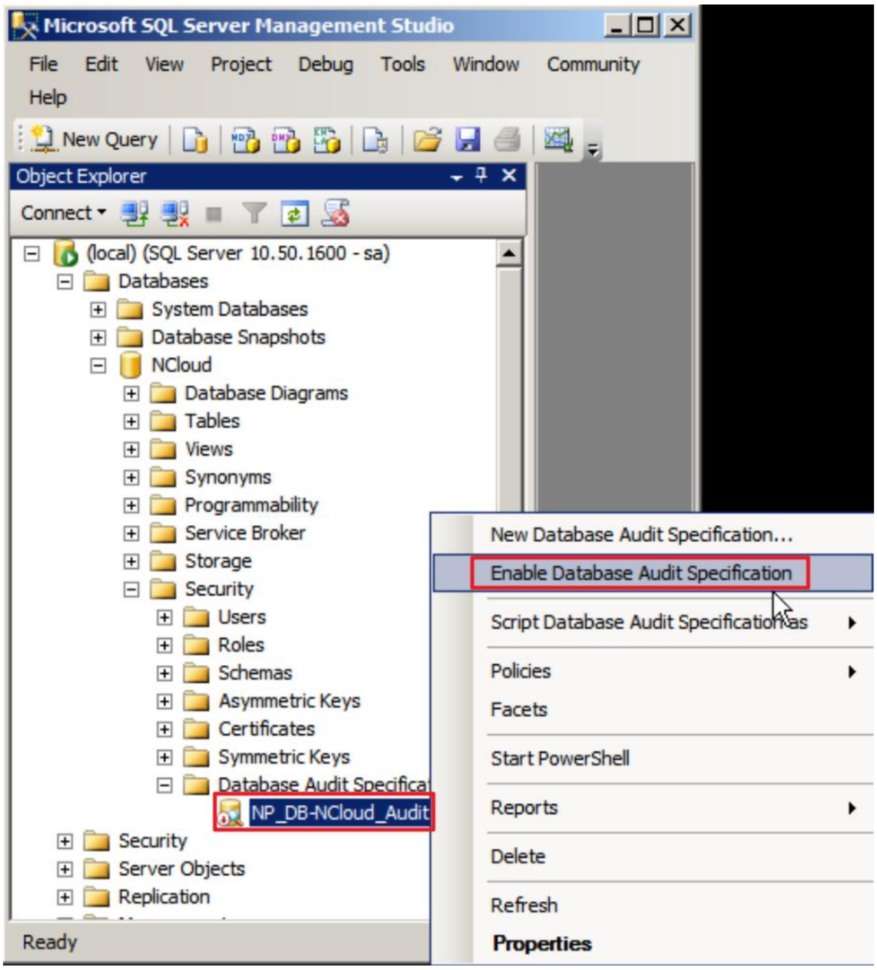
Name: NP_DB-NCloud_Audit

Audit: NP_Audit

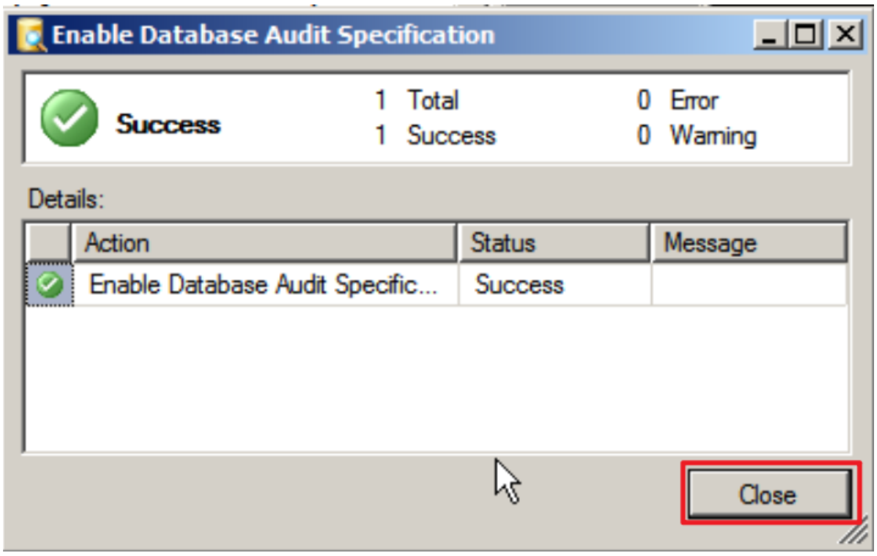
Actions:

	Audit Action Type	Object Class	Object Schema	Object Name
1	SCHEMA_OBJECT_PERMISSION_CHANGE_...			
2	SCHEMA_OBJECT_CHANGE_GROUP			
3	DATABASE_OWNERSHIP_CHANGE_GROUP			
4	DATABASE_OBJECT_OWNERSHIP_CHANGE...			
5	DATABASE_CHANGE_GROUP			
6	AUDIT_CHANGE_GROUP			
▸*7				

(9) In the database audit specification list, right-click “NP_DB-NCloud_Audit” → select “Enable Server Audit Specification.”



(10) Click “Close.”



Action	Status	Message
Enable Database Audit Specific...	Success	

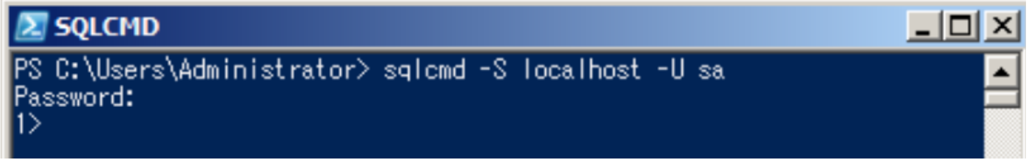
2.2.2.2 Configuring via Graphical User Interface (GUI)

(1) Open “Windows PowerShell.”

(2) Enter the command below to log in using either sa account:

<2.1>Using sa account:

```
PS C:\> sqlcmd -S localhost -U sa
```



```
PS C:\Users\Administrator> sqlcmd -S localhost -U sa
Password:
1>
```

Options:

-S [protocol:]server[instance_name][,port]

-U login_id

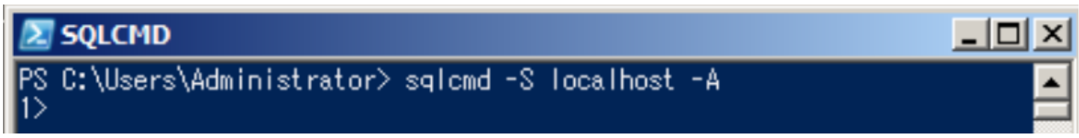
-P password

-A dedicated administrator connection

<2.2> Using Windows account:

Enter the command below to log in using Windows account:

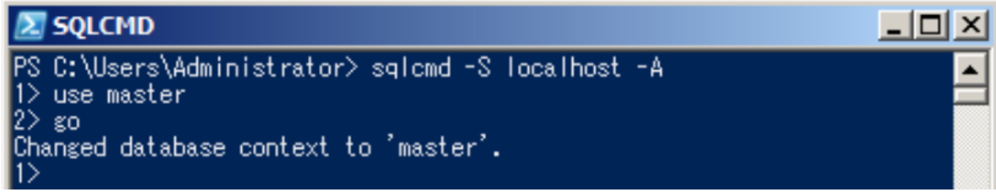
```
PS C:\> sqlcmd -S localhost -A
```



```
PS C:\Users\Administrator> sqlcmd -S localhost -A
1>
```

(3) Enter the command below to switch to the **master** database:

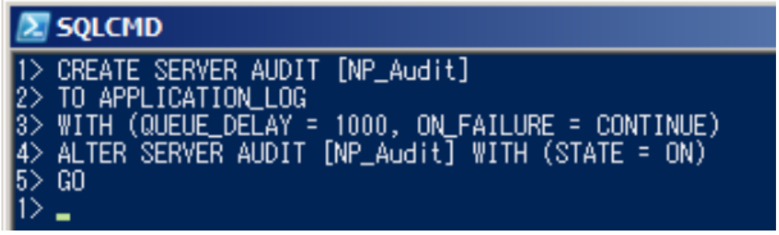
```
1 > use master
2 > go
```



```
PS C:\Users\Administrator> sqlcmd -S localhost -A
1> use master
2> go
Changed database context to 'master'.
1>
```

(4) Enter the audit name: NP_Audit → select audit destination: Application Log (this stores MS SQL audit logs in the Windows Event Viewer Application Log) → click “OK.”

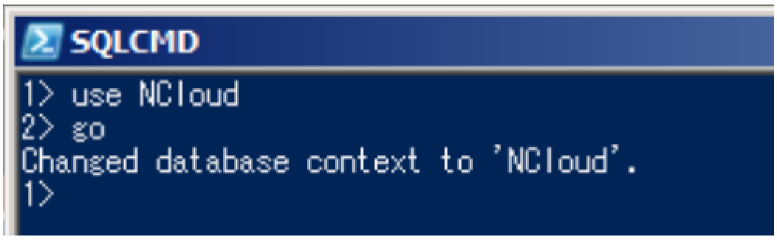
```
1 > CREATE SERVER AUDIT [ NP_Audit ]
2 > TO APPLICATION_LOG
3 > WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4 > ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5 > GO
```



```
1> CREATE SERVER AUDIT [NP_Audit]
2> TO APPLICATION_LOG
3> WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4> ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5> GO
1> _
```

(5) Enter the command below to switch to the target audit database (the example here is: NCloud).

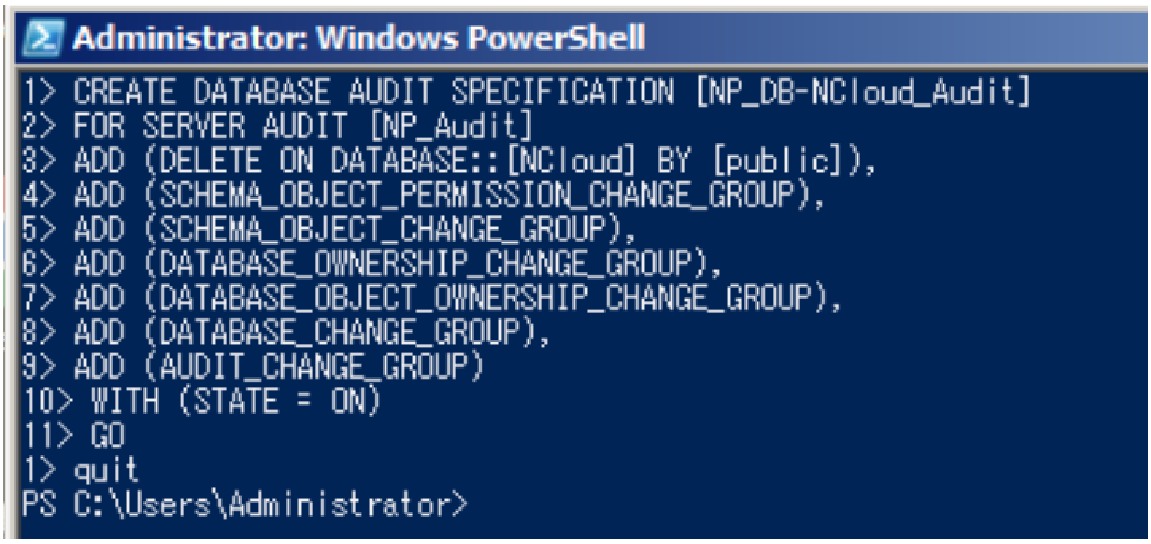
```
1 > use NCloud
2 > go
```



```
1> use NCloud
2> go
Changed database context to 'NCloud'.
1>
```

(6) Enter the command below to configure the audit for the database and add actions. For detailed information, refer to the SQL Server Audit Action Groups and Actions in the references.

```
1 > CREATE DATABASE AUDIT SPECIFICATION [ NP_DB-NCloud_Audit ]
2 > FOR SERVER AUDIT [NP_Audit]
3 > ADD (DELETE ON DATABASE::[ NCloud ] BY [public]),
4 > ADD (SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP),
5 > ADD (SCHEMA_OBJECT_CHANGE_GROUP),
6 > ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
7 > ADD (DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP),
8 > ADD (DATABASE_CHANGE_GROUP),
9 > ADD (AUDIT_CHANGE_GROUP)
10 > WITH (STATE = ON)
11 > GO
1 > quit
```



```
1> CREATE DATABASE AUDIT SPECIFICATION [NP_DB-NCloud_Audit]
2> FOR SERVER AUDIT [NP_Audit]
3> ADD (DELETE ON DATABASE::[NCloud] BY [public]),
4> ADD (SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP),
5> ADD (SCHEMA_OBJECT_CHANGE_GROUP),
6> ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
7> ADD (DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP),
8> ADD (DATABASE_CHANGE_GROUP),
9> ADD (AUDIT_CHANGE_GROUP)
10> WITH (STATE = ON)
11> GO
1> quit
PS C:\Users\Administrator>
```

Replace the text shown in red with the database audit specification name.

```
1 > CREATE DATABASE AUDIT SPECIFICATION [NP_DB-NCloud_Audit]
```

Replace the text shown in red with the target database name.

```
3 > ADD (DELETE ON DATABASE::[NCloud] BY [public])
```

2.3 Event Log Configuration

This is an optional configuration.

The following sections describe configuration methods for Domain and Workgroup environments.

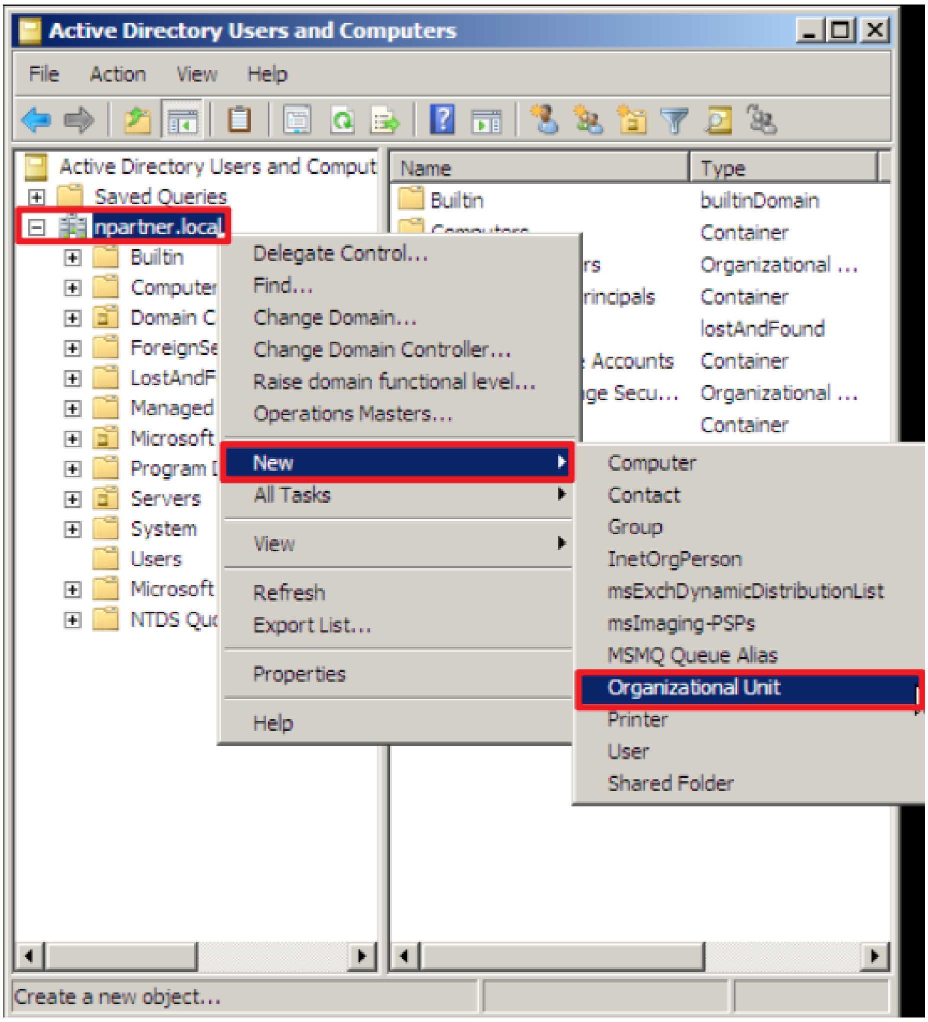
2.3.1 Domain

2.3.1.1 Organizational Unit (OU) Configuration

(1) Click “Active Directory Users and Computers.”

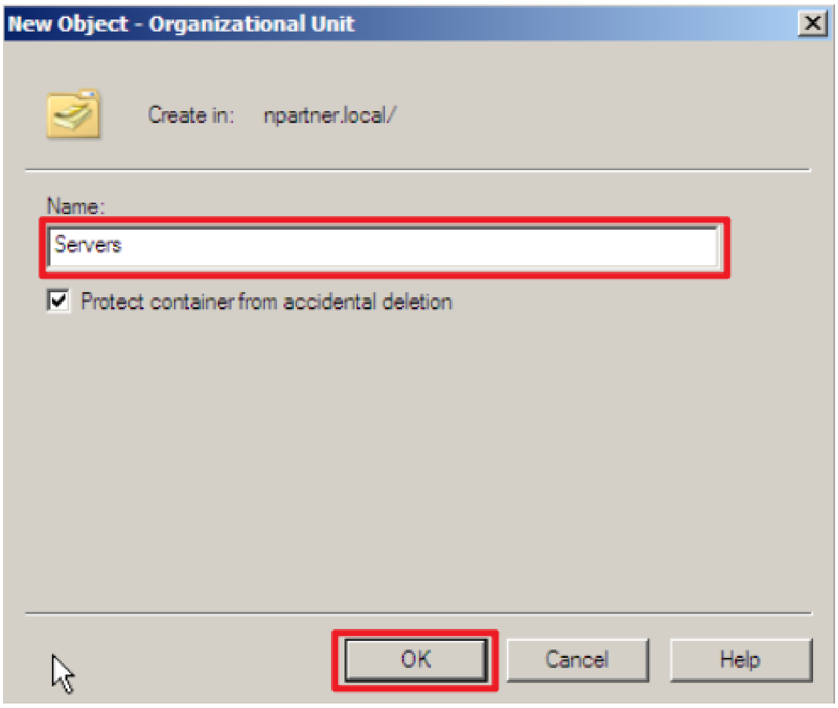
(2) Add an Organizational Unit

Right-click on “Domain Controllers, select “New,” and click “Organizational Unit.”



(3) Enter your Organizational Unit name: (in this example, it is "Servers")

Note: Please create the organizational unit name according to the customer's environment. → click "OK."



New Object - Organizational Unit

Create in: npartner.local/

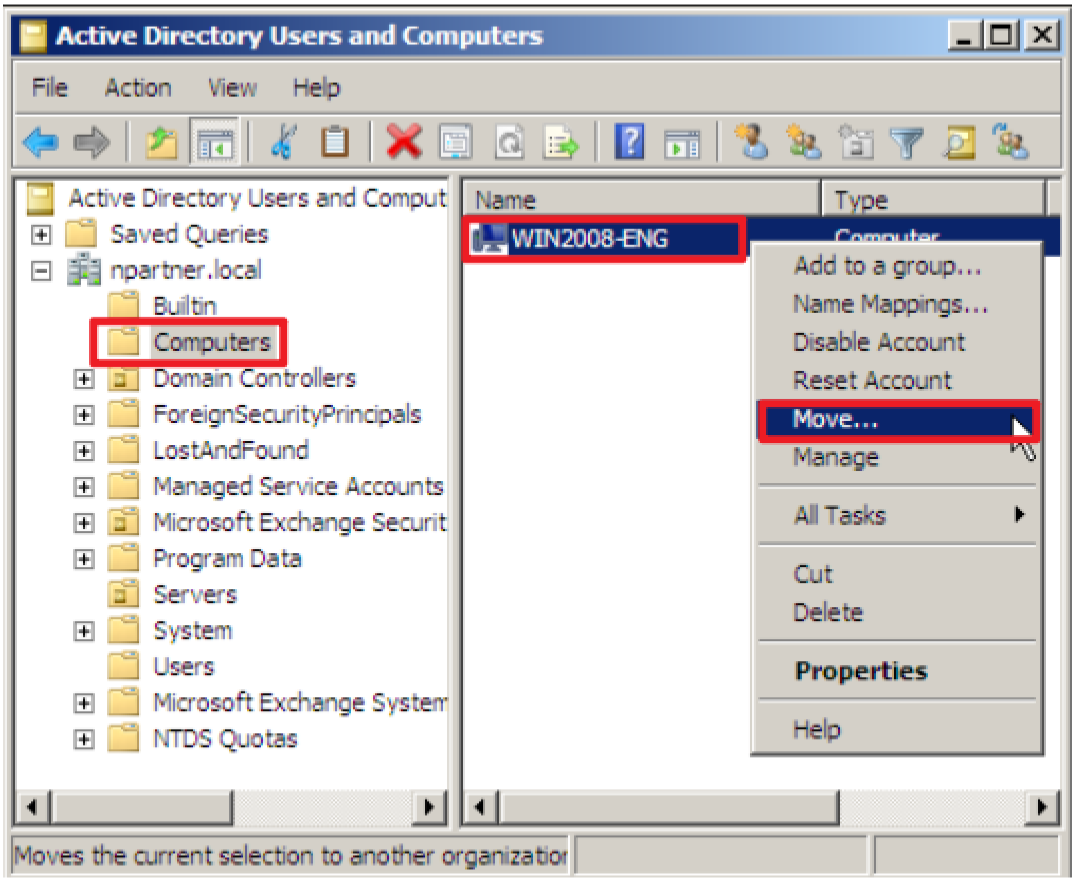
Name: Servers

☑ Protect container from accidental deletion

(4) Move the Server to your New Organizational Unit:

Select your organizational unit in "Domain Controllers" -> Right-click on the "WIN2008-AD-ENG" server.

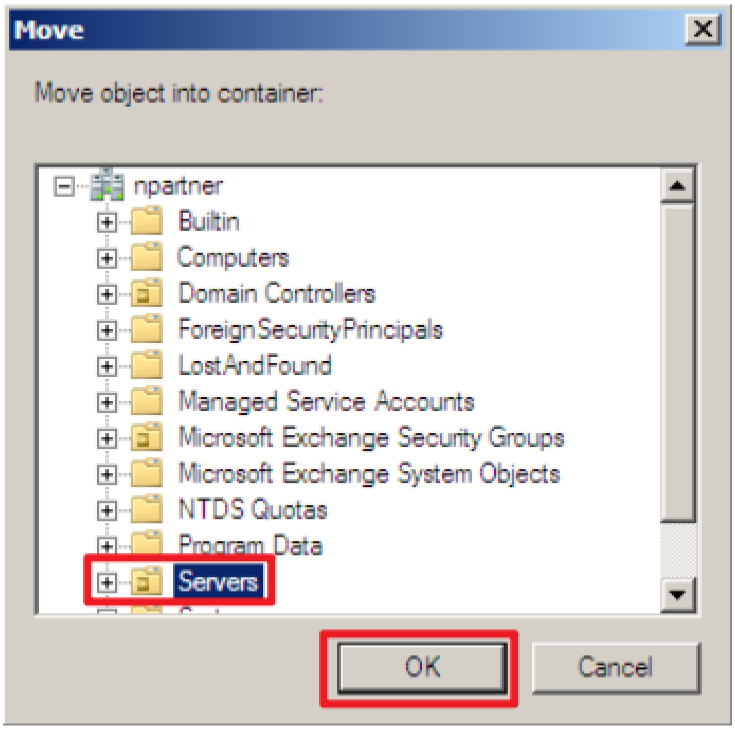
Note: Please select the Windows AD host according to the actual environment. → click "Move."



Moves the current selection to another organizatio

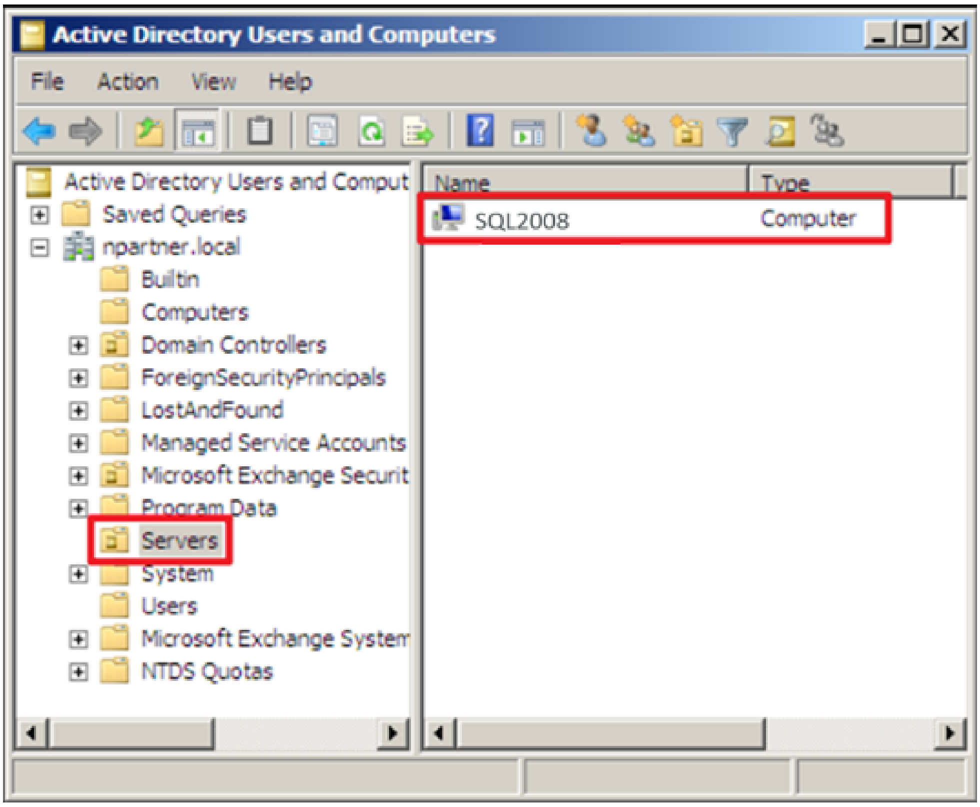
(5) Select your Organizational Unit:

Select your organizational unit (in this example, it is “Servers”) → click “OK.”



(6) Verify the Server Has Been Moved to your New Organizational Unit:

Expand your organizational unit folder (in this example, it is “Servers”) under “Domain Controllers” and confirm that the “SQL008” server has been moved.



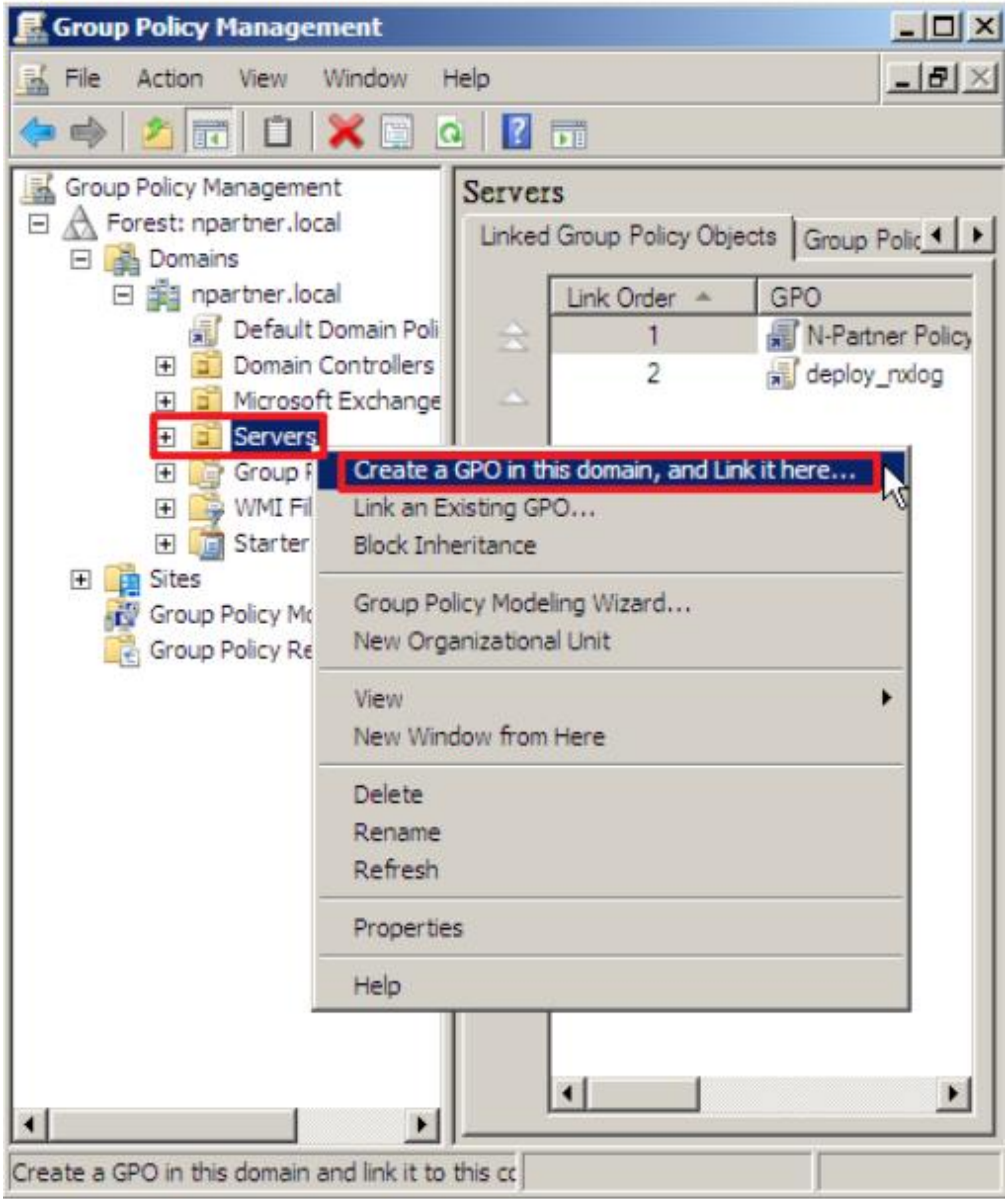
Name	Type
SQL2008	Computer

2.3.1.2 Group Policy Settings

(1) Click “Group Policy Management.”

(2) In the Servers organizational unit (OU), create a new Group Policy Object (GPO):

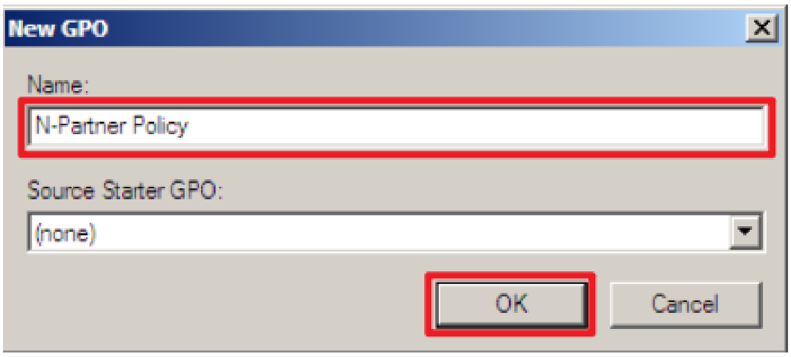
Right-click the [Servers] organizational unit → select “Create a GPO in this domain, and Link it here...”



(3) Edit your Group Policy Object

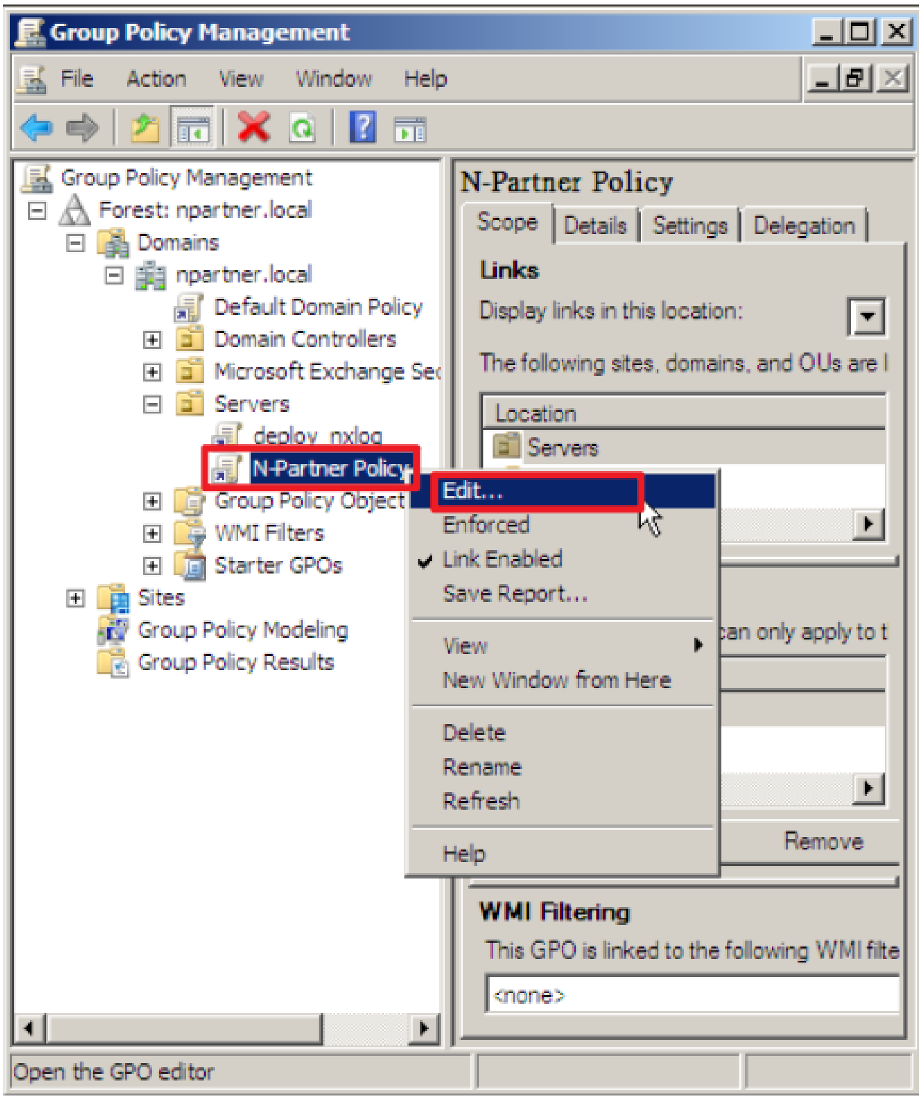
Enter your Group Policy Object name. (in this example, it is “N-Partner Policy”)

Note: Create your GPO name according to the actual environment. Then click “Edit.”



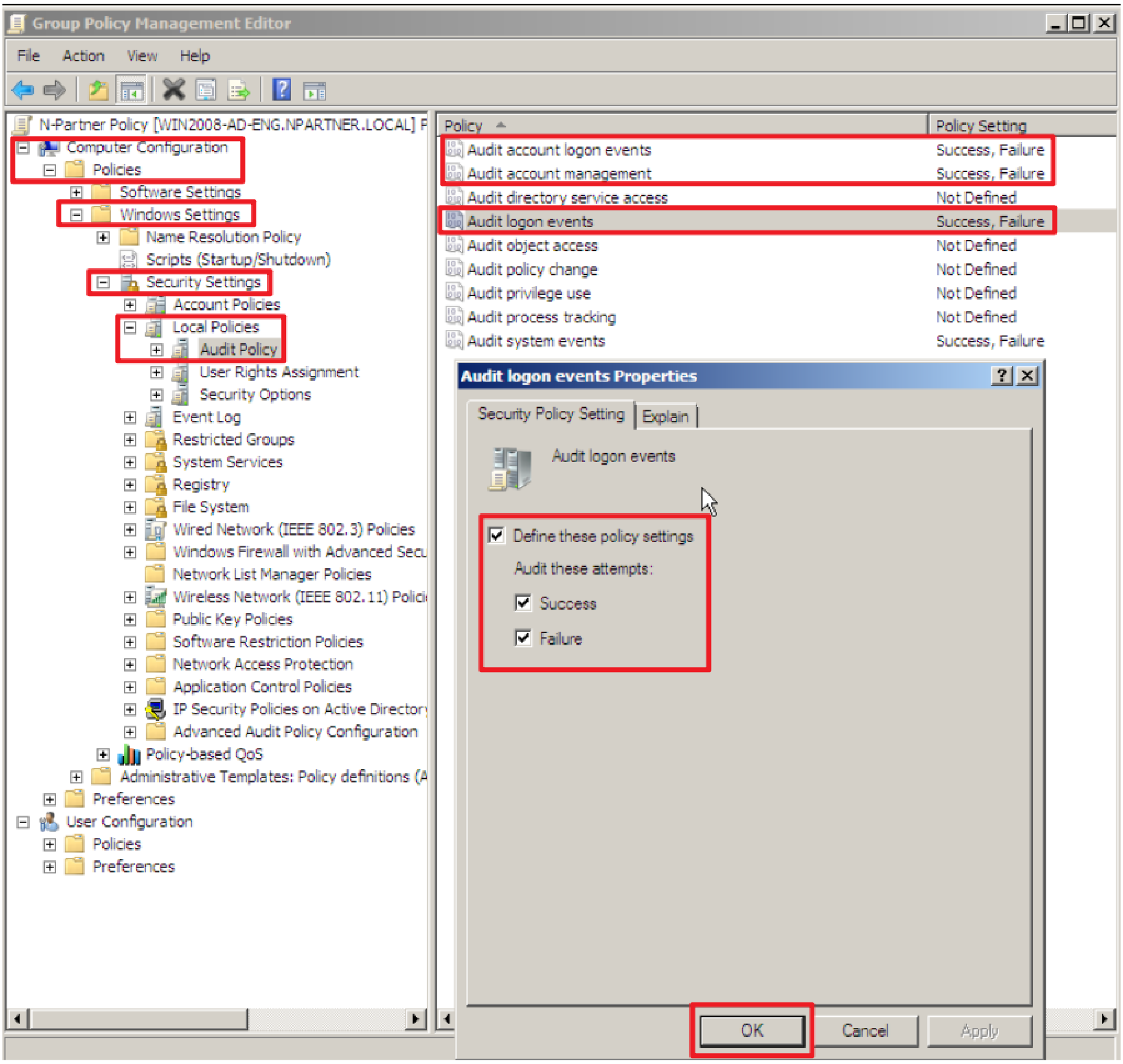
(4) Edit your Group Policy Object

In your group policy object, (in this example, it is “N-Partner Policy”) right-click and select “Edit.”



(5) Local Group Policies: Audit Policy

Expand folder “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” -> “Local Policies”-> “Audit Policy.” And click on “Audit account logon events,” “Audit account management,” and “Audit logon events,” → check “Define these policy settings”: Success, Failure. → click “OK.”


Group Policy Management Editor
File
Action
View
Help
N-Partner Policy [WIN2008-AD-ENG.NPARTNER.LOCAL] P
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Wireless Network (IEEE 802.11) Polici
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Director
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (A
Preferences
User Configuration
Policies
Preferences

Policy	Policy Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Not Defined
Audit logon events	Success, Failure
Audit object access	Not Defined
Audit policy change	Not Defined
Audit privilege use	Not Defined
Audit process tracking	Not Defined
Audit system events	Success, Failure

Audit logon events Properties

Security Policy Setting | Explain

Audit logon events

☑ Define these policy settings

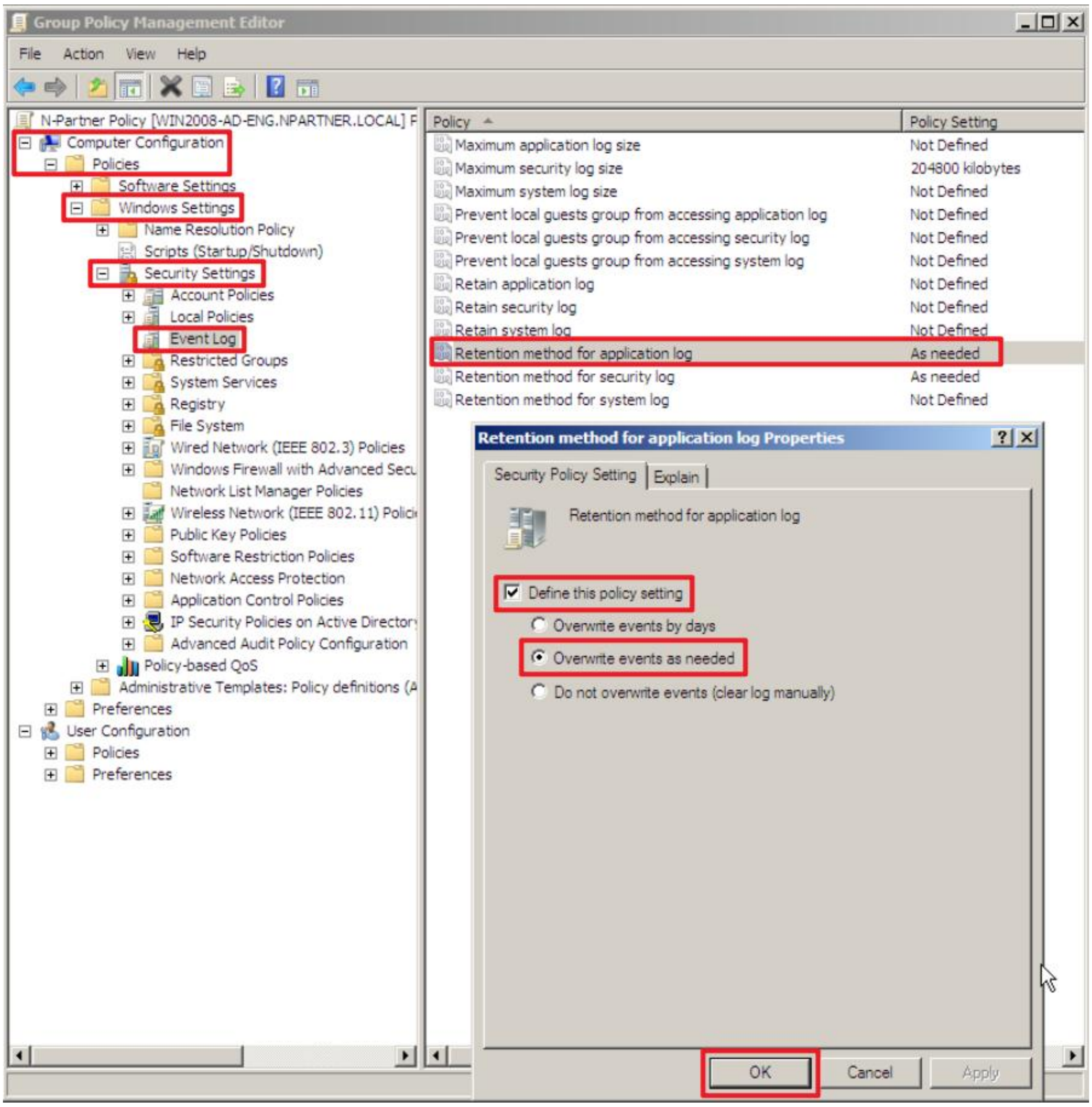
Audit these attempts:

☑ Success

☑ Failure

(6) Event Log: Application Log Retention Method

Expand “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” → select “Retention method for application log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”


Group Policy Management Editor
File
Action
View
Help
N-Partner Policy [WIN2008-AD-ENG.NPARTNER.LOCAL] P
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Wireless Network (IEEE 802.11) Polici
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Director
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (A
Preferences
User Configuration
Policies
Preferences

Policy	Policy Setting
Maximum application log size	Not Defined
Maximum security log size	204800 kilobytes
Maximum system log size	Not Defined
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	As needed
Retention method for security log	As needed
Retention method for system log	Not Defined

Retention method for application log Properties

Security Policy Setting | Explain

Retention method for application log

☑ Define this policy setting

○ Overwrite events by days

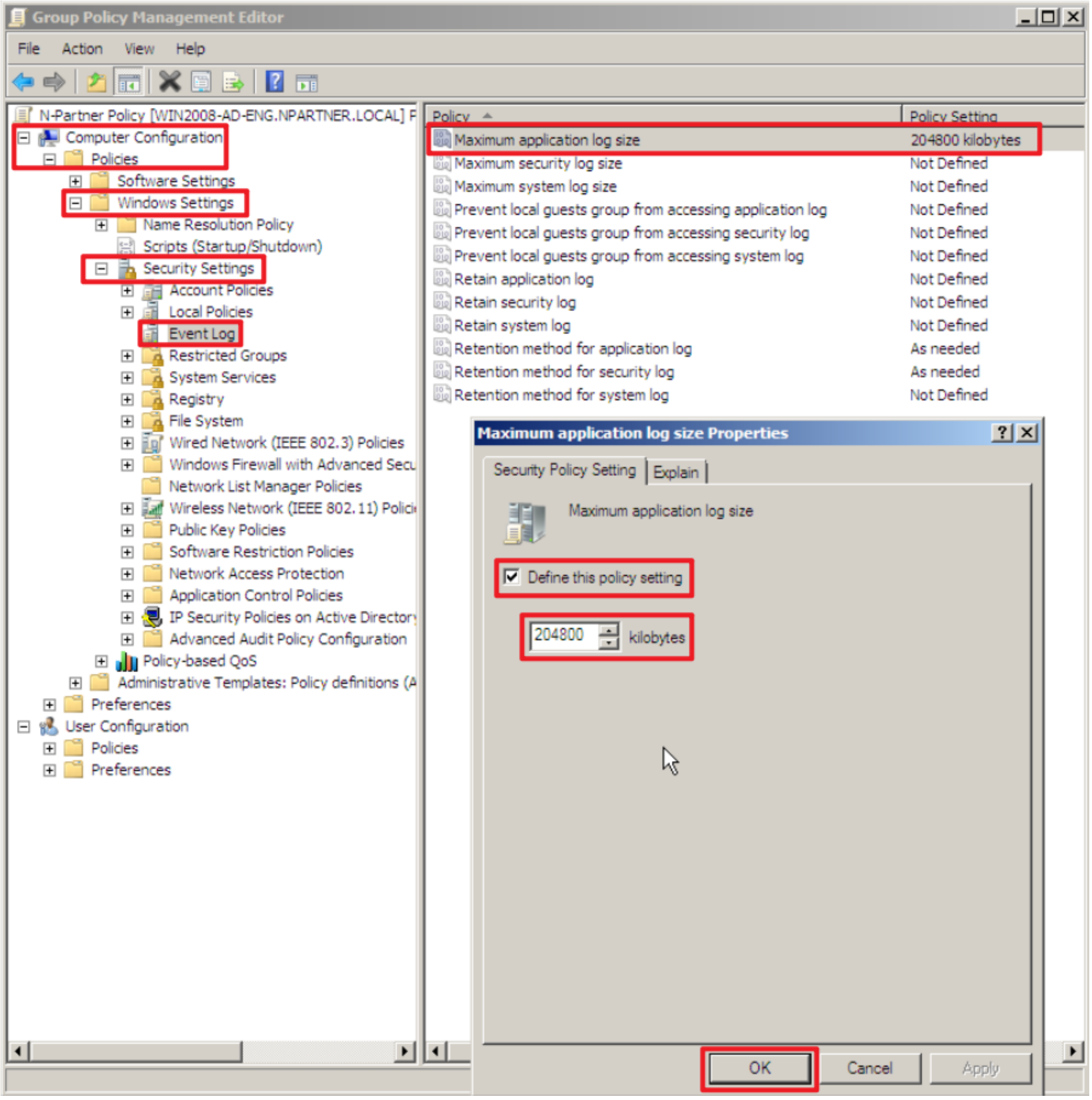
● Overwrite events as needed

○ Do not overwrite events (clear log manually)

(7) Event Logs: Maximum Size of Security Log

Expand folder “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” →And click on “Maximum application log size” → Check “Define this policy setting” → enter 204800 KB

Note: Please adjust the number based on the actual environment. → click “OK.”


Group Policy Management Editor
File
Action
View
Help
N-Partner Policy [WIN2008-AD-ENG.NPARTNER.LOCAL] F
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Wireless Network (IEEE 802.11) Polici
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Director
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (A
Preferences
User Configuration
Policies
Preferences
Security Policy Setting
Explain
OK
Cancel
Apply

Policy	Policy Setting
Maximum application log size	204800 kilobytes
Maximum security log size	Not Defined
Maximum system log size	Not Defined
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	As needed
Retention method for security log	As needed
Retention method for system log	Not Defined

Maximum application log size Properties

Maximum application log size

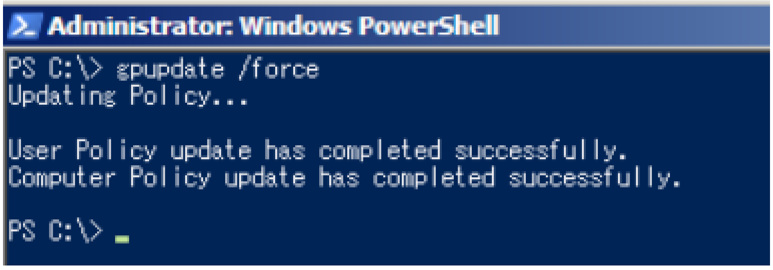
☑ Define this policy setting

204800 kilobytes

(8) On the AD domain server, open “Windows PowerShell.”

(9) Enter the command below to refresh group policy.

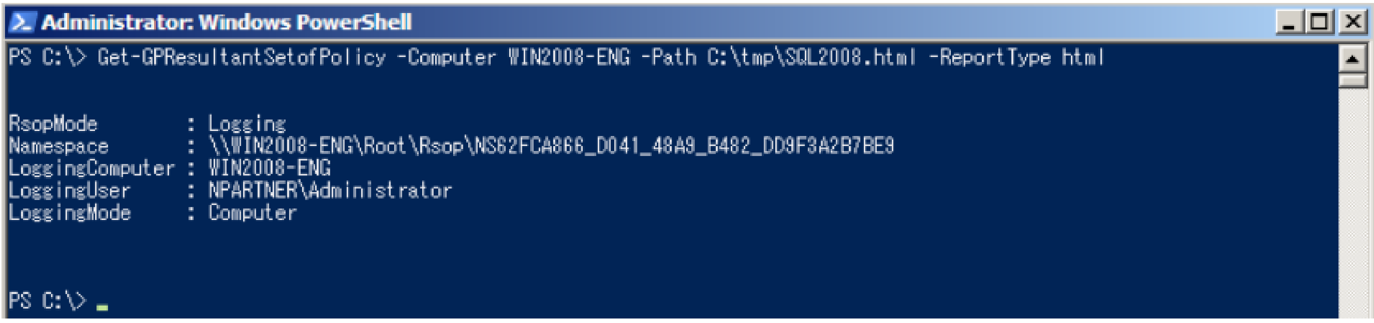
```
PS C:\> gpupdate /force
```



```
PS C:\> gpupdate /force
Updating Policy...

User Policy update has completed successfully.
Computer Policy update has completed successfully.

PS C:\> _
```

(10) Enter the command below to generate server group policy report.

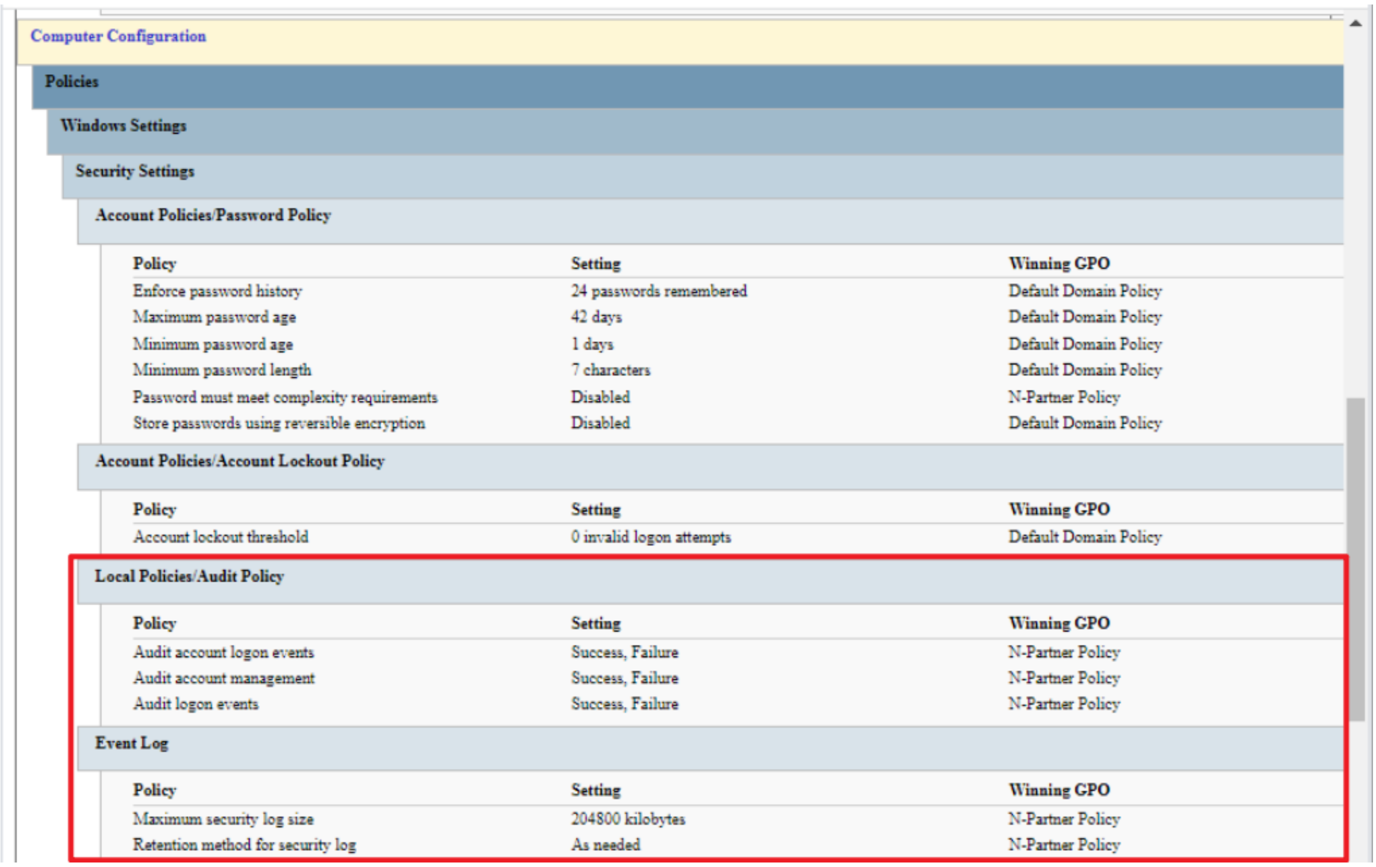
```
PS C:\> Get-GPResultantSetofPolicy -Computer WIN2008-ENG -Path C:\tmp\SQL2008.html -ReportType html
```



```
PS C:\> Get-GPResultantSetofPolicy -Computer WIN2008-ENG -Path C:\tmp\SQL2008.html -ReportType html


RsopMode        : Logging
Namespace       : \\WIN2008-ENG\Root\Rsop\NS62FCA866_D041_48A9_B482_DD9F3A2B7BE9
LoggingComputer : WIN2008-ENG
LoggingUser     : NPARTNER\Administrator
LoggingMode     : Computer



PS C:\> _
```

For the red text , please enter the MS SQL server name and the folder path/file name.

(11) Open the report and verify that your MS SQL server is applying the N-Partner Policy Group Policy.



Computer Configuration

Policies

Windows Settings

Security Settings

Account Policies/Password Policy

Policy	Setting	Winning GPO
Enforce password history	24 passwords remembered	Default Domain Policy
Maximum password age	42 days	Default Domain Policy
Minimum password age	1 days	Default Domain Policy
Minimum password length	7 characters	Default Domain Policy
Password must meet complexity requirements	Disabled	N-Partner Policy
Store passwords using reversible encryption	Disabled	Default Domain Policy

Account Policies/Account Lockout Policy

Policy	Setting	Winning GPO
Account lockout threshold	0 invalid logon attempts	Default Domain Policy

Local Policies/Audit Policy

Policy	Setting	Winning GPO
Audit account logon events	Success, Failure	N-Partner Policy
Audit account management	Success, Failure	N-Partner Policy
Audit logon events	Success, Failure	N-Partner Policy

Event Log

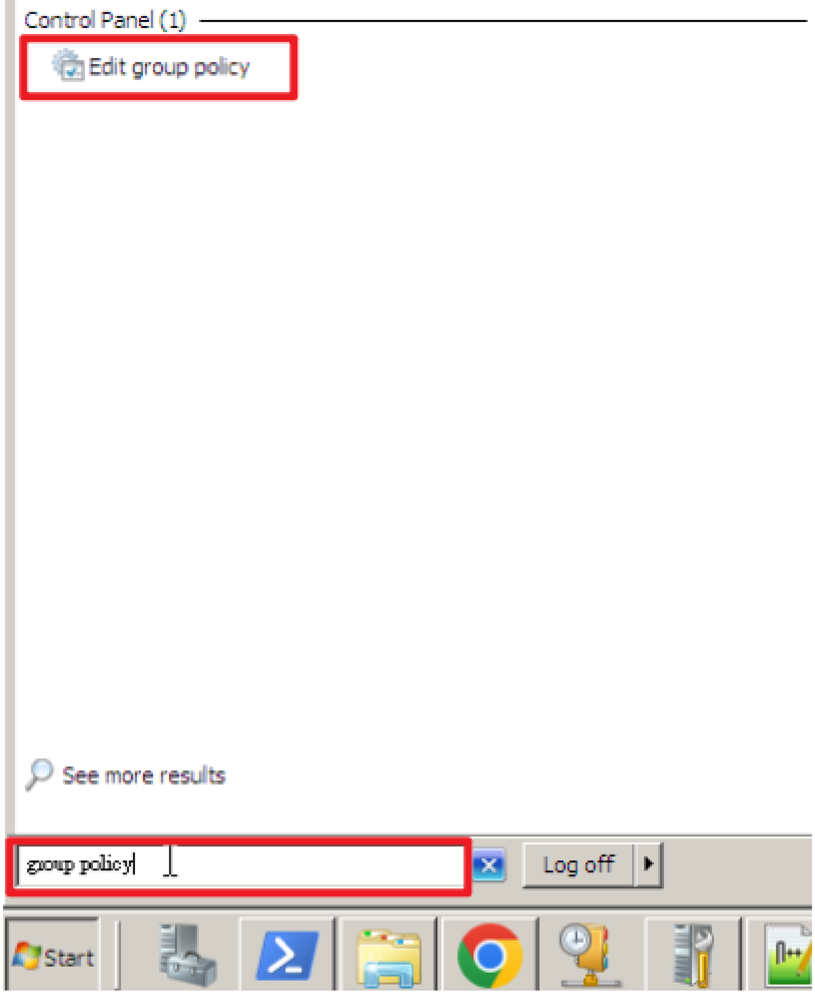
Policy	Setting	Winning GPO
Maximum security log size	204800 kilobytes	N-Partner Policy
Retention method for security log	As needed	N-Partner Policy

2.3.2 Workgroup

2.3.2.1 Audit Policy Configuration

(1) Open Local Group Policy Editor

Click on “Start” → enter “group policy” to search → click on “Edit Group Policy.”



Control Panel (1)

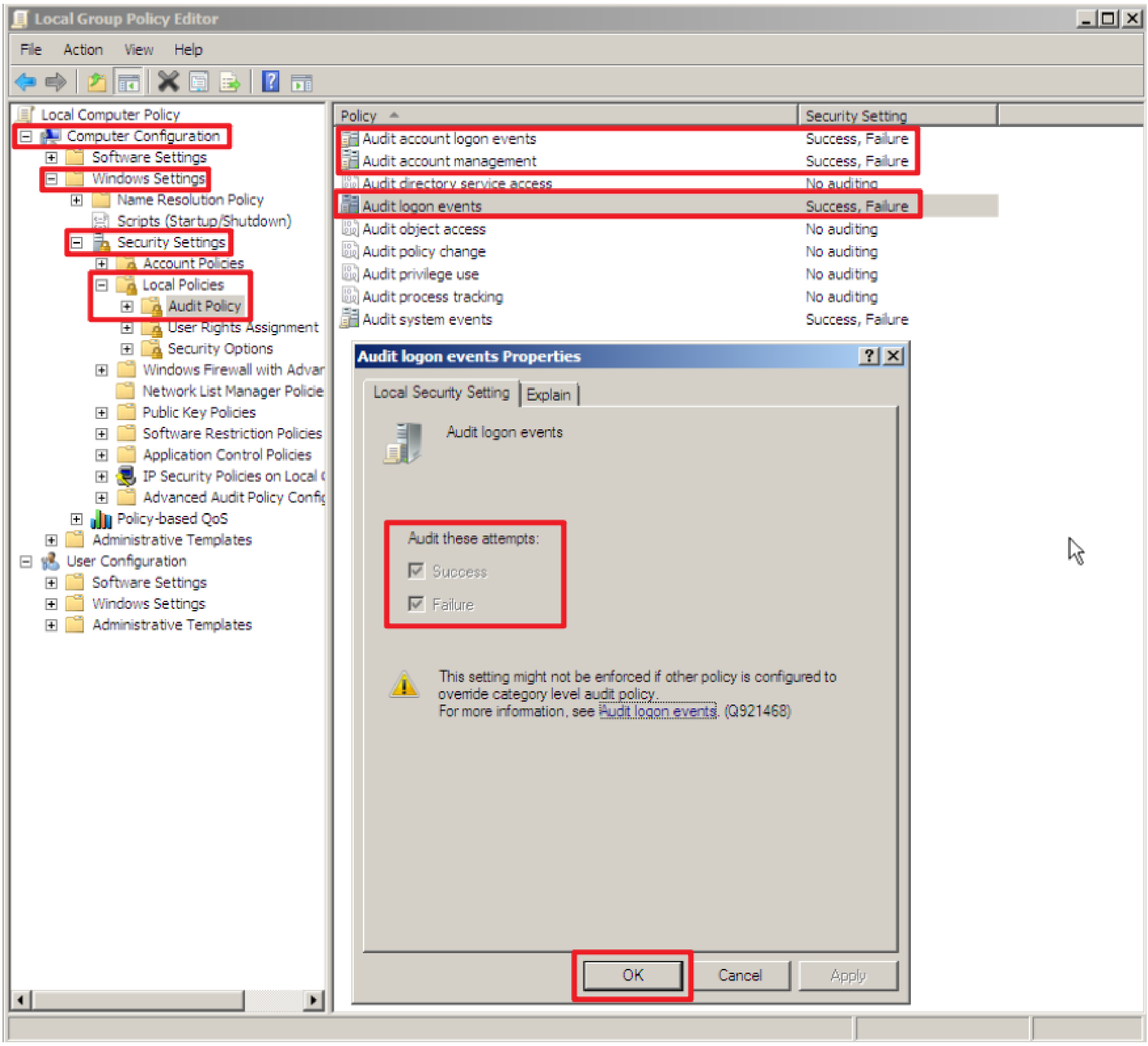
Edit group policy

See more results

group policy

(2) Local Group Policies: Audit Policy

Expand folder “Computer Configuration” → “Windows Settings” → “Security Settings” -> “Local Policies” → “Audit Policy.” And click on “Audit account logon events,” “Audit account management,” and “Audit logon events” items → check “Define these policy settings”: Success, Failure. → click “OK.”



Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	No auditing
Audit logon events	Success, Failure
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	Success, Failure

Audit logon events Properties

Audit logon events

Audit these attempts:

☑ Success

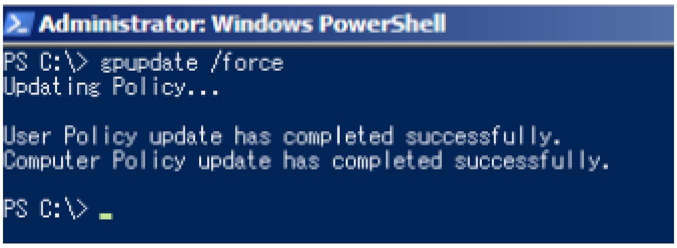
☑ Failure

This setting might not be enforced if other policy is configured to override category level audit policy.
For more information, see Audit logon events. (Q921468)

(3) Open “Windows PowerShell.”

(4) Enter the command below to refresh group policy.

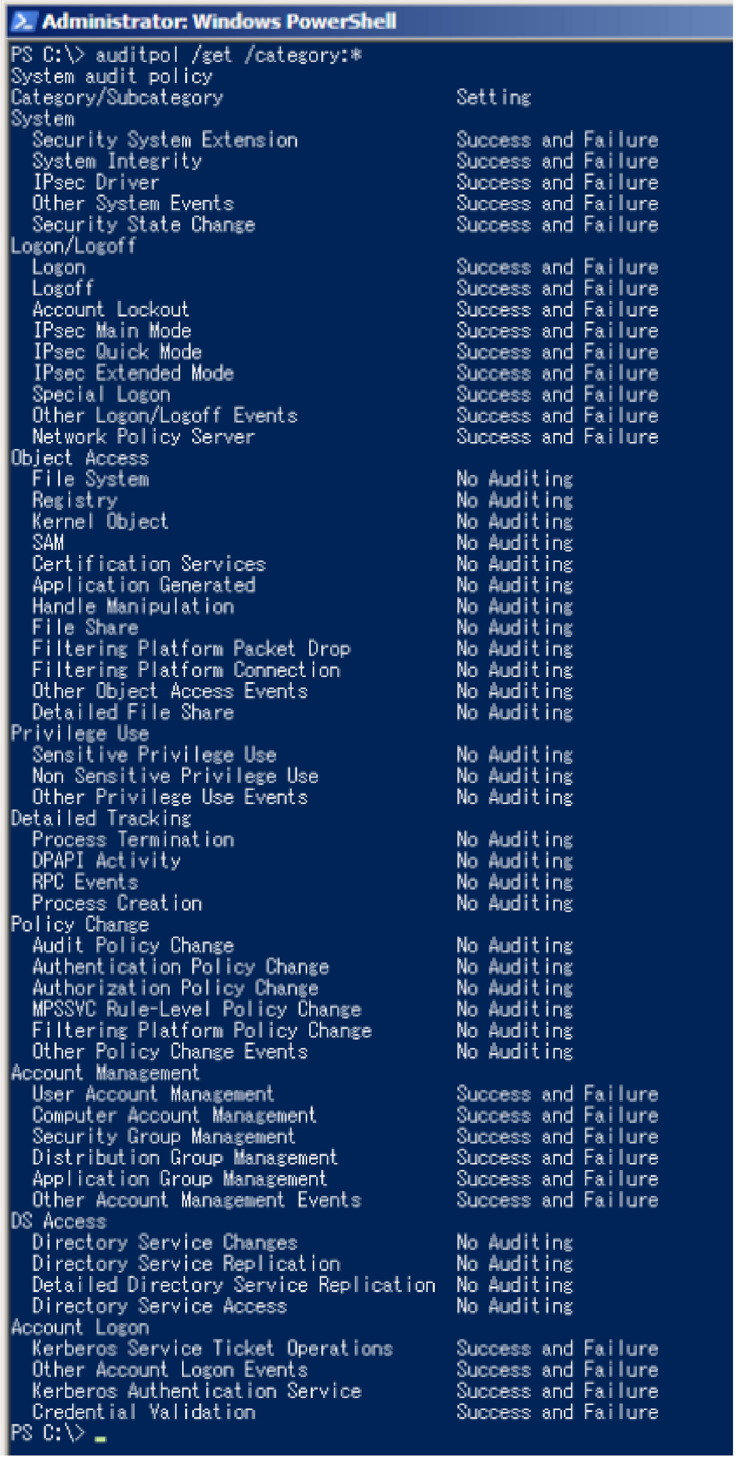
```
PS C:\> gpupdate /force
```



```
PS C:\> gpupdate /force
Updating Policy...

User Policy update has completed successfully.
Computer Policy update has completed successfully.

PS C:\> _
```

(5) Enter the command below to view group policy applied status.

```
PS C: \> auditpol /get /category:*
```

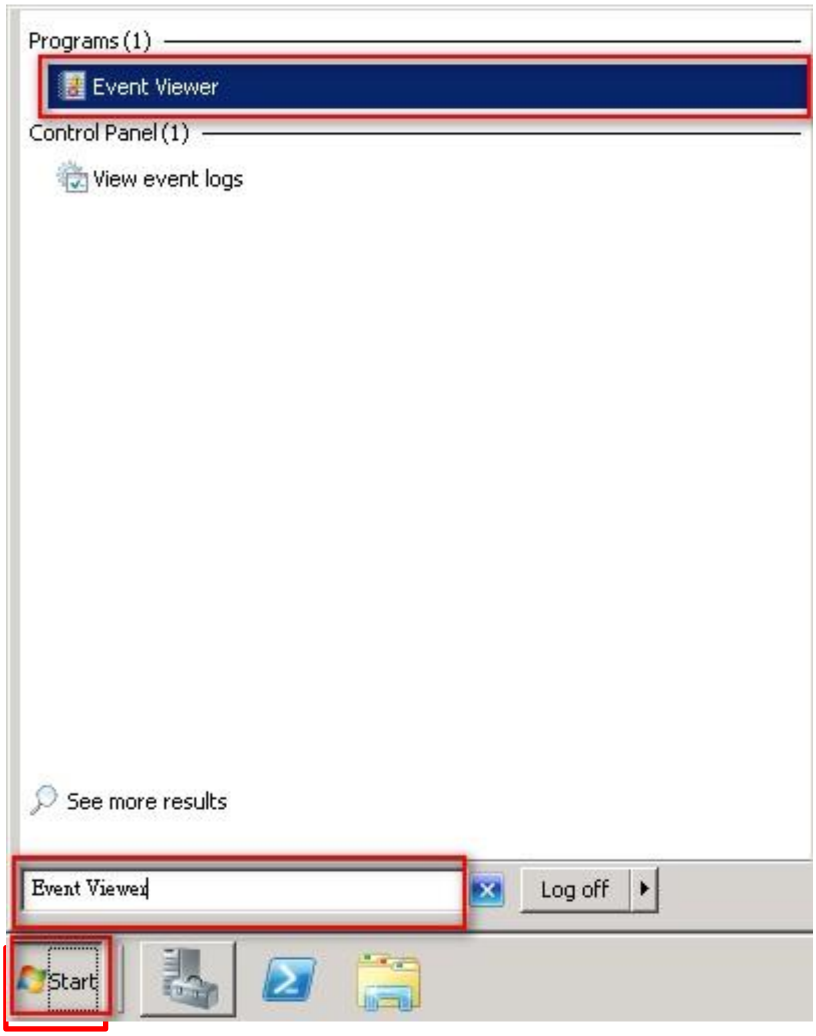


```
PS C:\> auditpol /get /category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               Success and Failure
  System Integrity                        Success and Failure
  IPsec Driver                            Success and Failure
  Other System Events                     Success and Failure
  Security State Change                   Success and Failure
Logon/Logoff
  Logon                                   Success and Failure
  Logoff                                  Success and Failure
  Account Lockout                         Success and Failure
  IPsec Main Mode                         Success and Failure
  IPsec Quick Mode                        Success and Failure
  IPsec Extended Mode                     Success and Failure
  Special Logon                           Success and Failure
  Other Logon/Logoff Events               Success and Failure
  Network Policy Server                   Success and Failure
Object Access
  File System                             No Auditing
  Registry                                No Auditing
  Kernel Object                           No Auditing
  SAM                                     No Auditing
  Certification Services                  No Auditing
  Application Generated                   No Auditing
  Handle Manipulation                     No Auditing
  File Share                              No Auditing
  Filtering Platform Packet Drop          No Auditing
  Filtering Platform Connection           No Auditing
  Other Object Access Events              No Auditing
  Detailed File Share                     No Auditing
Privilege Use
  Sensitive Privilege Use                 No Auditing
  Non Sensitive Privilege Use             No Auditing
  Other Privilege Use Events              No Auditing
Detailed Tracking
  Process Termination                     No Auditing
  DPAPI Activity                          No Auditing
  RPC Events                              No Auditing
  Process Creation                        No Auditing
Policy Change
  Audit Policy Change                     No Auditing
  Authentication Policy Change            No Auditing
  Authorization Policy Change             No Auditing
  MPSSVC Rule-Level Policy Change         No Auditing
  Filtering Platform Policy Change        No Auditing
  Other Policy Change Events              No Auditing
Account Management
  User Account Management                 Success and Failure
  Computer Account Management             Success and Failure
  Security Group Management               Success and Failure
  Distribution Group Management           Success and Failure
  Application Group Management            Success and Failure
  Other Account Management Events         Success and Failure
DS Access
  Directory Service Changes               No Auditing
  Directory Service Replication           No Auditing
  Detailed Directory Service Replication  No Auditing
  Directory Service Access                No Auditing
Account Logon
  Kerberos Service Ticket Operations      Success and Failure
  Other Account Logon Events              Success and Failure
  Kerberos Authentication Service         Success and Failure
  Credential Validation                   Success and Failure
PS C:\> _
```

2.3.2.2 Event Log Settings

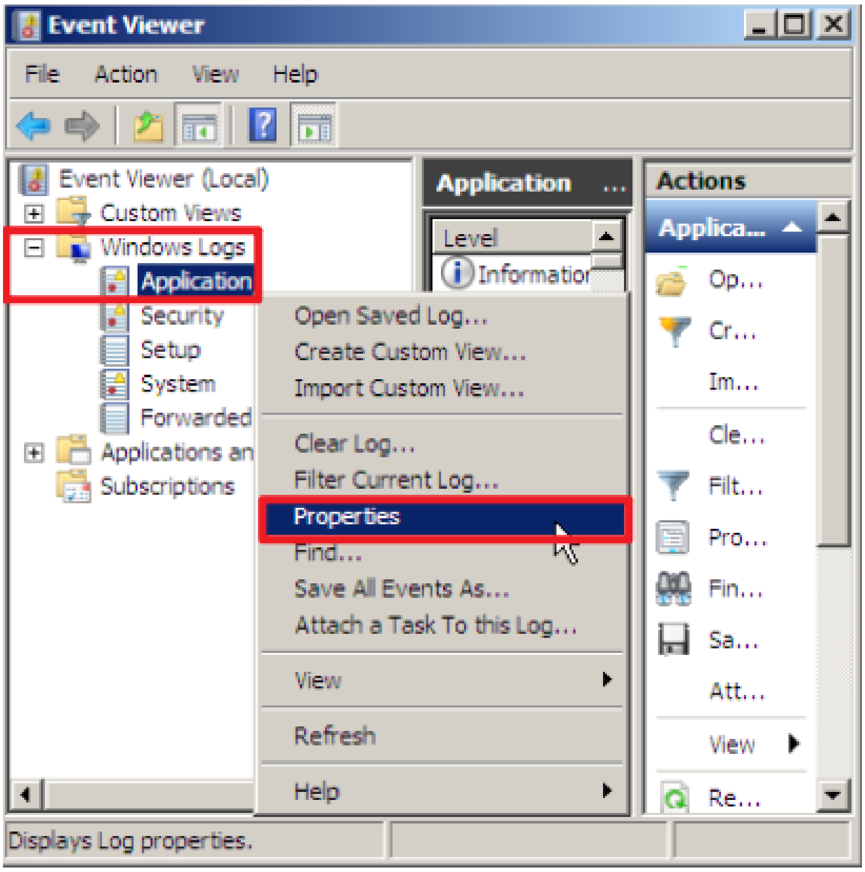
(1) Search for “Event Viewer”

Enter “Event Viewer” to search → click on “Event Viewer” in the search results.



(2) Edit Security Log

Expand folder “Windows Logs.” →right-click on “Application” → And click on “Properties.”

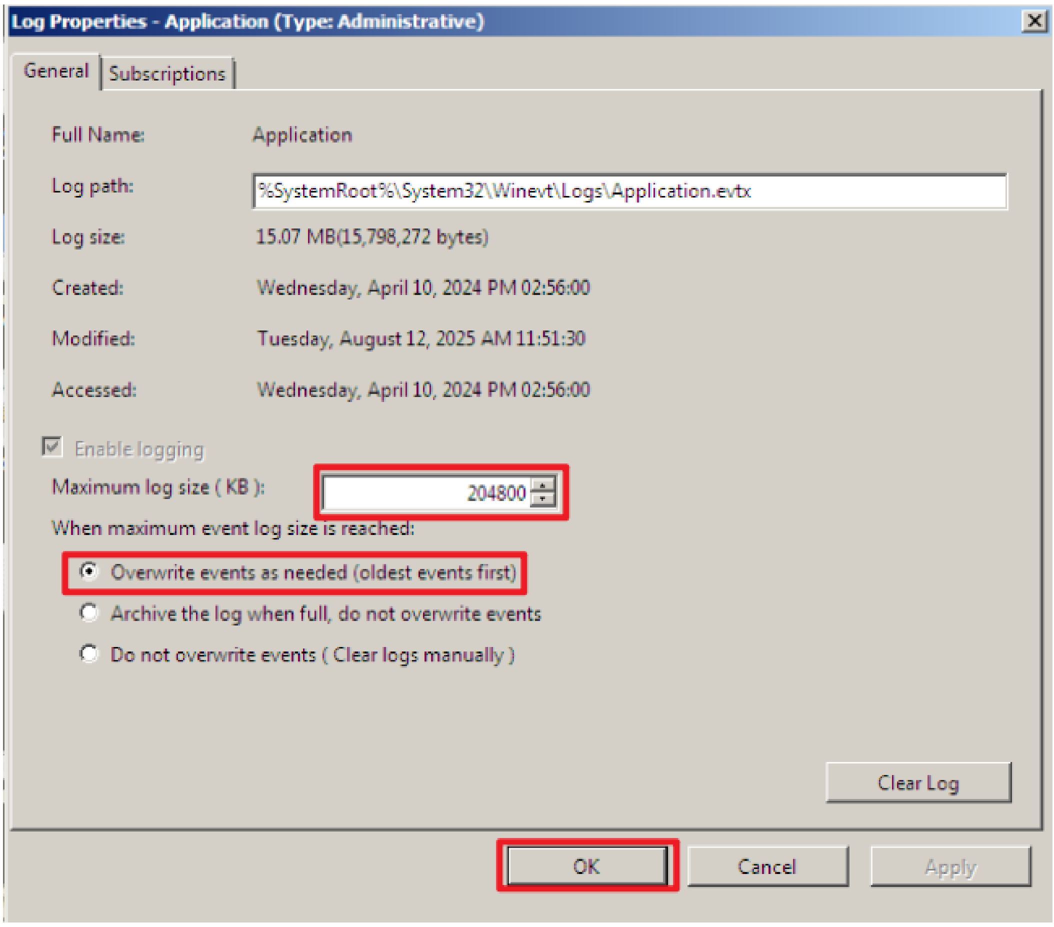


(3) Configure Security Log

Enter maximum log file size: 204800 KB

Note: Please adjust the number according to the actual environment.

→ click on "Overwrite events as needed" -> Click "OK."



Log Properties - Application (Type: Administrative)

General | Subscriptions

Full Name: Application

Log path: %SystemRoot%\System32\Winevt\Logs\Application.evtx

Log size: 15.07 MB(15,798,272 bytes)

Created: Wednesday, April 10, 2024 PM 02:56:00

Modified: Tuesday, August 12, 2025 AM 11:51:30

Accessed: Wednesday, April 10, 2024 PM 02:56:00

☑ Enable logging

Maximum log size (KB): 204800

When maximum event log size is reached:

● Overwrite events as needed (oldest events first)

○ Archive the log when full, do not overwrite events

○ Do not overwrite events (Clear logs manually)

3. SQL Server 2012

3.1 Login Auditing

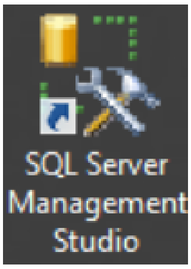
Enable login auditing to monitor SQL Server Database Engine login activities.

After configuration, the MS SQL Server service must be **restarted**.

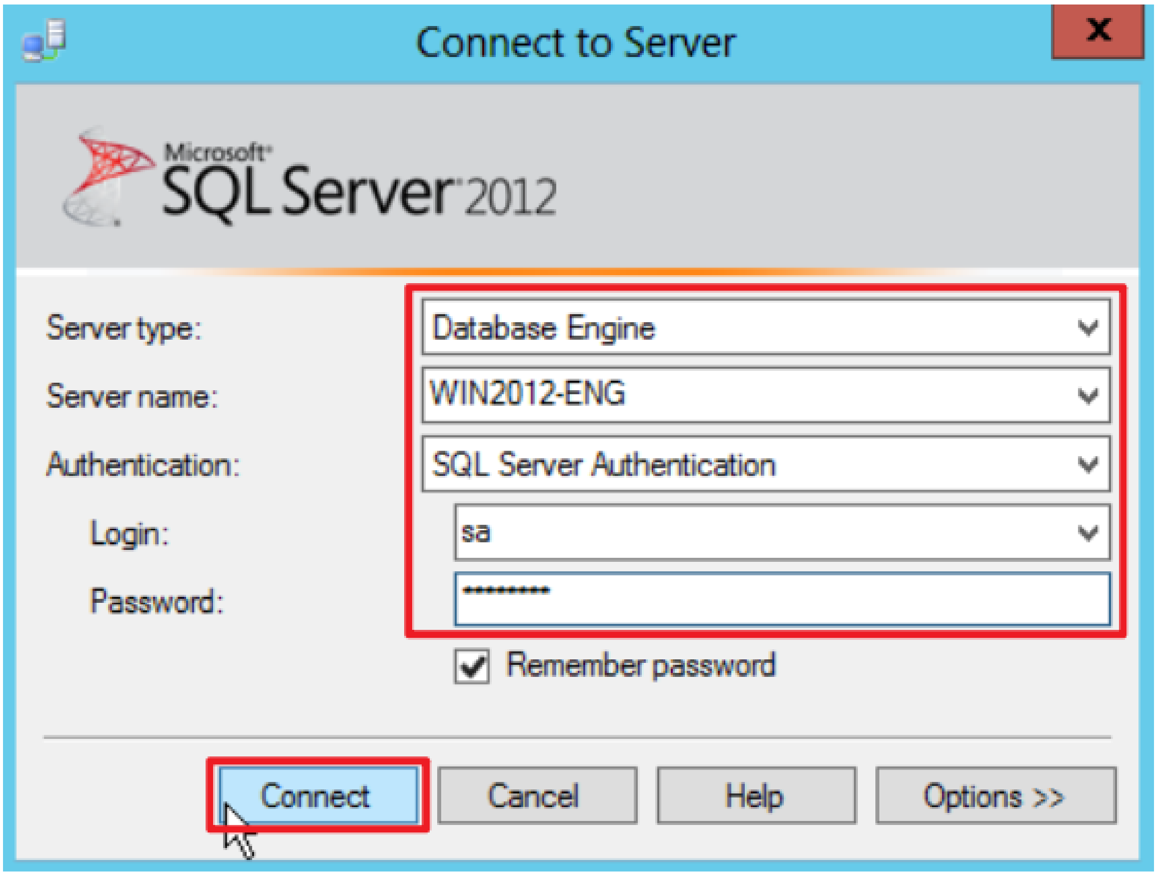
The following sections describe how to configure login auditing using both the graphical user interface (GUI) and command-line interface (CLI).

3.1.1 Configuring via Graphical User Interface (GUI)

(1) Open "SQL Server Management Studio (SSMS)."



(2) Enter the server's name → select the authentication method → click "Connect."



Server type: Database Engine

Server name: WIN2012-ENG

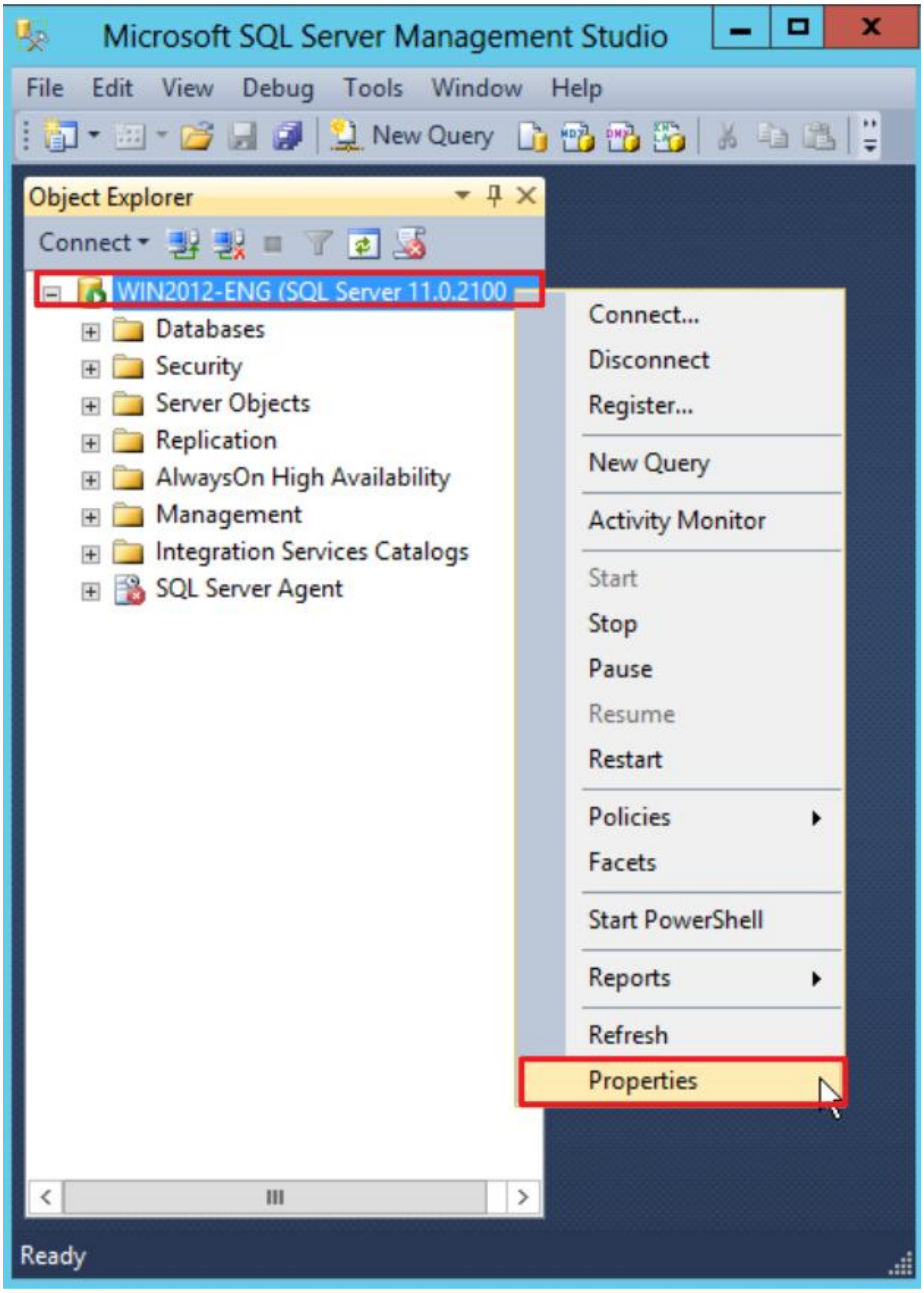
Authentication: SQL Server Authentication

Login: sa

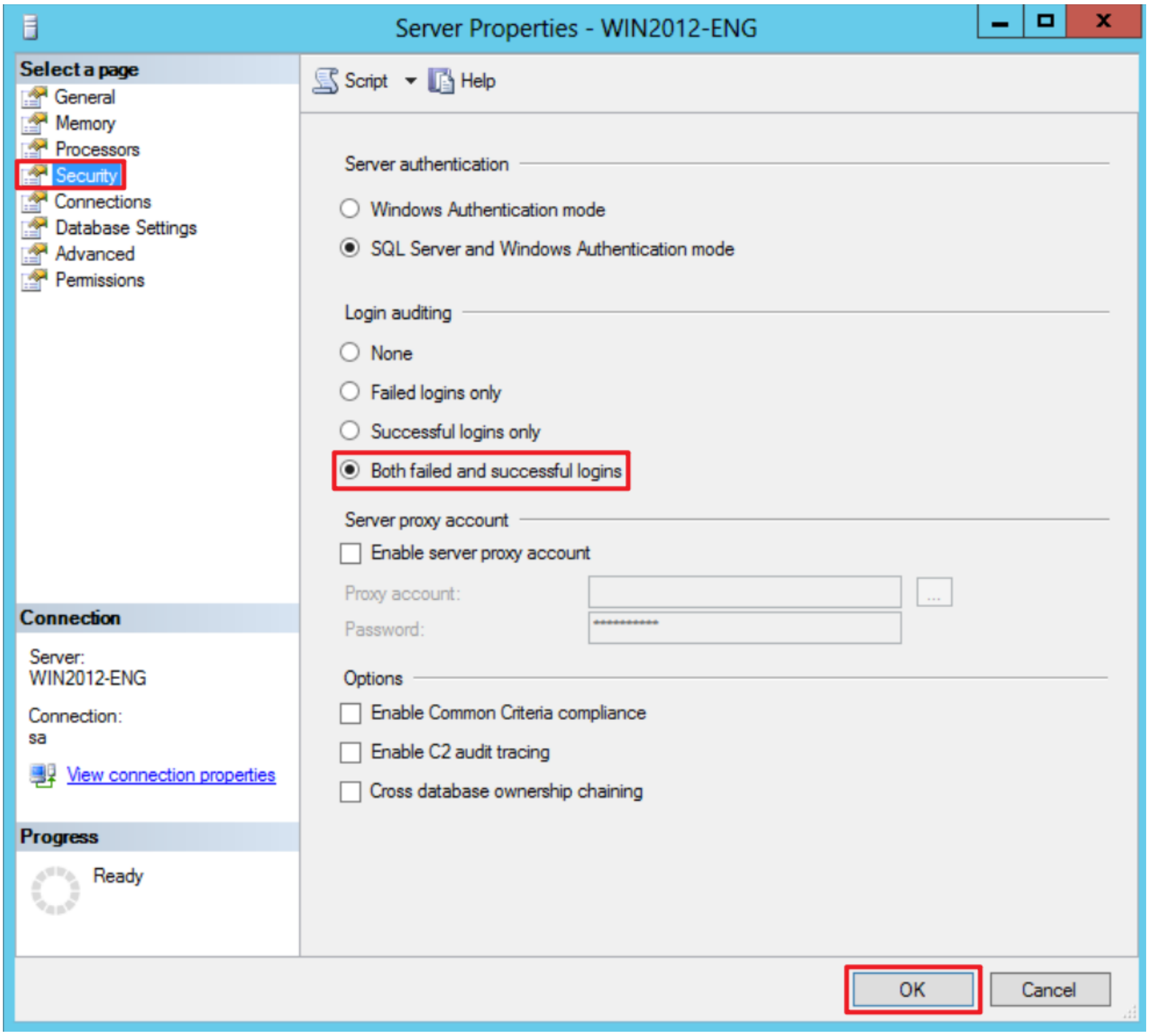
Password: *********

☑ Remember password

(3) In [Server Name] (the example here is WIN2012-ENG SQL Server 11.0.2100), right-click and select "Properties."



(4) On the Security page, under Login auditing, select “Both failed and successful logins” → click “OK”.



Server Properties - WIN2012-ENG

Select a page
- General
- Memory
- Processors
- Security
- Connections
- Database Settings
- Advanced
- Permissions

Connection

Server:
WIN2012-ENG

Connection:
sa

View connection properties

Progress

Ready

Server authentication

○ Windows Authentication mode
● SQL Server and Windows Authentication mode

Login auditing

○ None
○ Failed logins only
○ Successful logins only
● Both failed and successful logins

Server proxy account

□ Enable server proxy account

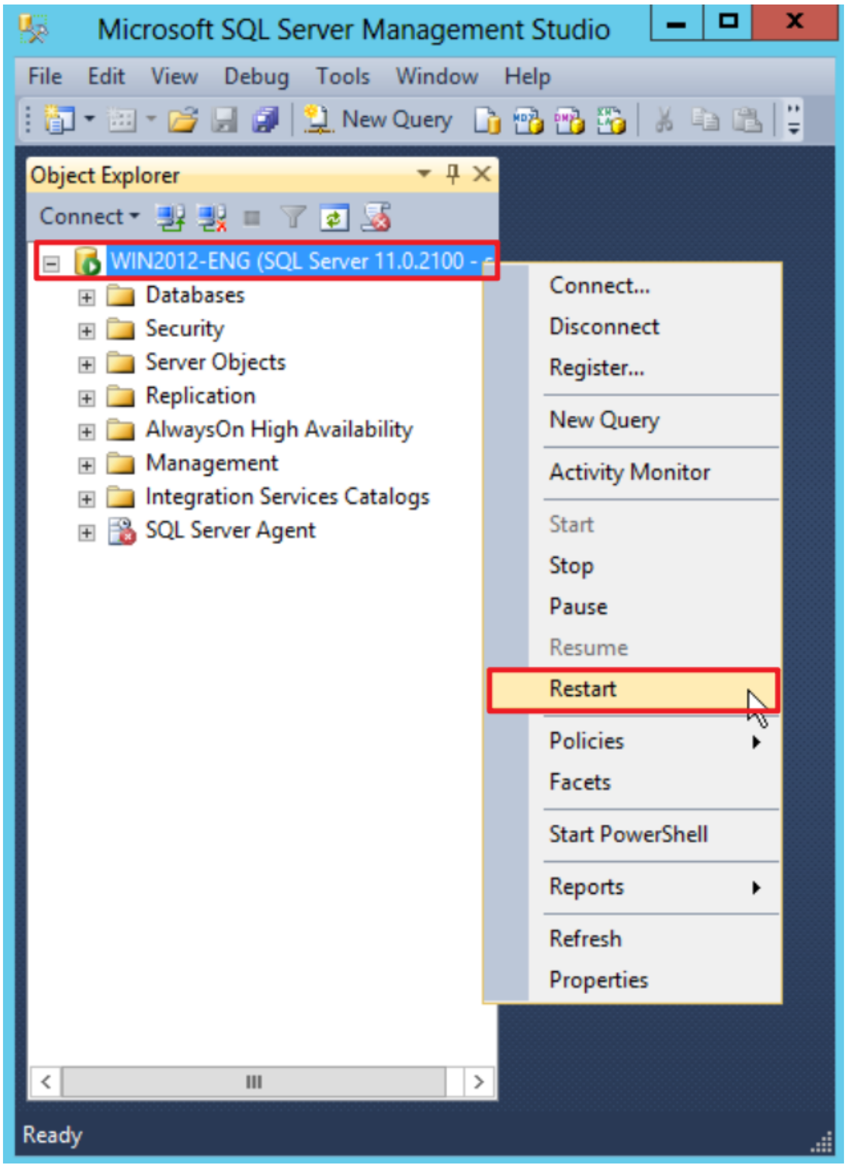
Proxy account:

Password: ***********

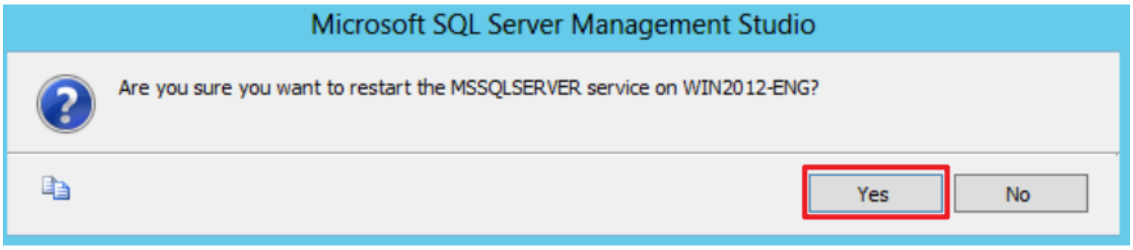
Options

□ Enable Common Criteria compliance
□ Enable C2 audit tracing
□ Cross database ownership chaining

(5) Restart the MS SQL Server service: right-click [Server Name] (the example here is WIN2012-ENG SQL Server 11.0.2100) → select “Restart.”

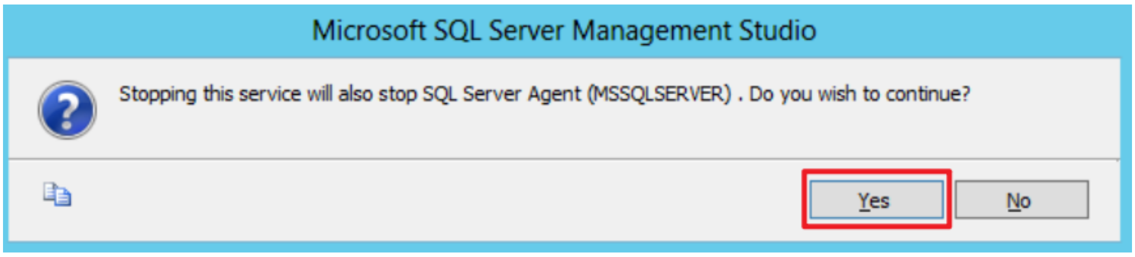


(6) Click “Yes” to restart the MS SQL Server service.



Are you sure you want to restart the MSSQLSERVER service on WIN2012-ENG?

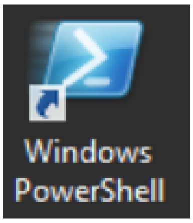
(7) Click “Yes” again to stop the SQL Server Agent service.



Stopping this service will also stop SQL Server Agent (MSSQLSERVER) . Do you wish to continue?

3.1.2 Configuring via Command-Line Interface (CLI)

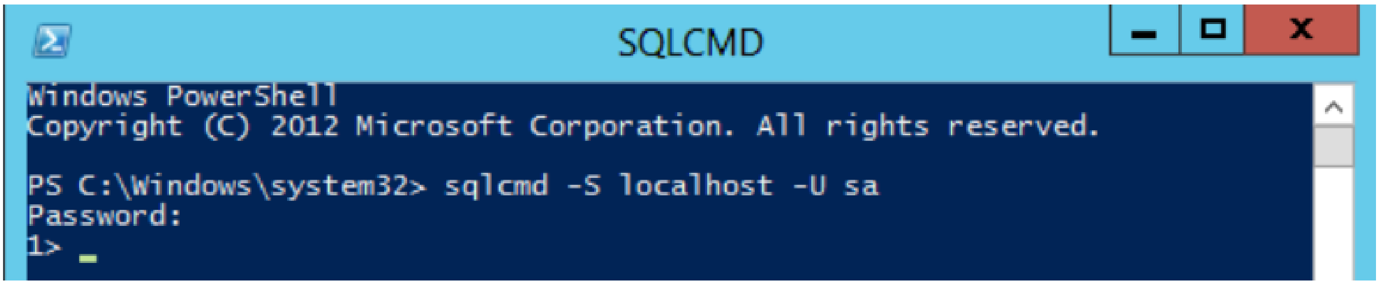
(1) Open “Windows PowerShell.”



(2) Enter the command below to log in using sa:

<2.1>Using sa account:

```
PS C:\> sqlcmd -S localhost -U sa
```



```
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> sqlcmd -S localhost -U sa
Password:
1> _
```

Options:

-S [protocol:]server[instance_name][,port]

-U login_id

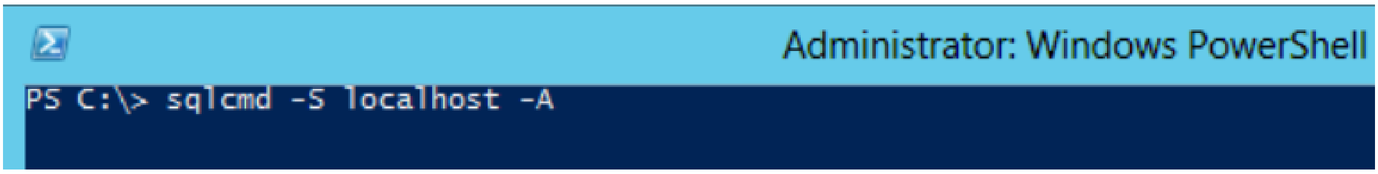
-P password

-A dedicated administrator connection

<2.2> Using Windows account:

Enter the command below to log in using Windows:

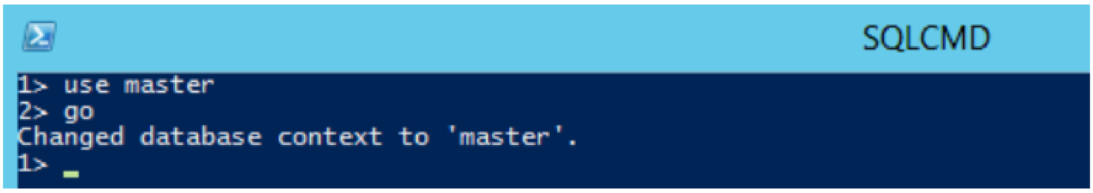
```
PS C:\> sqlcmd -S localhost -A
```



```
PS C:\> sqlcmd -S localhost -A
```

(3) Enter the command below to switch to the **master** database:

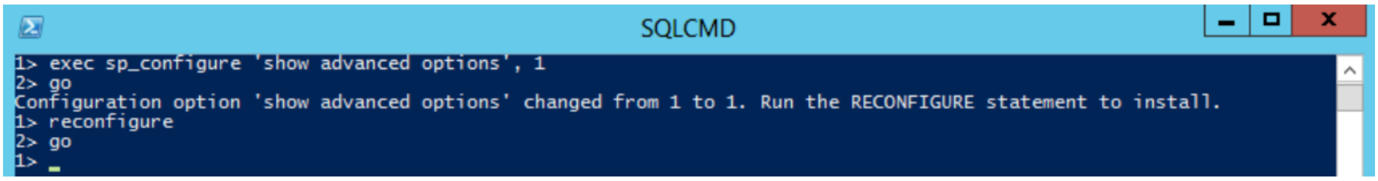
```
1 > use master

2 > go
```



```
1> use master
2> go
Changed database context to 'master'.
1> _
```

(4) Enter the command below to enable advanced options:

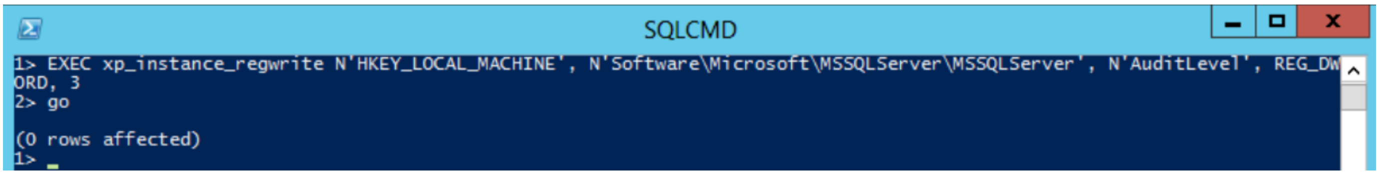
```
1 > exec sp_configure 'show advanced options', 1

2 > go

1 > reconfigure

2 > go
```



```
1> exec sp_configure 'show advanced options', 1
2> go
Configuration option 'show advanced options' changed from 1 to 1. Run the RECONFIGURE statement to install.
1> reconfigure
2> go
1> _
```

(5) Enter the command below to enable auditing for both failed and successful logins:

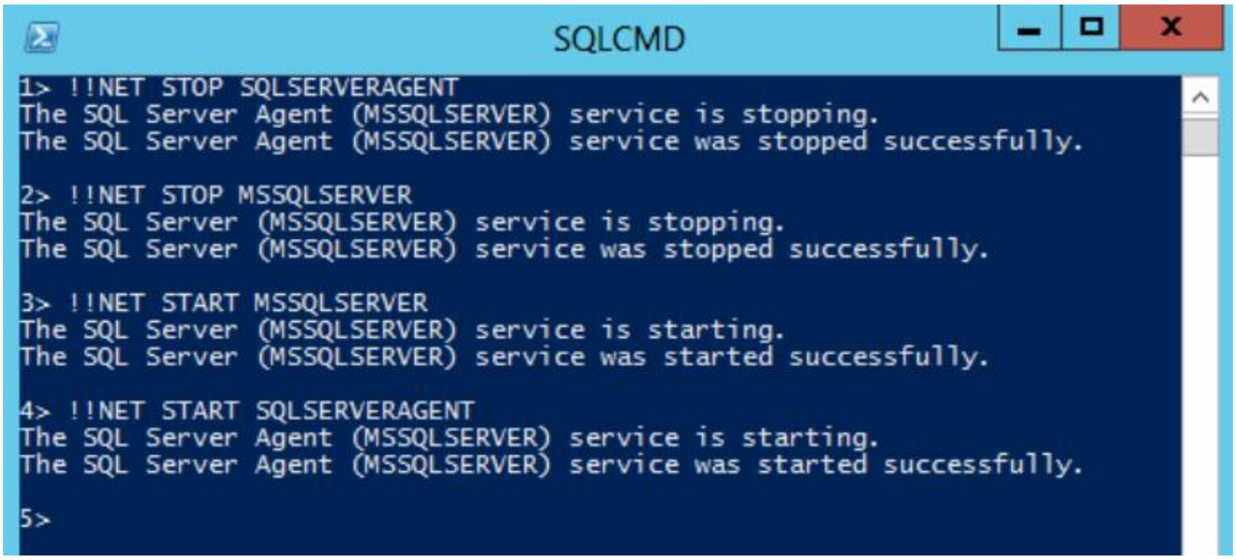
```
1 > EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE',

N'Software\Microsoft\MSSQLServer\MSSQLServer', N'AuditLevel', REG_DWORD, 3

2 > go
```



```
1> EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'Software\Microsoft\MSSQLServer\MSSQLServer', N'AuditLevel', REG_DW
ORD, 3
2> go

(0 rows affected)
1> _
```

(6) Enter the command below to restart the MS SQL Server services:

```
1 > !!NET STOP SQLSERVERAGENT
2 > !!NET STOP MSSQLSERVER
3 > !!NET START MSSQLSERVER
4 > !!NET START SQLSERVERAGENT
```



```
1> !!NET STOP SQLSERVERAGENT
The SQL Server Agent (MSSQLSERVER) service is stopping.
The SQL Server Agent (MSSQLSERVER) service was stopped successfully.

2> !!NET STOP MSSQLSERVER
The SQL Server (MSSQLSERVER) service is stopping.
The SQL Server (MSSQLSERVER) service was stopped successfully.

3> !!NET START MSSQLSERVER
The SQL Server (MSSQLSERVER) service is starting.
The SQL Server (MSSQLSERVER) service was started successfully.

4> !!NET START SQLSERVERAGENT
The SQL Server Agent (MSSQLSERVER) service is starting.
The SQL Server Agent (MSSQLSERVER) service was started successfully.

5>
```

3.2 Configuring Auditing

3.2.1 Server-Level Audit

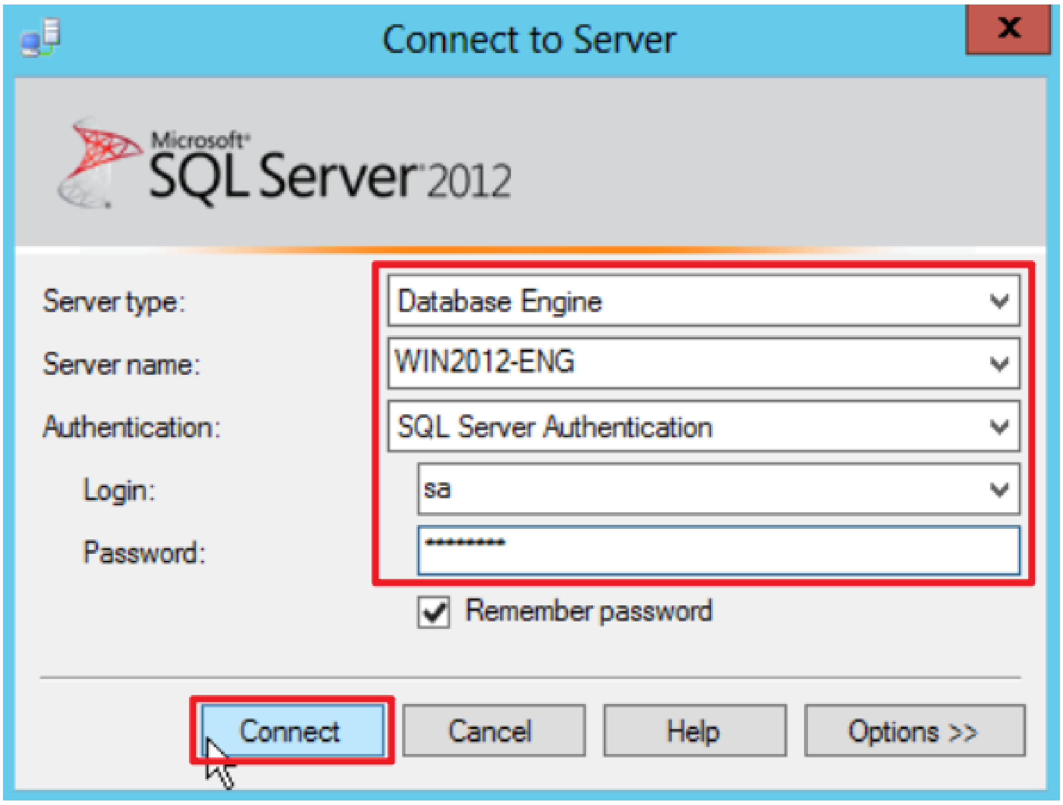
Enabling a server-level audit covers server operations such as administrative changes, login, and logout activities.

The following sections describe how to configure a server-level audit using the graphical user interface (GUI) and the command-line interface (CLI).

3.2.1.1 Configuring via Graphical User Interface (GUI)

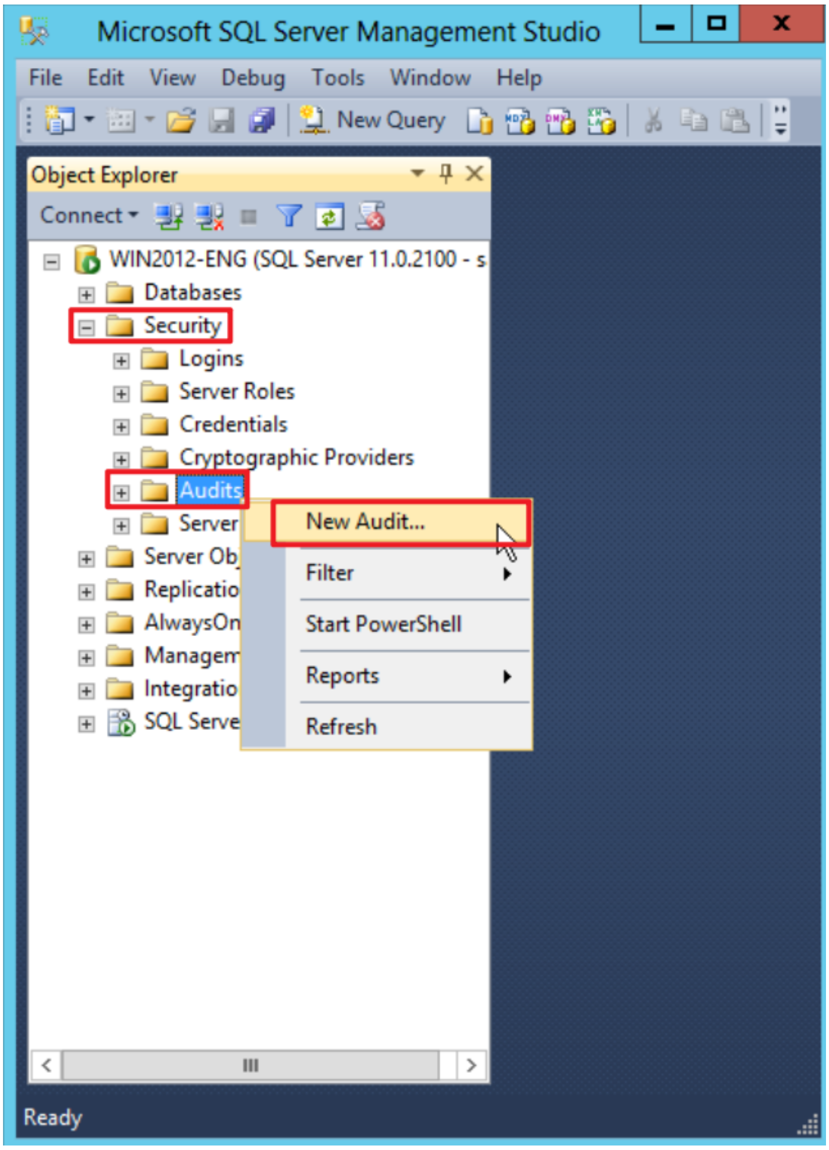
(1) Open "SQL Server Management Studio (SSMS)."

(2) Enter the server's name → select the authentication method → click "Connect."

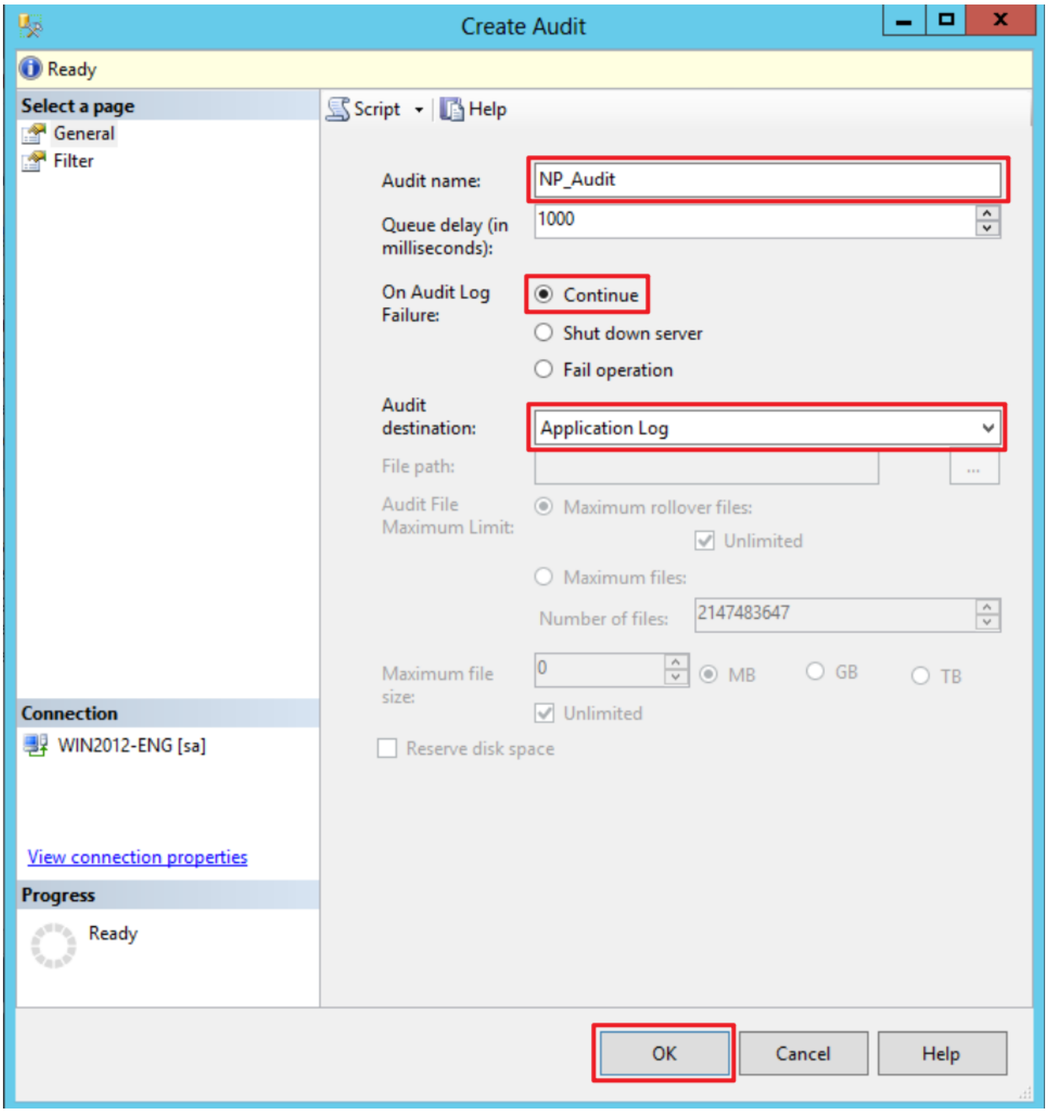


Server type: Database Engine
Server name: WIN2012-ENG
Authentication: SQL Server Authentication
Login: sa
Password: *********
☑ Remember password

(3) Expand “Security” → right-click “Audits” → select “New Audit...”



(4) Enter the audit name: (the example here is NP_Audit) → select “On audit log failure”: “Continue” → select audit destination: Application Log (this stores MS SQL audit logs in the Windows Event Viewer Application Log) → click “OK.”



Create Audit

Ready

Select a page
- General
- Filter

Script ▾ | Help

Audit name: NP_Audit

Queue delay (in milliseconds): 1000

On Audit Log Failure:
- ● Continue
- ○ Shut down server
- ○ Fail operation

Audit destination: Application Log

File path:

Audit File Maximum Limit:
- ● Maximum rollover files:
  - ☑ Unlimited
- ○ Maximum files:
  - Number of files: 2147483647

Maximum file size: 0 ● MB ○ GB ○ TB
- ☑ Unlimited

□ Reserve disk space

Connection

WIN2012-ENG [sa]

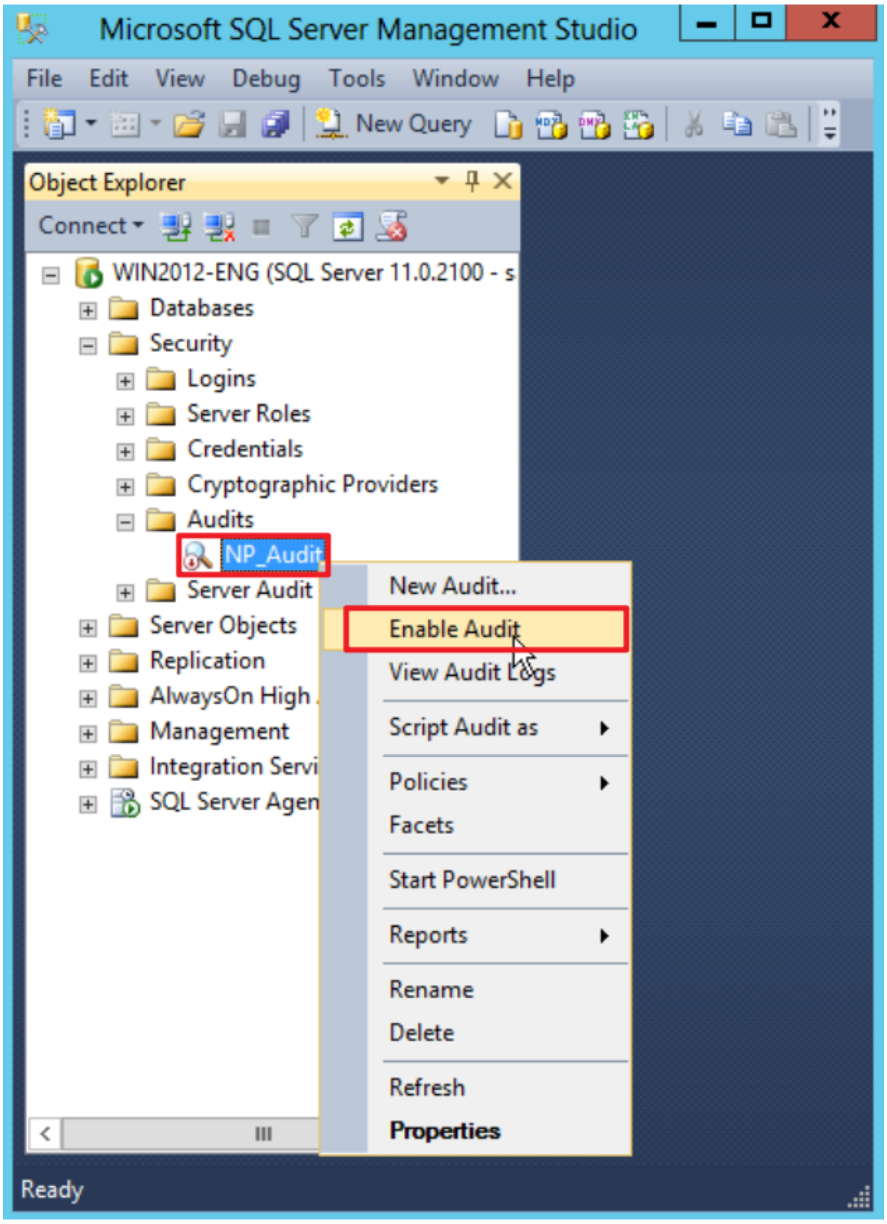
View connection properties

Progress

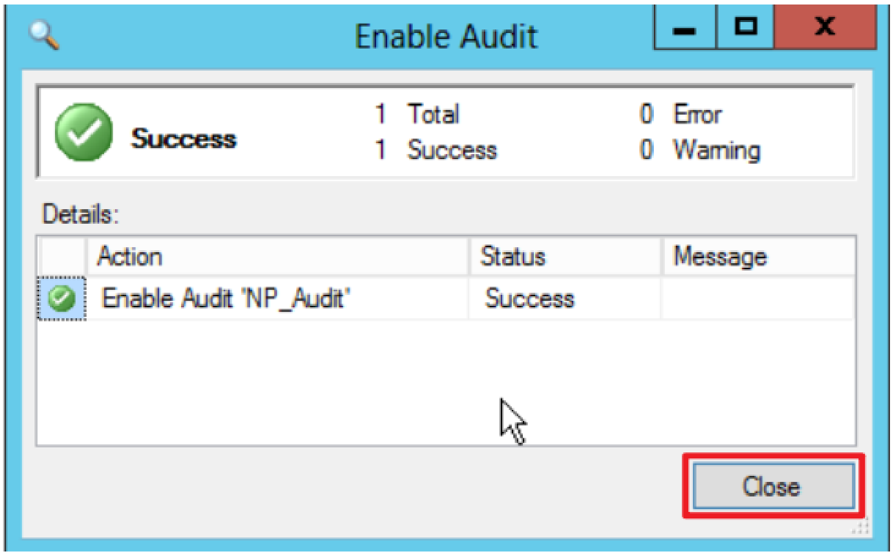
Ready

OK | Cancel | Help

(5) In the audit list, right-click "NP_Audit" → select "Enable Audit."



(6) Click "Close."



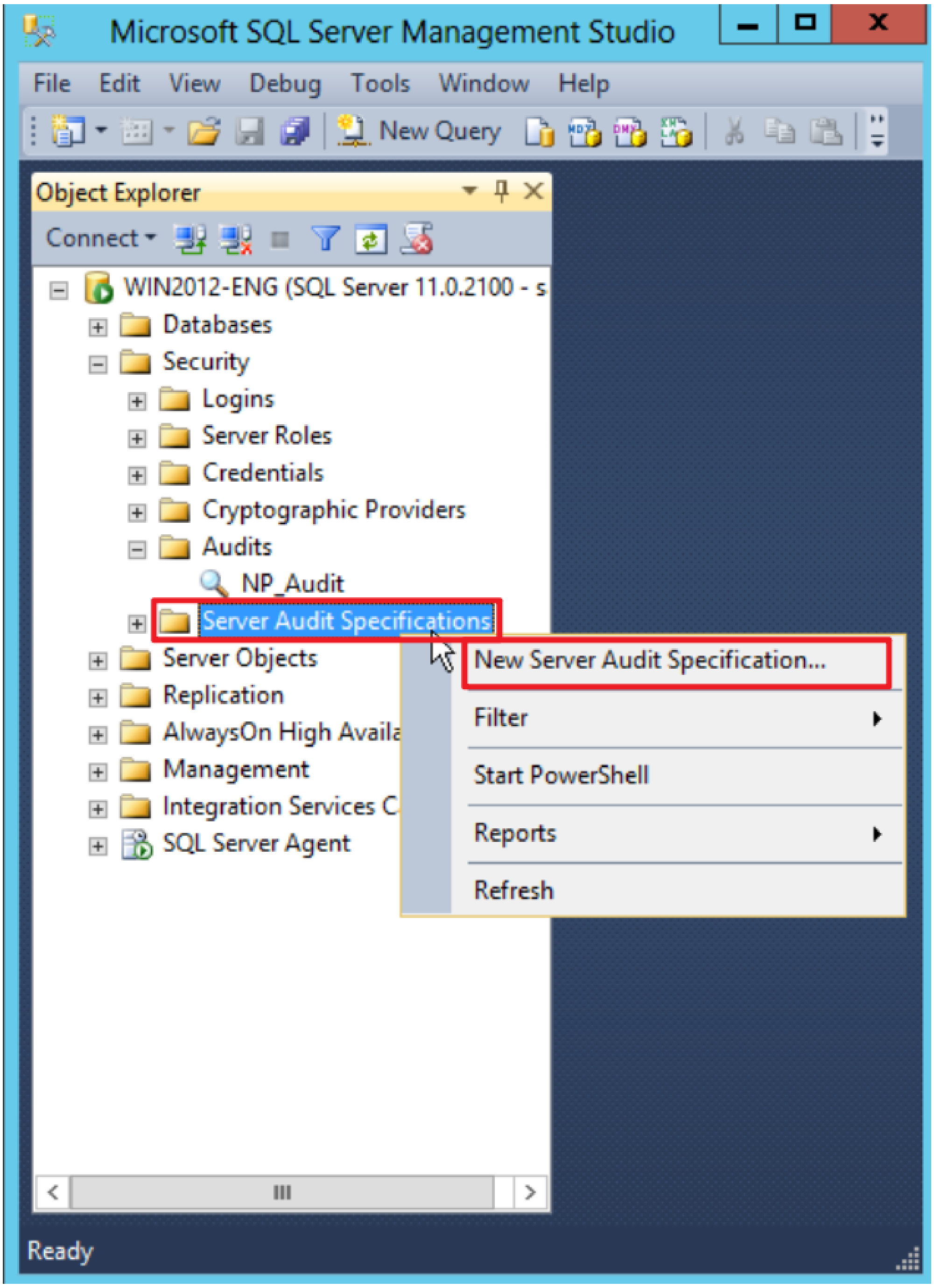
Success

1	Total	0	Error
1	Success	0	Warning

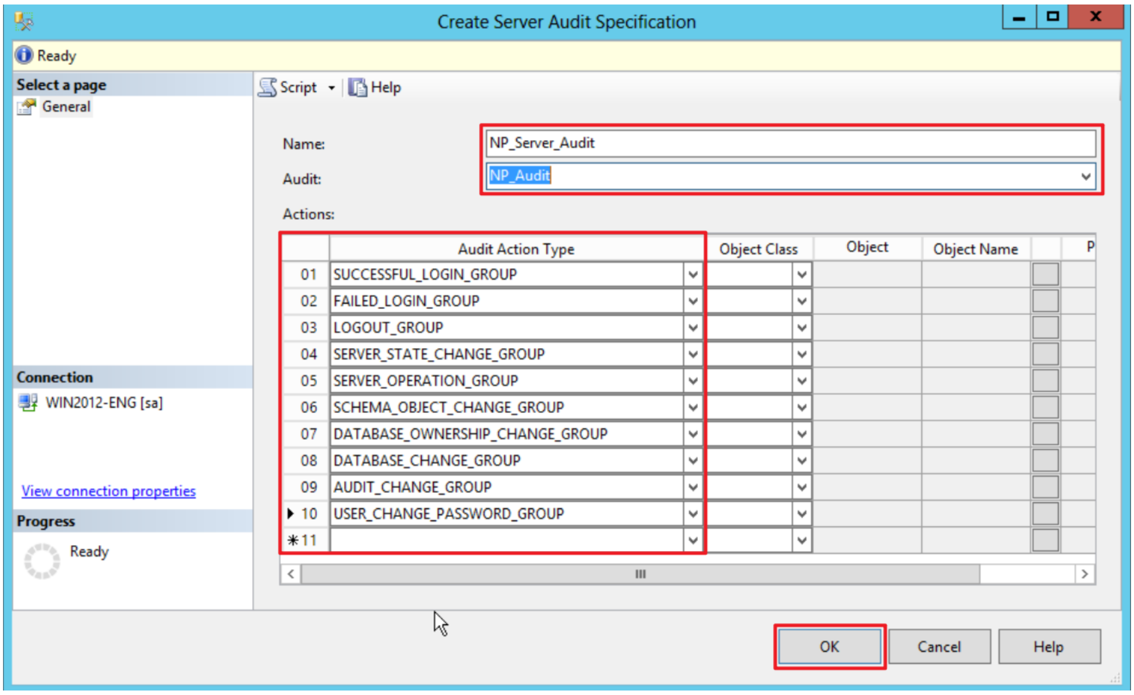
Details:

Action	Status	Message
Enable Audit 'NP_Audit'	Success	

(7) Right-click “Server Audit Specifications,” → select “New Server Audit Specification...”



(8) Enter the specification name: (the example here is NP_Server_Audit) → select audit: NP_Audit → select action(s) (refer to the **SQL Server Audit Action Groups and Actions** in the references for details) → click “OK.”



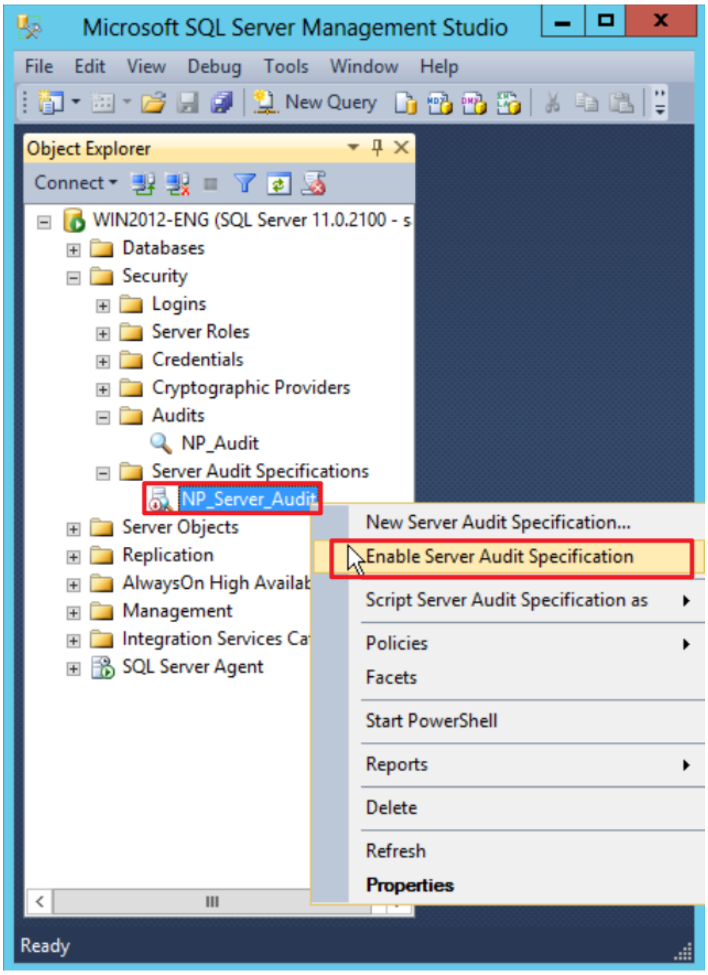
Name: NP_Server_Audit

Audit: NP_Audit

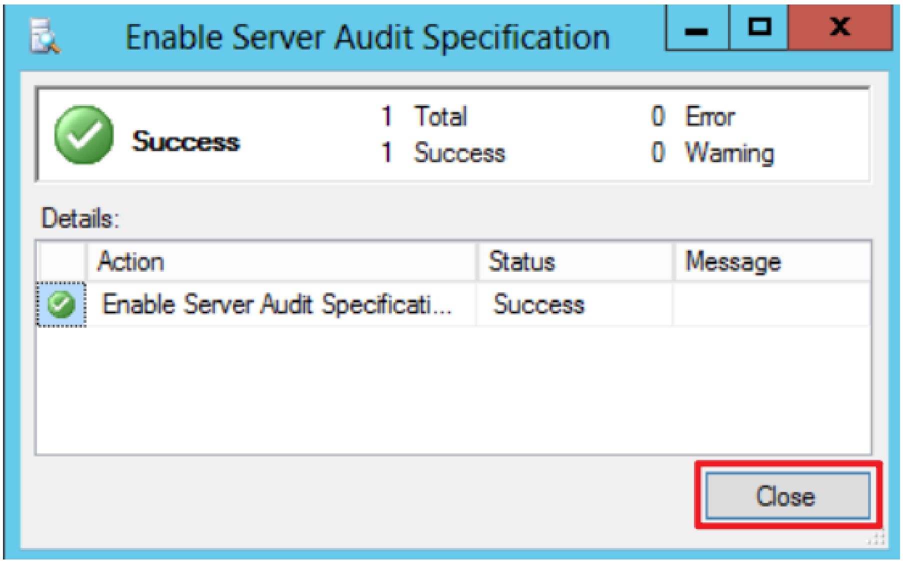
Actions:

	Audit Action Type	Object Class	Object	Object Name	P
01	SUCCESSFUL_LOGIN_GROUP				
02	FAILED_LOGIN_GROUP				
03	LOGOUT_GROUP				
04	SERVER_STATE_CHANGE_GROUP				
05	SERVER_OPERATION_GROUP				
06	SCHEMA_OBJECT_CHANGE_GROUP				
07	DATABASE_OWNERSHIP_CHANGE_GROUP				
08	DATABASE_CHANGE_GROUP				
09	AUDIT_CHANGE_GROUP				
10	USER_CHANGE_PASSWORD_GROUP				
*11					

(9) In the server audit specification list, right-click “NP_Server_Audit” → select “Enable Server Audit Specification.”



(10) Click “Close.”



Enable Server Audit Specification

Success	1	Total	0	Error
	1	Success	0	Warning

Details:

	Action	Status	Message
✓	Enable Server Audit Specificati...	Success	

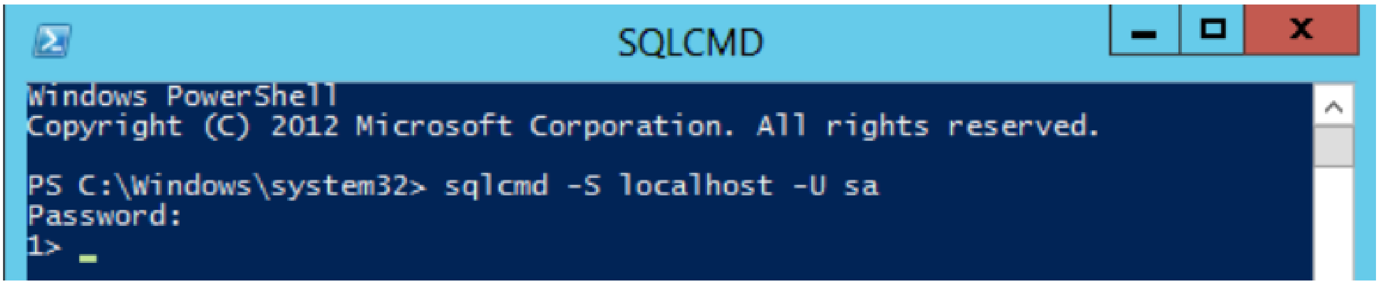
3.2.1.2 Configuring via Graphical User Interface (GUI)

(1) Open “Windows PowerShell.”

(2) Enter the command below to log in using either sa:

<2.1>Using sa account:

```
PS C:\> sqlcmd -S localhost -U sa
```



```
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> sqlcmd -S localhost -U sa
Password:
1> _
```

Options:

-S [protocol:]server[instance_name][,port]

-U login_id

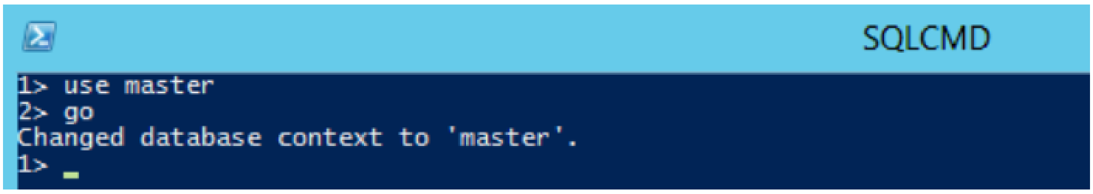
-P password

-A dedicated administrator connection

<2.2> Using Windows account:

Enter the command below to log in using Windows:

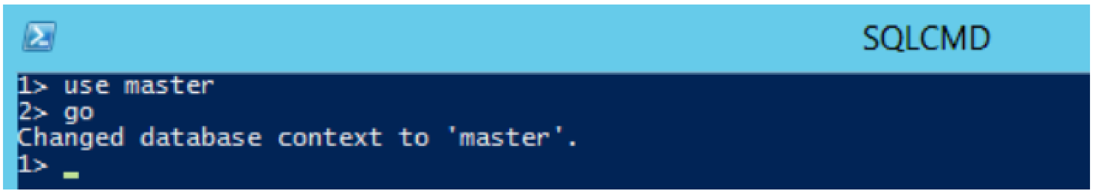
```
PS C:\> sqlcmd -S localhost -A
```



```
1> use master
2> go
Changed database context to 'master'.
1> _
```

(3) Enter the command below to switch to the **master** database:

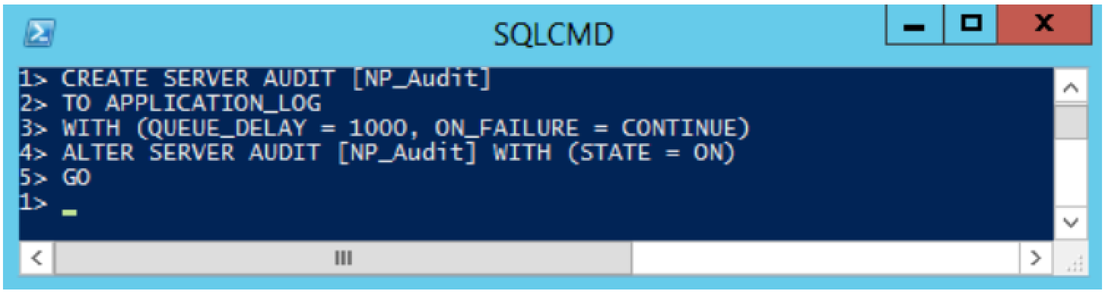
```
1 > use master
2 > go
```



```
1> use master
2> go
Changed database context to 'master'.
1> _
```

(4) Enter the audit name: NP_Audit → select audit destination: Application Log (this stores MS SQL audit logs in the Windows Event Viewer Application Log) → click "OK."

```
1 > CREATE SERVER AUDIT [ NP_Audit ]
2 > TO APPLICATION_LOG
3 > WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4 > ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5 > GO
```

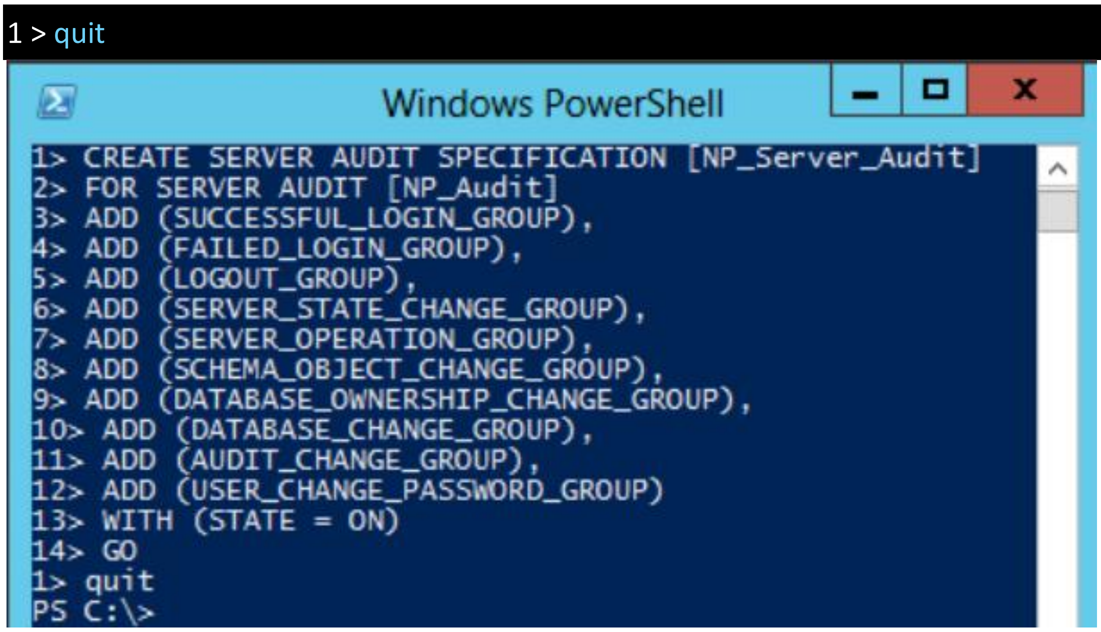


```
1> CREATE SERVER AUDIT [NP_Audit]
2> TO APPLICATION_LOG
3> WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4> ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5> GO
1> _
```

(5) Enter the command below to configure the server audit and add actions. For detailed information, refer to the SQL Server Audit Action Groups and Actions in the references.

```
1 > CREATE SERVER AUDIT SPECIFICATION [ NP_Server_Audit ]
2 > FOR SERVER AUDIT [NP_Audit]
3 > ADD (SUCCESSFUL_LOGIN_GROUP),
4 > ADD (FAILED_LOGIN_GROUP),
5 > ADD (LOGOUT_GROUP),
6 > ADD (SERVER_STATE_CHANGE_GROUP),
7 > ADD (SERVER_OPERATION_GROUP),
8 > ADD (SCHEMA_OBJECT_CHANGE_GROUP),
9 > ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
10 > ADD (DATABASE_CHANGE_GROUP),
11 > ADD (AUDIT_CHANGE_GROUP)
12 > ADD (USER_CHANGE_PASSWORD_GROUP)
13 >WITH (STATE = ON)
14> GO
```

```
1 > quit
```



```
1> CREATE SERVER AUDIT SPECIFICATION [NP_Server_Audit]
2> FOR SERVER AUDIT [NP_Audit]
3> ADD (SUCCESSFUL_LOGIN_GROUP),
4> ADD (FAILED_LOGIN_GROUP),
5> ADD (LOGOUT_GROUP),
6> ADD (SERVER_STATE_CHANGE_GROUP),
7> ADD (SERVER_OPERATION_GROUP),
8> ADD (SCHEMA_OBJECT_CHANGE_GROUP),
9> ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
10> ADD (DATABASE_CHANGE_GROUP),
11> ADD (AUDIT_CHANGE_GROUP),
12> ADD (USER_CHANGE_PASSWORD_GROUP)
13> WITH (STATE = ON)
14> GO
1> quit
PS C:\>
```

Replace the text shown in red with the server audit specification name.

3.2.2 Database-Level Audit

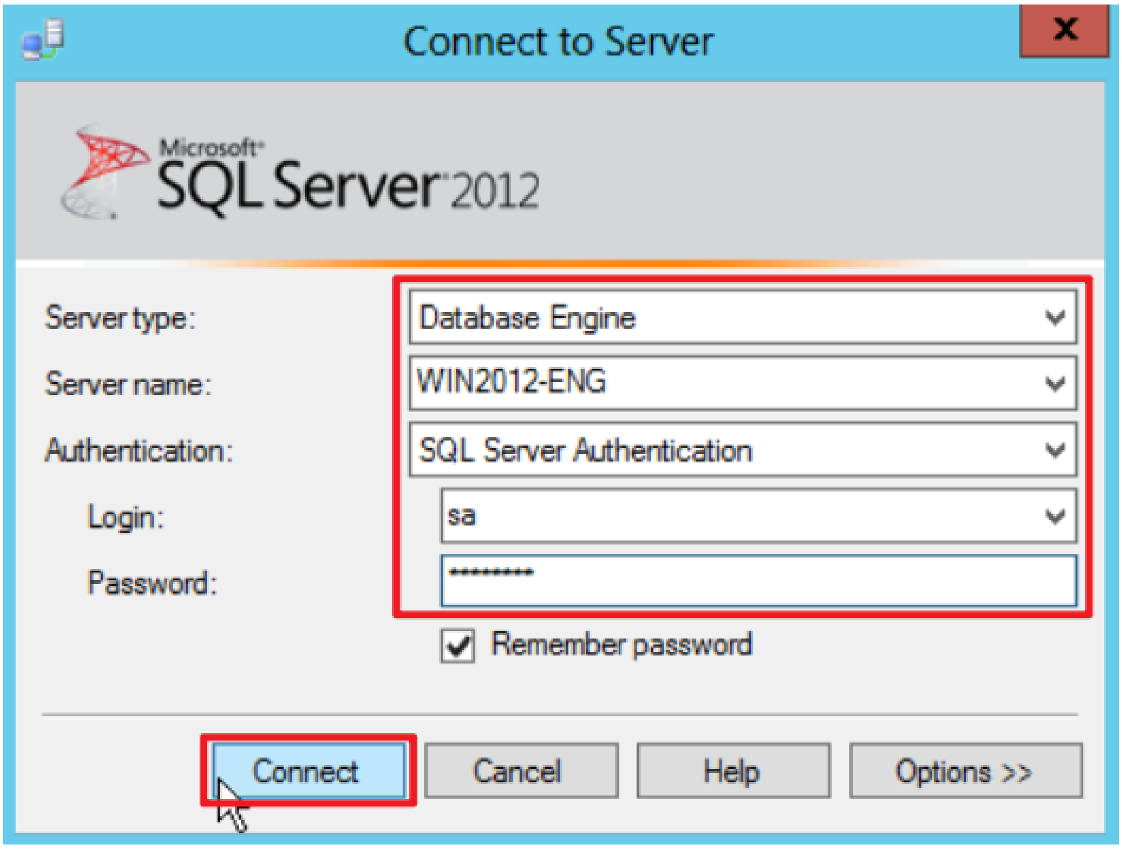
Enabling a database-level audit covers operations involving Data Manipulation Language (DML) and Data Definition Language (DDL) statements.

The following sections describe how to configure a database-level audit using the graphical user interface (GUI) and the command-line interface (CLI).

3.2.2.1 Configuring via Graphical User Interface (GUI)

(1) Open "SQL Server Management Studio (SSMS)."

(2) Enter the server's name → select the authentication method → click "Connect."



Server type: Database Engine

Server name: WIN2012-ENG

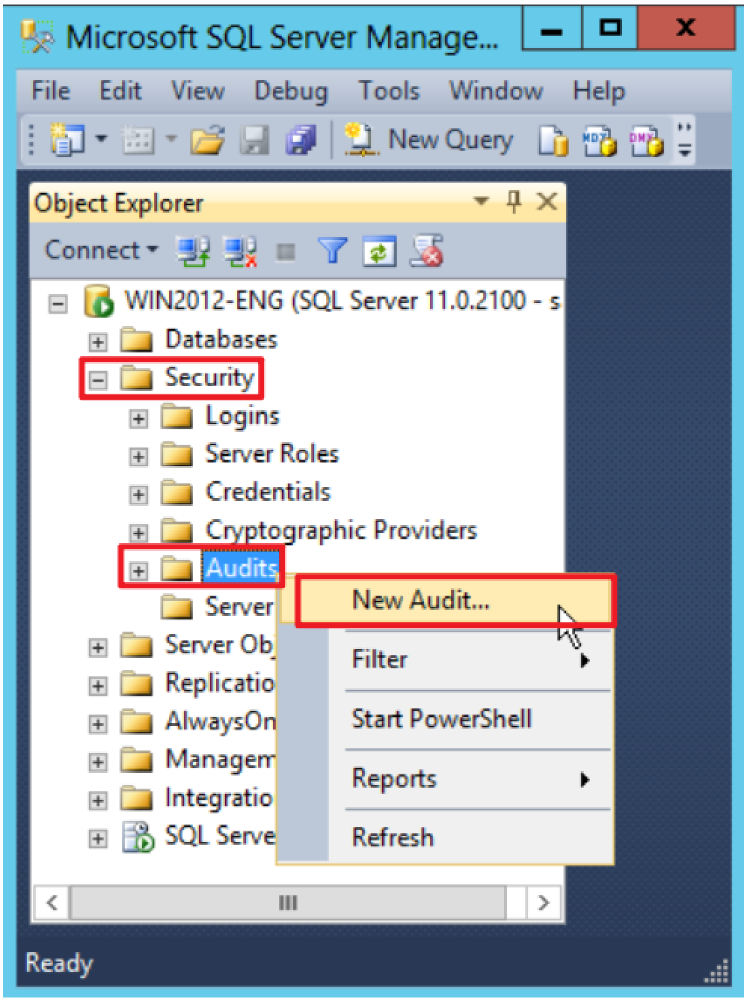
Authentication: SQL Server Authentication

Login: sa

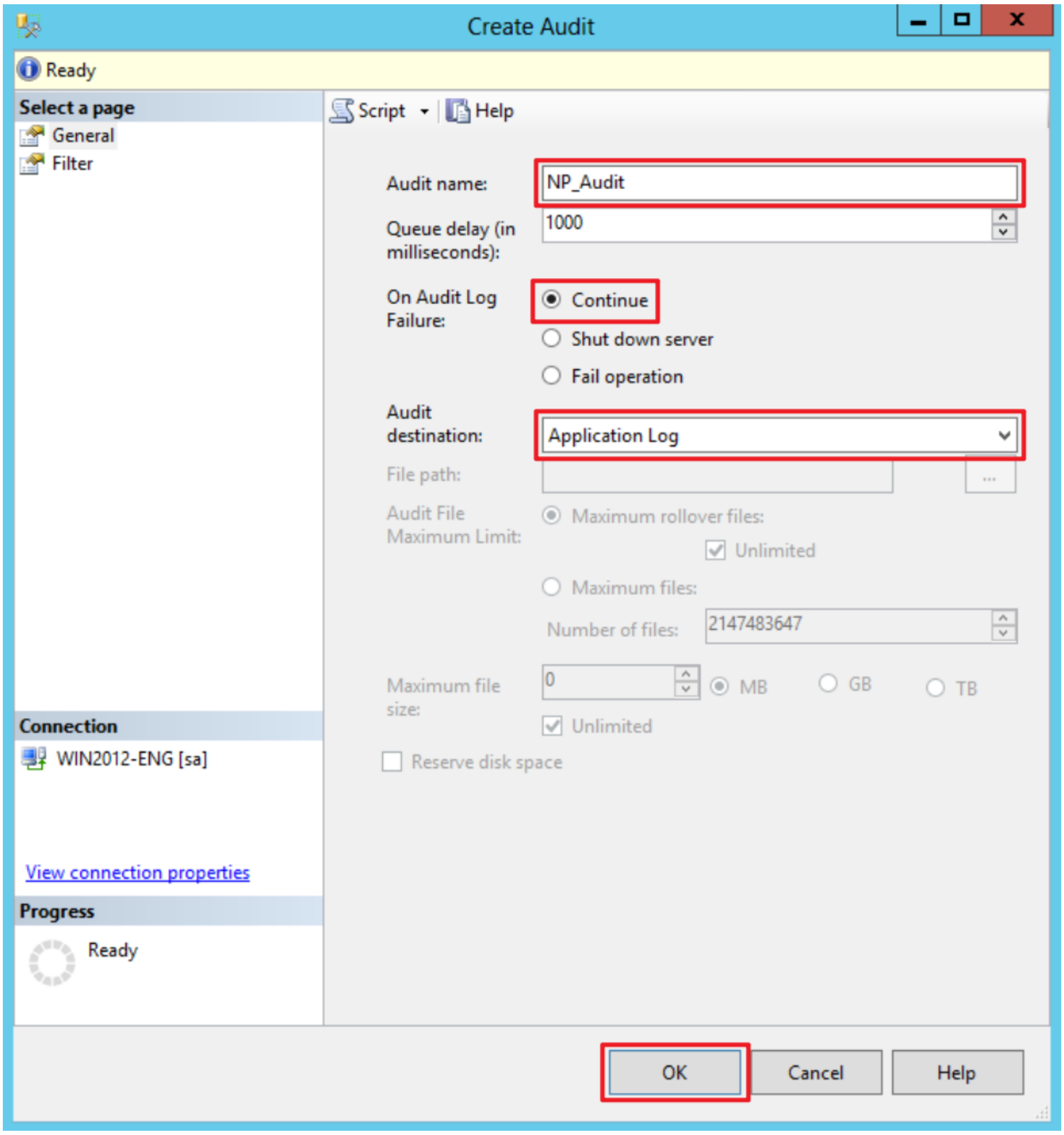
Password: *********

☑ Remember password

(3) Expand “Security” → right-click “Audits” → select “New Audit...”



(4) Enter the audit name: (the example here is NP_Audit) → select “On audit log failure”: “Continue” → select audit destination: Application Log (this stores MS SQL audit logs in the Windows Event Viewer Application Log) → click “OK.”



Connection: WIN2012-ENG [sa]

Audit name: NP_Audit

Queue delay (in milliseconds): 1000

On Audit Log Failure:
● Continue
○ Shut down server
○ Fail operation

Audit destination: Application Log

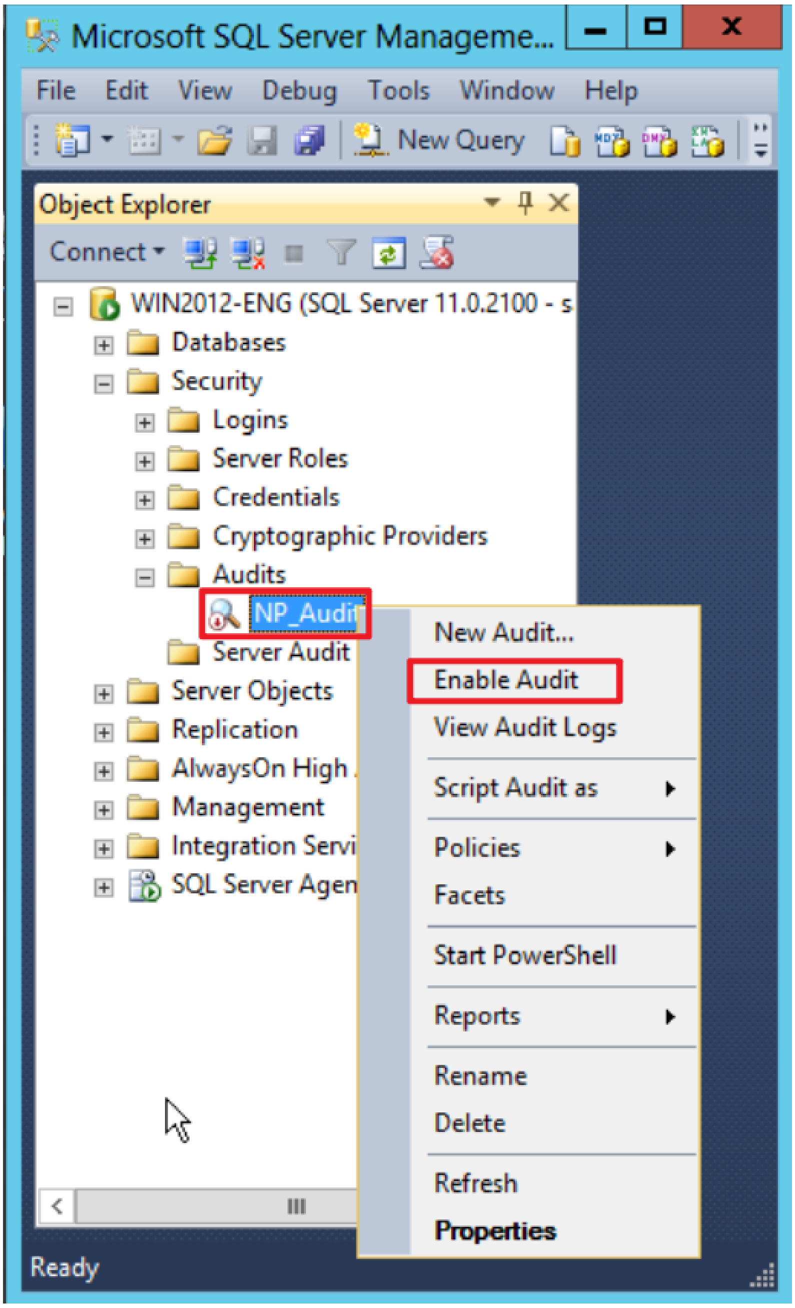
File path:

Audit File Maximum Limit:
● Maximum rollover files:
☑ Unlimited
○ Maximum files:
Number of files: 2147483647

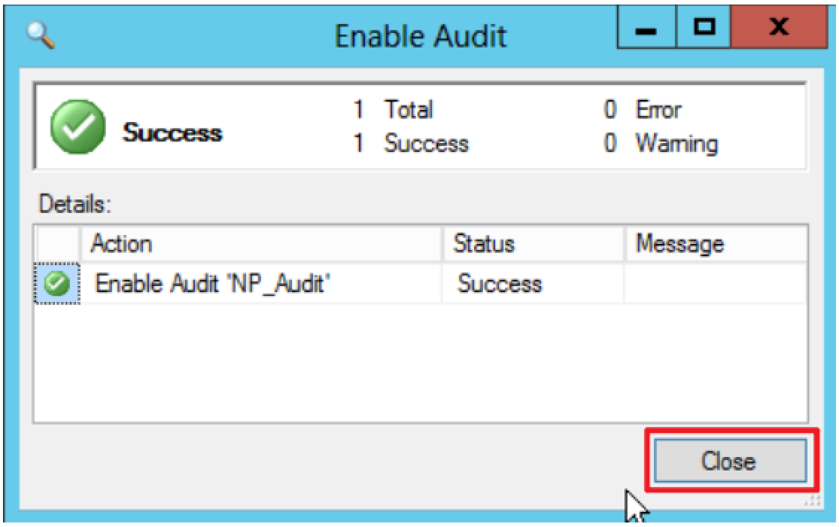
Maximum file size: 0 ● MB ○ GB ○ TB
☑ Unlimited

□ Reserve disk space

(5) In the audit list, right-click "NP_Audit" → select "Enable Audit."



(6) Click "Close."



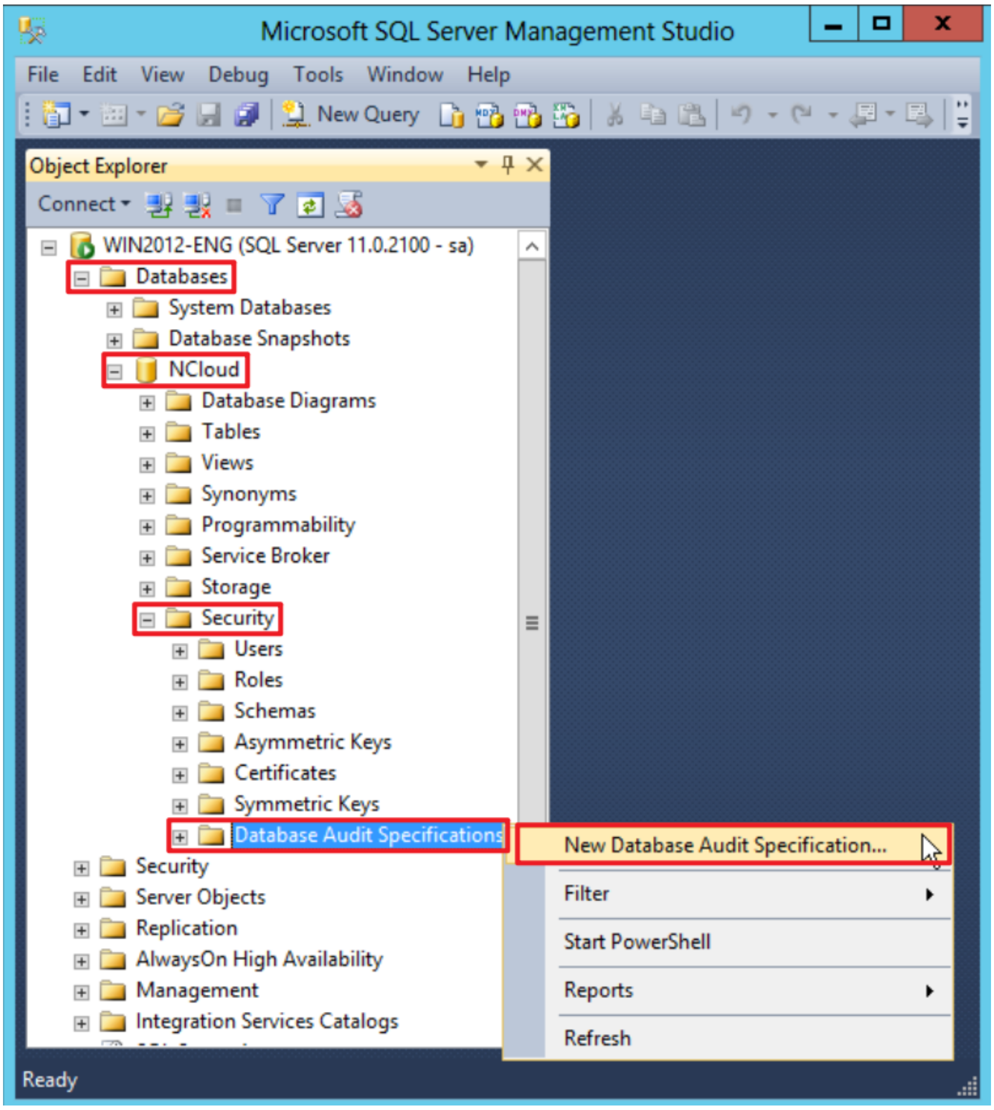
Success

1	Total	0	Error
1	Success	0	Warning

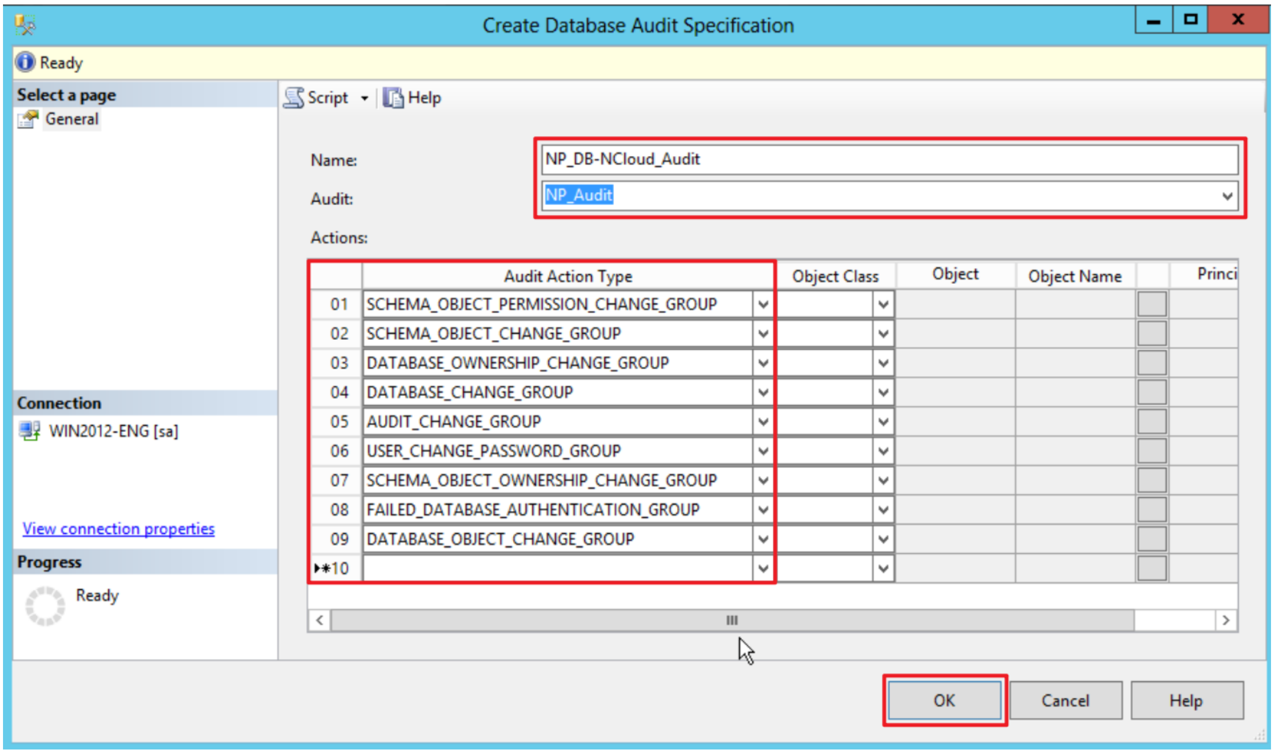
Details:

Action	Status	Message
Enable Audit 'NP_Audit'	Success	

(7) In “Databases,” select the target database (the example here is : NCloud) → expand “Security” → right-click “Database Audit Specifications” → select "New Database Audit Specification...”



(8) Enter the specification name: (the example here is NP_DB-NCloud_Audit) → select audit: NP_Audit and action(s) → select action(s) (refer to the **SQL Server Audit Action Groups and Actions** in the references for details) → click "OK."



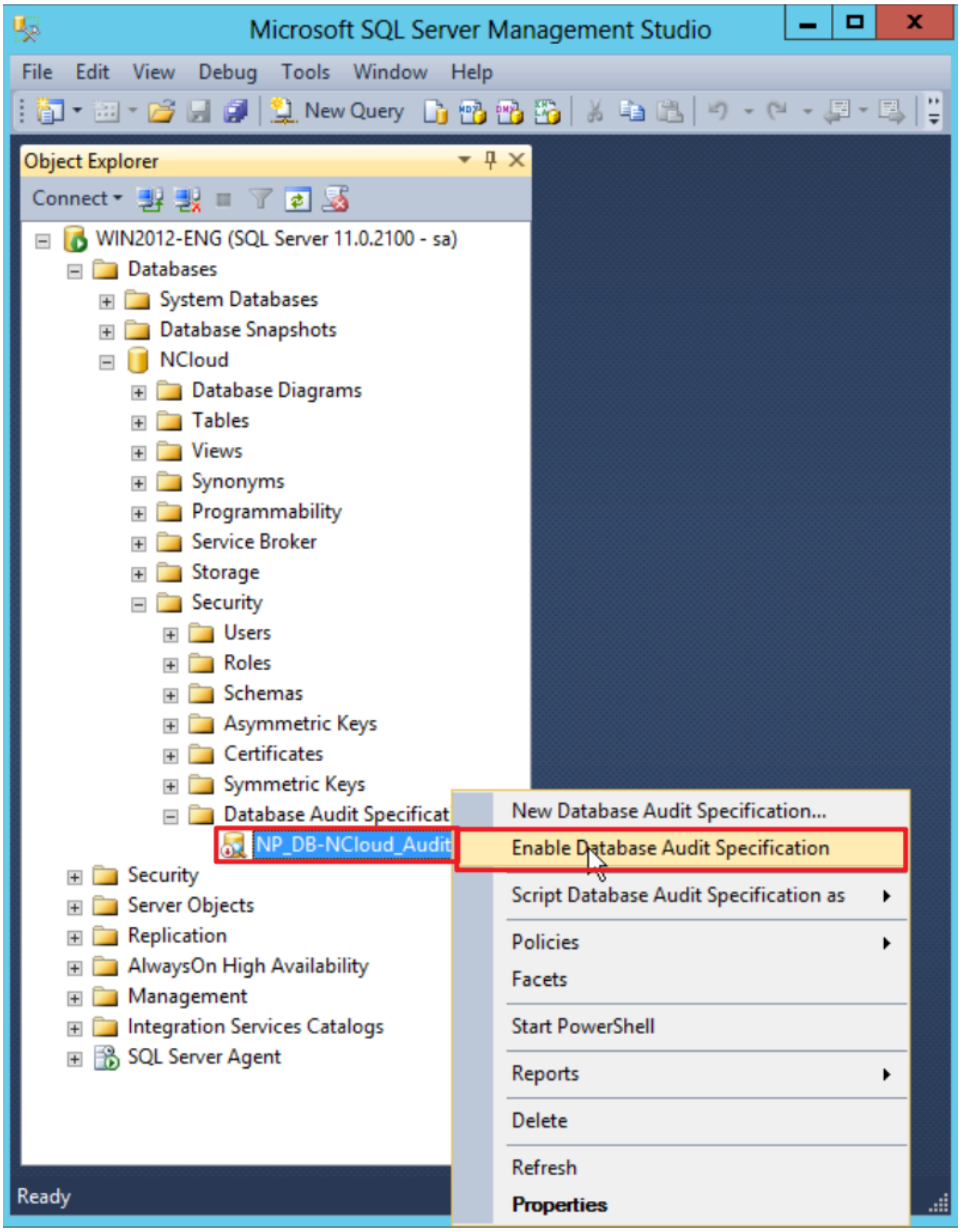
Name: NP_DB-NCloud_Audit

Audit: NP_Audit

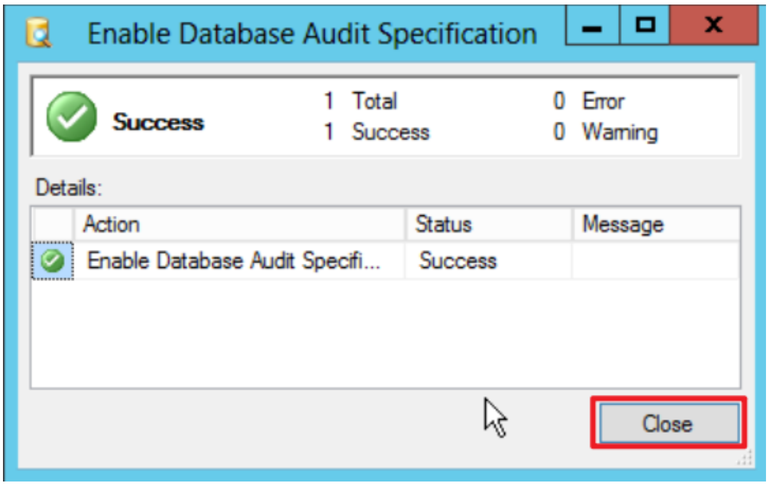
Actions:

	Audit Action Type	Object Class	Object	Object Name	Princi
01	SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP				
02	SCHEMA_OBJECT_CHANGE_GROUP				
03	DATABASE_OWNERSHIP_CHANGE_GROUP				
04	DATABASE_CHANGE_GROUP				
05	AUDIT_CHANGE_GROUP				
06	USER_CHANGE_PASSWORD_GROUP				
07	SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP				
08	FAILED_DATABASE_AUTHENTICATION_GROUP				
09	DATABASE_OBJECT_CHANGE_GROUP				
*10					

(9) In the database audit specification list, right-click "NP_DB-NCloud_Audit" → select "Enable Server Audit Specification."



(10) Click "Close."



Success

1 Total	0 Error
1 Success	0 Warning

Details:

Action	Status	Message
Enable Database Audit Specifi...	Success	

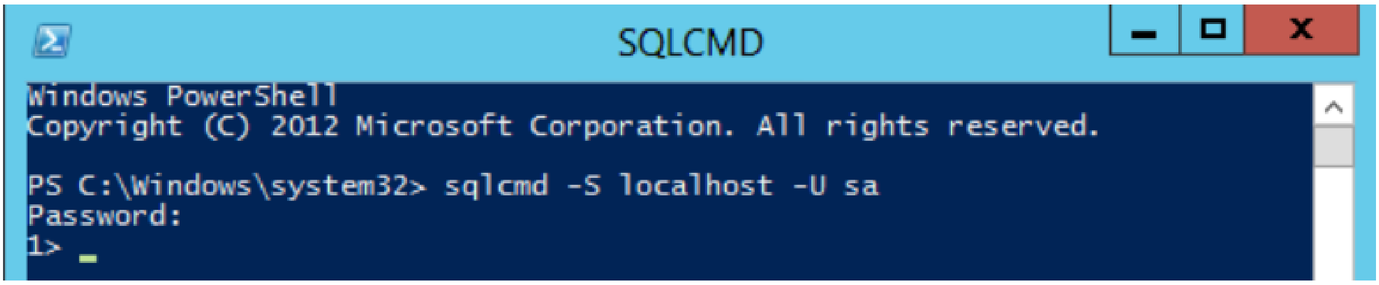
3.2.2.2 Configuring via Graphical User Interface (GUI)

(1) Open "Windows PowerShell."

(2) Enter the command below to log in using either sa:

<2.1>Using sa account:

```
PS C:\> sqlcmd -S localhost -U sa
```



```
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> sqlcmd -S localhost -U sa
Password:
1> _
```

Options:

-S [protocol:]server[instance_name][,port]

-U login_id

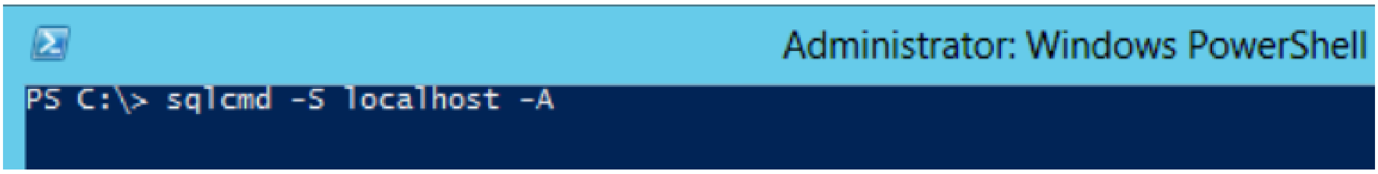
-P password

-A dedicated administrator connection

<2.2> Using Windows account:

Enter the command below to log in using Windows account:

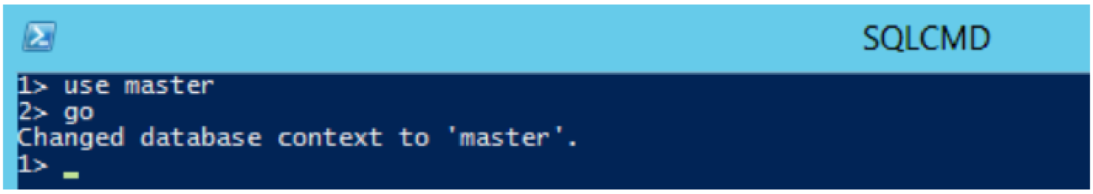
```
PS C:\> sqlcmd -S localhost -A
```



```
PS C:\> sqlcmd -S localhost -A
```

(3) Enter the command below to switch to the **master** database:

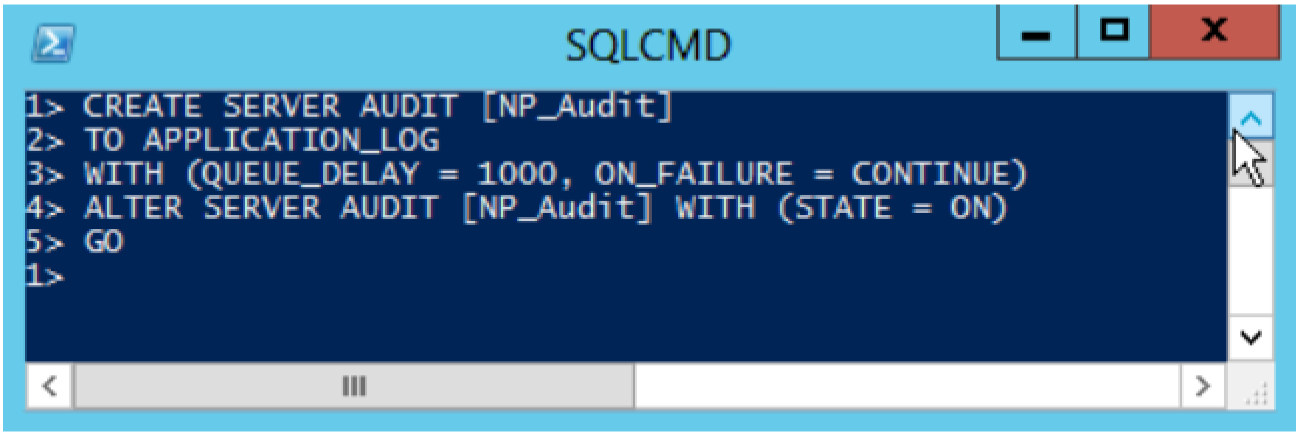
```
1 > use master
2 > go
```



```
1> use master
2> go
Changed database context to 'master'.
1> _
```

(4) Enter the audit name: NP_Audit → select audit destination: Application Log (this stores MS SQL audit logs in the Windows Event Viewer Application Log) → click “OK.”

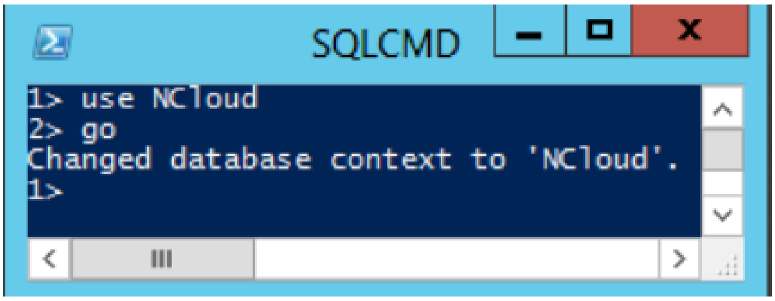
```
1 > CREATE SERVER AUDIT [ NP_Audit ]
2 > TO APPLICATION_LOG
3 > WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4 > ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5 > GO
```



```
1> CREATE SERVER AUDIT [NP_Audit]
2> TO APPLICATION_LOG
3> WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4> ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5> GO
1>
```

(5) Enter the command below to switch to the target audit database (the example here is: NCloud).

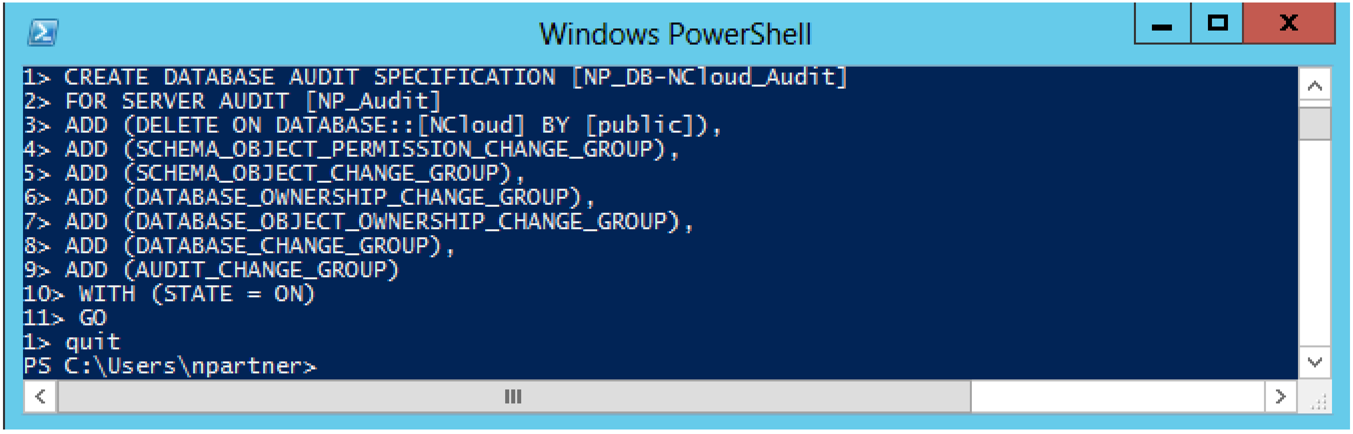
```
1 > use NCloud
2 > go
```



```
1> use NCloud
2> go
Changed database context to 'NCloud'.
1>
```

(6) Enter the command below to configure the audit for the database and add actions. For detailed information, refer to the **SQL Server Audit Action Groups and Actions** in the references.

```
1 > CREATE DATABASE AUDIT SPECIFICATION [ NP_DB-NCloud_Audit ]
2 > FOR SERVER AUDIT [NP_Audit]
3 > ADD (DELETE ON DATABASE::[ NCloud ] BY [public]),
4 > ADD (SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP),
5 > ADD (SCHEMA_OBJECT_CHANGE_GROUP),
6 > ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
7 > ADD (DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP),
8 > ADD (DATABASE_CHANGE_GROUP),
9 > ADD (AUDIT_CHANGE_GROUP)
10 > WITH (STATE = ON)
11 > GO
1 > quit
```



```
1> CREATE DATABASE AUDIT SPECIFICATION [NP_DB-NCloud_Audit]
2> FOR SERVER AUDIT [NP_Audit]
3> ADD (DELETE ON DATABASE::[NCloud] BY [public]),
4> ADD (SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP),
5> ADD (SCHEMA_OBJECT_CHANGE_GROUP),
6> ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
7> ADD (DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP),
8> ADD (DATABASE_CHANGE_GROUP),
9> ADD (AUDIT_CHANGE_GROUP)
10> WITH (STATE = ON)
11> GO
1> quit
PS C:\Users\npartner>
```

Replace the text shown in red with the database audit specification name.

```
1 > CREATE DATABASE AUDIT SPECIFICATION [NP_DB-NCloud_Audit]
```

Replace the text shown in red with the target database name.

```
3 > ADD (DELETE ON DATABASE::[NCloud] BY [public])
```

3.3 Event Log Configuration

This is an optional configuration.

The following sections describe configuration methods for Domain and Workgroup environments.

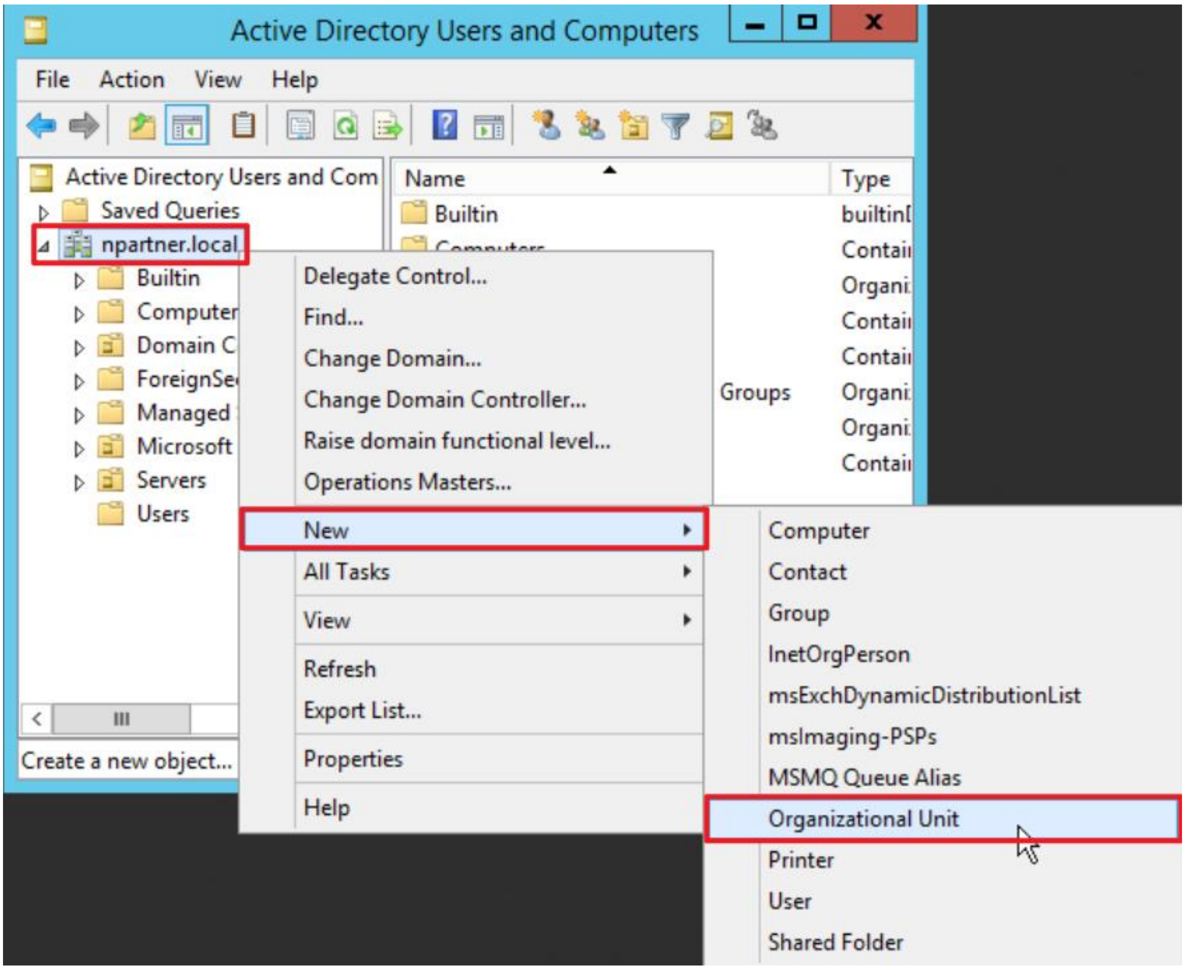
3.3.1 Domain

3.3.1.1 Organizational Unit (OU) Configuration

(1) Click “Active Directory Users and Computers.”

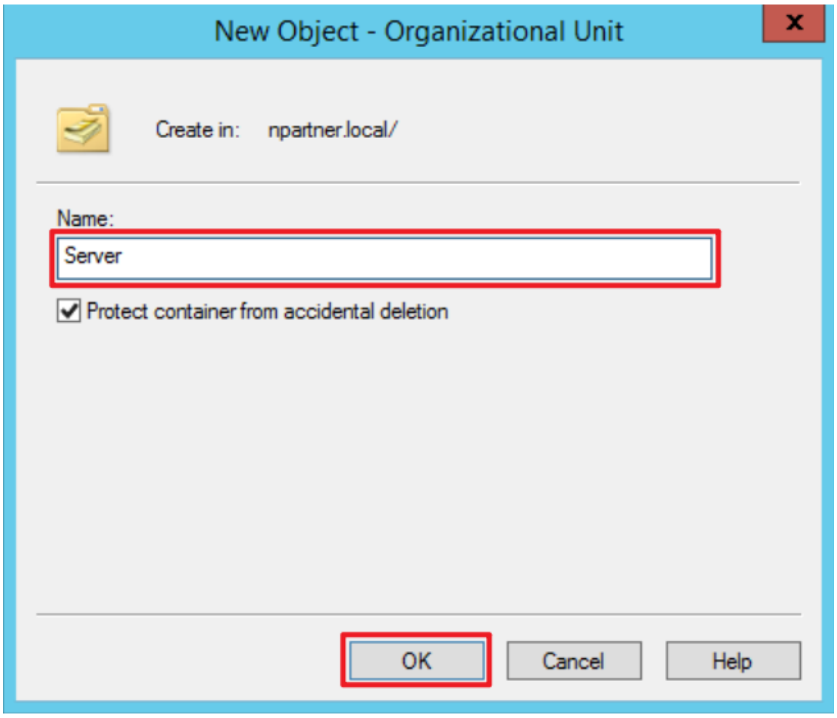
(2) Add an Organizational Unit

Right-click on “Domain Controllers, select “New,” and click “Organizational Unit.”



(3) Enter your Organizational Unit name: (in this example, it is "Servers")

Note: Please create the organizational unit name according to the customer's environment. → click "OK."

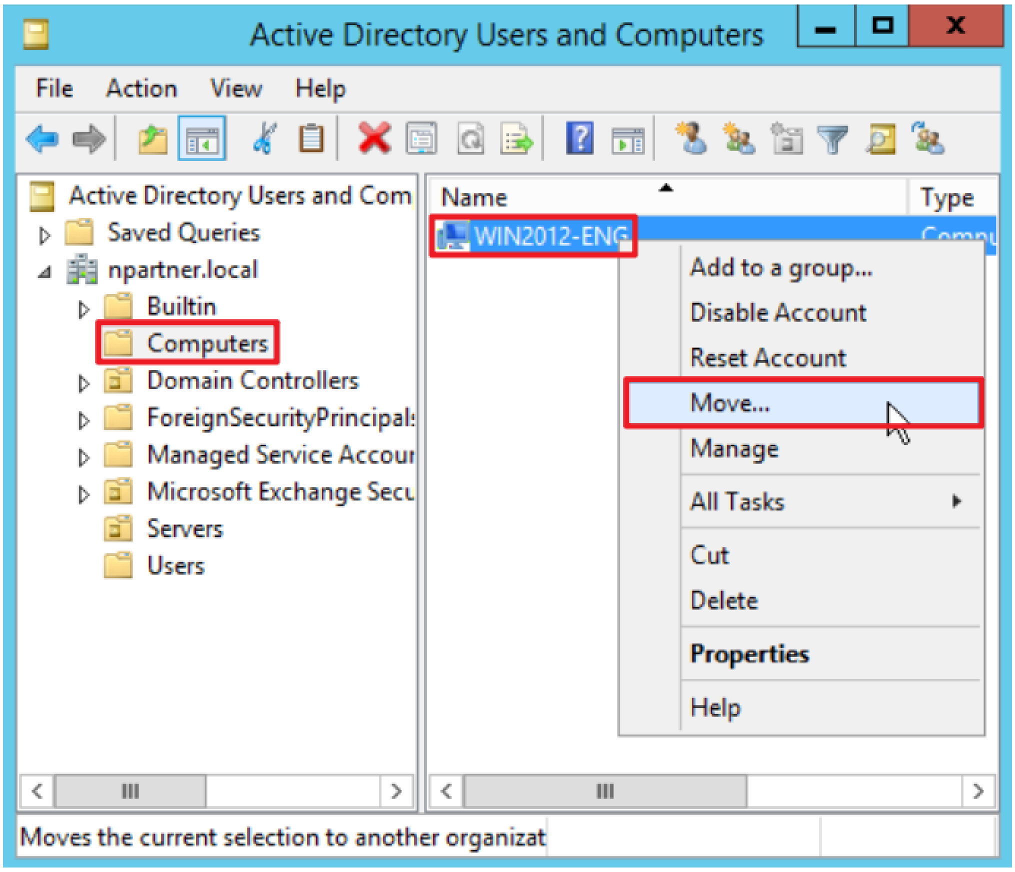


New Object - Organizational Unit
Create in: npartner.local/
Name:
Server
☑ Protect container from accidental deletion
OK
Cancel
Help

(4) Move the Server to your New Organizational Unit:

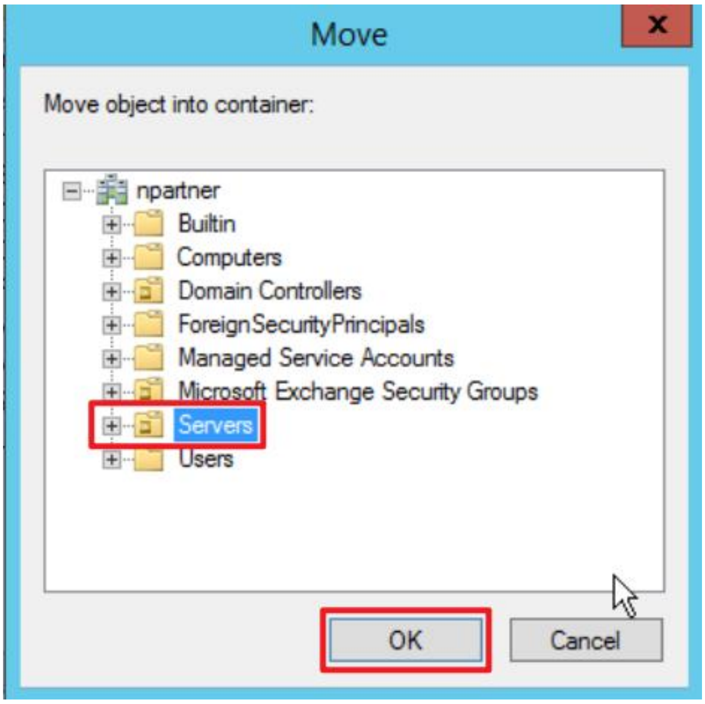
Select your organizational unit in "Domain Controllers" -> Right-click on the "WIN2012" server.

Note: Please select the MS SQL server according to the actual environment. → click "Move."



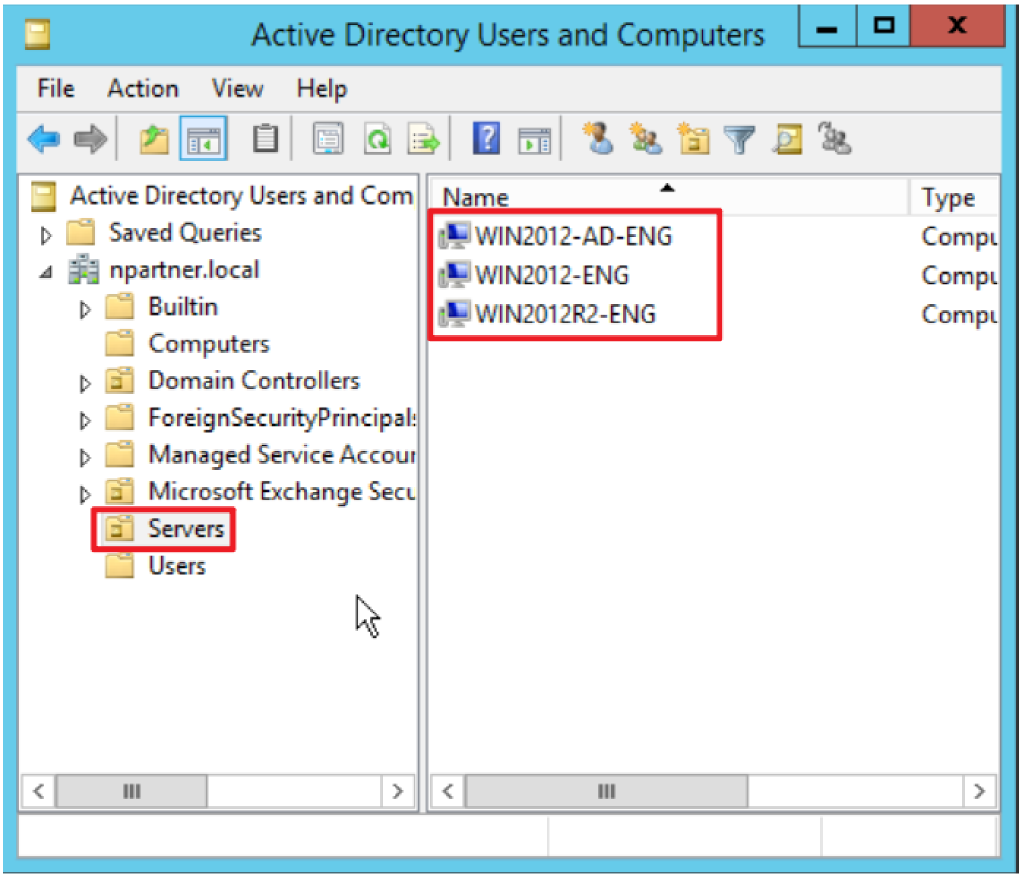
(5) Select your Organizational Unit:

Select your organizational unit (in this example, it is “Servers”) → Click “OK.”



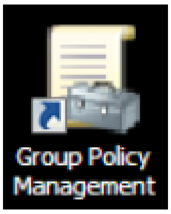
(6) Verify the Server Has Been Moved to your New Organizational Unit:

Expand your organizational unit folder (in this example, it is “Servers”) and confirm that the “WIN2012-ENG” server has been moved.



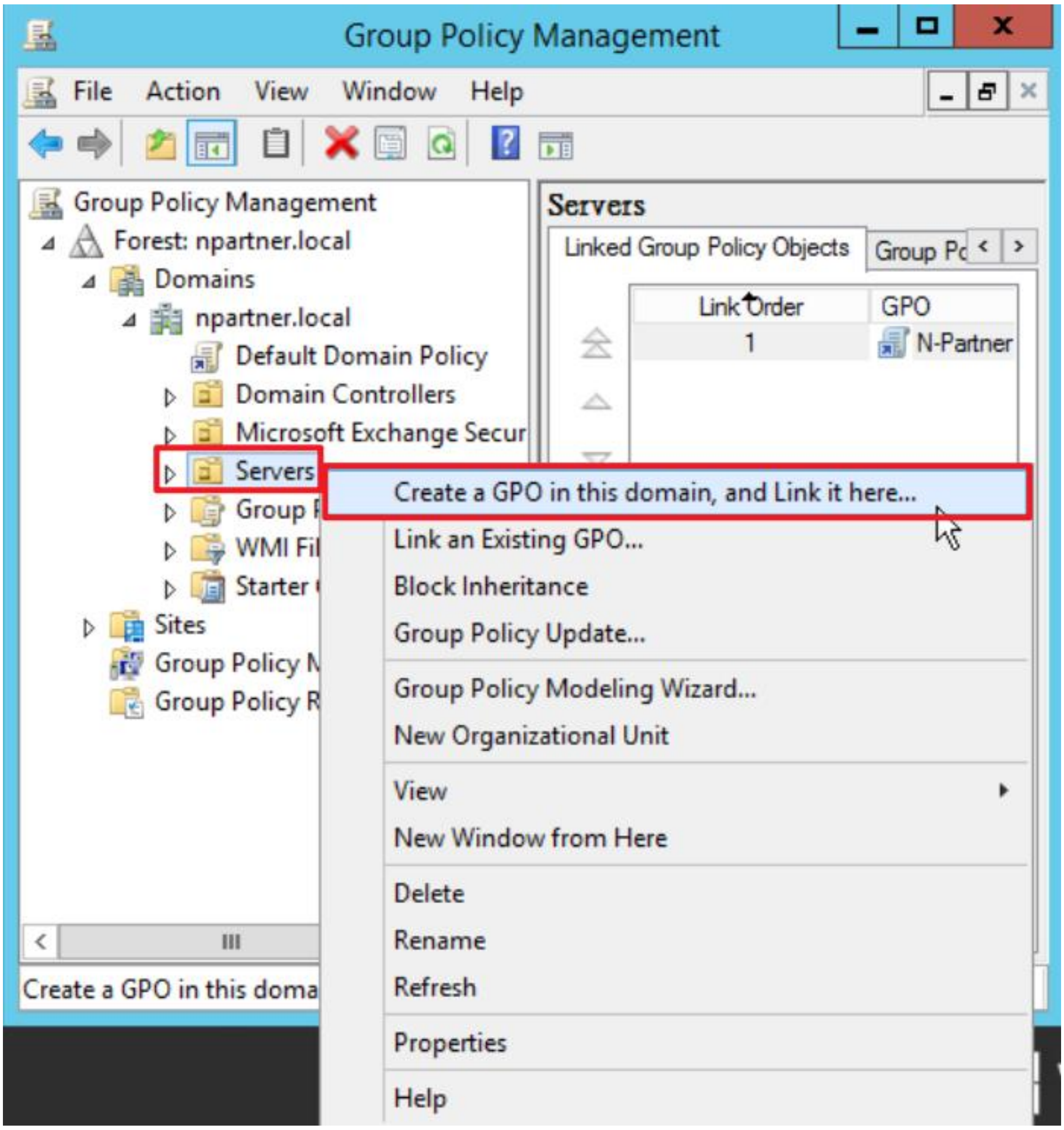
3.3.1.2 Group Policy Settings

(1) Click “Group Policy Management.”



(2) In the Servers organizational unit (OU), create a new Group Policy Object (GPO):

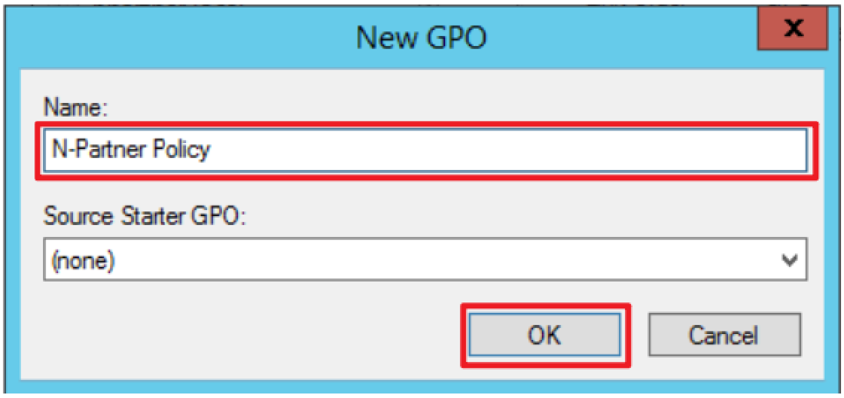
Right-click the [Servers] organizational unit → select “Create a GPO in this domain, and Link it here...”



(3) Edit your Group Policy Object

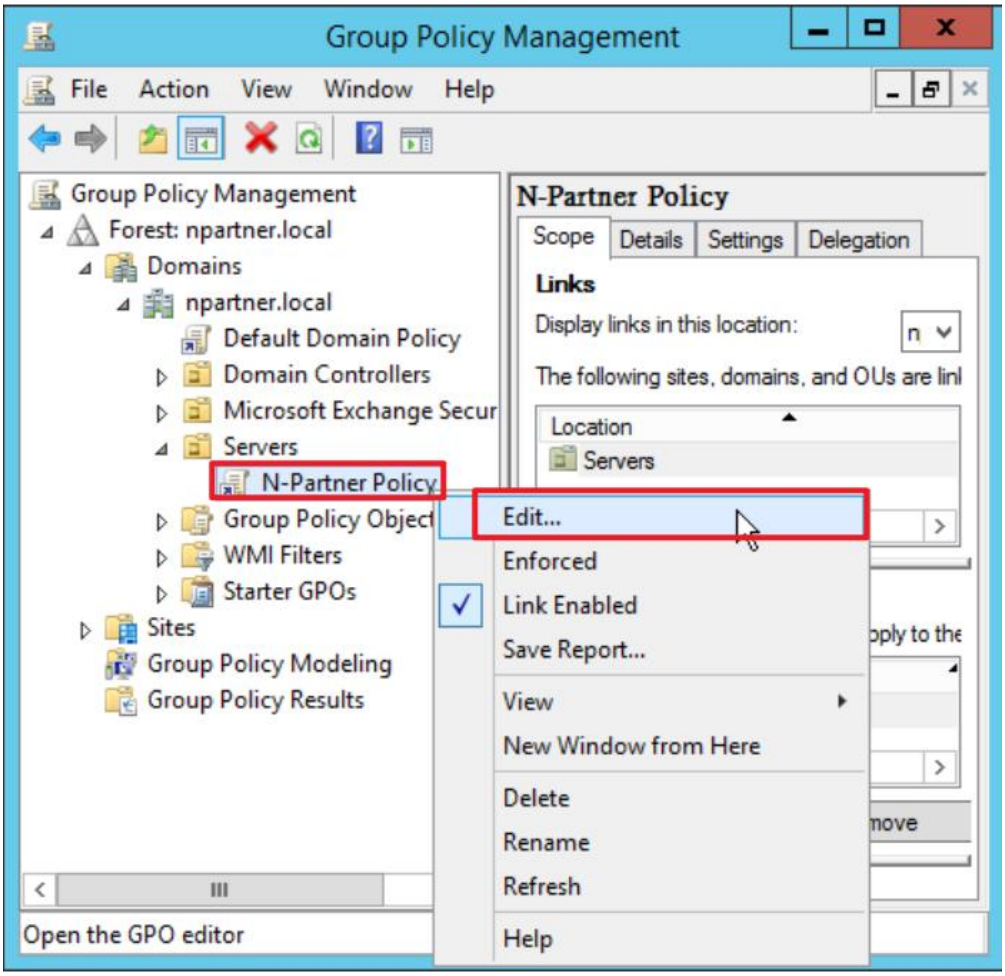
Enter your Group Policy Object name. (in this example, it is “N-Partner Policy”)

Note: Create your GPO name according to the actual environment. Then click “Edit.”



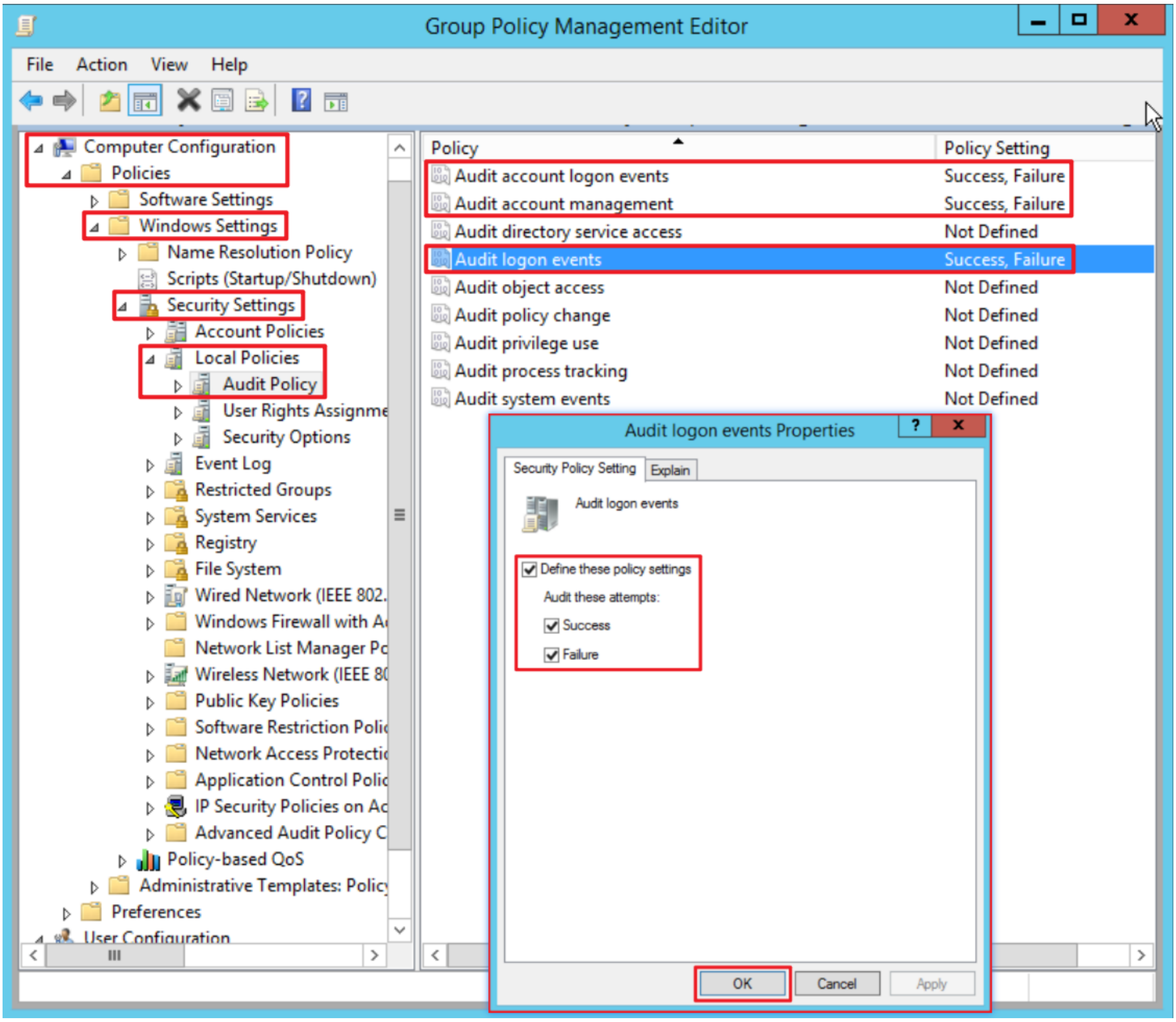
(4) Edit your Group Policy Object

In your group policy object, (in this example, it is “N-Partner Policy”) right-click and select “Edit.”



(5) Local Group Policies: Audit Policy

Expand folder “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Local Policies” → “Audit Policy.” And click on “Audit account logon events,” “Audit account management,” and “Audit logon events,” → check “Define these policy settings”: Success, Failure. → click “OK.”



Policy	Policy Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Not Defined
Audit logon events	Success, Failure
Audit object access	Not Defined
Audit policy change	Not Defined
Audit privilege use	Not Defined
Audit process tracking	Not Defined
Audit system events	Not Defined

Audit logon events Properties

Security Policy Setting | Explain

Audit logon events

☑ Define these policy settings

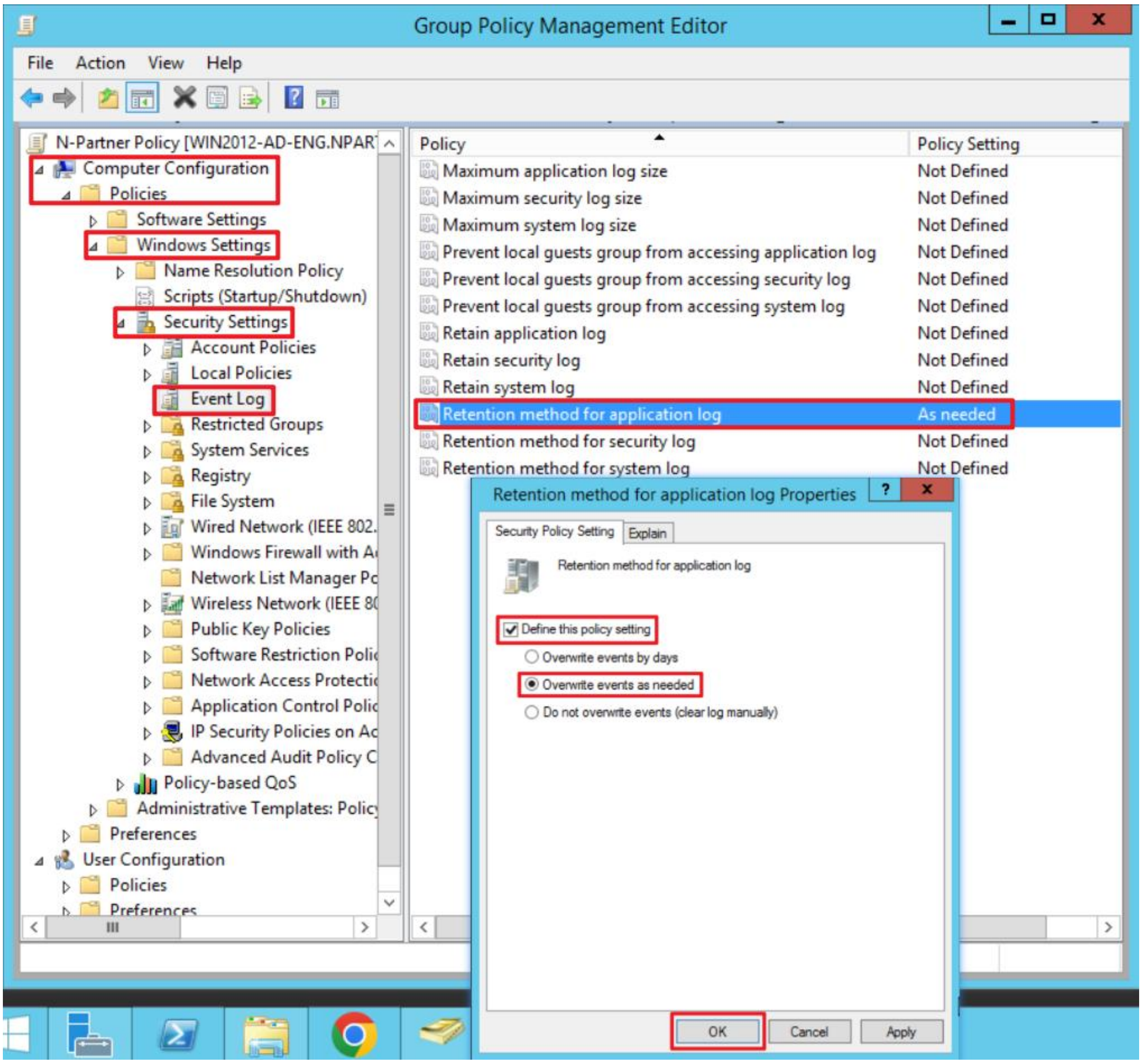
Audit these attempts:

☑ Success

☑ Failure

(6) Event Log: Application Log Retention Method

Expand “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” → select “Retention method for application log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



Policy	Policy Setting
Maximum application log size	Not Defined
Maximum security log size	Not Defined
Maximum system log size	Not Defined
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	As needed
Retention method for security log	Not Defined
Retention method for system log	Not Defined

Retention method for application log Properties

Security Policy Setting | Explain

Retention method for application log

☑ Define this policy setting

○ Overwrite events by days

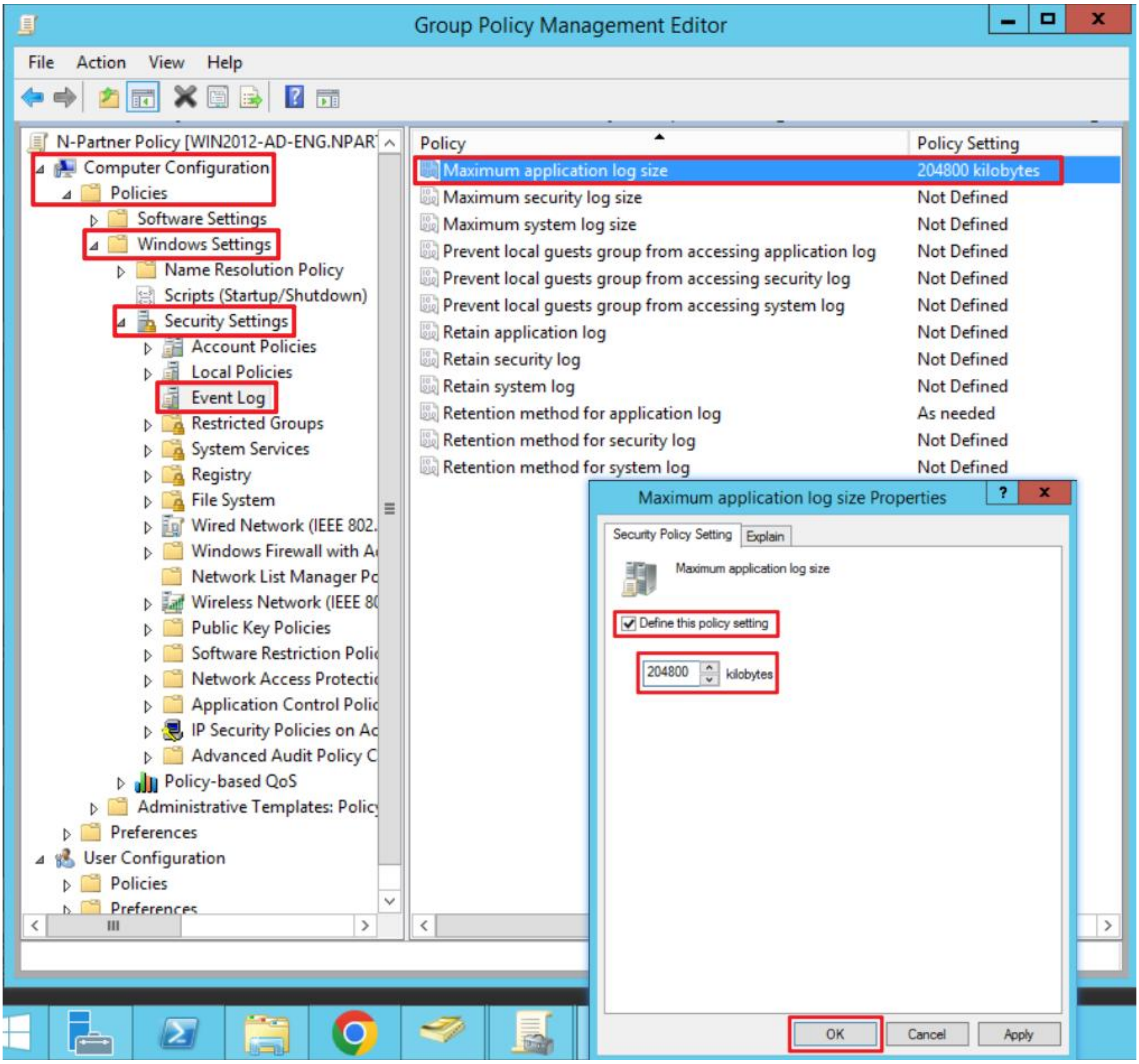
● Overwrite events as needed

○ Do not overwrite events (clear log manually)

(7) Event Logs: Maximum Size of Security Log

Expand folder “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” →And click on “Maximum application log size” → Check “Define this policy setting” → enter 204800 KB

Note: Please adjust the number based on the actual environment. → click “OK.”



- N-Partner Policy [WIN2012-AD-ENG.NPAR
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
        - Name Resolution Policy
        - Scripts (Startup/Shutdown)
        - Security Settings
          - Account Policies
          - Local Policies
          - Event Log
          - Restricted Groups
          - System Services
          - Registry
          - File System
          - Wired Network (IEEE 802.
          - Windows Firewall with A
          - Network List Manager Pc
          - Wireless Network (IEEE 8(
          - Public Key Policies
          - Software Restriction Polic
          - Network Access Protecti
          - Application Control Polic
          - IP Security Policies on Ac
          - Advanced Audit Policy C
        - Policy-based QoS
      - Administrative Templates: Policy
    - Preferences
  - User Configuration
    - Policies
    - Preferences

Policy	Policy Setting
Maximum application log size	204800 kilobytes
Maximum security log size	Not Defined
Maximum system log size	Not Defined
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	As needed
Retention method for security log	Not Defined
Retention method for system log	Not Defined

Maximum application log size Properties

Security Policy Setting | Explain

Maximum application log size

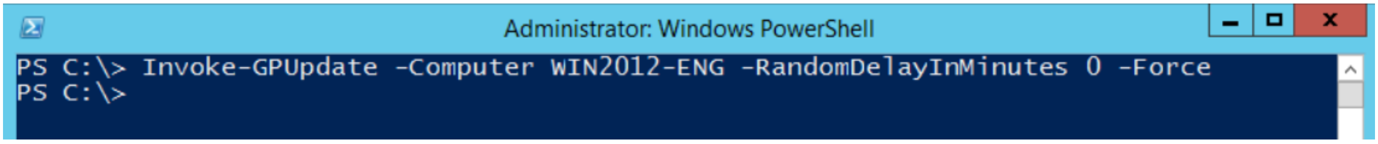
☑ Define this policy setting

204800 kilobytes

(8) On the AD domain server, open “Windows PowerShell.”

(8) Enter the command below to refresh group policy.

```
PS C:\> Invoke-GPUpdate -Computer WIN2012-ENG -RandomDelayInMinutes 0 -Force
```

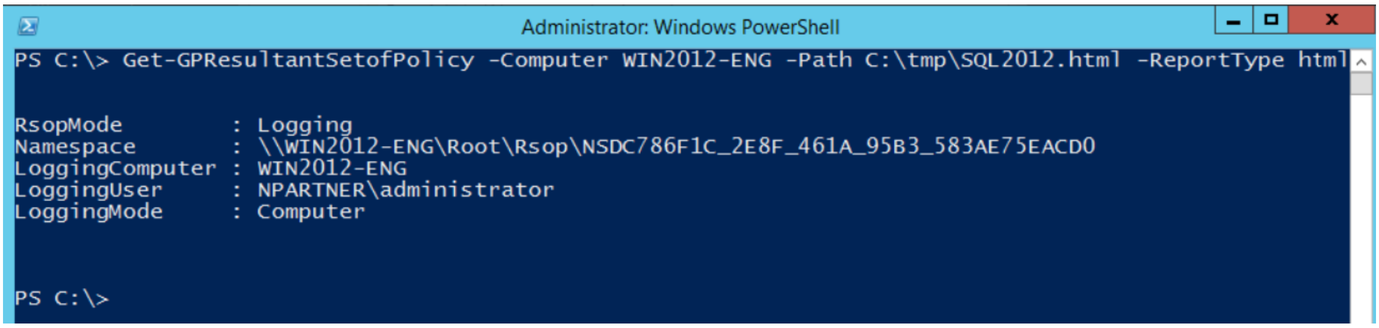


```
PS C:\> Invoke-GPUpdate -Computer WIN2012-ENG -RandomDelayInMinutes 0 -Force
PS C:\>
```

Replace the text shown in red with the MS SQL server name.

(9) Enter the command below to generate server group policy report.

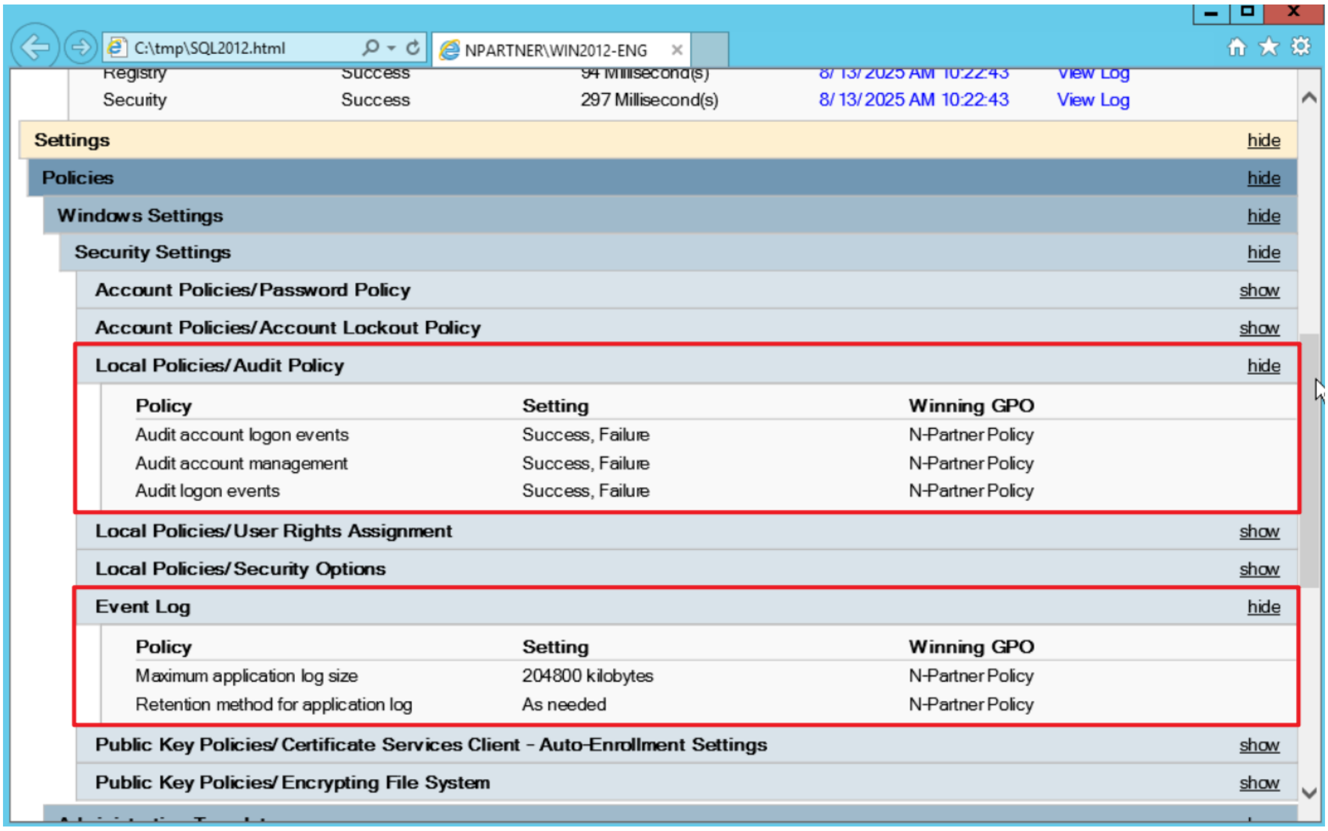
```
PS C:\> Get-GPResultantSetofPolicy -Computer WIN2012-ENG -Path C:\tmp\WIN2012.htnl -ReportType.html
```



```
PS C:\> Get-GPResultantSetofPolicy -Computer WIN2012-ENG -Path C:\tmp\SQL2012.html -ReportType html


RsopMode        : Logging
Namespace       : \\WIN2012-ENG\Root\Rsop\NSDC786F1C_2E8F_461A_95B3_583AE75EACD0
LoggingComputer : WIN2012-ENG
LoggingUser     : NPARTNER\administrator
LoggingMode     : Computer



PS C:\>
```

For the red text , please enter the MS SQL server name and the folder path/file name.

(11) Open the report and verify that your MS SQL server is applying the N-Partner Policy Group Policy.



Registry	Success	94 Millisecond(s)	8/13/2025 AM 10:22:43	View Log
Security	Success	297 Millisecond(s)	8/13/2025 AM 10:22:43	View Log

Settings hide

Policies hide

Windows Settings hide

Security Settings hide

Account Policies/Password Policy show

Account Policies/Account Lockout Policy show

Local Policies/Audit Policy hide

Policy	Setting	Winning GPO
Audit account logon events	Success, Failure	N-Partner Policy
Audit account management	Success, Failure	N-Partner Policy
Audit logon events	Success, Failure	N-Partner Policy

Local Policies/User Rights Assignment show

Local Policies/Security Options show

Event Log hide

Policy	Setting	Winning GPO
Maximum application log size	204800 kilobytes	N-Partner Policy
Retention method for application log	As needed	N-Partner Policy

Public Key Policies/Certificate Services Client - Auto-Enrollment Settings show

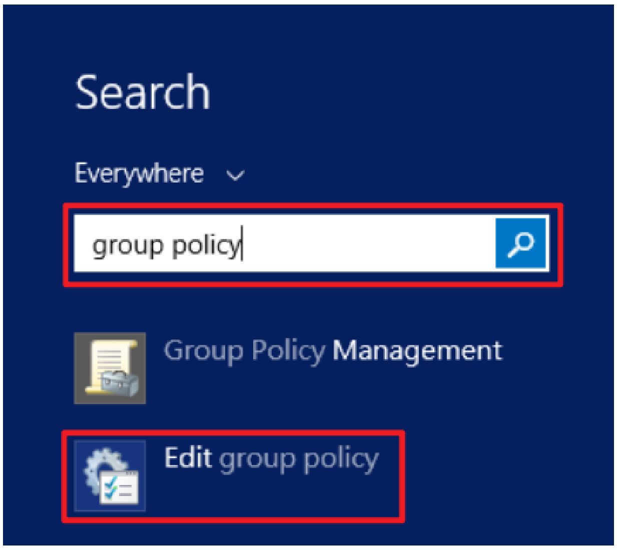
Public Key Policies/Encrypting File System show

3.3.2 Workgroup

3.3.2.1 Audit Policy Configuration

(1) Open Local Group Policy Editor

Click on “Start” → enter “group policy” to search → click on “Edit Group Policy.”



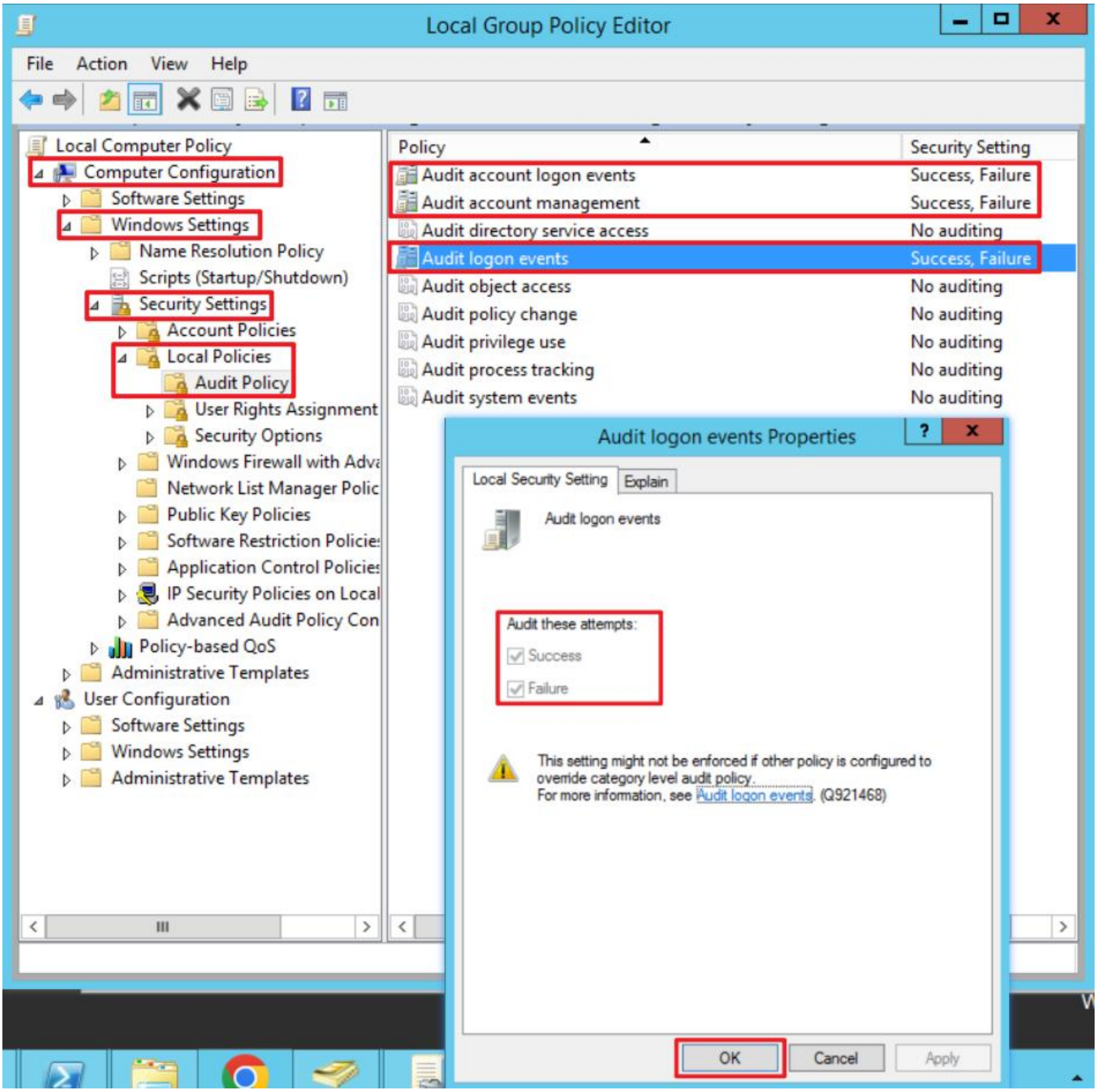
Search

Everywhere

group policy

(2) Local Group Policies: Audit Policy

Expand folder “Computer Configuration” → “Windows Settings” → “Security Settings” -> “Local Policies” → “Audit Policy.” And click on “Audit account logon events,” “Audit account management,” and “Audit logon events” items → check “Define these policy settings”: Success, Failure. → click “OK.”



Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	No auditing
Audit logon events	Success, Failure
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

Audit logon events Properties

Local Security Setting | Explain

Audit logon events

Audit these attempts:

☑ Success

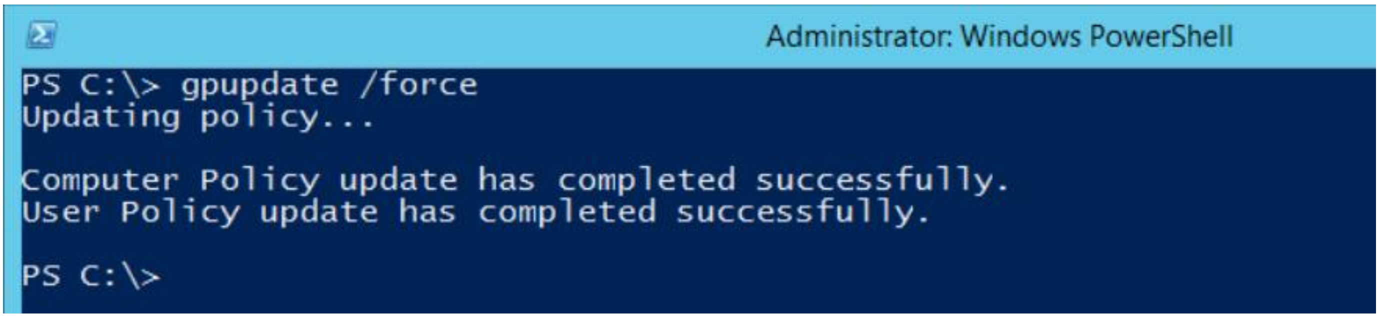
☑ Failure

This setting might not be enforced if other policy is configured to override category level audit policy.
For more information, see Audit logon events. (Q921468)

(3) Open “Windows PowerShell.”

(4) Enter the command below to refresh group policy.

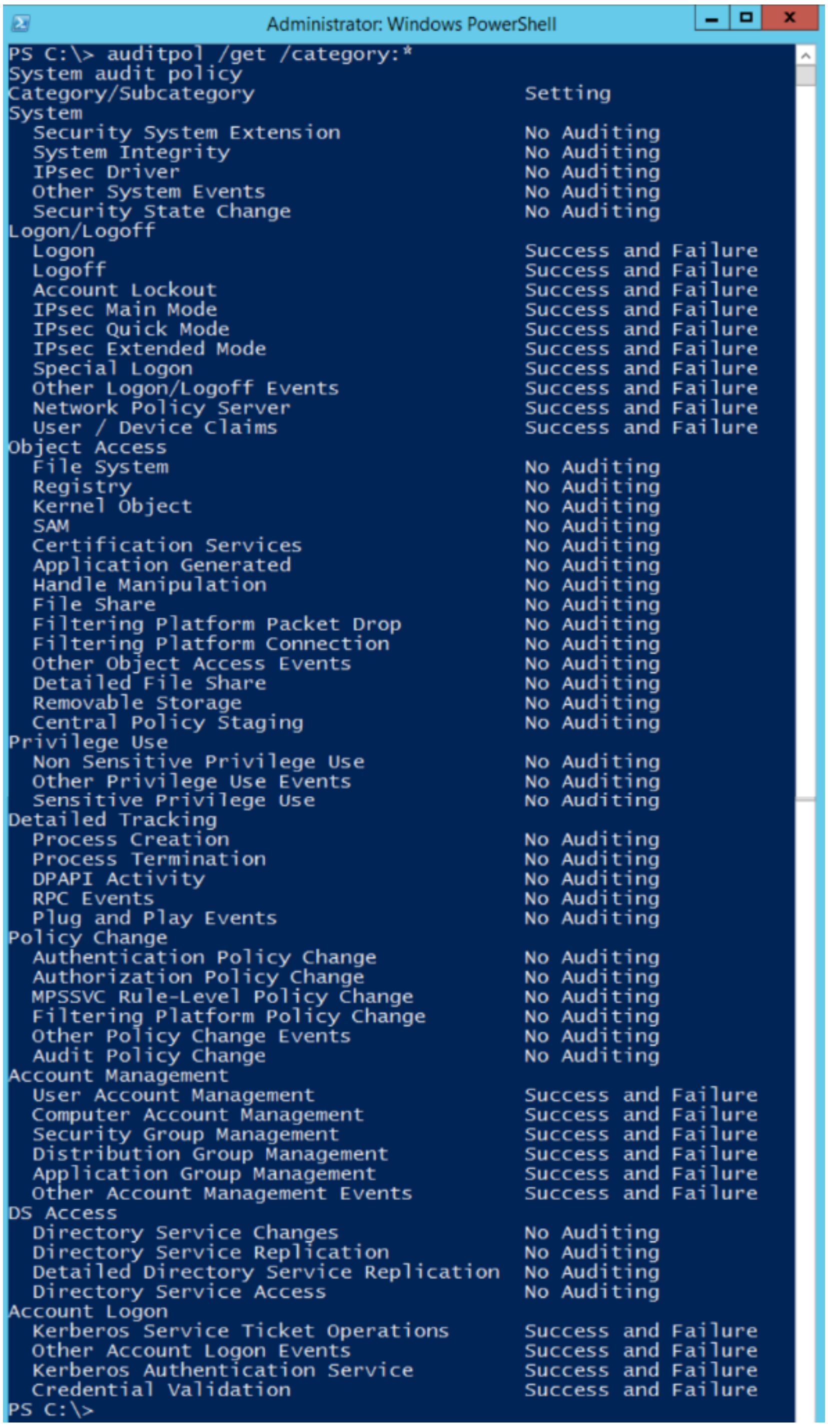
```
PS C:\> gpupdate /force
```



```
PS C:\> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

PS C:\>
```

(5) Enter the command below to view group policy applied status.

```
PS C: \> auditpol /get /category:*
```

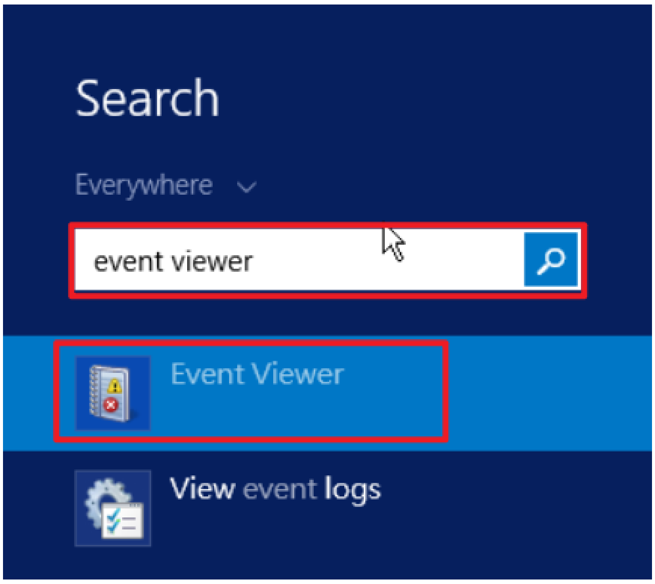


```
PS C:\> auditpol /get /category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               No Auditing
  System Integrity                        No Auditing
  IPsec Driver                            No Auditing
  Other System Events                     No Auditing
  Security State Change                   No Auditing
Logon/Logoff
  Logon                                   Success and Failure
  Logoff                                  Success and Failure
  Account Lockout                         Success and Failure
  IPsec Main Mode                         Success and Failure
  IPsec Quick Mode                        Success and Failure
  IPsec Extended Mode                     Success and Failure
  Special Logon                           Success and Failure
  Other Logon/Logoff Events               Success and Failure
  Network Policy Server                   Success and Failure
  User / Device Claims                    Success and Failure
Object Access
  File System                             No Auditing
  Registry                                No Auditing
  Kernel Object                           No Auditing
  SAM                                     No Auditing
  Certification Services                  No Auditing
  Application Generated                   No Auditing
  Handle Manipulation                     No Auditing
  File Share                              No Auditing
  Filtering Platform Packet Drop          No Auditing
  Filtering Platform Connection           No Auditing
  Other Object Access Events              No Auditing
  Detailed File Share                     No Auditing
  Removable Storage                       No Auditing
  Central Policy Staging                  No Auditing
Privilege Use
  Non Sensitive Privilege Use             No Auditing
  Other Privilege Use Events              No Auditing
  Sensitive Privilege Use                 No Auditing
Detailed Tracking
  Process Creation                        No Auditing
  Process Termination                     No Auditing
  DPAPI Activity                          No Auditing
  RPC Events                              No Auditing
  Plug and Play Events                    No Auditing
Policy Change
  Authentication Policy Change            No Auditing
  Authorization Policy Change             No Auditing
  MPSSVC Rule-Level Policy Change         No Auditing
  Filtering Platform Policy Change        No Auditing
  Other Policy Change Events              No Auditing
  Audit Policy Change                     No Auditing
Account Management
  User Account Management                 Success and Failure
  Computer Account Management             Success and Failure
  Security Group Management               Success and Failure
  Distribution Group Management           Success and Failure
  Application Group Management            Success and Failure
  Other Account Management Events         Success and Failure
DS Access
  Directory Service Changes               No Auditing
  Directory Service Replication           No Auditing
  Detailed Directory Service Replication  No Auditing
  Directory Service Access                No Auditing
Account Logon
  Kerberos Service Ticket Operations      Success and Failure
  Other Account Logon Events              Success and Failure
  Kerberos Authentication Service         Success and Failure
  Credential Validation                   Success and Failure
PS C:\>
```

3.3.2.2 Event Log Settings

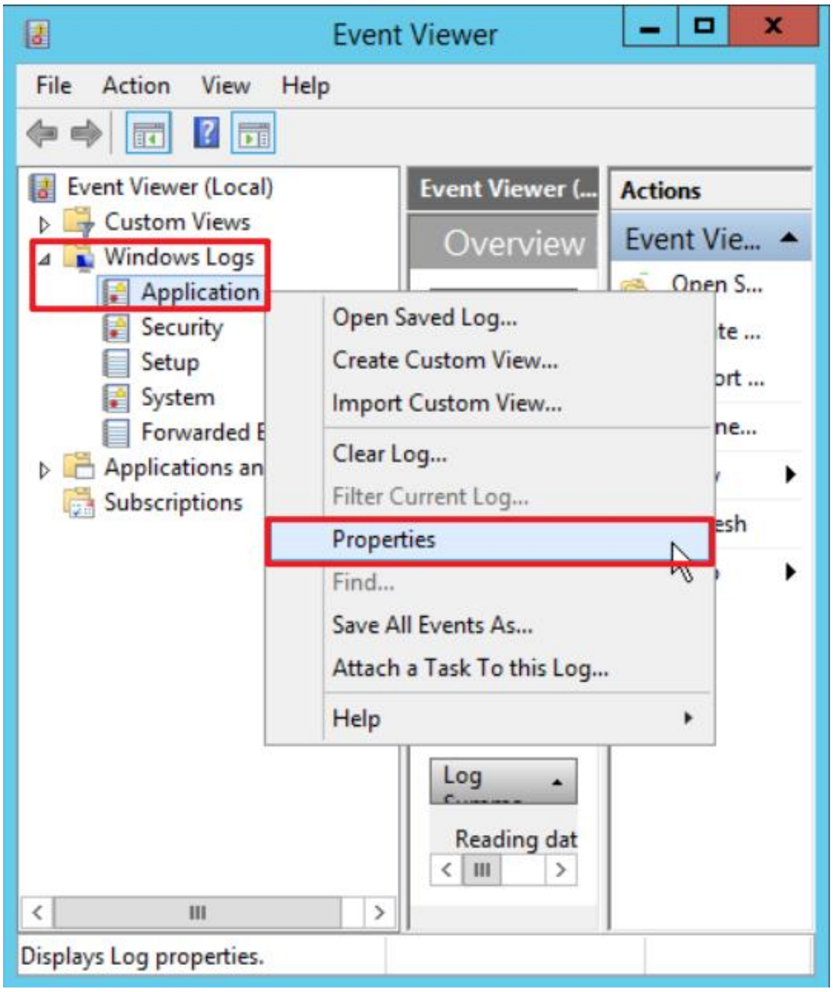
(1) Search for “Event Viewer”

Enter “Event Viewer” to search → click on “Event Viewer” in the search results.



(2) Edit Security Log

Expand folder “Windows Logs” → right-click on “Application” → And click on “Properties.”

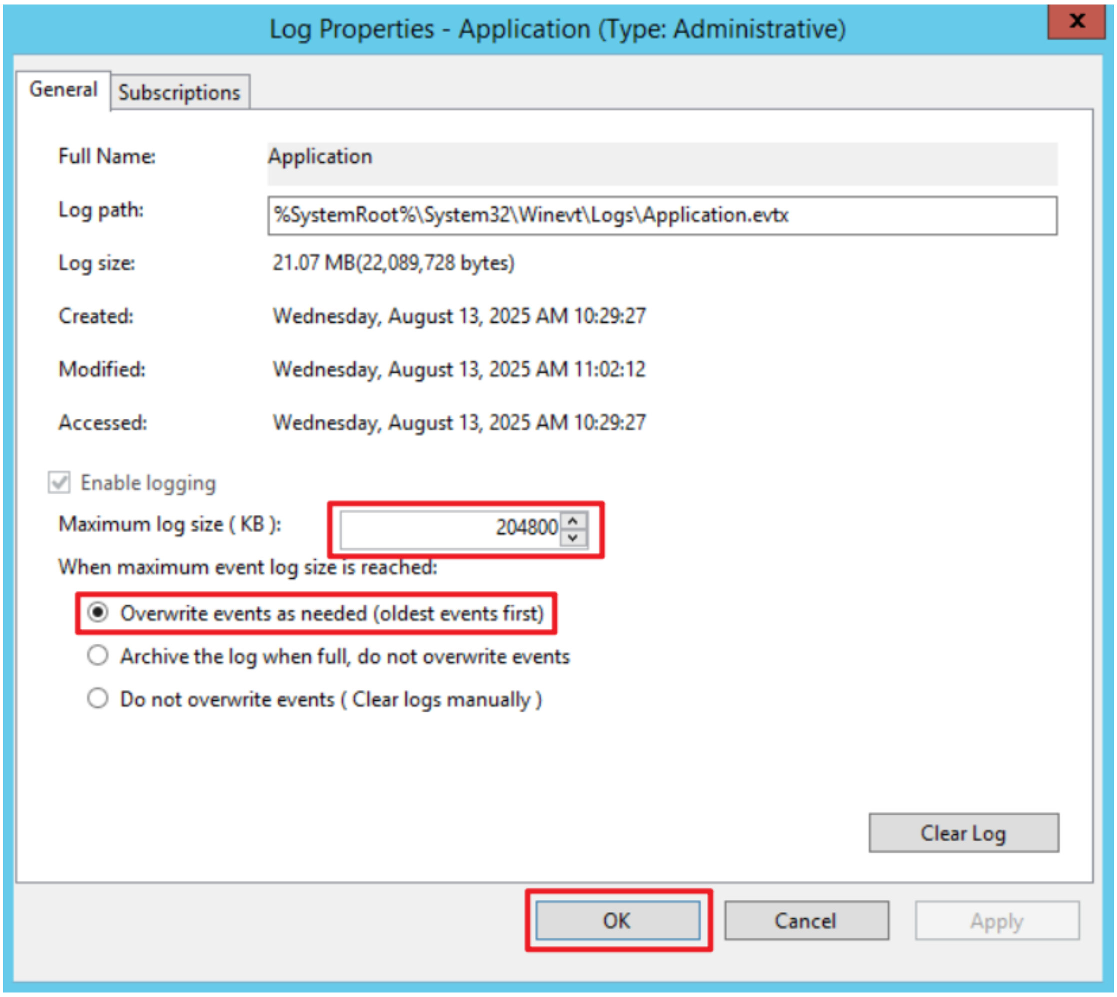


(3) Configure Security Log

Enter maximum log file size: 204800 KB

Note: Please adjust the number according to the actual environment.

→ click on “Overwrite events as needed” → click “OK.”



Log Properties - Application (Type: Administrative)

Full Name: Application

Log path: %SystemRoot%\System32\Winevt\Logs\Application.evtx

Log size: 21.07 MB(22,089,728 bytes)

Created: Wednesday, August 13, 2025 AM 10:29:27

Modified: Wednesday, August 13, 2025 AM 11:02:12

Accessed: Wednesday, August 13, 2025 AM 10:29:27

☑ Enable logging

Maximum log size (KB): 204800

When maximum event log size is reached:

● Overwrite events as needed (oldest events first)

○ Archive the log when full, do not overwrite events

○ Do not overwrite events (Clear logs manually)

4. SQL Server 2016

4.1 Login Auditing

Enable login auditing to monitor SQL Server Database Engine login activities.

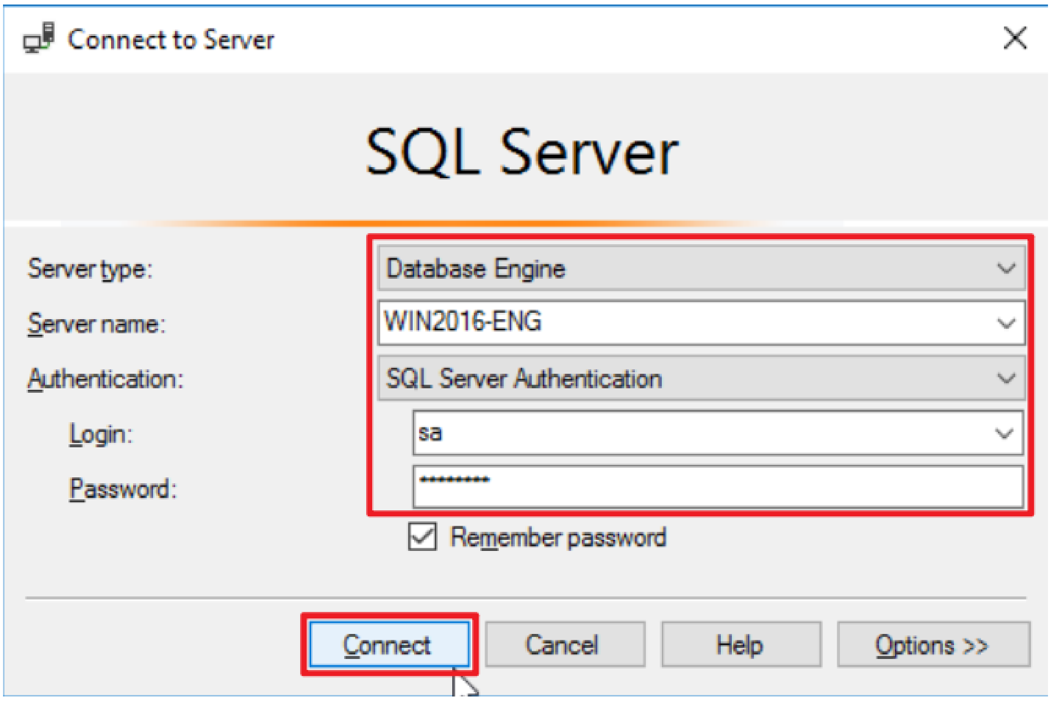
After configuration, the MS SQL Server service must be **restarted**.

The following sections describe how to configure login auditing using both the graphical user interface (GUI) and command-line interface (CLI).

4.1.1 Configuring via Graphical User Interface (GUI)

(1) Open “SQL Server Management Studio (SSMS).”

(2) Enter the server’s name → select the authentication method → click “Connect.”



Connect to Server

SQL Server

Server type: Database Engine

Server name: WIN2016-ENG

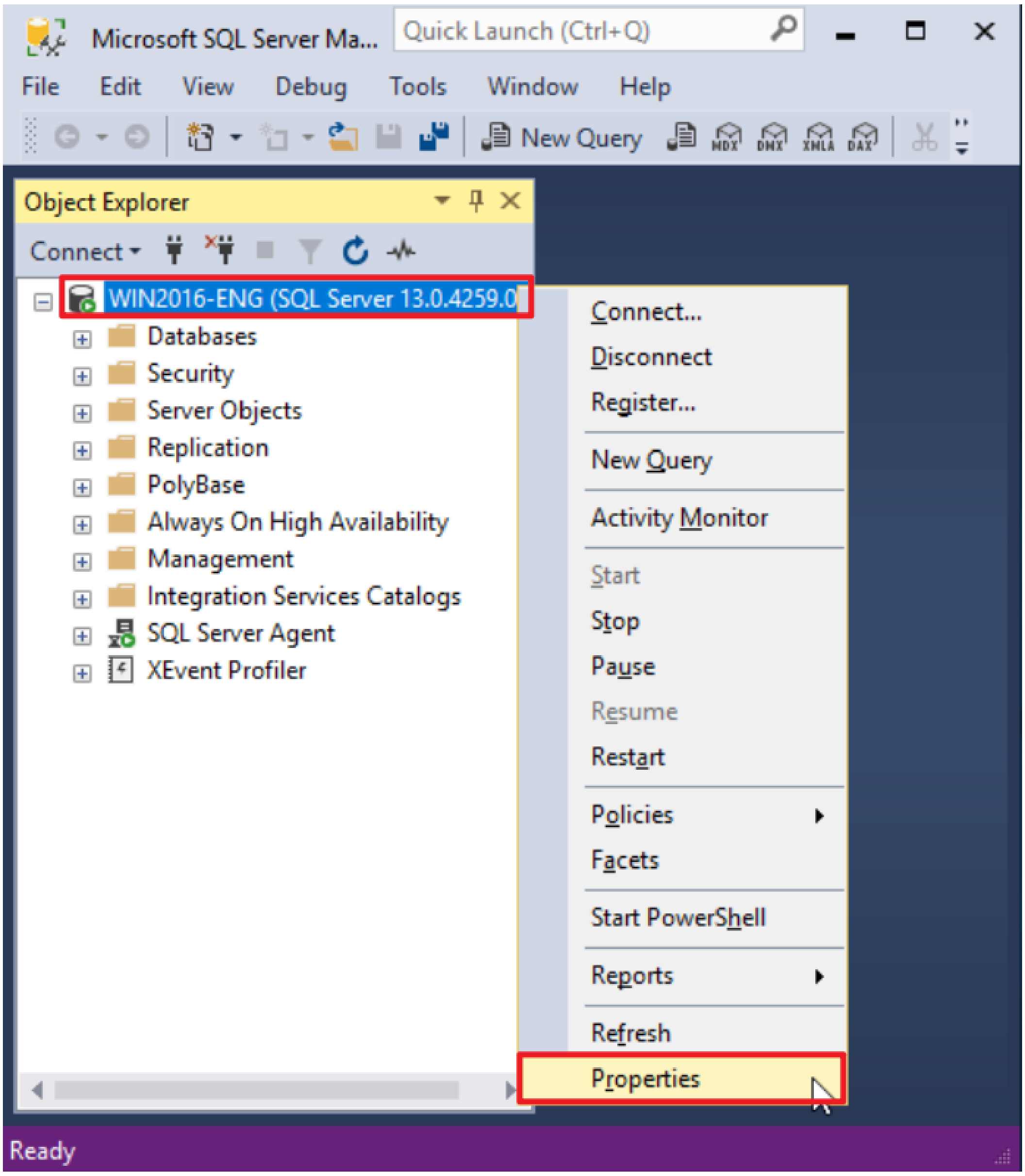
Authentication: SQL Server Authentication

Login: sa

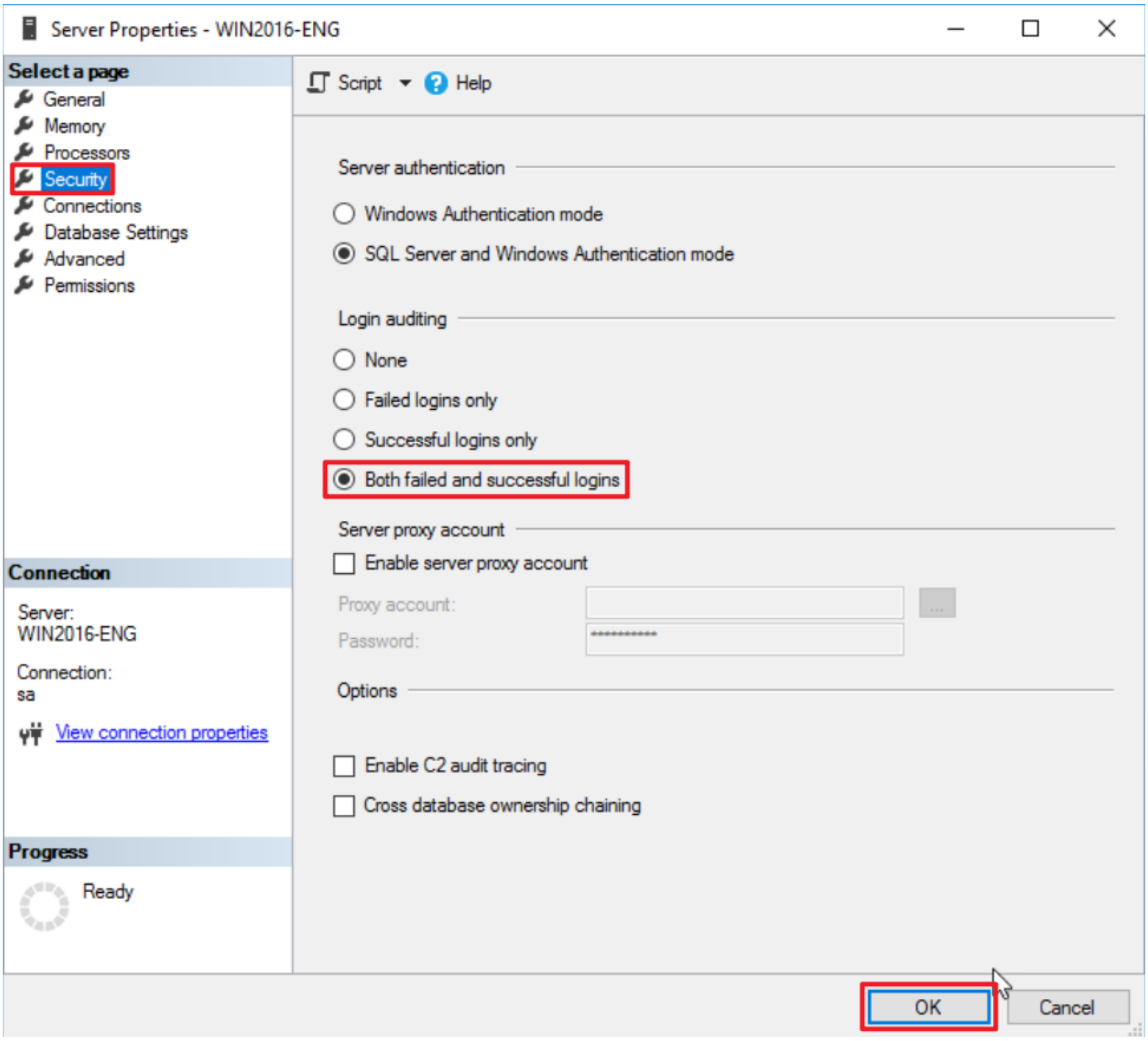
Password: *********

☑ Remember password

(3) In [Server Name] (the example here is WIN2016-ENG SQL Server 13.0.4259), right-click and select "Properties."



(4) On the Security page, under Login auditing, select “Both failed and successful logins” → click “OK”.



Server Properties - WIN2016-ENG

Select a page
- General
- Memory
- Processors
- Security
- Connections
- Database Settings
- Advanced
- Permissions

Connection

Server:
WIN2016-ENG

Connection:
sa

View connection properties

Progress

Ready

Server authentication

○ Windows Authentication mode

● SQL Server and Windows Authentication mode

Login auditing

○ None

○ Failed logins only

○ Successful logins only

● Both failed and successful logins

Server proxy account

□ Enable server proxy account

Proxy account:

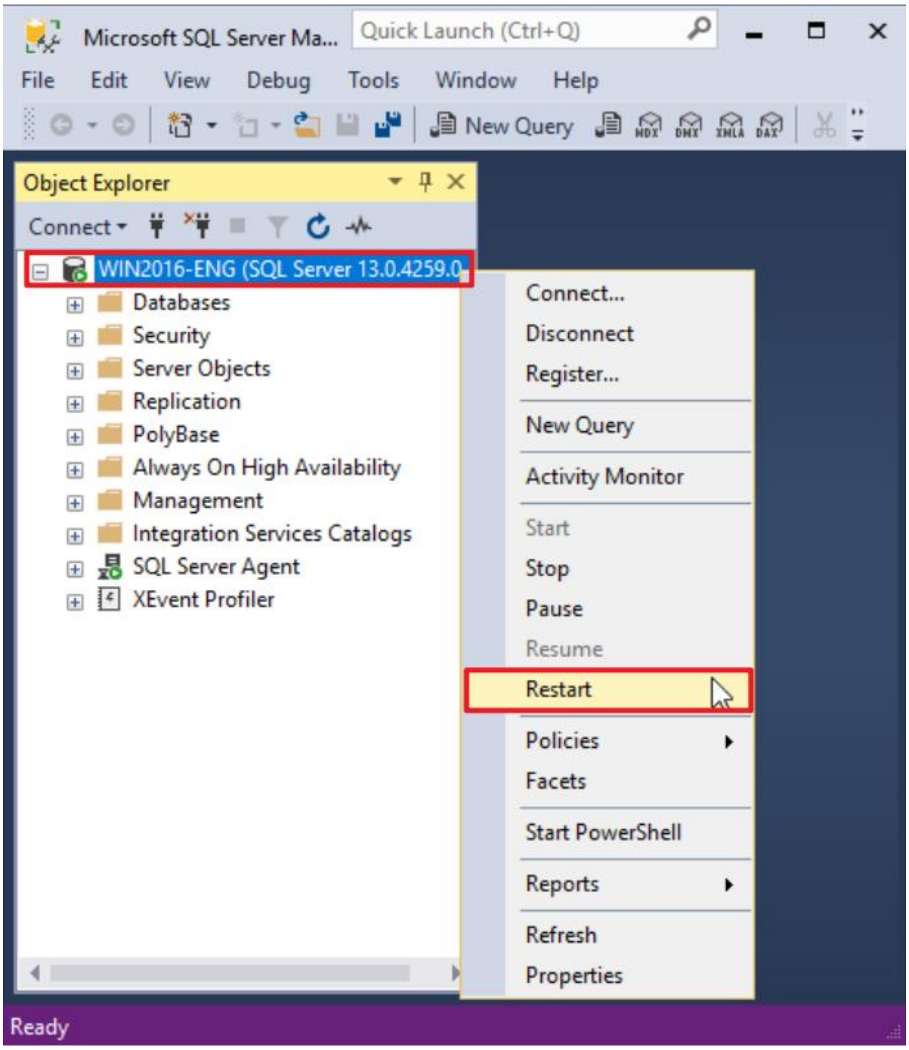
Password: ************

Options

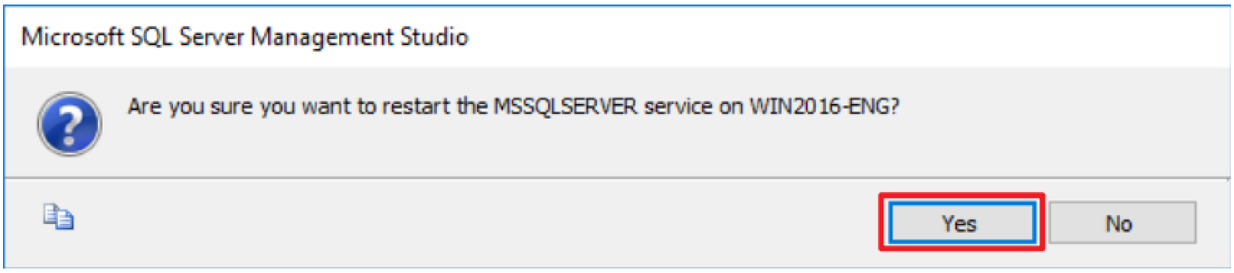
□ Enable C2 audit tracing

□ Cross database ownership chaining

(5) Restart the MS SQL Server service: right-click [Server Name] (the example here is WIN2016-ENG SQL Server 13.0.4259) → select “Restart.”

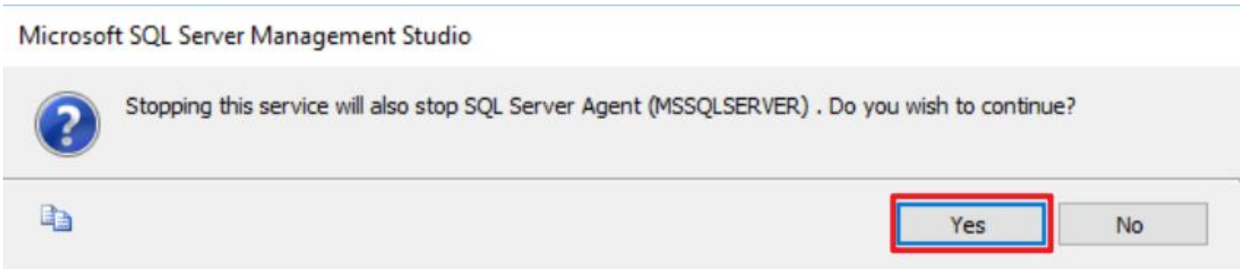


(6) Click “Yes” to restart the MS SQL Server service.


Microsoft SQL Server Management Studio

Are you sure you want to restart the MSSQLSERVER service on WIN2016-ENG?

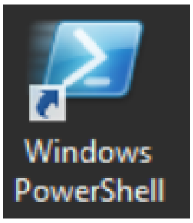
(7) Click “Yes” again to stop the SQL Server Agent service.


Microsoft SQL Server Management Studio

Stopping this service will also stop SQL Server Agent (MSSQLSERVER) . Do you wish to continue?

4.1.2 Configuring via Command-Line Interface (CLI)

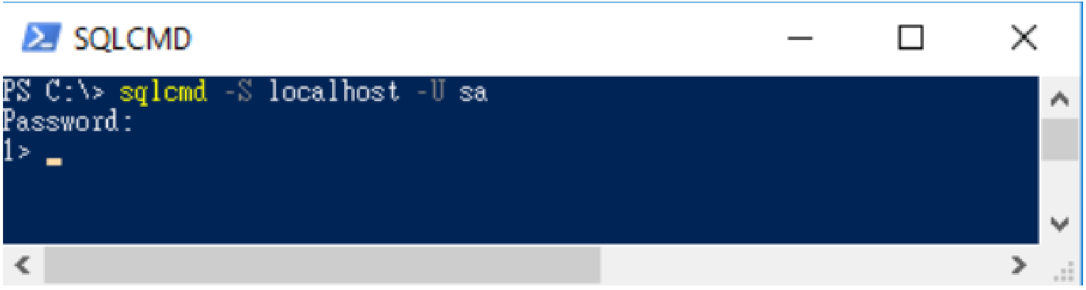
(1) Open "Windows PowerShell."



(2) Enter the command below to log in using sa:

<2.1>Using sa account:

```
PS C:\> sqlcmd -S localhost -U sa
```



```
PS C:\> sqlcmd -S localhost -U sa
Password:
1> _
```

Options:

-S [protocol:]server[instance_name][,port]

-U login_id

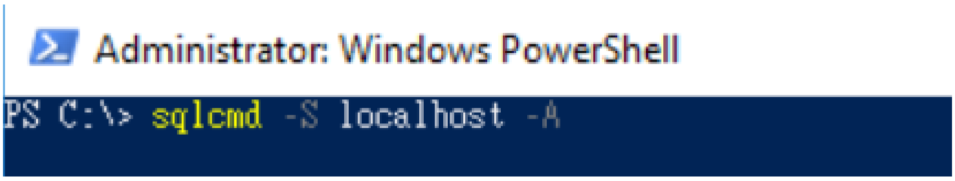
-P password

-A dedicated administrator connection

<2.2> Using Windows account:

Enter the command below to log in using Windows:

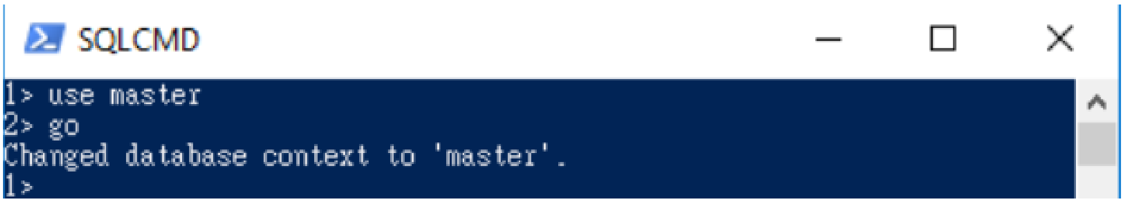
```
PS C:\> sqlcmd -S localhost -A
```



```
PS C:\> sqlcmd -S localhost -A
```

(3) Enter the command below to switch to the **master** database:

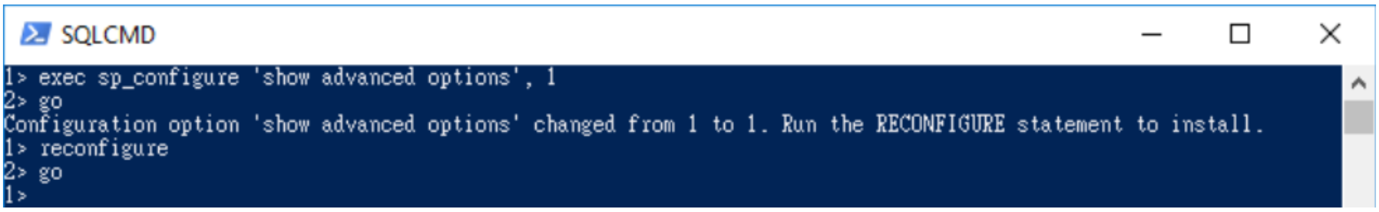
```
1 > use master
2 > go
```



```
1> use master
2> go
Changed database context to 'master'.
1>
```

(4) Enter the command below to enable advanced options:

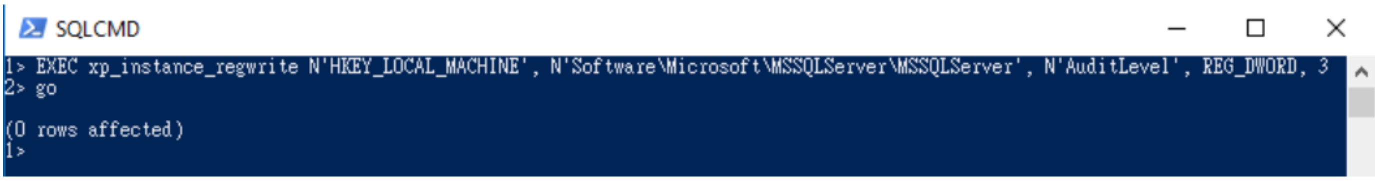
```
1 > exec sp_configure 'show advanced options', 1
2 > go
1 > reconfigure
2 > go
```



```
1> exec sp_configure 'show advanced options', 1
2> go
Configuration option 'show advanced options' changed from 1 to 1. Run the RECONFIGURE statement to install.
1> reconfigure
2> go
1>
```

(5) Enter the command below to enable auditing for both failed and successful logins:

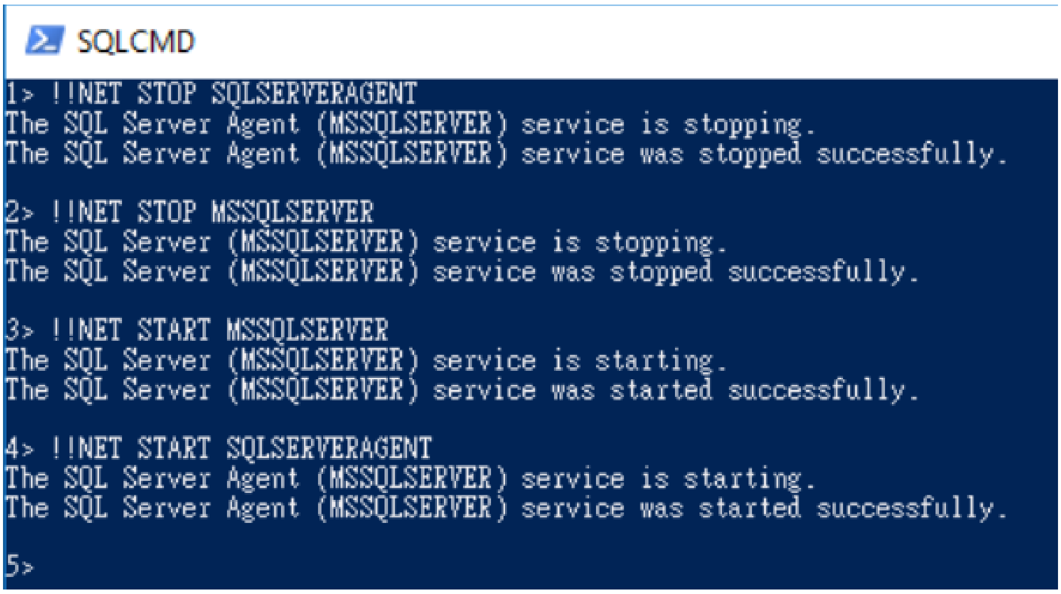
```
1 > EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE',
N'Software\Microsoft\MSSQLServer\MSSQLServer', N'AuditLevel', REG_DWORD, 3
2 > go
```



```
1> EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'Software\Microsoft\MSSQLServer\MSSQLServer', N'AuditLevel', REG_DWORD, 3
2> go

(0 rows affected)
1>
```

(7) Enter the command below to restart the MS SQL Server services:

```
1 > !!NET STOP SQLSERVERAGENT
2 > !!NET STOP MSSQLSERVER
3 > !!NET START MSSQLSERVER
4 > !!NET START SQLSERVERAGENT
```



```
1> !!NET STOP SQLSERVERAGENT
The SQL Server Agent (MSSQLSERVER) service is stopping.
The SQL Server Agent (MSSQLSERVER) service was stopped successfully.

2> !!NET STOP MSSQLSERVER
The SQL Server (MSSQLSERVER) service is stopping.
The SQL Server (MSSQLSERVER) service was stopped successfully.

3> !!NET START MSSQLSERVER
The SQL Server (MSSQLSERVER) service is starting.
The SQL Server (MSSQLSERVER) service was started successfully.

4> !!NET START SQLSERVERAGENT
The SQL Server Agent (MSSQLSERVER) service is starting.
The SQL Server Agent (MSSQLSERVER) service was started successfully.

5>
```

4.2 Configuring Auditing

4.2.1 Server-Level Audit

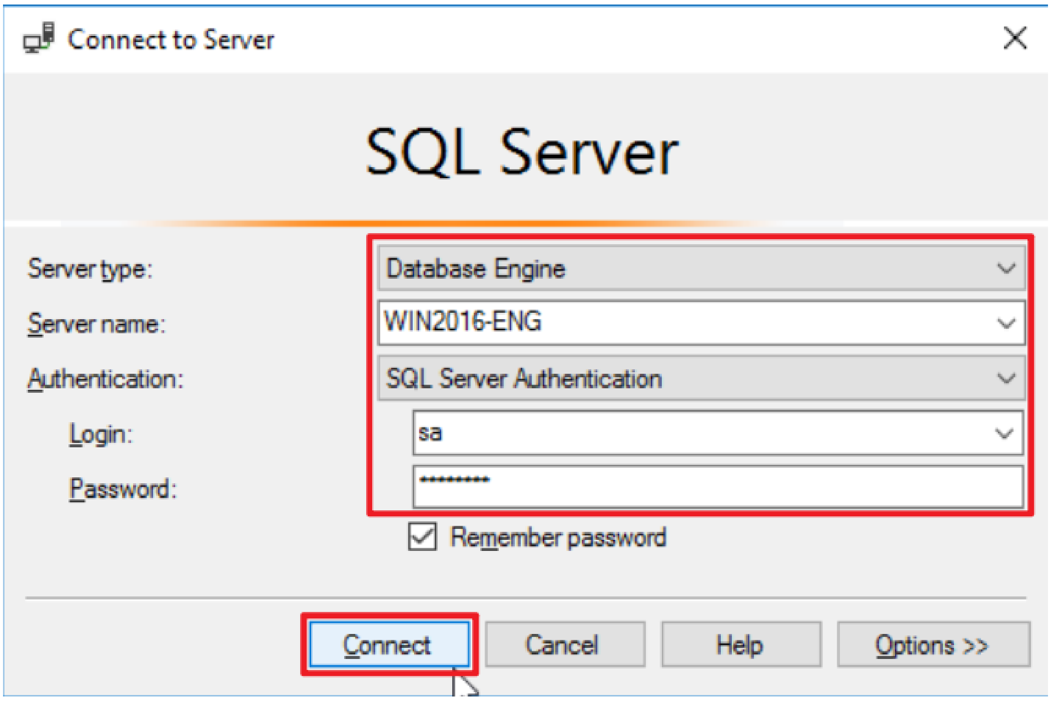
Enabling a server-level audit covers server operations such as administrative changes, login, and logout activities.

The following sections describe how to configure a server-level audit using the graphical user interface (GUI) and the command-line interface (CLI).

4.2.1.1 Configuring via Graphical User Interface (GUI)

(1) Open “SQL Server Management Studio (SSMS).”

(2) Enter the server’s name → select the authentication method → click “Connect.”



Connect to Server

SQL Server

Server type: Database Engine

Server name: WIN2016-ENG

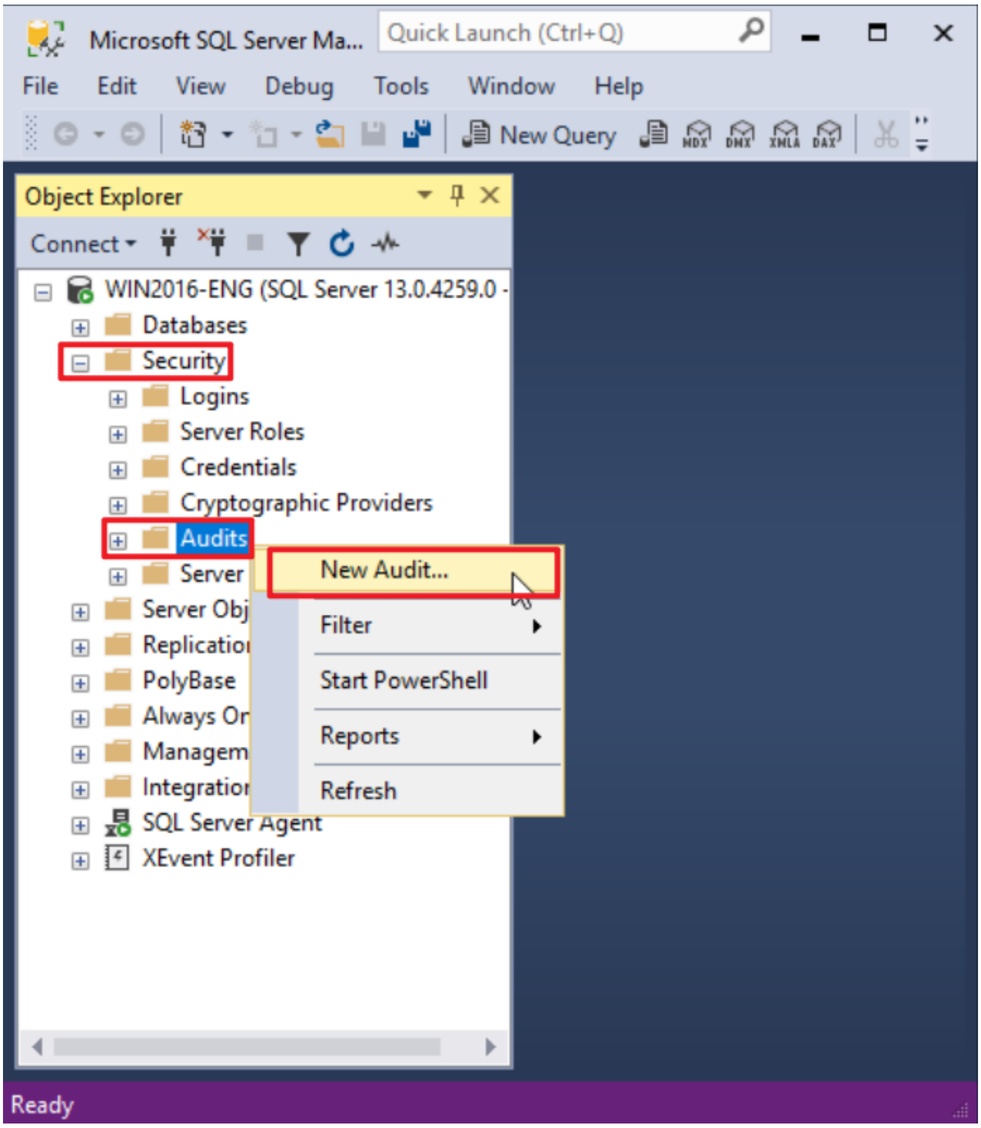
Authentication: SQL Server Authentication

Login: sa

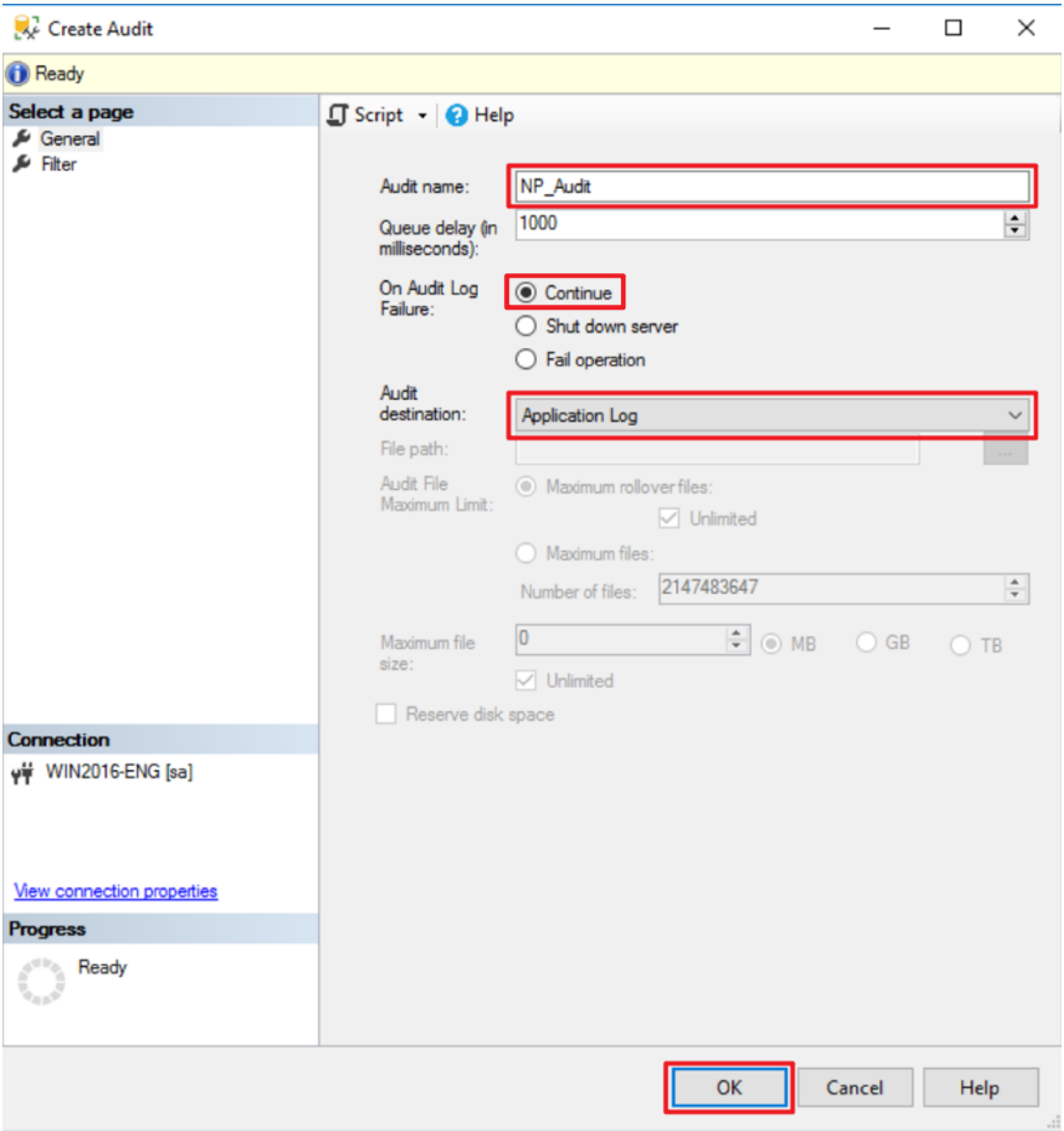
Password: *********

☑ Remember password

(3) Expand “Security” → right-click “Audits” → select “New Audit...”



(4) Enter the audit name: (the example here is NP_Audit) → select “On audit log failure”: “Continue” → select audit destination: Application Log (this stores MS SQL audit logs in the Windows Event Viewer Application Log) → click “OK.”



Create Audit

Ready

Select a page
- General
- Filter

Script ▾ | Help

Audit name: NP_Audit

Queue delay (in milliseconds): 1000

On Audit Log Failure:
- ● Continue
- ○ Shut down server
- ○ Fail operation

Audit destination: Application Log

File path:

Audit File Maximum Limit:
- ● Maximum rollover files:
  - ☑ Unlimited
- ○ Maximum files:

Number of files: 2147483647

Maximum file size: 0 ● MB ○ GB ○ TB

☑ Unlimited

□ Reserve disk space

Connection

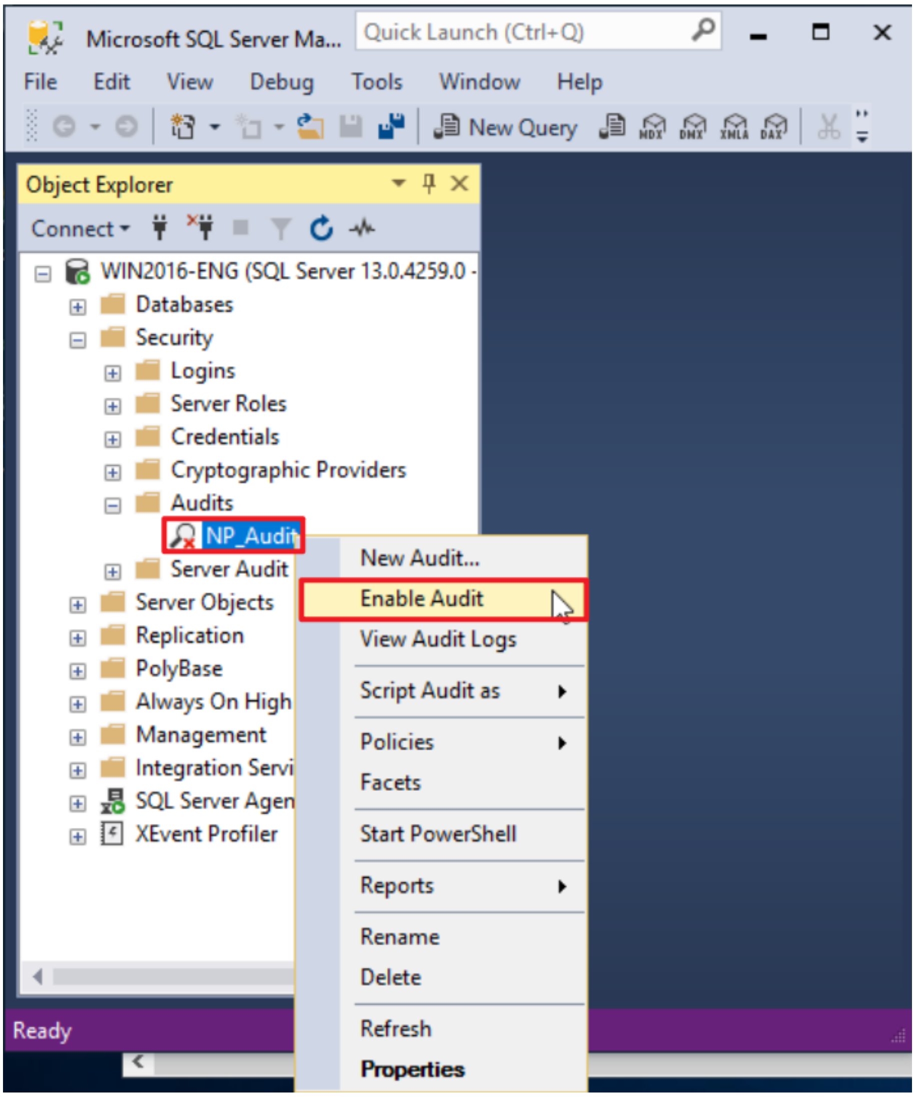
WIN2016-ENG [sa]

View connection properties

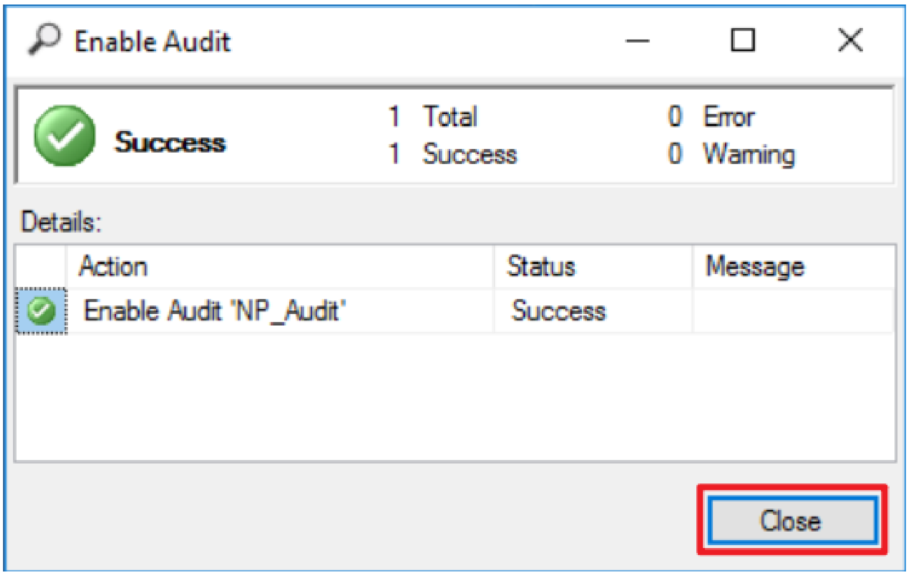
Progress

Ready

(5) In the audit list, right-click "NP_Audit" → select "Enable Audit."



(6) Click "Close."



Enable Audit

Success

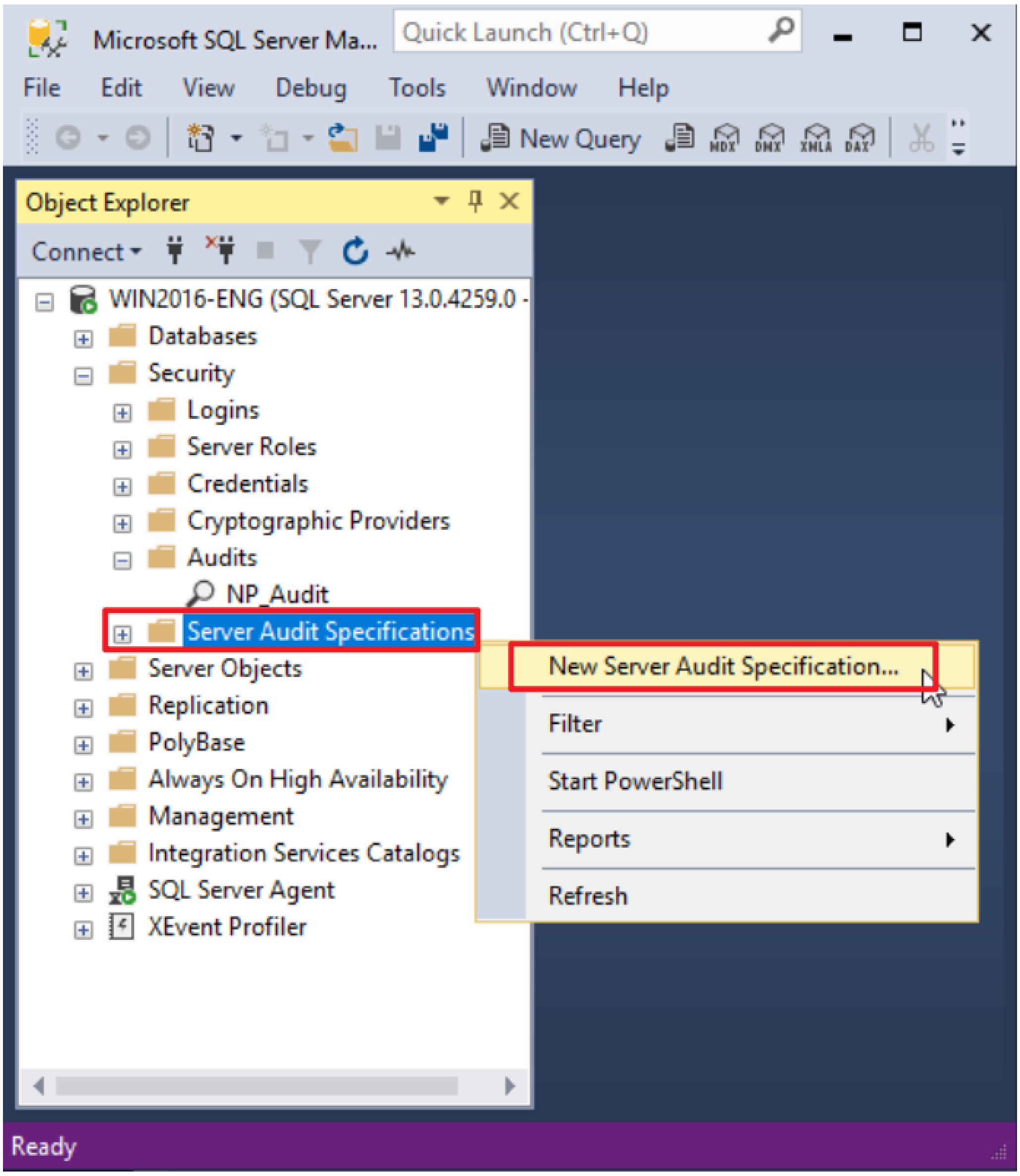
1 Total
1 Success

0 Error
0 Warning

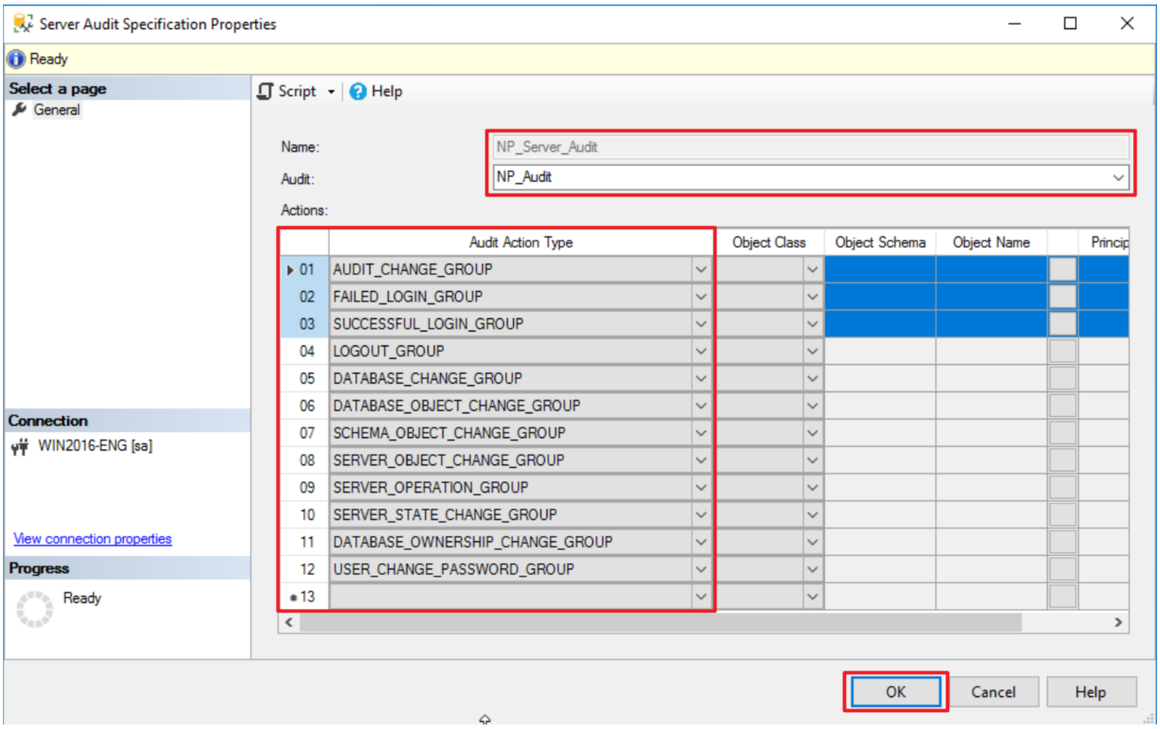
Details:

Action	Status	Message
Enable Audit 'NP_Audit'	Success	

(7) Right-click “Server Audit Specifications,” → select “New Server Audit Specification…”



(8) Enter the specification name: (the example here is NP_Server_Audit) → select audit: NP_Audit → select action(s) (refer to the [SQL Server Audit Action Groups and Actions]() in the references for details) → click "OK."



Server Audit Specification Properties

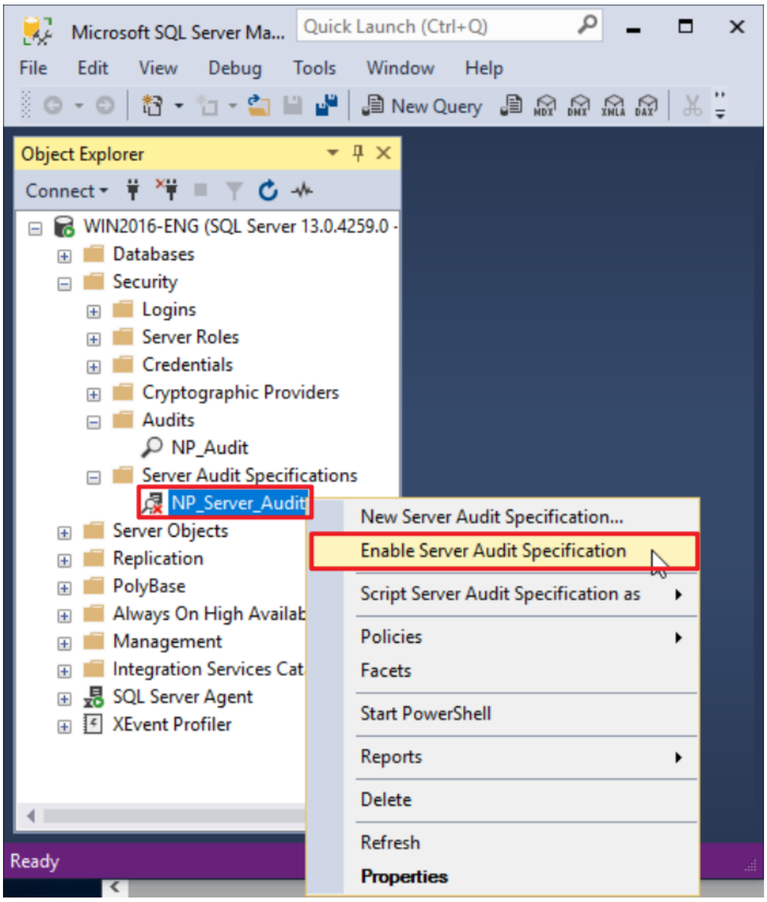
Name: NP_Server_Audit

Audit: NP_Audit

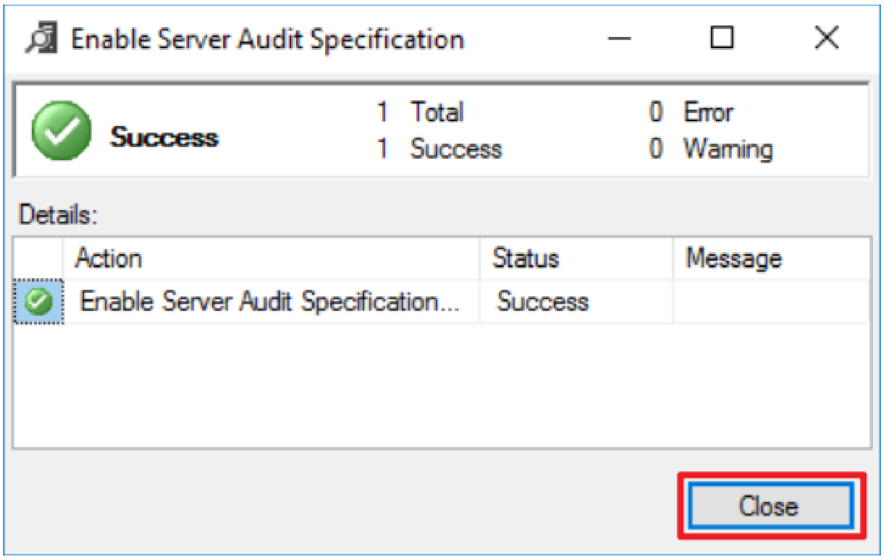
Actions:

	Audit Action Type	Object Class	Object Schema	Object Name	Princip
01	AUDIT_CHANGE_GROUP				
02	FAILED_LOGIN_GROUP				
03	SUCCESSFUL_LOGIN_GROUP				
04	LOGOUT_GROUP				
05	DATABASE_CHANGE_GROUP				
06	DATABASE_OBJECT_CHANGE_GROUP				
07	SCHEMA_OBJECT_CHANGE_GROUP				
08	SERVER_OBJECT_CHANGE_GROUP				
09	SERVER_OPERATION_GROUP				
10	SERVER_STATE_CHANGE_GROUP				
11	DATABASE_OWNERSHIP_CHANGE_GROUP				
12	USER_CHANGE_PASSWORD_GROUP				
13					

(9) In the server audit specification list, right-click "NP_Server_Audit" → select "Enable Server Audit Specification."



(10) Click “Close.”



Enable Server Audit Specification

Success

1 Total

1 Success

0 Error

0 Warning

Details:

Action	Status	Message
Enable Server Audit Specification...	Success	

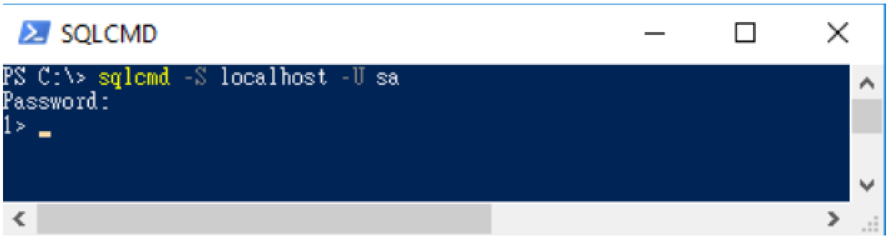
4.2.1.2 Configuring via Graphical User Interface (GUI)

(1) Open “Windows PowerShell.”

(2) Enter the command below to log in using either sa:

<2.1>Using sa account:

```
PS C:\> sqlcmd -S localhost -U sa
```



```
PS C:\> sqlcmd -S localhost -U sa
Password:
1> _
```

Options:

-S [protocol:]server[instance_name][,port]

-U login_id

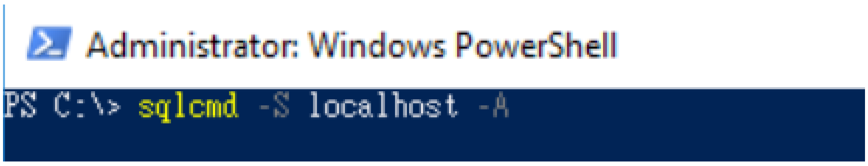
-P password

-A dedicated administrator connection

<2.2> Using Windows account:

Enter the command below to log in using Windows:

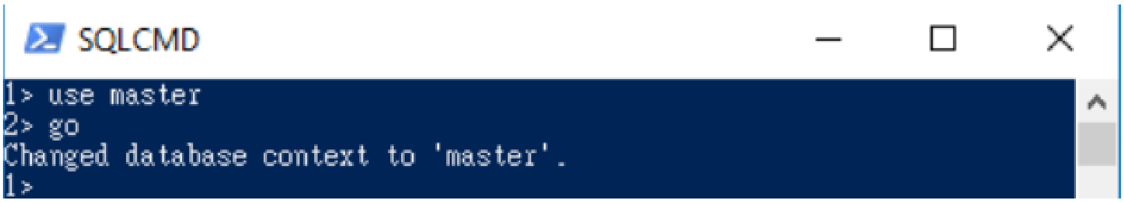
```
PS C:\> sqlcmd -S localhost -A
```



```
PS C:\> sqlcmd -S localhost -A
```

(3) Enter the command below to switch to the **master** database:

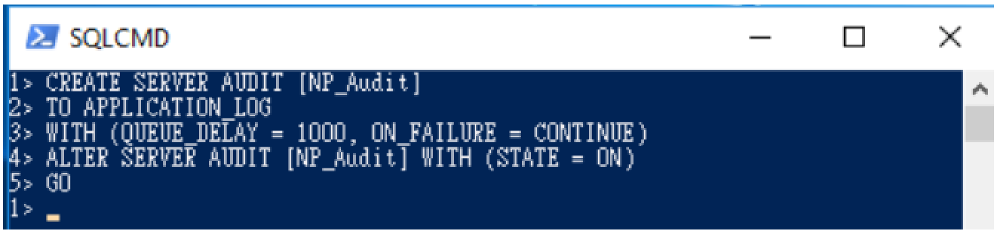
```
1 > use master
2 > go
```



```
1> use master
2> go
Changed database context to 'master'.
1>
```

(4) Enter the audit name: NP_Audit → select audit destination: Application Log (this stores MS SQL audit logs in the Windows Event Viewer Application Log) → click “OK.”

```
1 > CREATE SERVER AUDIT [ NP_Audit ]
2 > TO APPLICATION_LOG
3 > WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4 > ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5 > GO
```

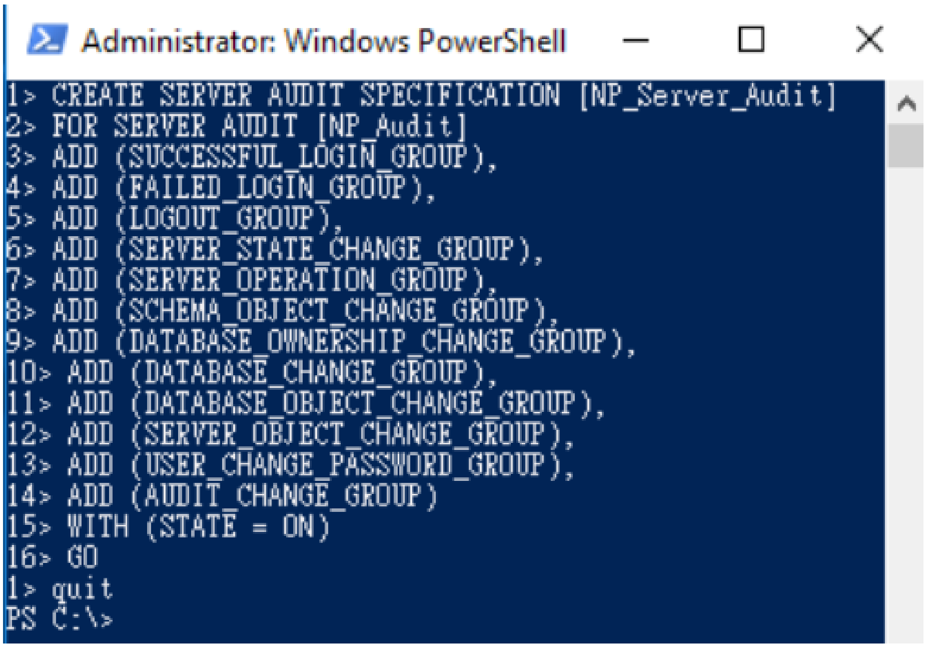


```
1> CREATE SERVER AUDIT [NP_Audit]
2> TO APPLICATION_LOG
3> WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4> ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5> GO
1> _
```

(5) Enter the command below to configure the server audit and add actions. For detailed information, refer to the **SQL Server Audit Action Groups and Actions** in the references.

```
1 > CREATE SERVER AUDIT SPECIFICATION [ NP_Server_Audit ]
2 > FOR SERVER AUDIT [NP_Audit]
3 > ADD (SUCCESSFUL_LOGIN_GROUP),
4 > ADD (FAILED_LOGIN_GROUP),
5 > ADD (LOGOUT_GROUP),
6 > ADD (SERVER_STATE_CHANGE_GROUP),
7 > ADD (SERVER_OPERATION_GROUP),
8 > ADD (SCHEMA_OBJECT_CHANGE_GROUP),
9 > ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
10 > ADD (DATABASE_CHANGE_GROUP),
11 > ADD (DATABASE_OBJECT_CHANGE_GROUP),
12 > ADD (SERVER_OBJECT_CHANGE_GROUP),
13 > ADD (USER_CHANGE_PASSWORD_GROUP)
14 > ADD (AUDIT_CHANGE_GROUP)
15> WITH (STATE = ON)
```

```
16 > GO
1 > quit
```



```
1> CREATE SERVER AUDIT SPECIFICATION [NP_Server_Audit]
2> FOR SERVER AUDIT [NP_Audit]
3> ADD (SUCCESSFUL_LOGIN_GROUP),
4> ADD (FAILED_LOGIN_GROUP),
5> ADD (LOGOUT_GROUP),
6> ADD (SERVER_STATE_CHANGE_GROUP),
7> ADD (SERVER_OPERATION_GROUP),
8> ADD (SCHEMA_OBJECT_CHANGE_GROUP),
9> ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
10> ADD (DATABASE_CHANGE_GROUP),
11> ADD (DATABASE_OBJECT_CHANGE_GROUP),
12> ADD (SERVER_OBJECT_CHANGE_GROUP),
13> ADD (USER_CHANGE_PASSWORD_GROUP),
14> ADD (AUDIT_CHANGE_GROUP)
15> WITH (STATE = ON)
16> GO
1> quit
PS C:\>
```

Replace the text shown in red with the server audit specification name.

4.2.2 Database-Level Audit

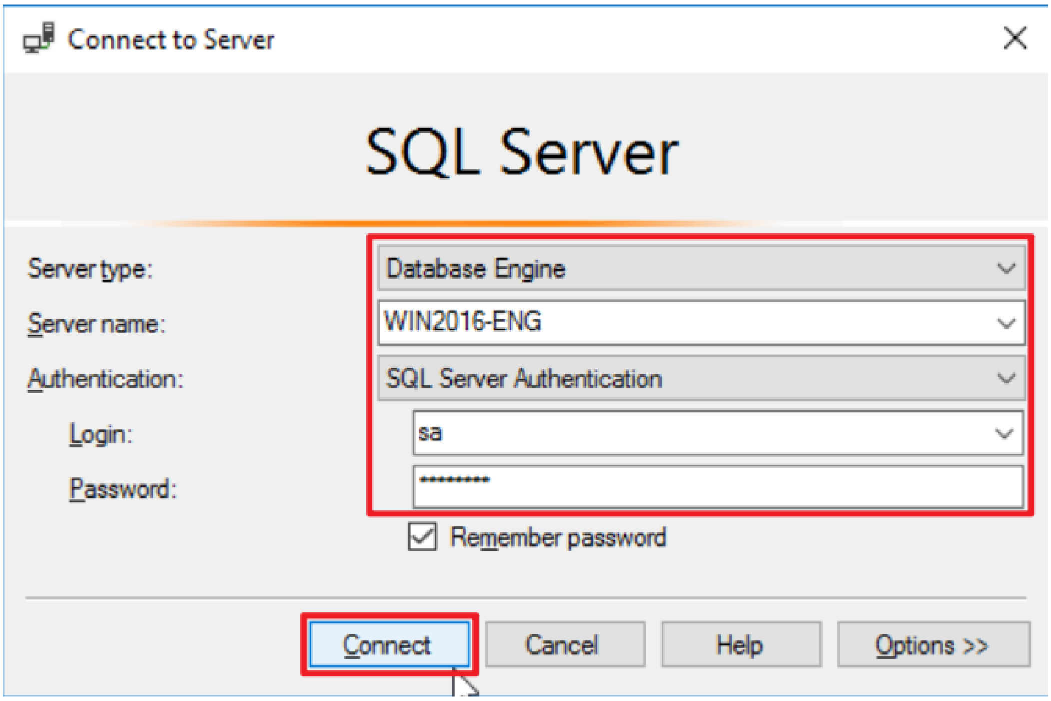
Enabling a database-level audit covers operations involving Data Manipulation Language (DML) and Data Definition Language (DDL) statements.

The following sections describe how to configure a database-level audit using the graphical user interface (GUI) and the command-line interface (CLI).

4.2.2.1 Configuring via Graphical User Interface (GUI)

(1) Open "SQL Server Management Studio (SSMS)."

(2) Enter the server's name → select the authentication method → click "Connect."



Connect to Server

SQL Server

Server type: Database Engine

Server name: WIN2016-ENG

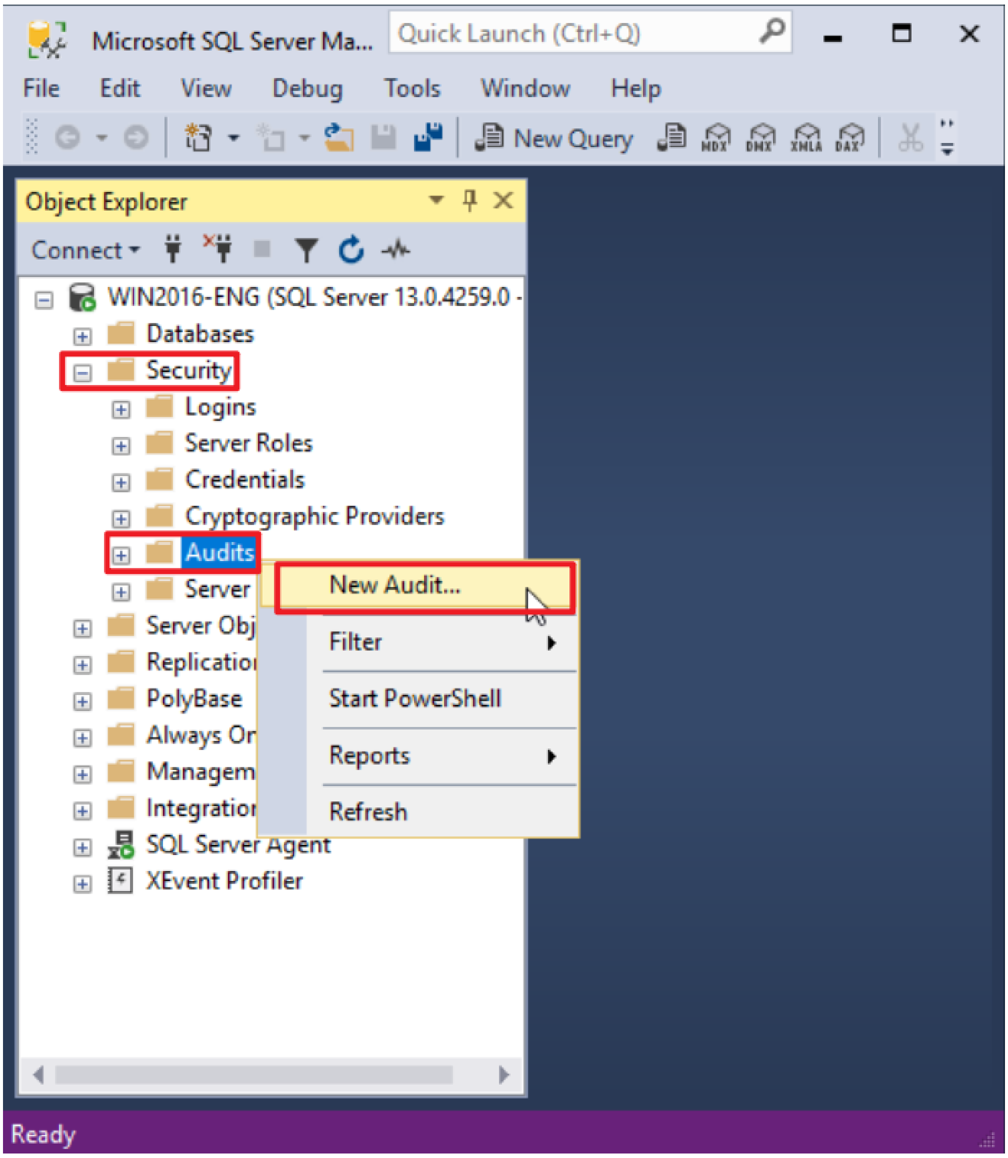
Authentication: SQL Server Authentication

Login: sa

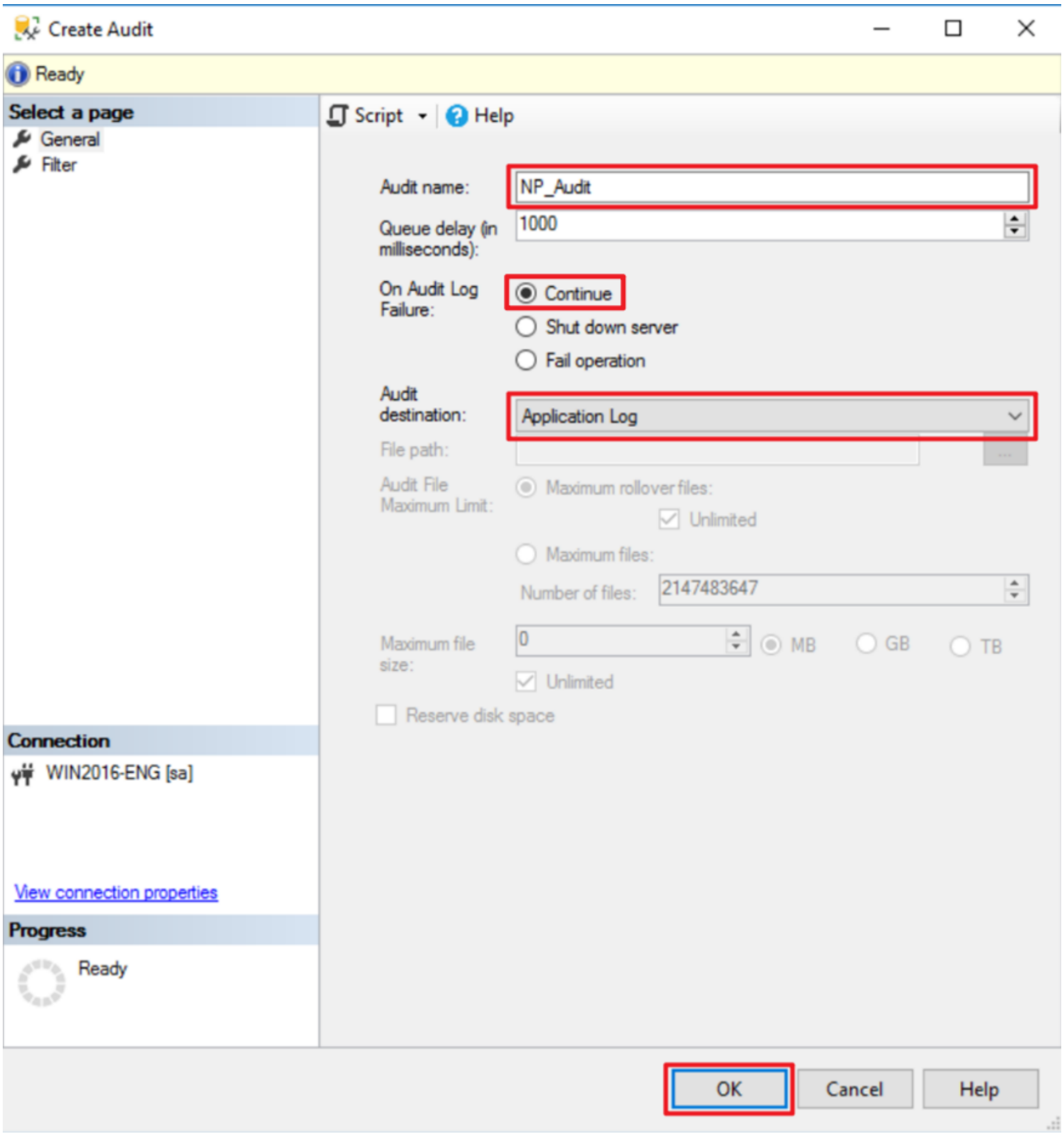
Password: *********

☑ Remember password

(3) Expand “Security” → right-click “Audits” → select “New Audit...”



(4) Enter the audit name: (the example here is NP_Audit) → select "On audit log failure": "Continue" → select audit destination: Application Log (this stores MS SQL audit logs in the Windows Event Viewer Application Log) → click "OK."



Audit name: NP_Audit

Queue delay (in milliseconds): 1000

On Audit Log Failure:
● Continue
○ Shut down server
○ Fail operation

Audit destination: Application Log

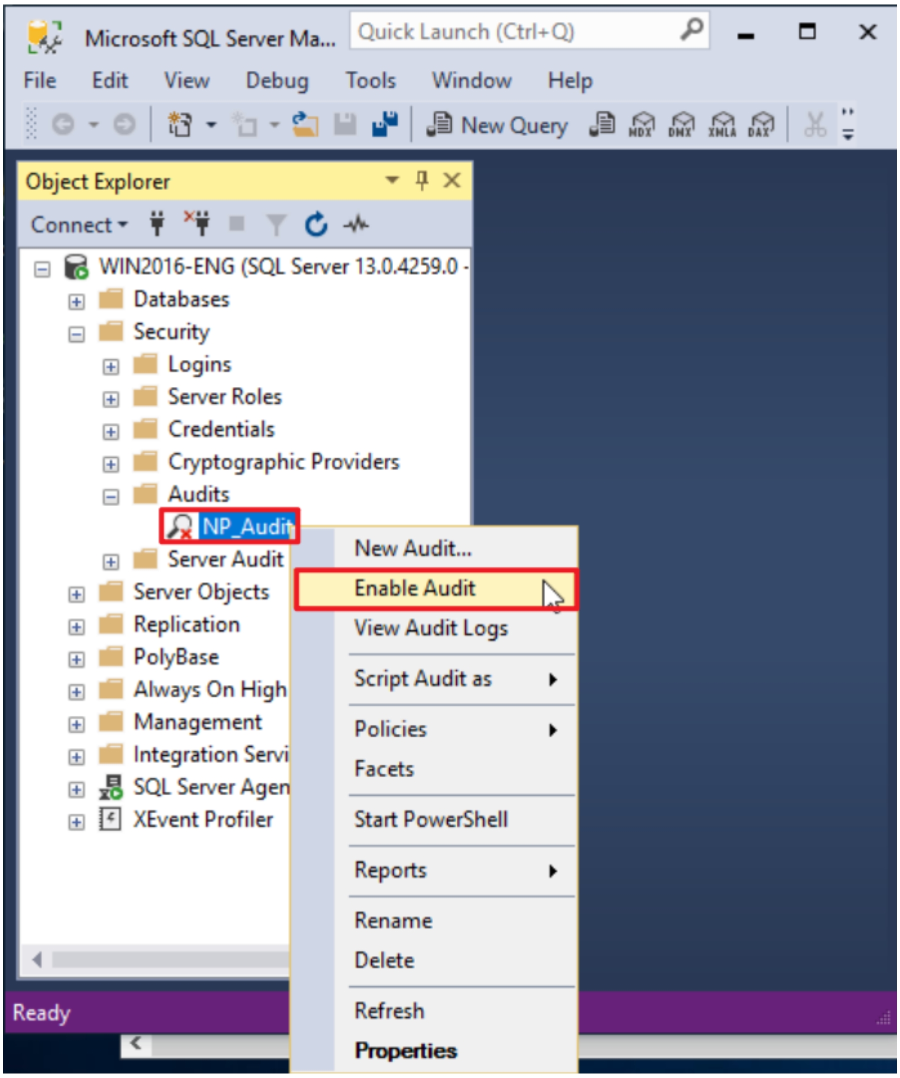
File path:

Audit File Maximum Limit:
● Maximum rollover files:
☑ Unlimited
○ Maximum files:
Number of files: 2147483647

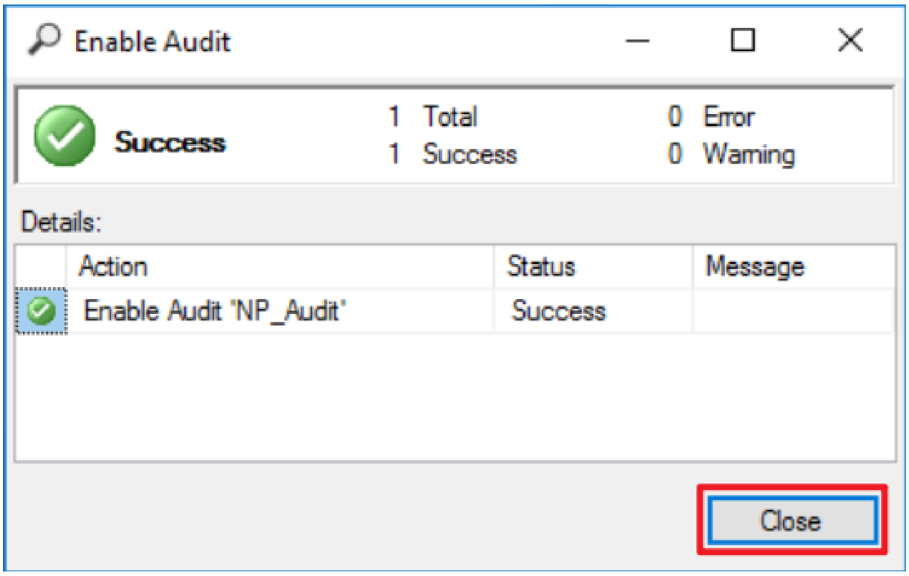
Maximum file size: 0 ● MB ○ GB ○ TB
☑ Unlimited

□ Reserve disk space

(5) In the audit list, right-click "NP_Audit" → select "Enable Audit."



(6) Click "Close."


Enable Audit

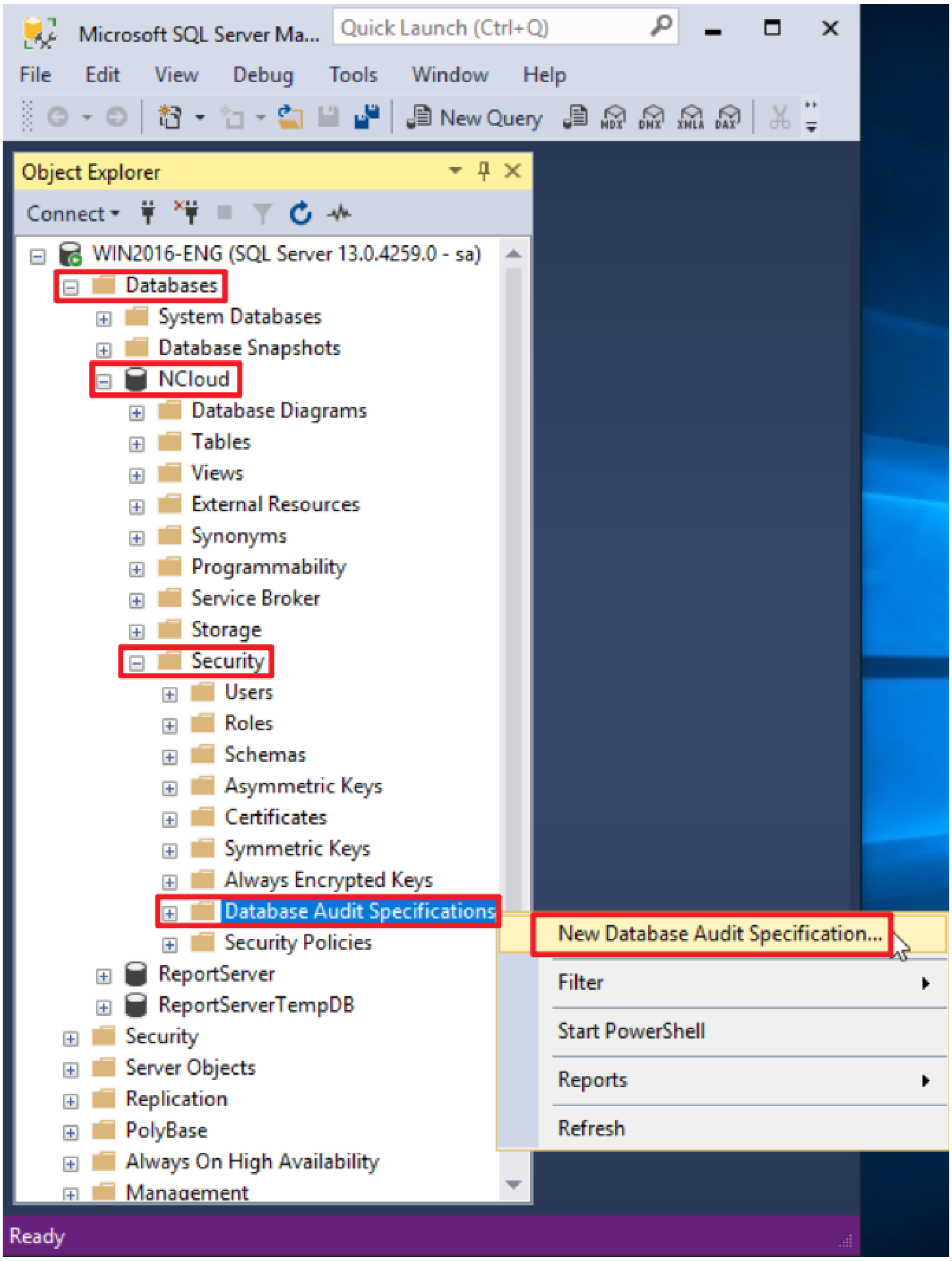
Success

1 Total
1 Success
0 Error
0 Warning

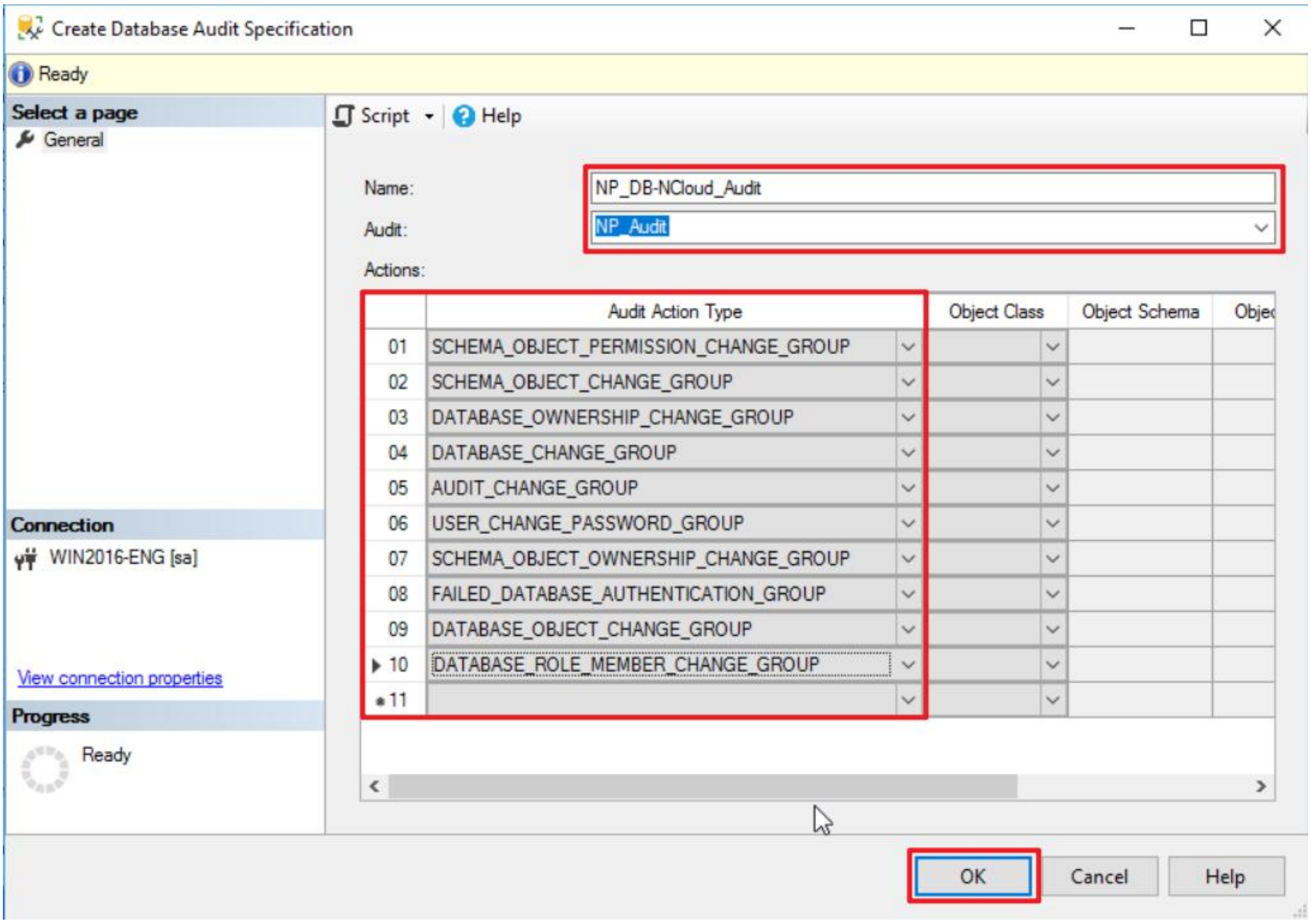
Details:

Action	Status	Message
Enable Audit 'NP_Audit'	Success	

(7) In “Databases,” select the target database (the example here is : NCloud) → expand “Security” → right-click “Database Audit Specifications” → select "New Database Audit Specification...”



(8) Enter the specification name: (the example here is NP_DB-NCloud_Audit) → select audit: NP_Audit and action(s) → select action(s) (refer to the **SQL Server Audit Action Groups and Actions** in the references for details) → click "OK."



Create Database Audit Specification

Ready

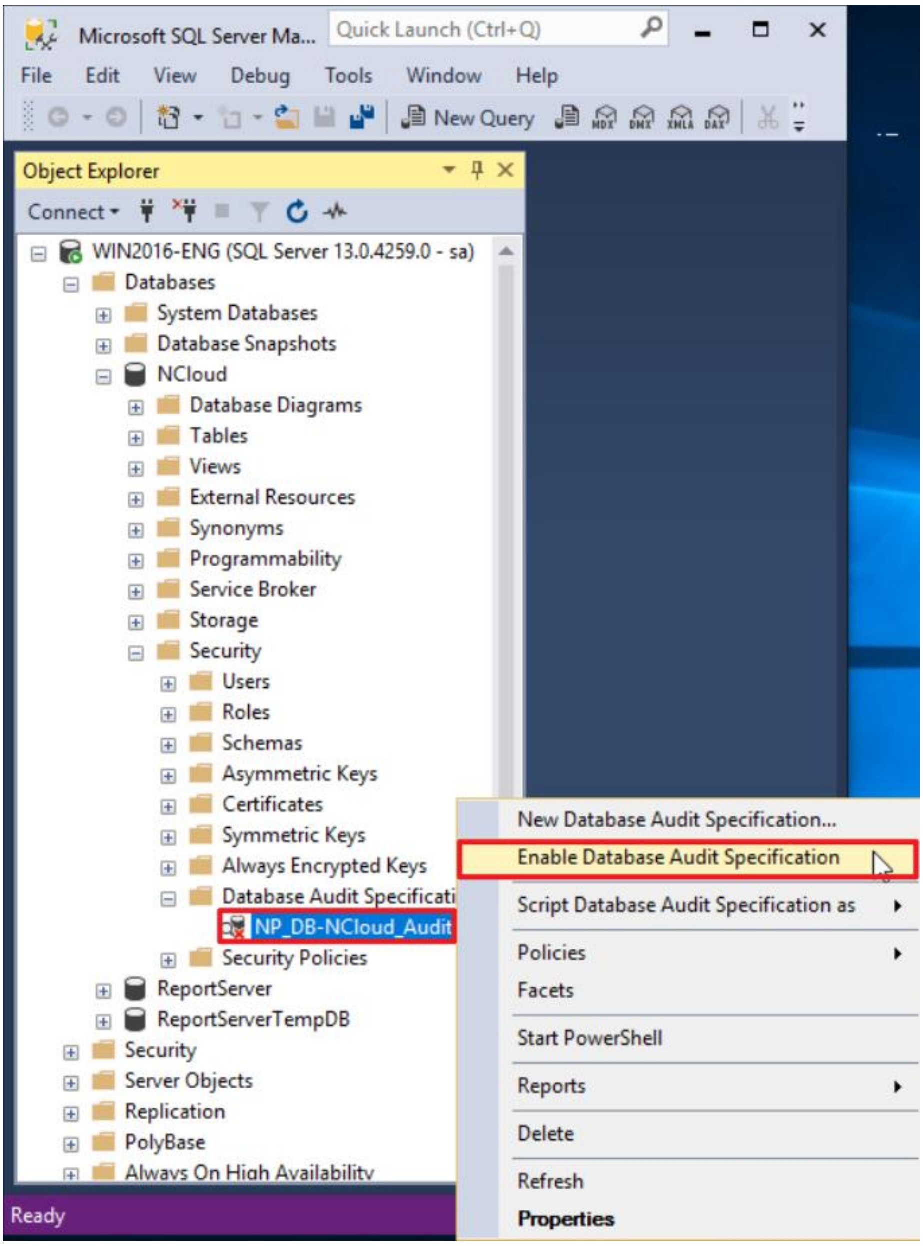
Name: NP_DB-NCloud_Audit

Audit: NP_Audit

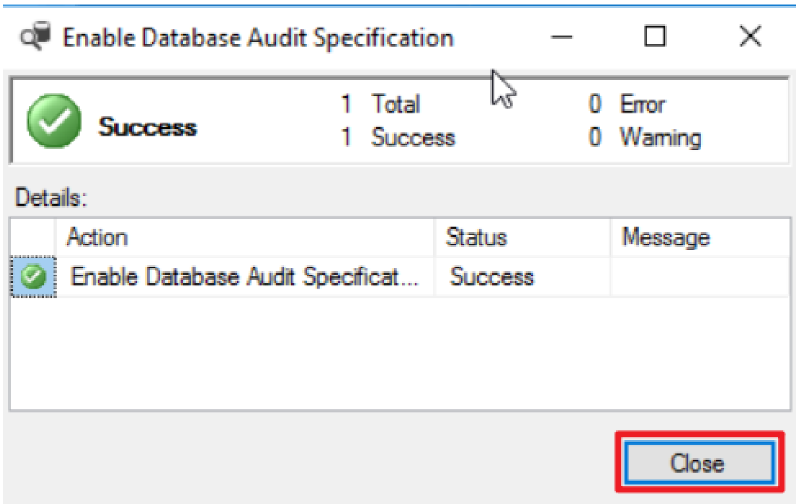
Actions:

	Audit Action Type	Object Class	Object Schema	Objec
01	SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP			
02	SCHEMA_OBJECT_CHANGE_GROUP			
03	DATABASE_OWNERSHIP_CHANGE_GROUP			
04	DATABASE_CHANGE_GROUP			
05	AUDIT_CHANGE_GROUP			
06	USER_CHANGE_PASSWORD_GROUP			
07	SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP			
08	FAILED_DATABASE_AUTHENTICATION_GROUP			
09	DATABASE_OBJECT_CHANGE_GROUP			
10	DATABASE_ROLE_MEMBER_CHANGE_GROUP			
11				

(9) In the database audit specification list, right-click “NP_DB-NCloud_Audit” → select “Enable Server Audit Specification.”



(10) Click “Close.”


Enable Database Audit Specification

Success — 1 Total, 1 Success, 0 Error, 0 Warning

Details:

Action	Status	Message
Enable Database Audit Specificat...	Success	

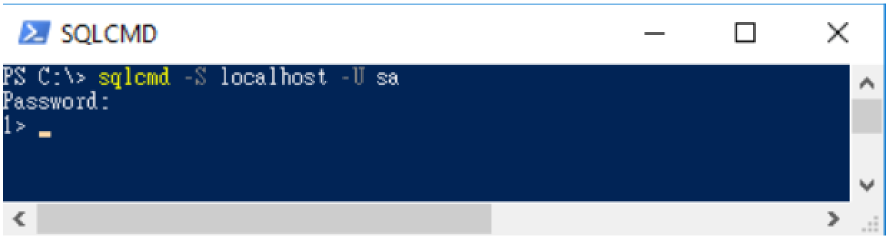
4.2.2.2 Configuring via Graphical User Interface (GUI)

(1) Open “Windows PowerShell.”

(2) Enter the command below to log in using either sa:

<2.1>Using sa account:

```
PS C:\> sqlcmd -S localhost -U sa
```



```
PS C:\> sqlcmd -S localhost -U sa
Password:
1> _
```

Options:

-S [protocol:]server[instance_name][,port]

-U login_id

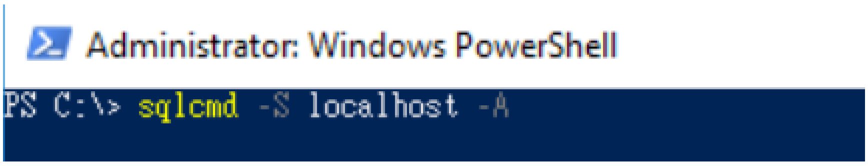
-P password

-A dedicated administrator connection

<2.2> Using Windows account:

Enter the command below to log in using Windows account:

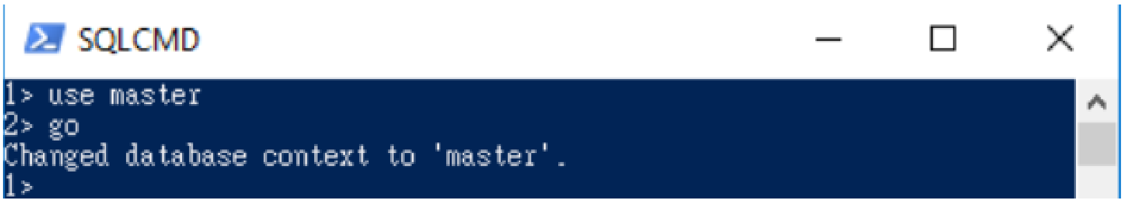
```
PS C:\> sqlcmd -S localhost -A
```



```
PS C:\> sqlcmd -S localhost -A
```

(3) Enter the command below to switch to the **master** database:

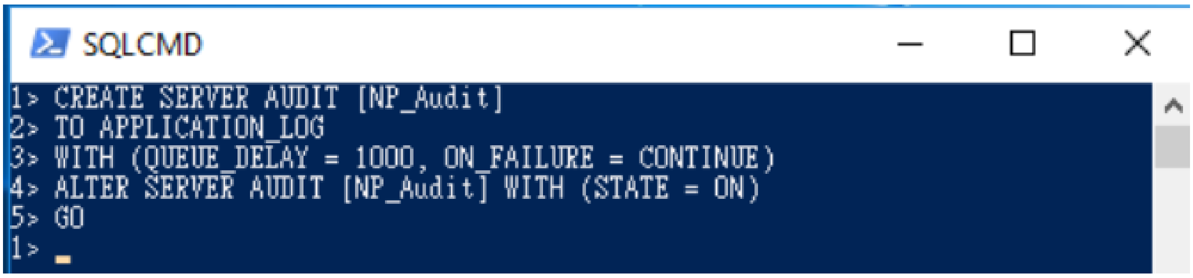
```
1 > use master
2 > go
```



```
1> use master
2> go
Changed database context to 'master'.
1>
```

(4) Enter the audit name: NP_Audit → select audit destination: Application Log (this stores MS SQL audit logs in the Windows Event Viewer Application Log) → click “OK.”

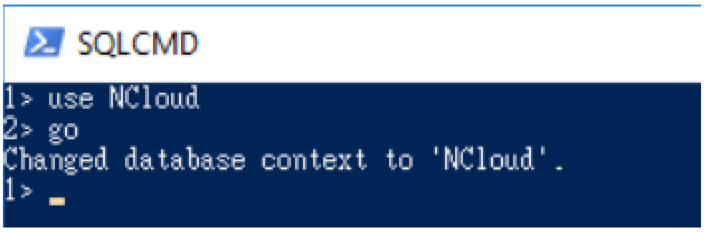
```
1 > CREATE SERVER AUDIT [ NP_Audit ]
2 > TO APPLICATION_LOG
3 > WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4 > ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5 > GO
```



```
1> CREATE SERVER AUDIT [NP_Audit]
2> TO APPLICATION_LOG
3> WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4> ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5> GO
1> _
```

(5) Enter the command below to switch to the target audit database (the example here is: NCloud).

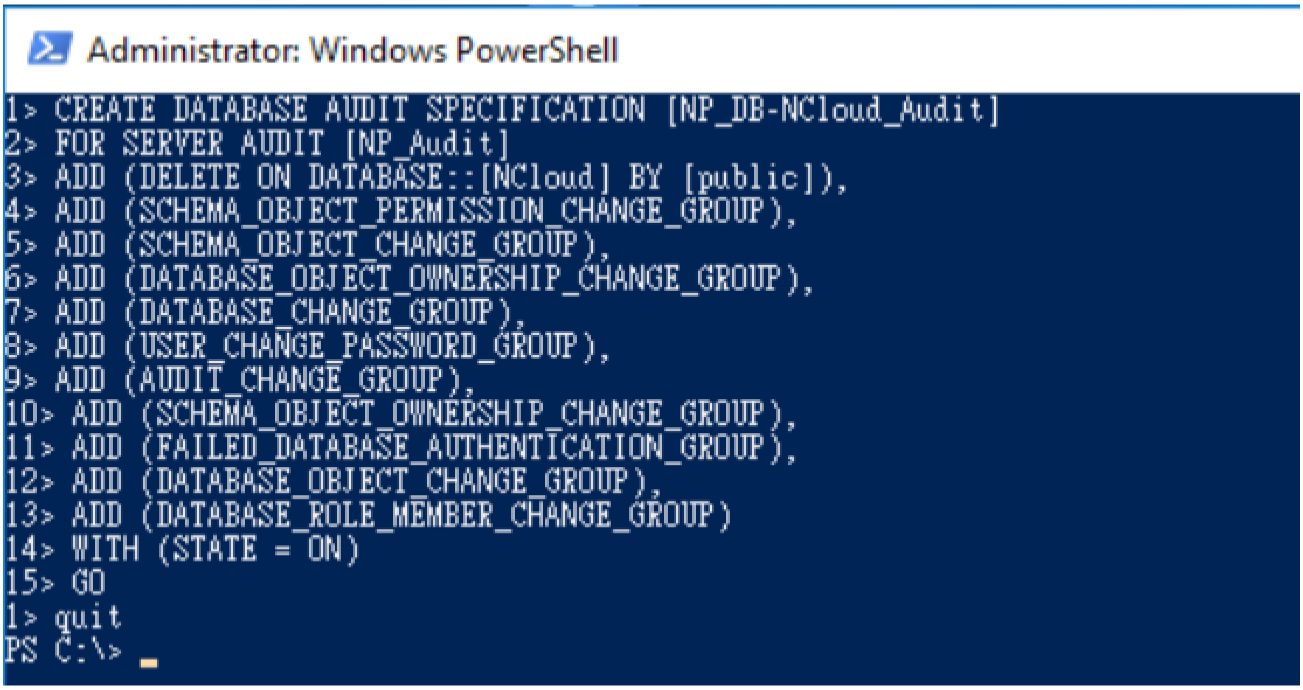
```
1 > use NCloud
2 > go
```



```
1> use NCloud
2> go
Changed database context to 'NCloud'.
1> _
```

(6) Enter the command below to configure the audit for the database and add actions. For detailed information, refer to the SQL Server Audit Action Groups and Actions in the references.

```
1 > CREATE DATABASE AUDIT SPECIFICATION [ NP_DB-NCloud_Audit ]
2 > FOR SERVER AUDIT [NP_Audit]
3 > ADD (DELETE ON DATABASE::[ NCloud ] BY [public]),
4 > ADD (SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP),
5 > ADD (SCHEMA_OBJECT_CHANGE_GROUP),
6 > ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
7 > ADD (DATABASE _CHANGE_GROUP),
8 > ADD (AUDIT_CHANGE_GROUP),
9 > ADD (USER_CHANGE_PASSWORD_GROUP),
10 > ADD (SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP),
11 > ADD (FAILED_DATABASE_AUTHENTICATION_GROUP),
12 > ADD (DATABASE_OBJECT_CHANGE_GROUP),
13 > ADD (DATABASE_ROLE_MEMBER_CHANGE_GROUP)
14 > WITH (STATE = ON)
15 > GO
1 > quit
```



Administrator: Windows PowerShell

```
1> CREATE DATABASE AUDIT SPECIFICATION [NP_DB-NCloud_Audit]
2> FOR SERVER AUDIT [NP_Audit]
3> ADD (DELETE ON DATABASE::[NCloud] BY [public]),
4> ADD (SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP),
5> ADD (SCHEMA_OBJECT_CHANGE_GROUP),
6> ADD (DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP),
7> ADD (DATABASE_CHANGE_GROUP),
8> ADD (USER_CHANGE_PASSWORD_GROUP),
9> ADD (AUDIT_CHANGE_GROUP),
10> ADD (SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP),
11> ADD (FAILED_DATABASE_AUTHENTICATION_GROUP),
12> ADD (DATABASE_OBJECT_CHANGE_GROUP),
13> ADD (DATABASE_ROLE_MEMBER_CHANGE_GROUP)
14> WITH (STATE = ON)
15> GO
1> quit
PS C:\> _
```

Replace the text shown in red with the database audit specification name.

```
1 > CREATE DATABASE AUDIT SPECIFICATION [NP_DB-NCloud_Audit]
```

Replace the text shown in red with the target database name.

```
3 > ADD (DELETE ON DATABASE::[NCloud] BY [public])
```

4.3 Event Log Configuration

This is an optional configuration.

The following sections describe configuration methods for Domain and Workgroup environments.

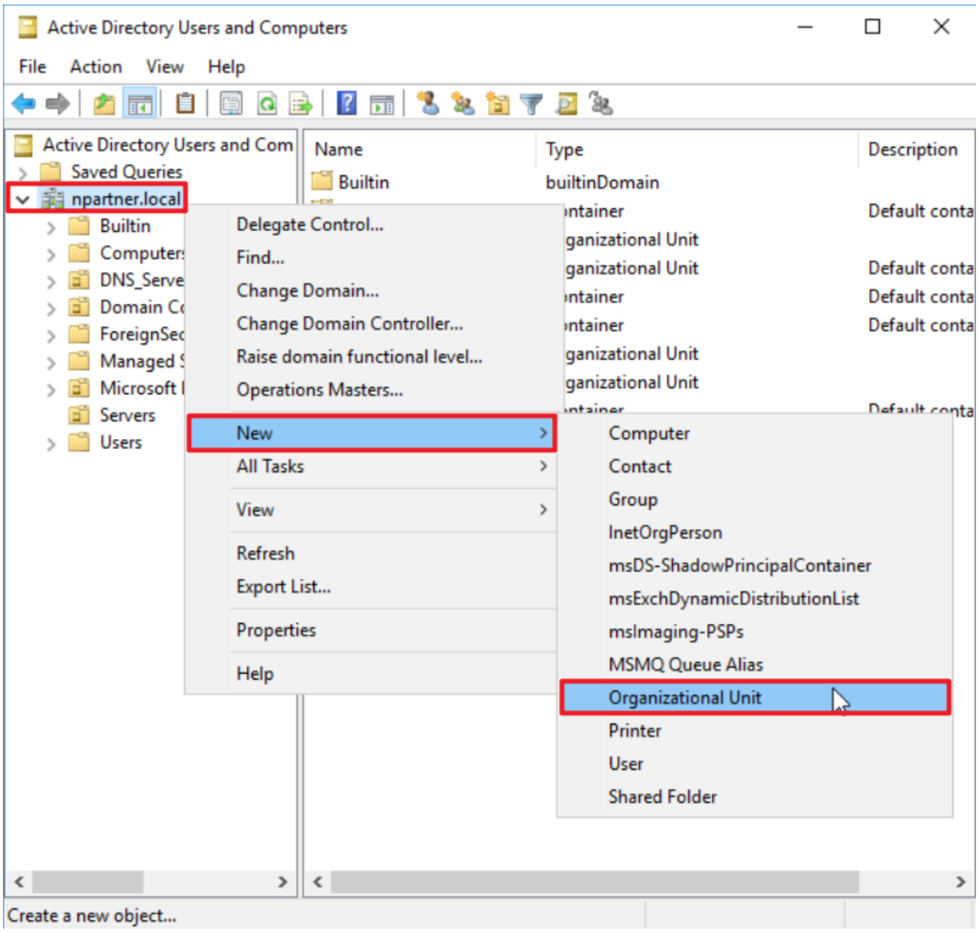
4.3.1 Domain

4.3.1.1 Organizational Unit (OU) Configuration

(1) Click “Active Directory Users and Computers.”

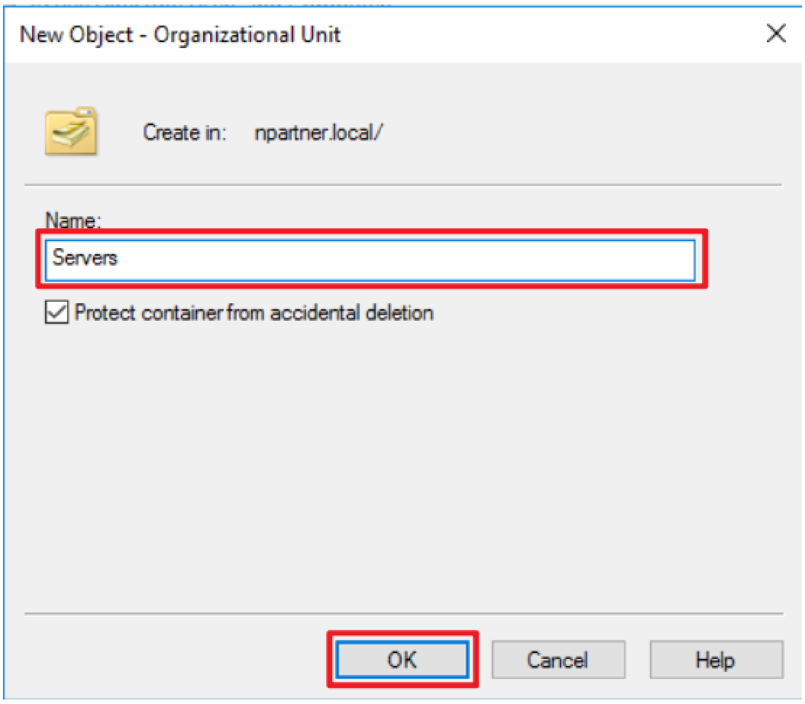
(2) Add an Organizational Unit

Right-click on “Domain Controllers, select “New,” and click “Organizational Unit.”



(3) Enter your Organizational Unit name: (in this example, it is “Servers”)

Note: Please create the organizational unit name according to the customer's environment. → click “OK.”



New Object - Organizational Unit

Create in: npartner.local/

Name:

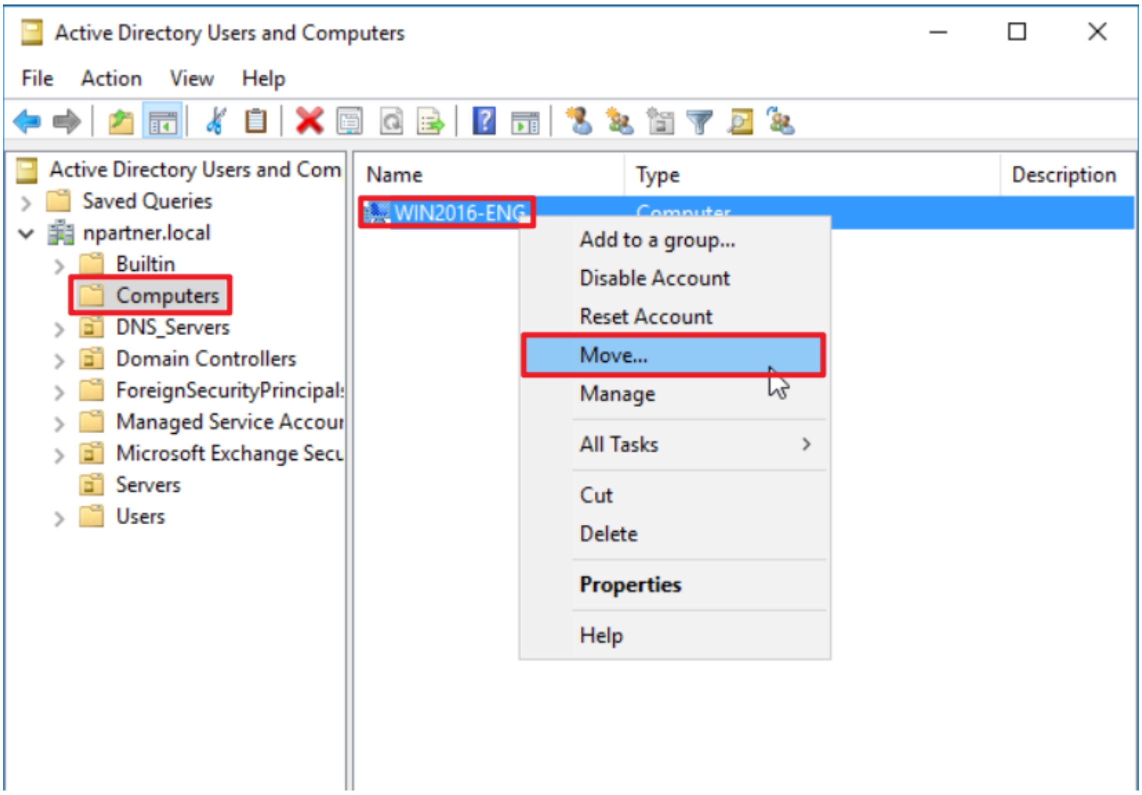
Servers

☑ Protect container from accidental deletion

(4) Move the Server to your New Organizational Unit:

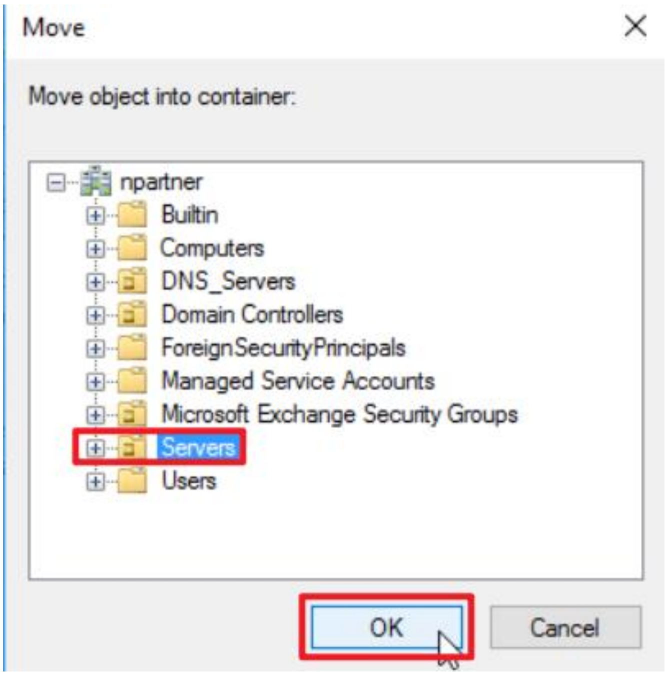
Select your organizational unit in “Domain Controllers” -> Right-click on the “WIN2016” server.

Note: Please select the MS SQL server according to the actual environment. → click “Move.”



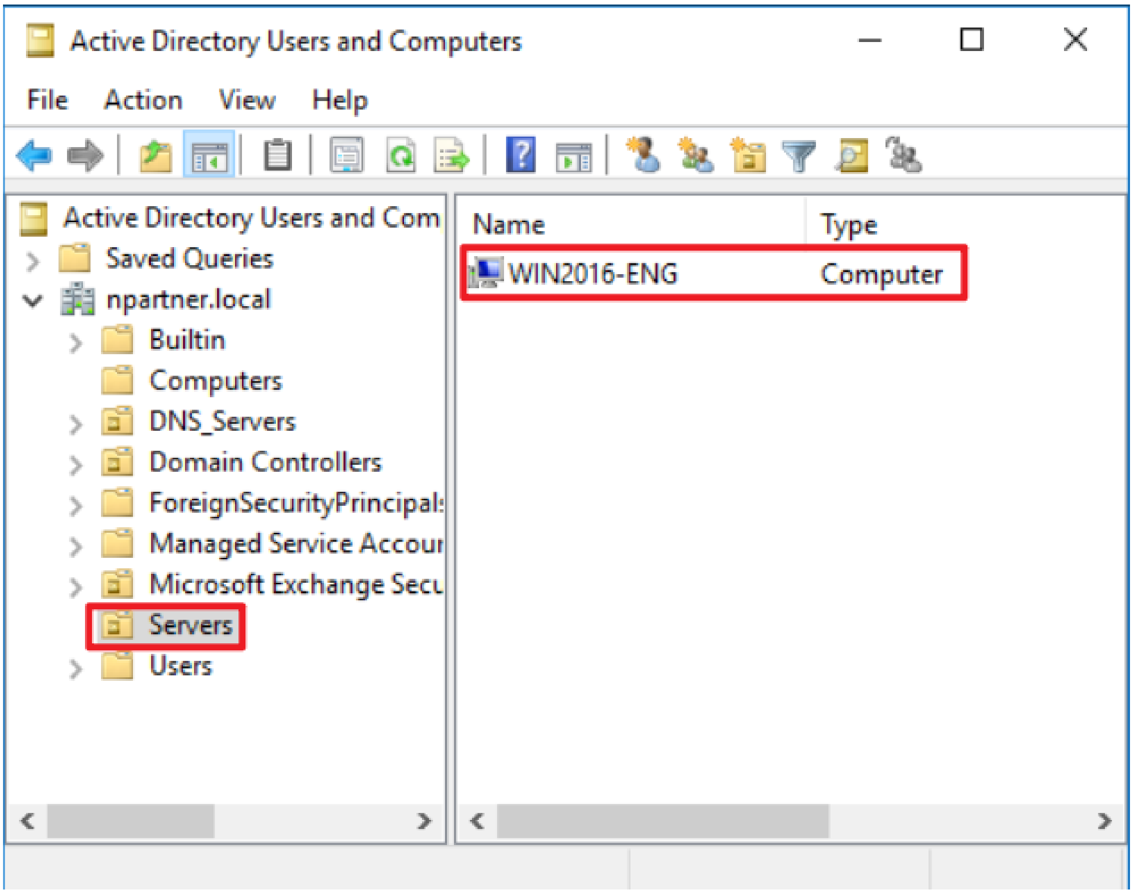
(5) Select your Organizational Unit:

Select your organizational unit (in this example, it is “Servers”) → click “OK.”



(6) Verify the Server Has Been Moved to your New Organizational Unit:

Expand your organizational unit folder (in this example, it is “Servers”) and confirm that the “WIN2016-ENG” server has been moved.



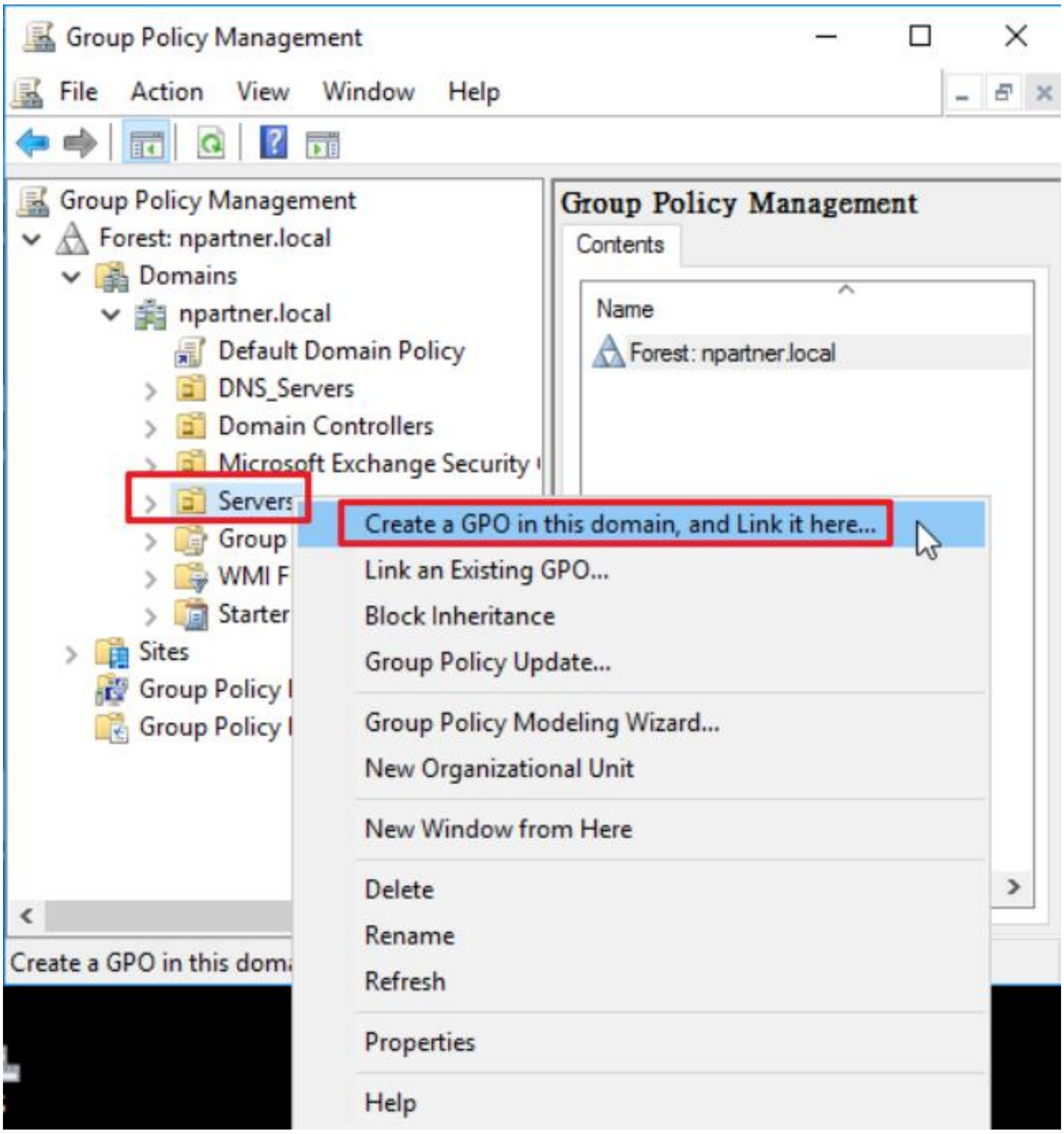
Name	Type
WIN2016-ENG	Computer

4.3.1.2 Group Policy Settings

(1) Click “Group Policy Management.”

(2) In the Servers organizational unit (OU), create a new Group Policy Object (GPO):

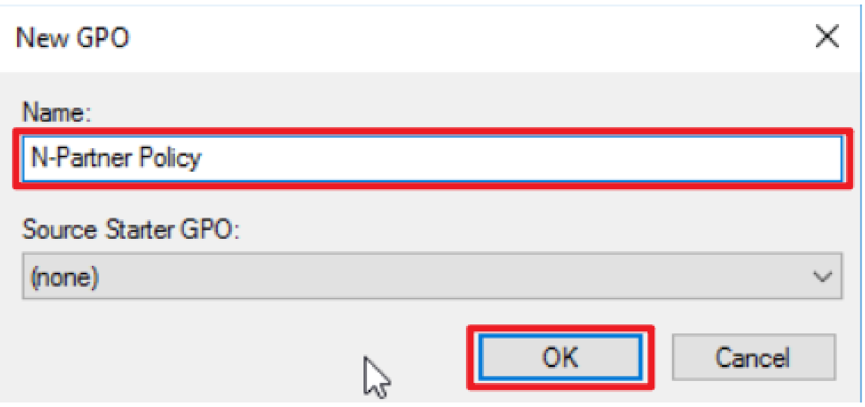
Right-click the [Servers] organizational unit → select “Create a GPO in this domain, and Link it here...”



(3) Edit your Group Policy Object

Enter your Group Policy Object name. (in this example, it is "N-Partner Policy")

Note: Create your GPO name according to the actual environment. Then click "Edit."



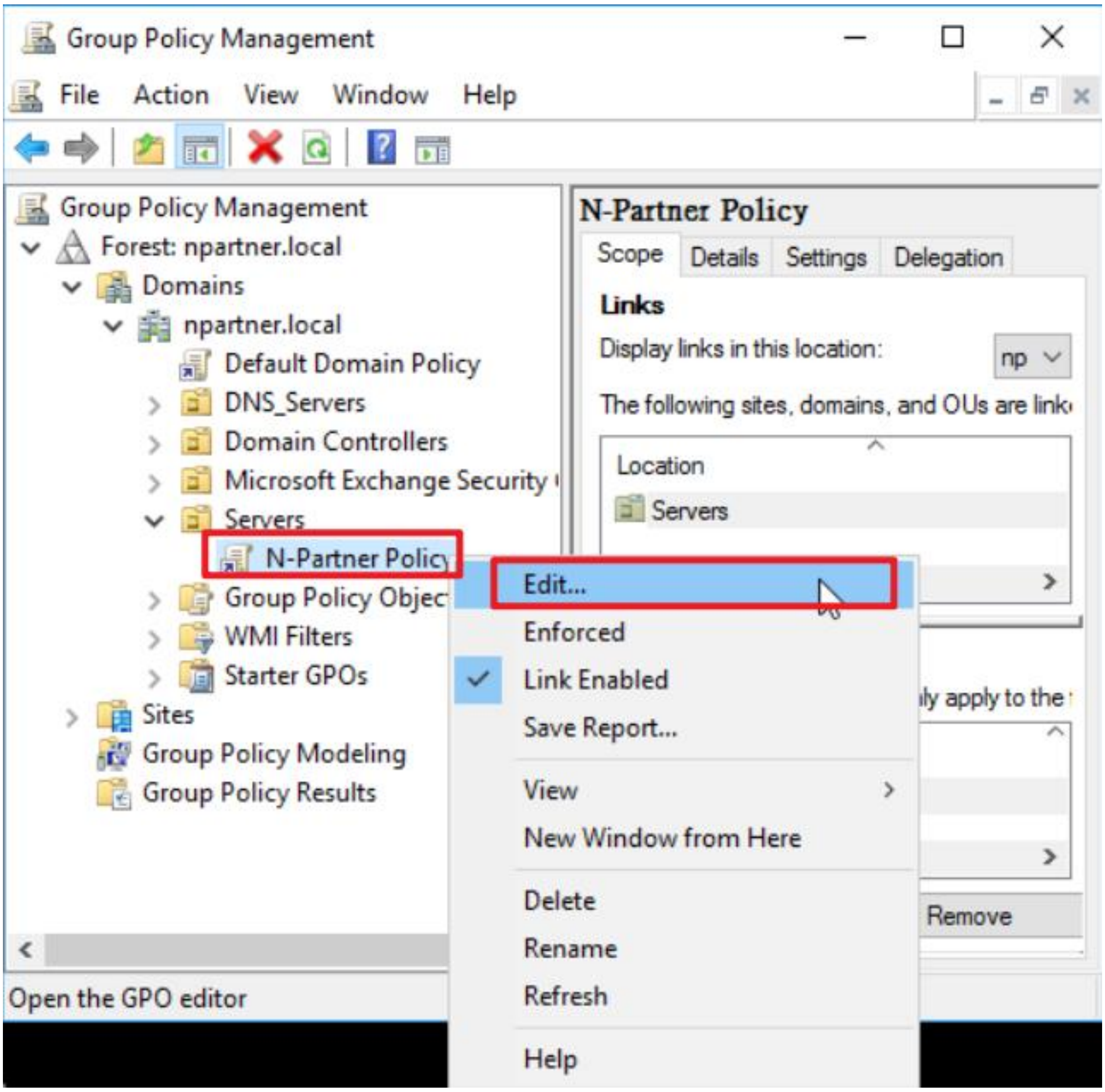
New GPO

Name: N-Partner Policy

Source Starter GPO: (none)

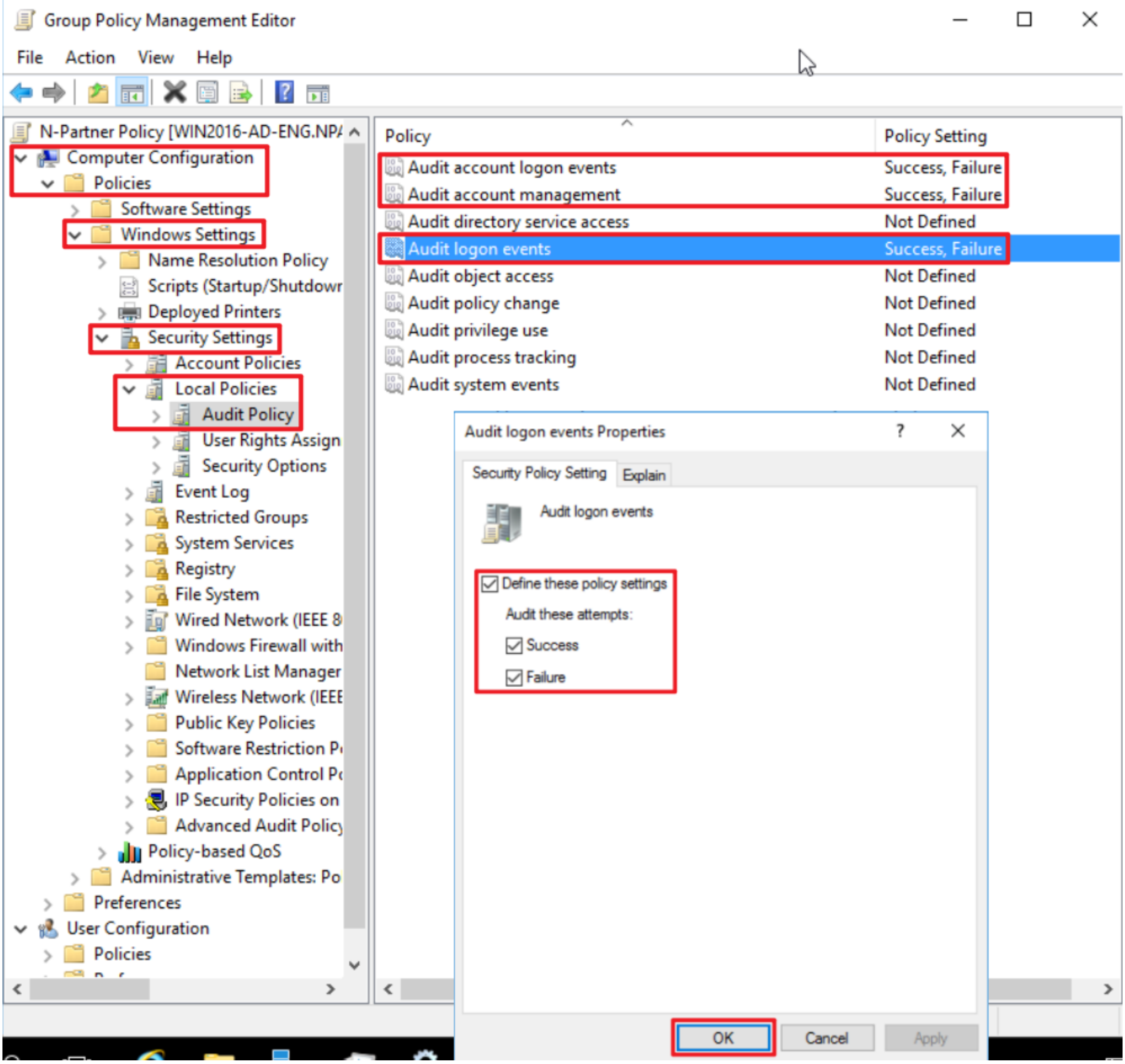
(4) Edit your Group Policy Object

In your group policy object, (in this example, it is "N-Partner Policy")
right-click and select "Edit."



(5) Local Group Policies: Audit Policy

Expand folder “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Local Policies” → “Audit Policy.” And click on “Audit account logon events,” “Audit account management,” and “Audit logon events,” → check “Define these policy settings”: Success, Failure. → click “OK.”



Policy	Policy Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Not Defined
Audit logon events	Success, Failure
Audit object access	Not Defined
Audit policy change	Not Defined
Audit privilege use	Not Defined
Audit process tracking	Not Defined
Audit system events	Not Defined

Audit logon events Properties

Security Policy Setting | Explain

Audit logon events

☑ Define these policy settings

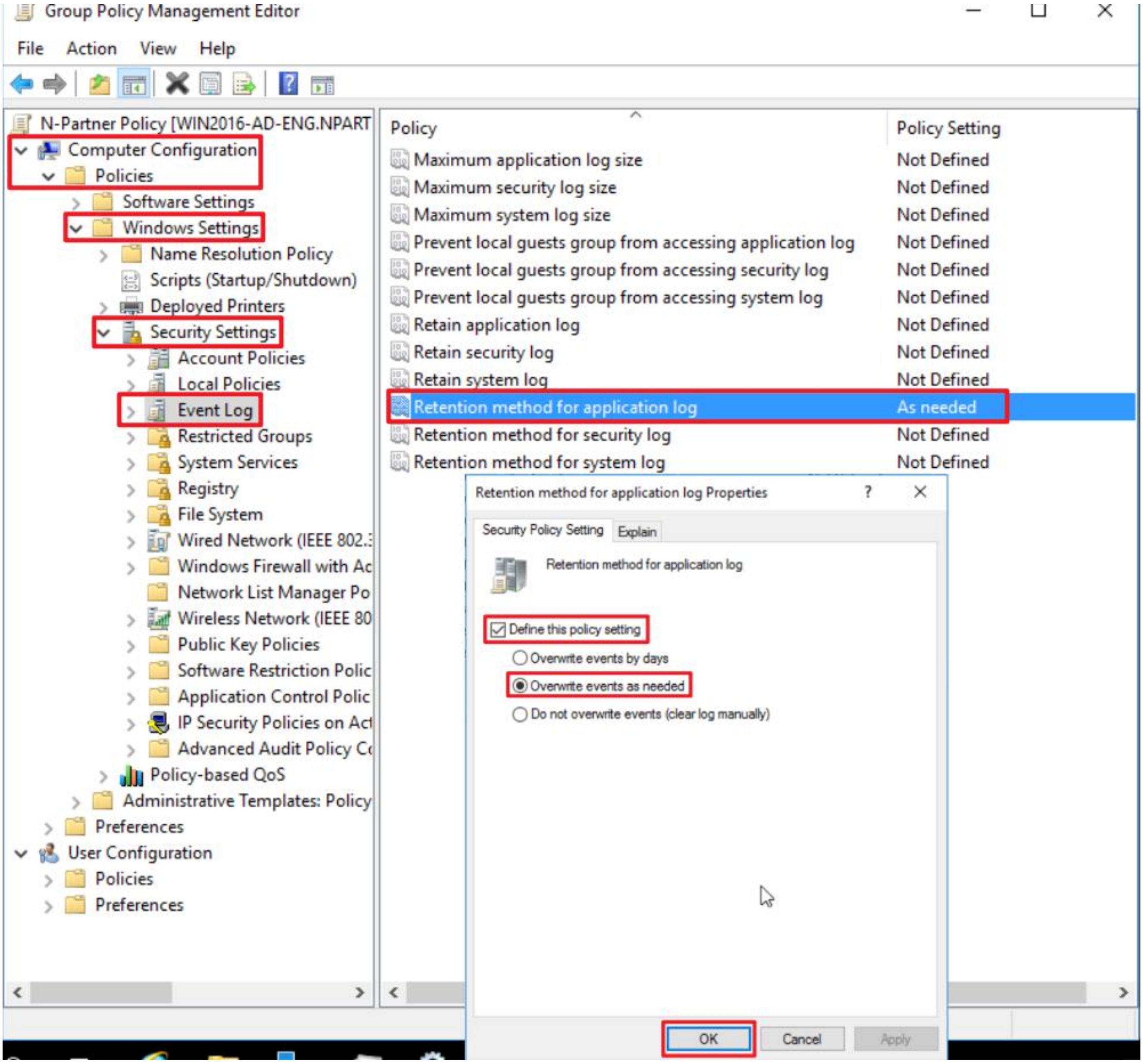
Audit these attempts:

☑ Success

☑ Failure

(6) Event Log: Application Log Retention Method

Expand “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” → select “Retention method for application log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



Group Policy Management Editor

Policy	Policy Setting
Maximum application log size	Not Defined
Maximum security log size	Not Defined
Maximum system log size	Not Defined
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	As needed
Retention method for security log	Not Defined
Retention method for system log	Not Defined

Retention method for application log Properties

Retention method for application log

☑ Define this policy setting

○ Overwrite events by days

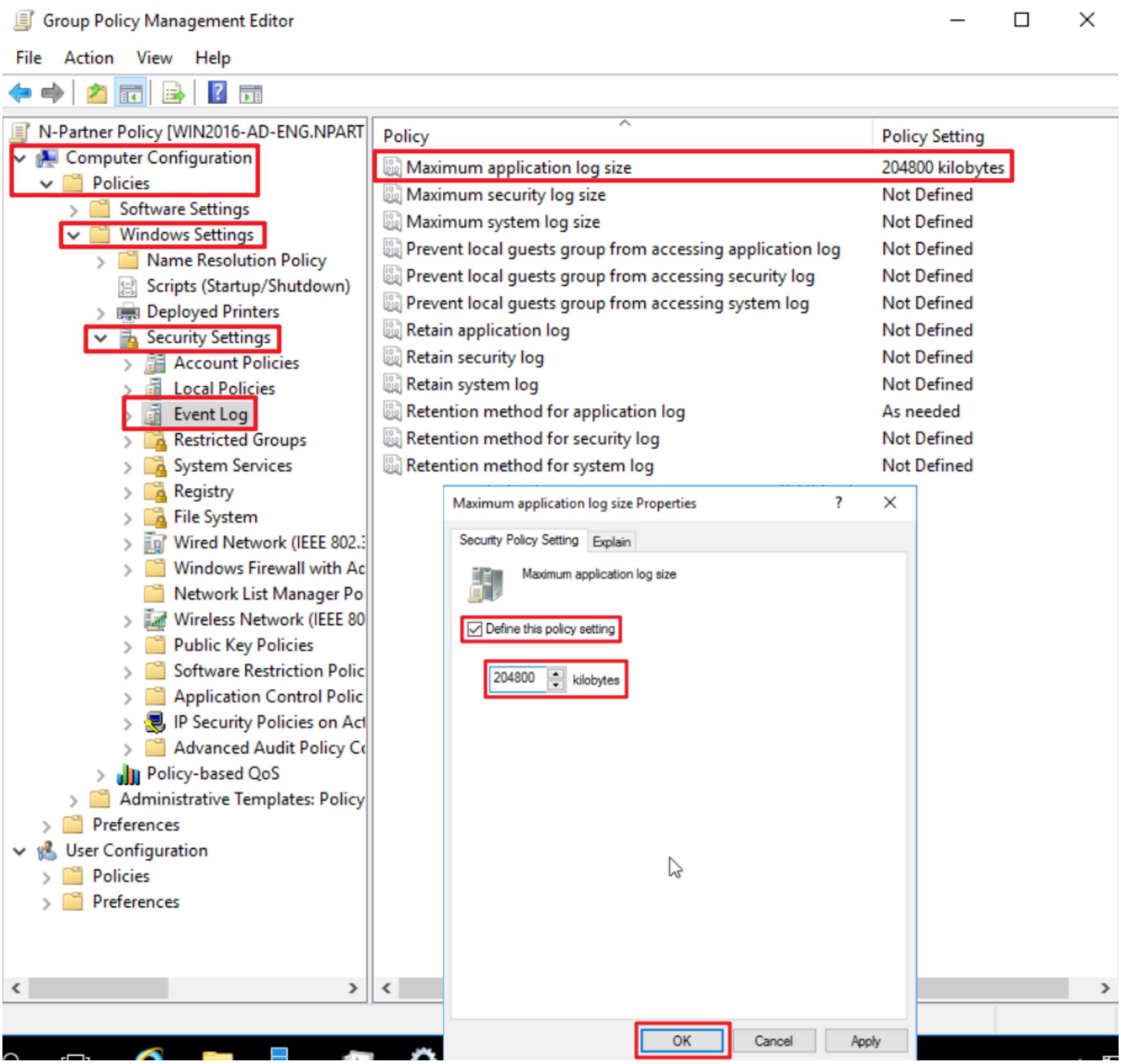
● Overwrite events as needed

○ Do not overwrite events (clear log manually)

(7) Event Logs: Maximum Size of Security Log

Expand folder “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” →And click on “Maximum application log size” → Check “Define this policy setting” → enter 204800 KB

Note: Please adjust the number based on the actual environment. → click “OK.”



Policy	Policy Setting
Maximum application log size	204800 kilobytes
Maximum security log size	Not Defined
Maximum system log size	Not Defined
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	As needed
Retention method for security log	Not Defined
Retention method for system log	Not Defined

Maximum application log size Properties

Security Policy Setting | Explain

Maximum application log size

☑ Define this policy setting

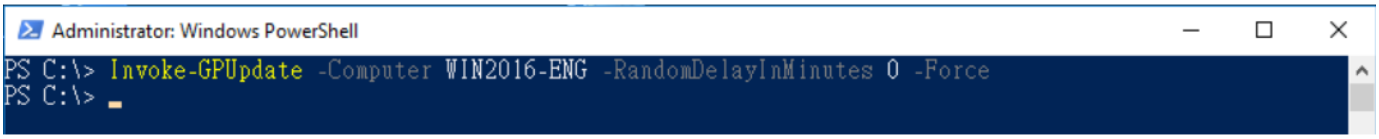
204800 kilobytes

OK | Cancel | Apply

(8) On the AD domain server, open “Windows PowerShell.”

(9) Enter the command below to refresh group policy.

```
PS C:\> Invoke-GPUpdate -Computer WIN2016-ENG -RandomDelayInMinutes 0 -Force
```

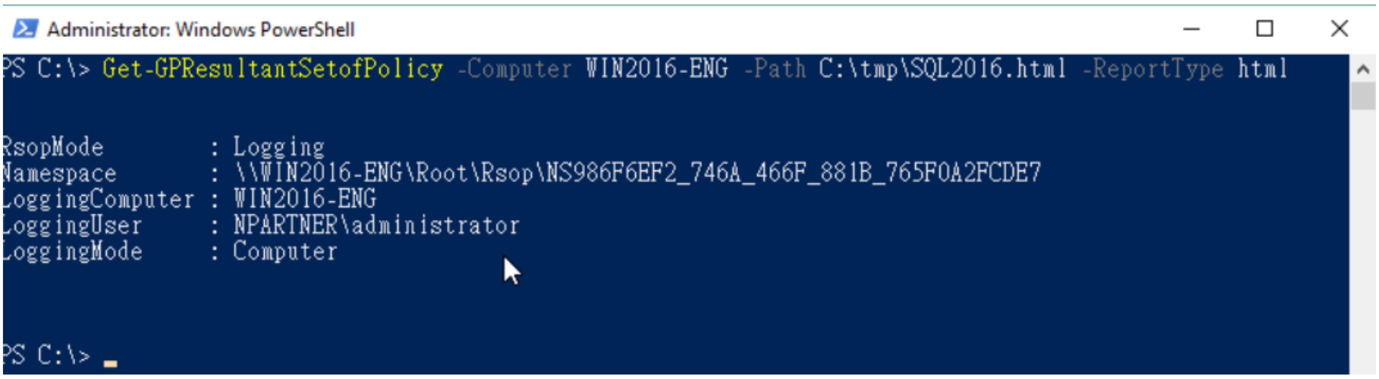


```
PS C:\> Invoke-GPUpdate -Computer WIN2016-ENG -RandomDelayInMinutes 0 -Force
PS C:\> _
```

Replace the text shown in red with the MS SQL server name.

(10) Enter the command below to generate server group policy report.

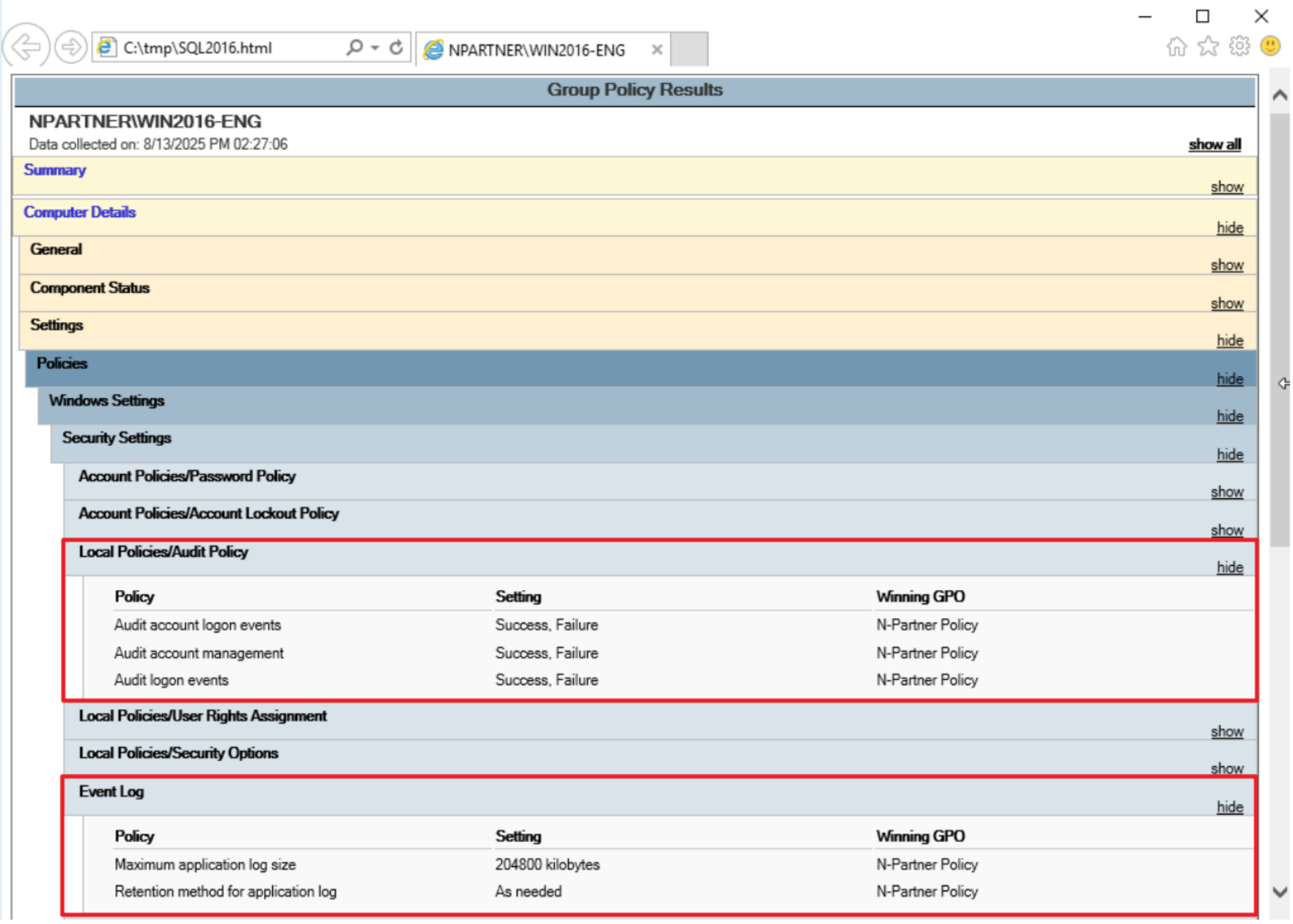
```
PS C:\> Get-GPResultantSetofPolicy -Computer WIN2016-ENG -Path C:\tmp\SQL2016.html -ReportType html
```



```
PS C:\> Get-GPResultantSetofPolicy -Computer WIN2016-ENG -Path C:\tmp\SQL2016.html -ReportType html


RsopMode        : Logging
Namespace       : \\WIN2016-ENG\Root\Rsop\NS986F6EF2_746A_466F_881B_765F0A2FCDE7
LoggingComputer : WIN2016-ENG
LoggingUser     : NPARTNER\administrator
LoggingMode     : Computer



PS C:\> _
```

For the red text , please enter the MS SQL server name and the folder path/file name.

(11) Open the report and verify that your MS SQL server is applying the N-Partner Policy Group Policy.



Group Policy Results

NPARTNER\WIN2016-ENG

Data collected on: 8/13/2025 PM 02:27:06 show all

Summary show

Computer Details hide

General show

Component Status show

Settings hide

Policies hide

Windows Settings hide

Security Settings hide

Account Policies/Password Policy show

Account Policies/Account Lockout Policy show

Local Policies/Audit Policy hide

Policy	Setting	Winning GPO
Audit account logon events	Success, Failure	N-Partner Policy
Audit account management	Success, Failure	N-Partner Policy
Audit logon events	Success, Failure	N-Partner Policy

Local Policies/User Rights Assignment show

Local Policies/Security Options show

Event Log hide

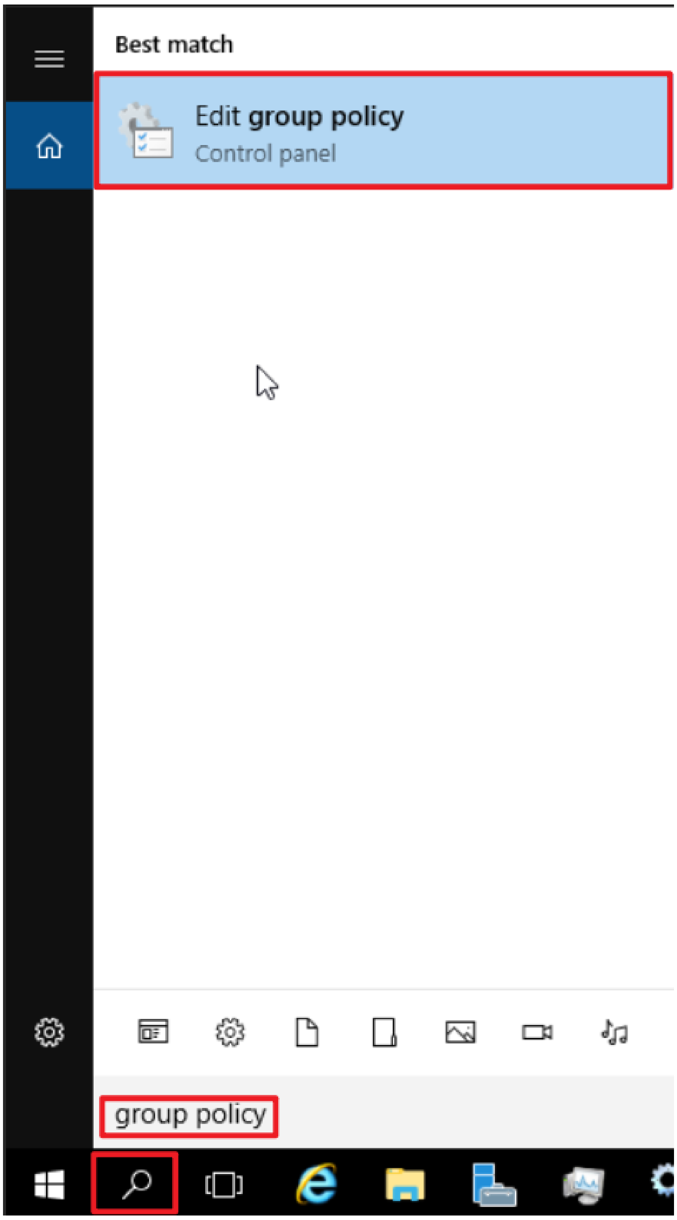
Policy	Setting	Winning GPO
Maximum application log size	204800 kilobytes	N-Partner Policy
Retention method for application log	As needed	N-Partner Policy

4.3.2 Workgroup

4.3.2.1 Audit Policy Configuration

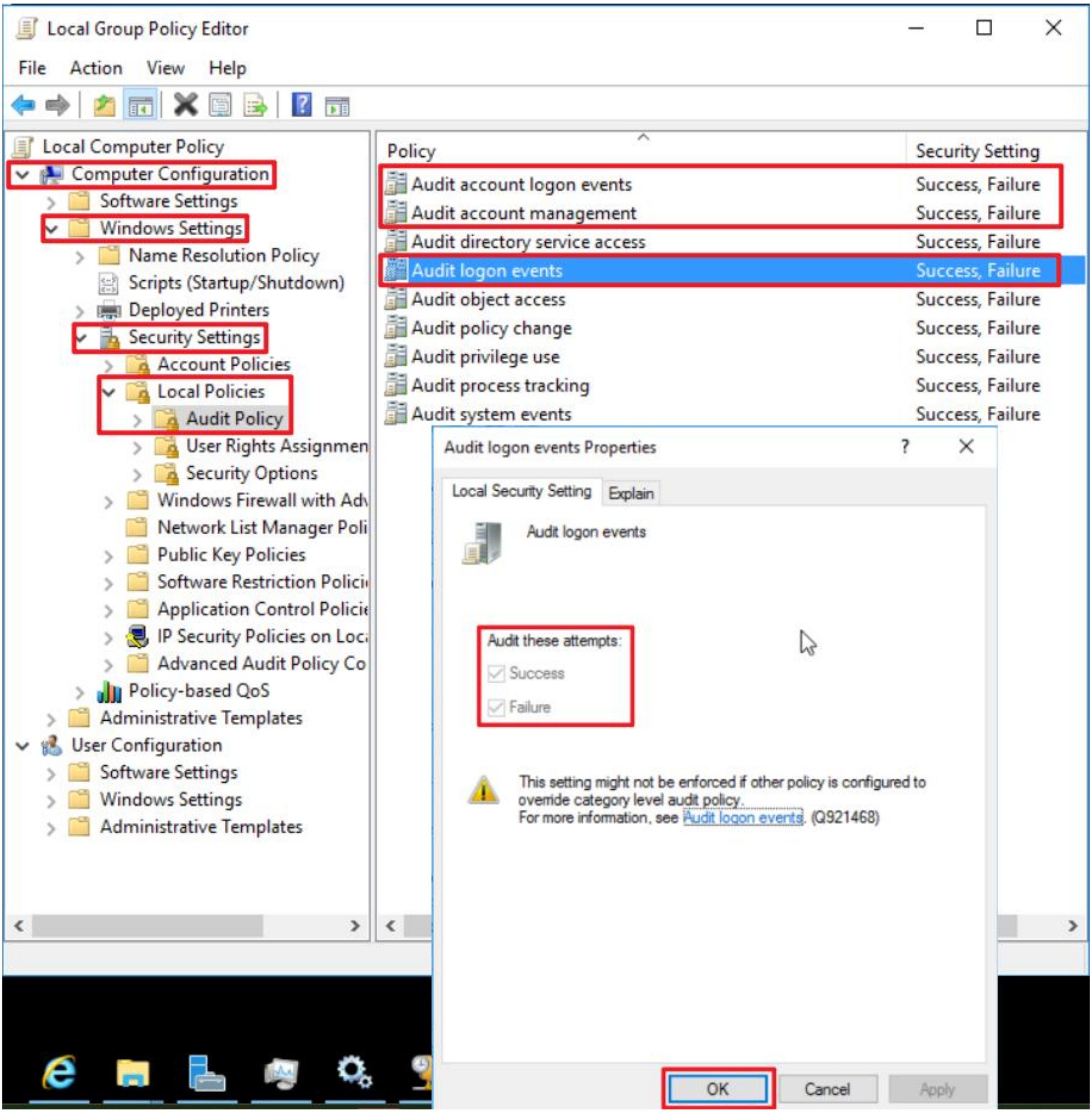
(1) Open Local Group Policy Editor

Click on “Start” → enter “group policy” to search → click on “Edit Group Policy.”



(2) Local Group Policies: Audit Policy

Expand folder “Computer Configuration” → “Windows Settings” → “Security Settings” -> “Local Policies” → “Audit Policy.” And click on “Audit account logon events,” “Audit account management,” and “Audit logon events” items → check “Define these policy settings”: Success, Failure. → click “OK.”



Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	Success, Failure
Audit system events	Success, Failure

Audit logon events Properties

Audit logon events

Audit these attempts:

☑ Success

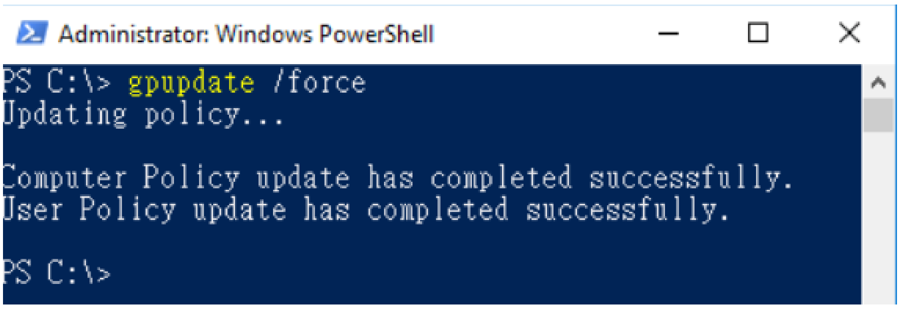
☑ Failure

This setting might not be enforced if other policy is configured to override category level audit policy.
For more information, see Audit logon events. (Q921468)

(3) Open “Windows PowerShell.”

(4) Enter the command below to refresh group policy.

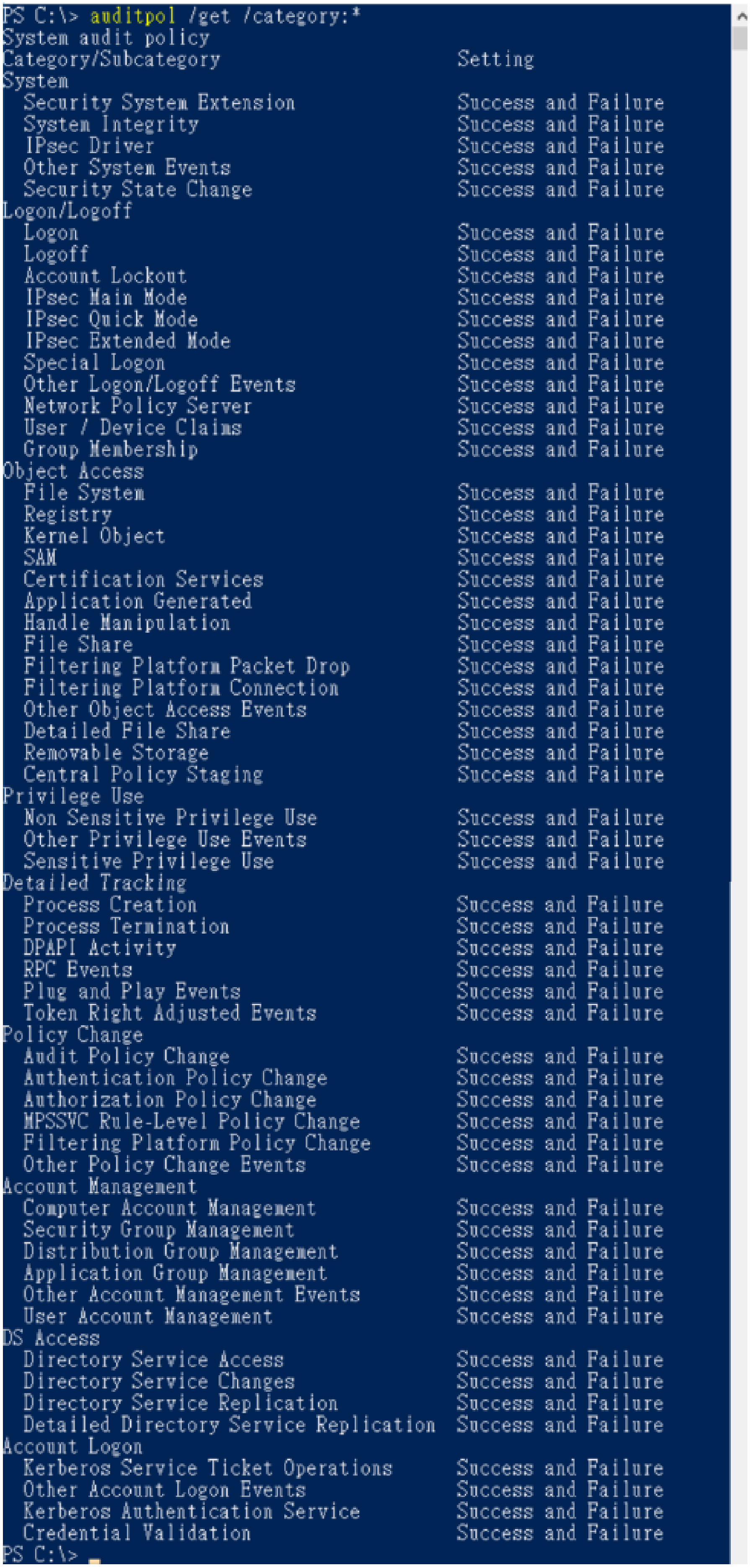
```
PS C:\> gpupdate /force
```



```
PS C:\> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

PS C:\>
```

(5) Enter the command below to view group policy applied status.

```
PS C: \> auditpol /get /category:*
```

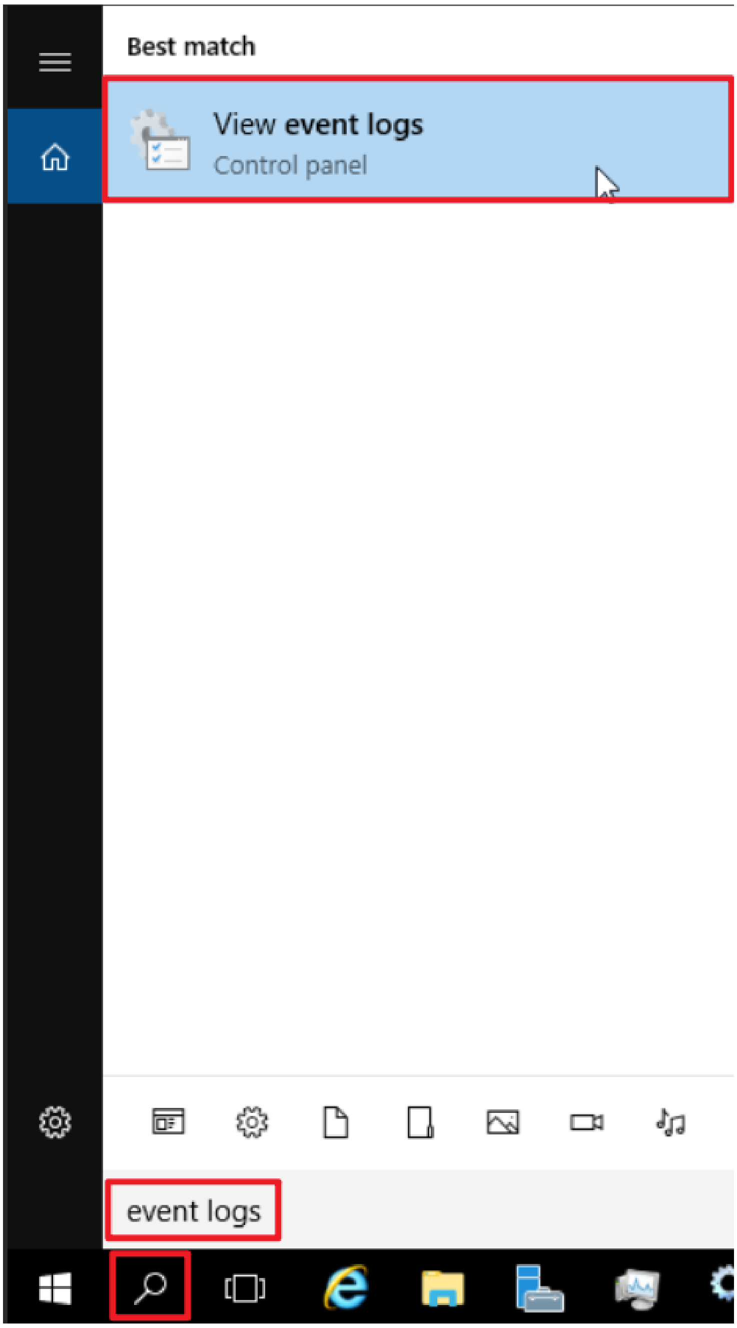


```
PS C:\> auditpol /get /category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               Success and Failure
  System Integrity                        Success and Failure
  IPsec Driver                            Success and Failure
  Other System Events                     Success and Failure
  Security State Change                   Success and Failure
Logon/Logoff
  Logon                                   Success and Failure
  Logoff                                  Success and Failure
  Account Lockout                         Success and Failure
  IPsec Main Mode                         Success and Failure
  IPsec Quick Mode                        Success and Failure
  IPsec Extended Mode                     Success and Failure
  Special Logon                           Success and Failure
  Other Logon/Logoff Events               Success and Failure
  Network Policy Server                   Success and Failure
  User / Device Claims                    Success and Failure
  Group Membership                        Success and Failure
Object Access
  File System                             Success and Failure
  Registry                                Success and Failure
  Kernel Object                           Success and Failure
  SAM                                     Success and Failure
  Certification Services                  Success and Failure
  Application Generated                   Success and Failure
  Handle Manipulation                     Success and Failure
  File Share                              Success and Failure
  Filtering Platform Packet Drop          Success and Failure
  Filtering Platform Connection           Success and Failure
  Other Object Access Events              Success and Failure
  Detailed File Share                     Success and Failure
  Removable Storage                       Success and Failure
  Central Policy Staging                  Success and Failure
Privilege Use
  Non Sensitive Privilege Use             Success and Failure
  Other Privilege Use Events              Success and Failure
  Sensitive Privilege Use                 Success and Failure
Detailed Tracking
  Process Creation                        Success and Failure
  Process Termination                     Success and Failure
  DPAPI Activity                          Success and Failure
  RPC Events                              Success and Failure
  Plug and Play Events                    Success and Failure
  Token Right Adjusted Events             Success and Failure
Policy Change
  Audit Policy Change                     Success and Failure
  Authentication Policy Change            Success and Failure
  Authorization Policy Change             Success and Failure
  MPSSVC Rule-Level Policy Change         Success and Failure
  Filtering Platform Policy Change        Success and Failure
  Other Policy Change Events              Success and Failure
Account Management
  Computer Account Management             Success and Failure
  Security Group Management               Success and Failure
  Distribution Group Management           Success and Failure
  Application Group Management            Success and Failure
  Other Account Management Events         Success and Failure
  User Account Management                 Success and Failure
DS Access
  Directory Service Access                Success and Failure
  Directory Service Changes               Success and Failure
  Directory Service Replication           Success and Failure
  Detailed Directory Service Replication  Success and Failure
Account Logon
  Kerberos Service Ticket Operations      Success and Failure
  Other Account Logon Events              Success and Failure
  Kerberos Authentication Service         Success and Failure
  Credential Validation                   Success and Failure
PS C:\>
```

4.3.2.2 Event Log Settings

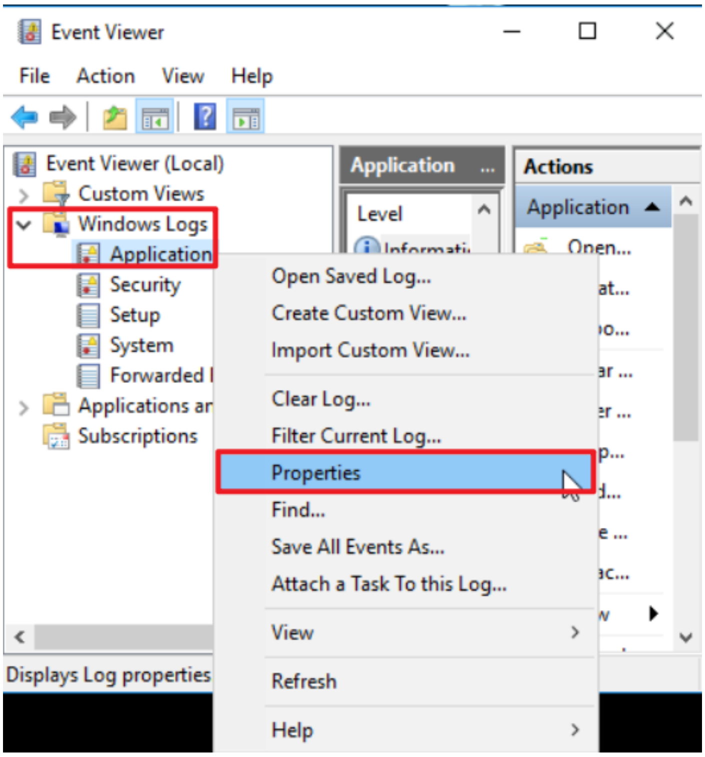
(1) Search for “Event Viewer”

Enter “Event Viewer” to search → click on “Event Viewer” in the search results.



(2) Edit Security Log

Expand folder “Windows Logs” → right-click on “Application” → And click on “Properties.”

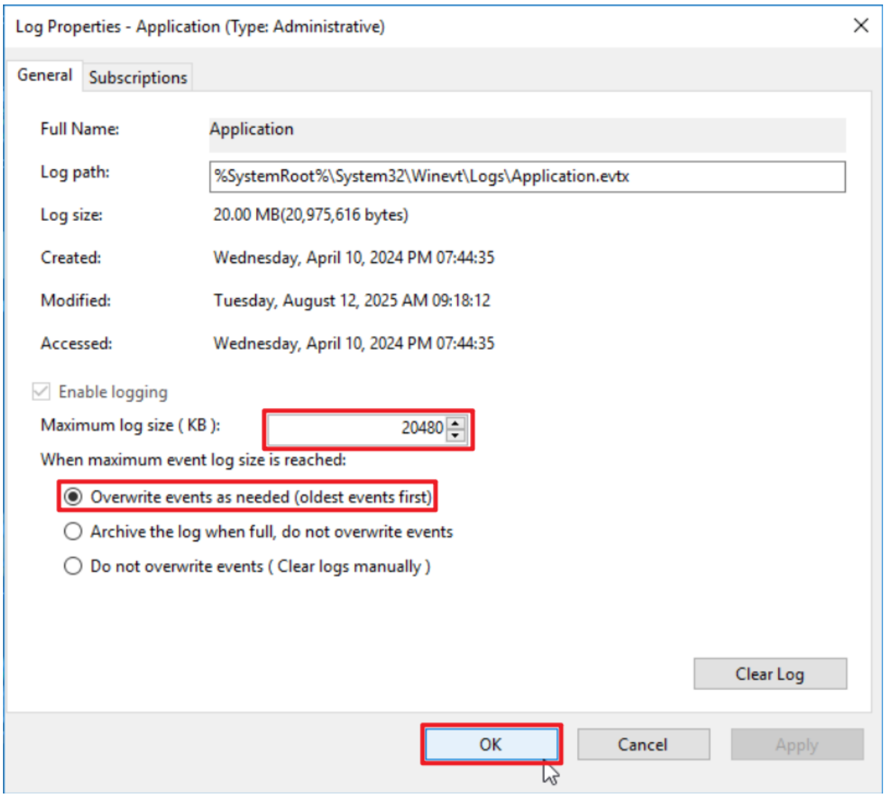


(3) Configure Security Log

Enter maximum log file size: 204800 KB

Note: Please adjust the number according to the actual environment.

→ click on “Overwrite events as needed (oldest events first)” → click “OK.”


Log Properties - Application (Type: Administrative)

General Subscriptions

Full Name: Application

Log path: %SystemRoot%\System32\Winevt\Logs\Application.evtx

Log size: 20.00 MB(20,975,616 bytes)

Created: Wednesday, April 10, 2024 PM 07:44:35

Modified: Tuesday, August 12, 2025 AM 09:18:12

Accessed: Wednesday, April 10, 2024 PM 07:44:35

☑ Enable logging

Maximum log size (KB): 20480

When maximum event log size is reached:

● Overwrite events as needed (oldest events first)

○ Archive the log when full, do not overwrite events

○ Do not overwrite events (Clear logs manually)

5. SQL Server 2019

5.1 Login Auditing

Enable login auditing to monitor SQL Server Database Engine login activities.

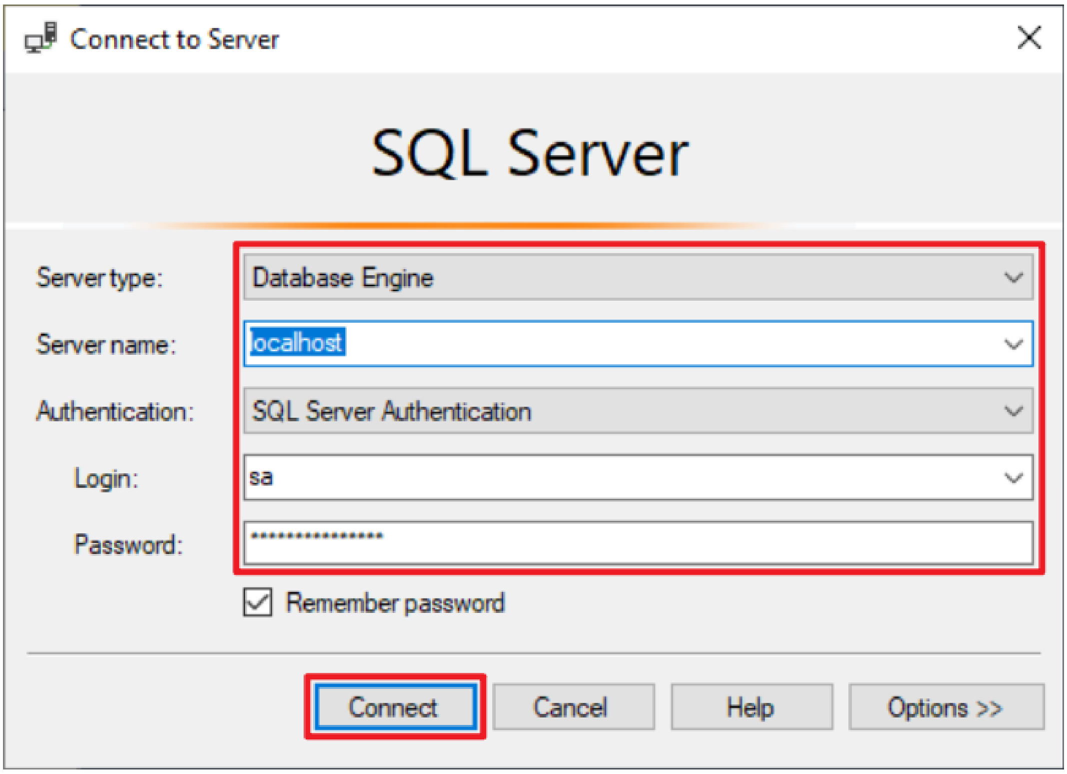
After configuration, the MS SQL Server service must be **restarted**.

The following sections describe how to configure login auditing using both the graphical user interface (GUI) and command-line interface (CLI).

5.1.1 Configuring via Graphical User Interface (GUI)

(1) Open "SQL Server Management Studio (SSMS)."

(2) Enter the server's name → select the authentication method → click "Connect."



Connect to Server

SQL Server

Server type: Database Engine

Server name: localhost

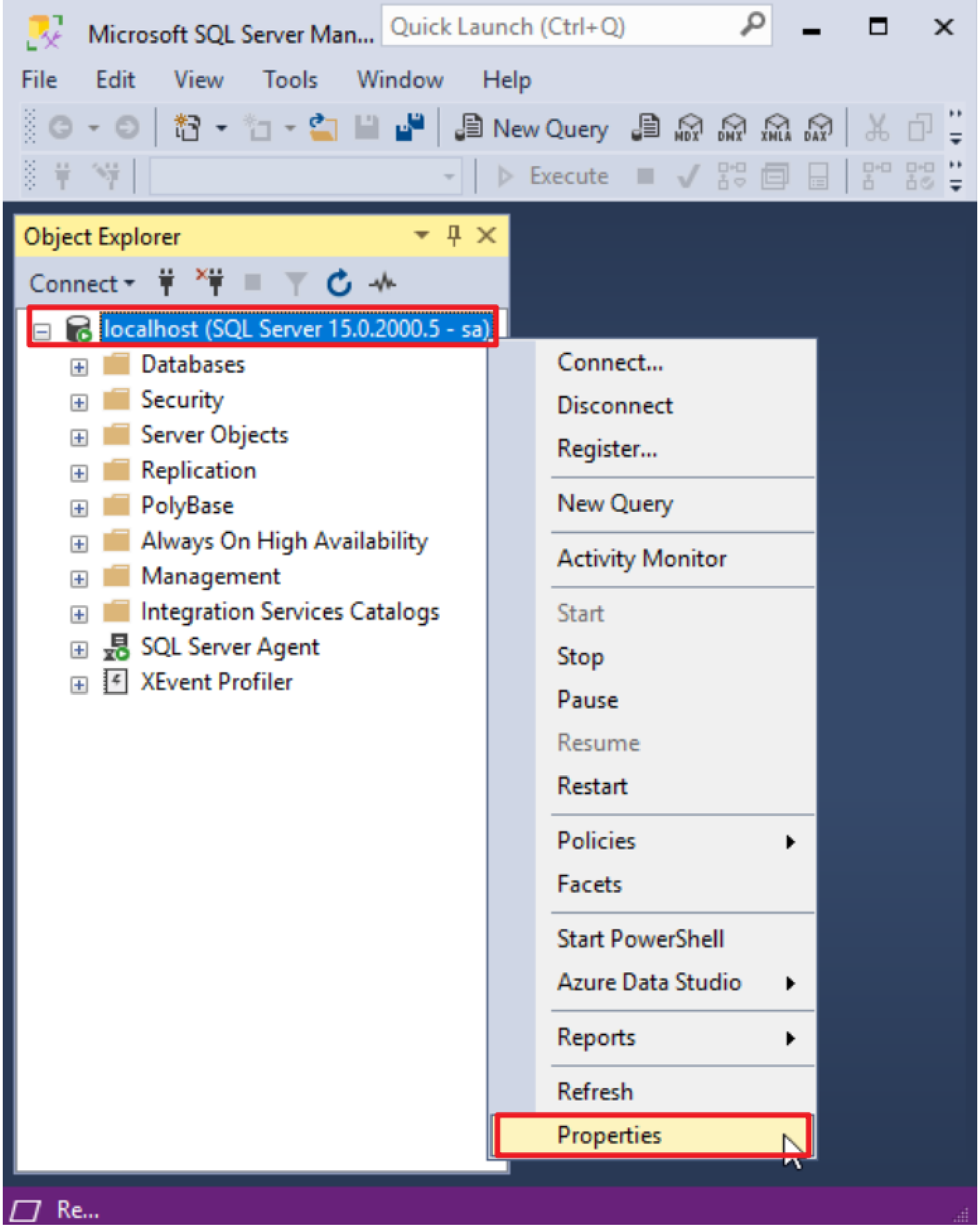
Authentication: SQL Server Authentication

Login: sa

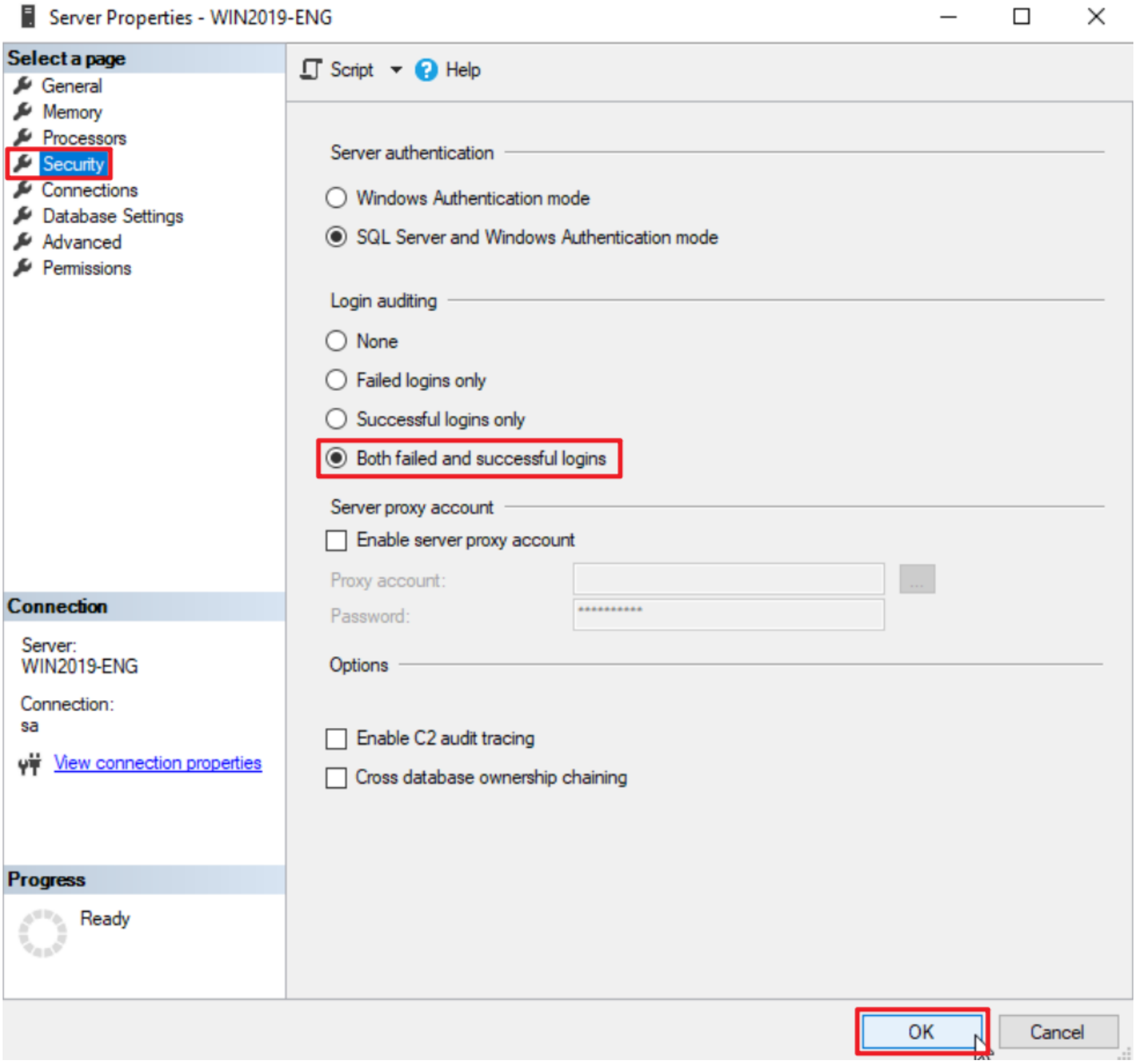
Password: ***************

☑ Remember password

(3) In [Server Name] (the example here is SQL Server 15.0.2000.5), right-click and select “Properties.”



(4) On the Security page, under Login auditing, select “Both failed and successful logins” → click “OK”.



Server Properties - WIN2019-ENG

Server authentication

○ Windows Authentication mode

● SQL Server and Windows Authentication mode

Login auditing

○ None

○ Failed logins only

○ Successful logins only

● Both failed and successful logins

Server proxy account

□ Enable server proxy account

Proxy account:

Password: ***********

Options

□ Enable C2 audit tracing

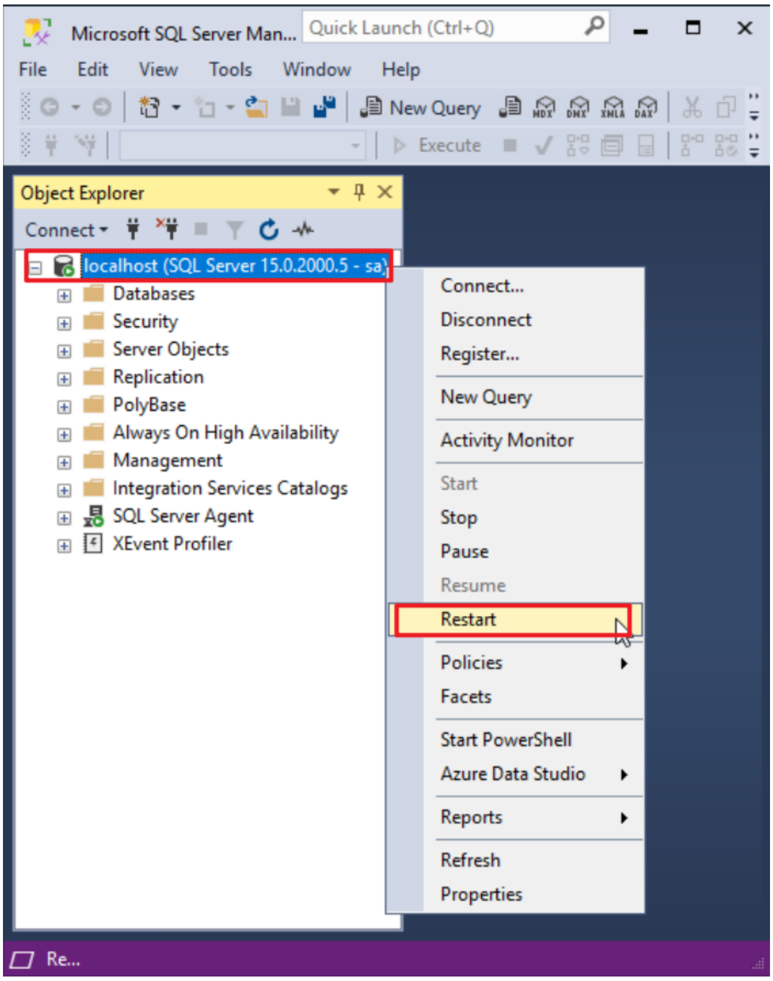
□ Cross database ownership chaining

Connection

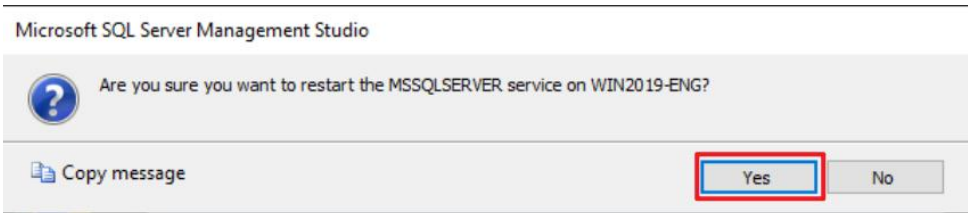
Server:
WIN2019-ENG

Connection:
sa

(5) Restart the MS SQL Server service: right-click [Server Name] (the example here is SQL Server 15.0.2000.5) → select "Restart."



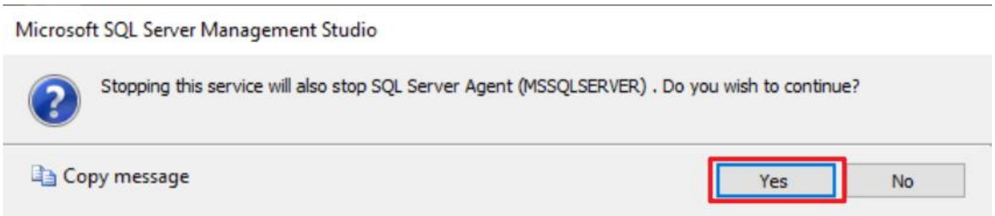
(6) Click "Yes" to restart the MS SQL Server service.



Microsoft SQL Server Management Studio

Are you sure you want to restart the MSSQLSERVER service on WIN2019-ENG?

(7) Click "Yes" again to stop the SQL Server Agent service.

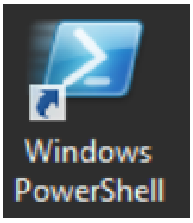


Microsoft SQL Server Management Studio

Stopping this service will also stop SQL Server Agent (MSSQLSERVER) . Do you wish to continue?

5.1.2 Configuring via Command-Line Interface (CLI)

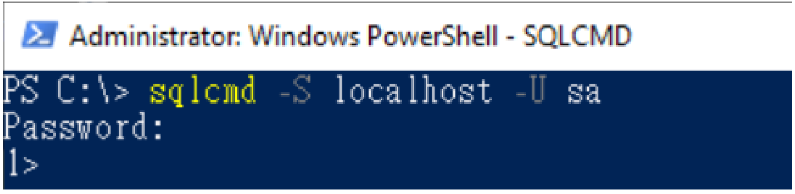
(1) Open “Windows PowerShell.”



(2) Enter the command below to log in using sa:

<2.1>Using sa account:

```
PS C:\> sqlcmd -S localhost -U sa
```



```
PS C:\> sqlcmd -S localhost -U sa
Password:
1>
```

Options:

-S [protocol:]server[instance_name][,port]

-U login_id

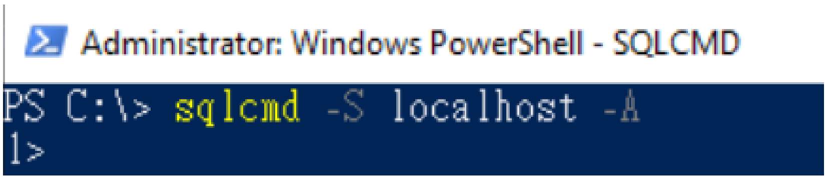
-P password

-A dedicated administrator connection

<2.2> Using Windows account:

Enter the command below to log in using Windows:

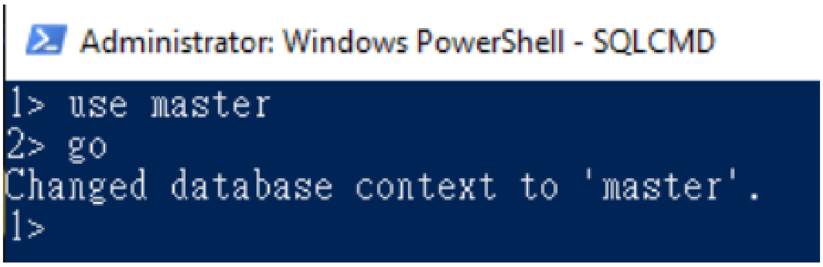
```
PS C:\> sqlcmd -S localhost -A
```



```
PS C:\> sqlcmd -S localhost -A
1>
```

(3) Enter the command below to switch to the **master** database:

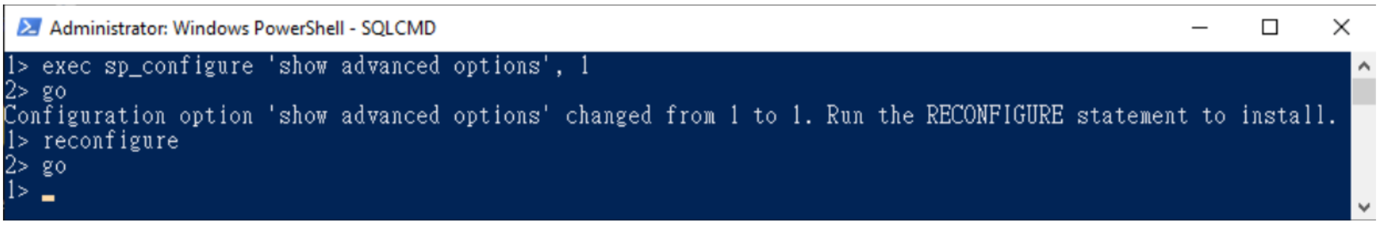
```
1 > use master
2 > go
```



```
1> use master
2> go
Changed database context to 'master'.
1>
```

(4) Enter the command below to enable advanced options:

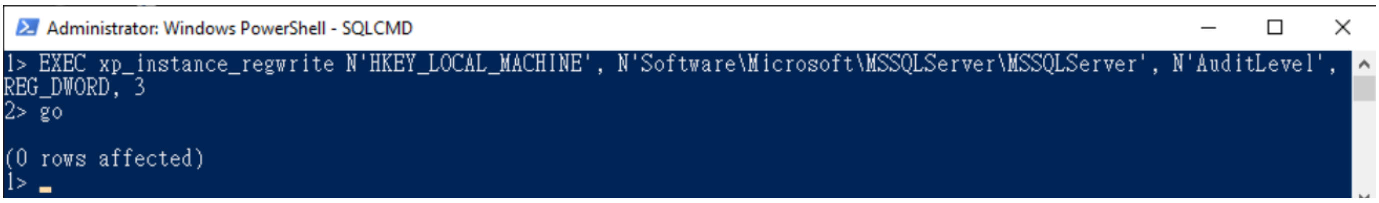
```
1 > exec sp_configure 'show advanced options', 1
2 > go
1 > reconfigure
2 > go
```



```
1> exec sp_configure 'show advanced options', 1
2> go
Configuration option 'show advanced options' changed from 1 to 1. Run the RECONFIGURE statement to install.
1> reconfigure
2> go
1> _
```

(5) Enter the command below to enable auditing for both failed and successful logins:

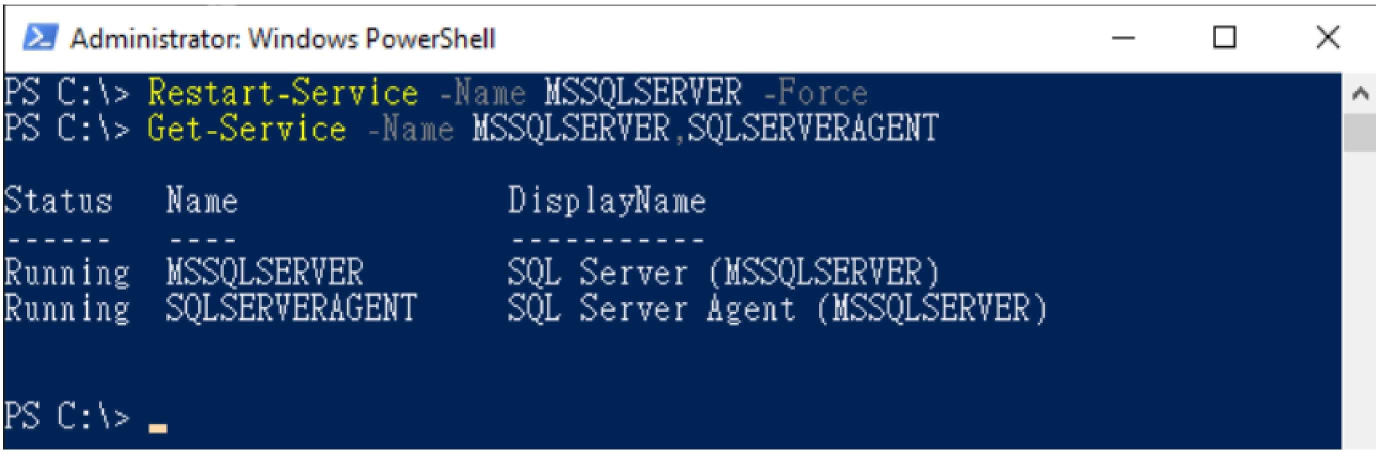
```
1 > EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE',
N'Software\Microsoft\MSSQLServer\MSSQLServer', N'AuditLevel', REG_DWORD, 3
2 > go
```



```
1> EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'Software\Microsoft\MSSQLServer\MSSQLServer', N'AuditLevel',
REG_DWORD, 3
2> go

(0 rows affected)
1> _
```

(6) Enter the command below to restart the MS SQL Server services:

```
PS C:\> Restart-Service -Name MSSQLSERVER -Force
PS C:\> Get-Service -Name MSSQLSERVER,SQLSERVERAGENT
```



```
PS C:\> Restart-Service -Name MSSQLSERVER -Force
PS C:\> Get-Service -Name MSSQLSERVER,SQLSERVERAGENT

Status   Name               DisplayName
------   ----               -----------
Running  MSSQLSERVER        SQL Server (MSSQLSERVER)
Running  SQLSERVERAGENT     SQL Server Agent (MSSQLSERVER)


PS C:\> _
```

5.2 Configuring Auditing

5.2.1 Server-Level Audit

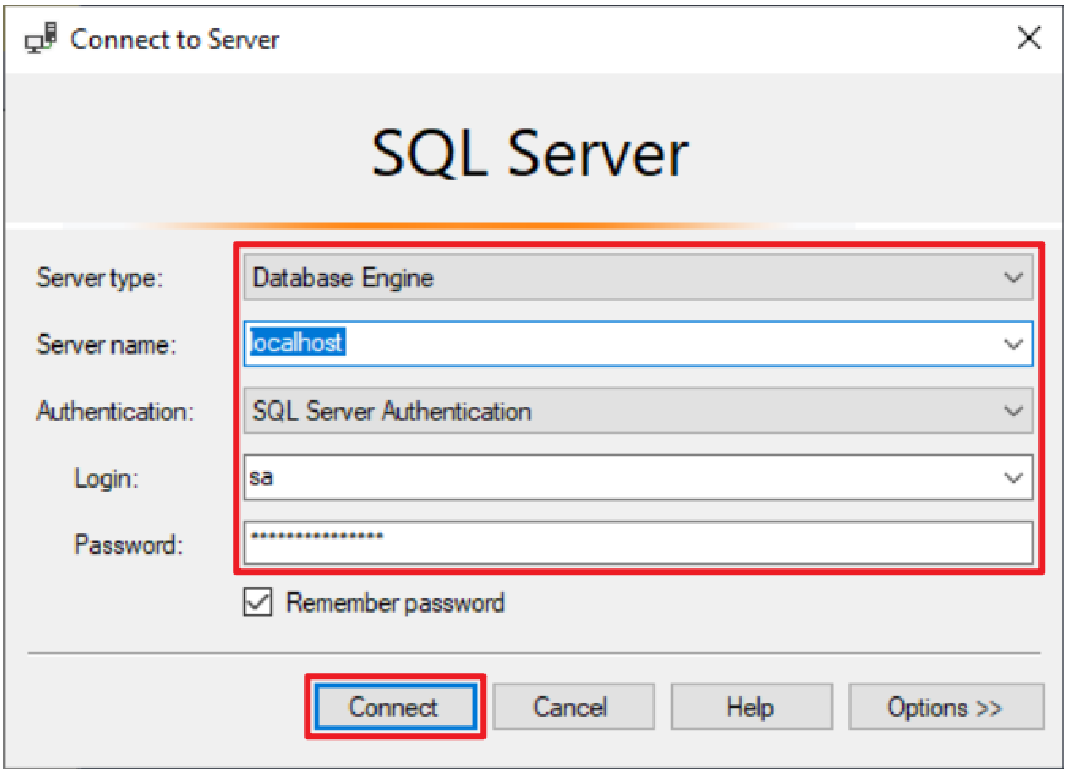
Enabling a server-level audit covers server operations such as administrative changes, login, and logout activities.

The following sections describe how to configure a server-level audit using the graphical user interface (GUI) and the command-line interface (CLI).

5.2.1.1 Configuring via Graphical User Interface (GUI)

(1) Open “SQL Server Management Studio (SSMS).”

(2) Enter the server’s name → select the authentication method → click “Connect.”



Server type: Database Engine

Server name: localhost

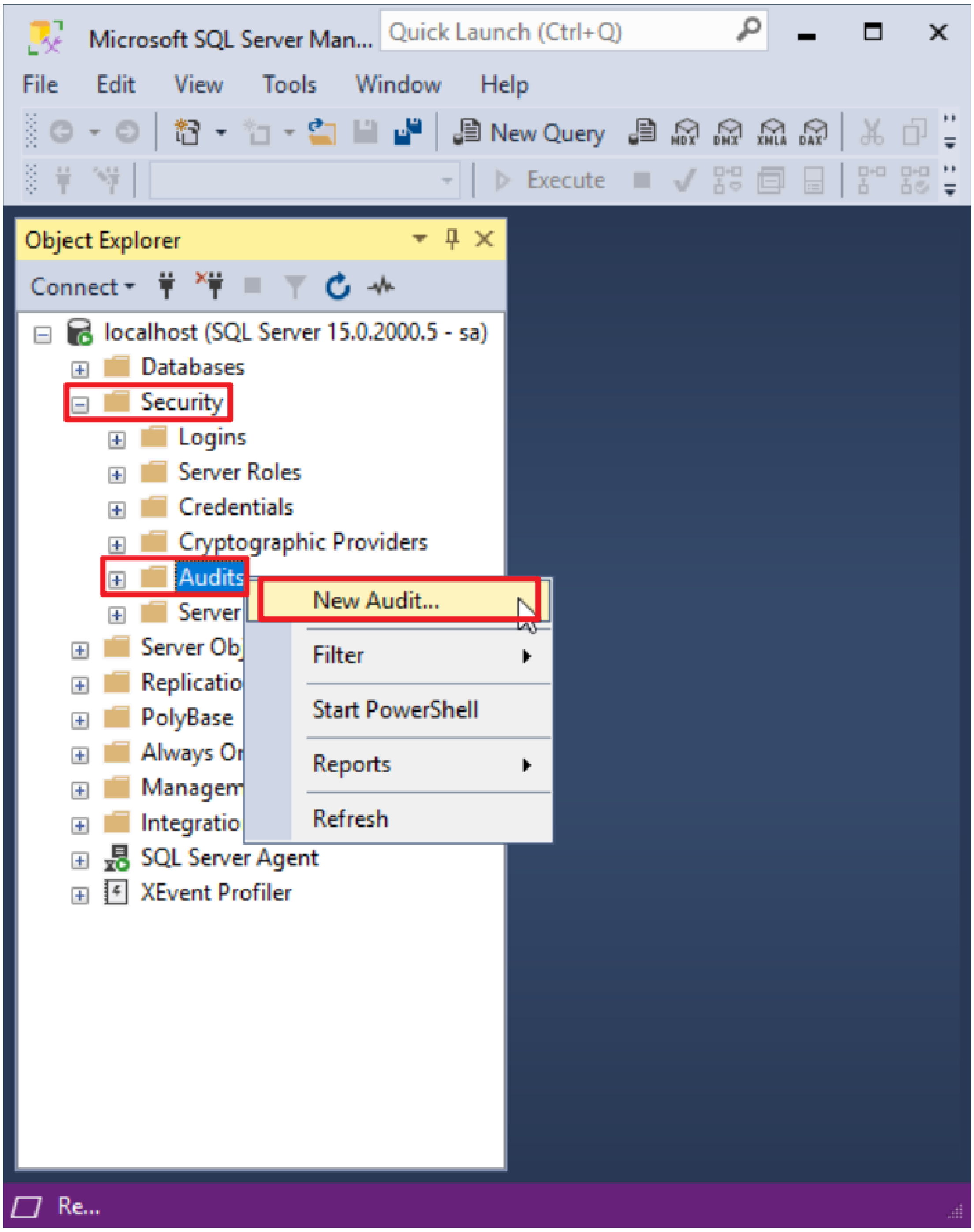
Authentication: SQL Server Authentication

Login: sa

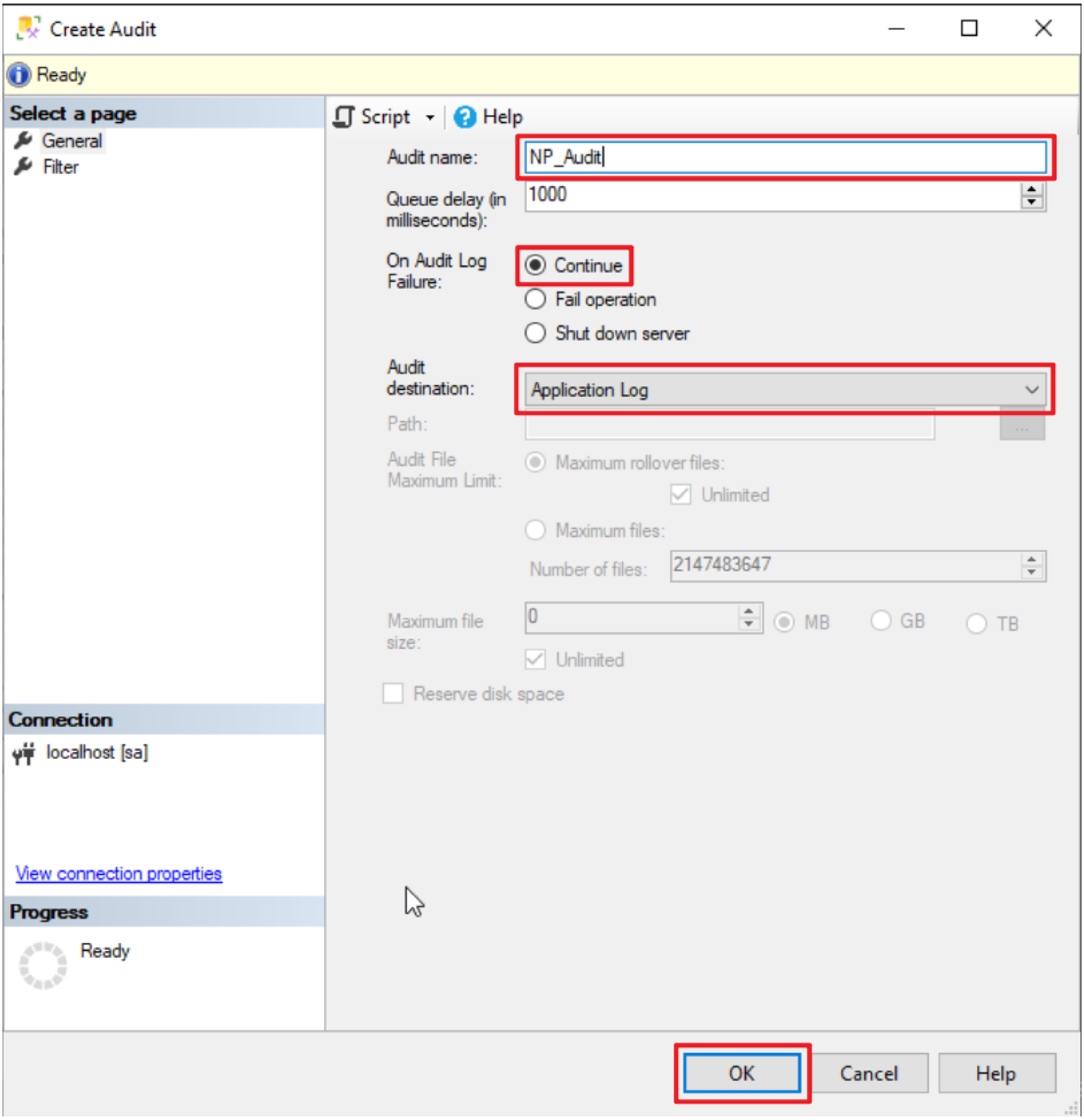
Password: ****************

☑ Remember password

(3) Expand “Security” → right-click “Audits” → select “New Audit...”



(4) Enter the audit name: (the example here is NP_Audit) → select “On audit log failure”: “Continue” → select audit destination: Application Log (this stores MS SQL audit logs in the Windows Event Viewer Application Log) → click “OK.”



Create Audit

Ready

Select a page
- General
- Filter

Script ▾ | Help

Audit name: NP_Audit

Queue delay (in milliseconds): 1000

On Audit Log Failure:
● Continue
○ Fail operation
○ Shut down server

Audit destination: Application Log

Path:

Audit File Maximum Limit:
● Maximum rollover files:
☑ Unlimited
○ Maximum files:
Number of files: 2147483647

Maximum file size: 0 ● MB ○ GB ○ TB
☑ Unlimited

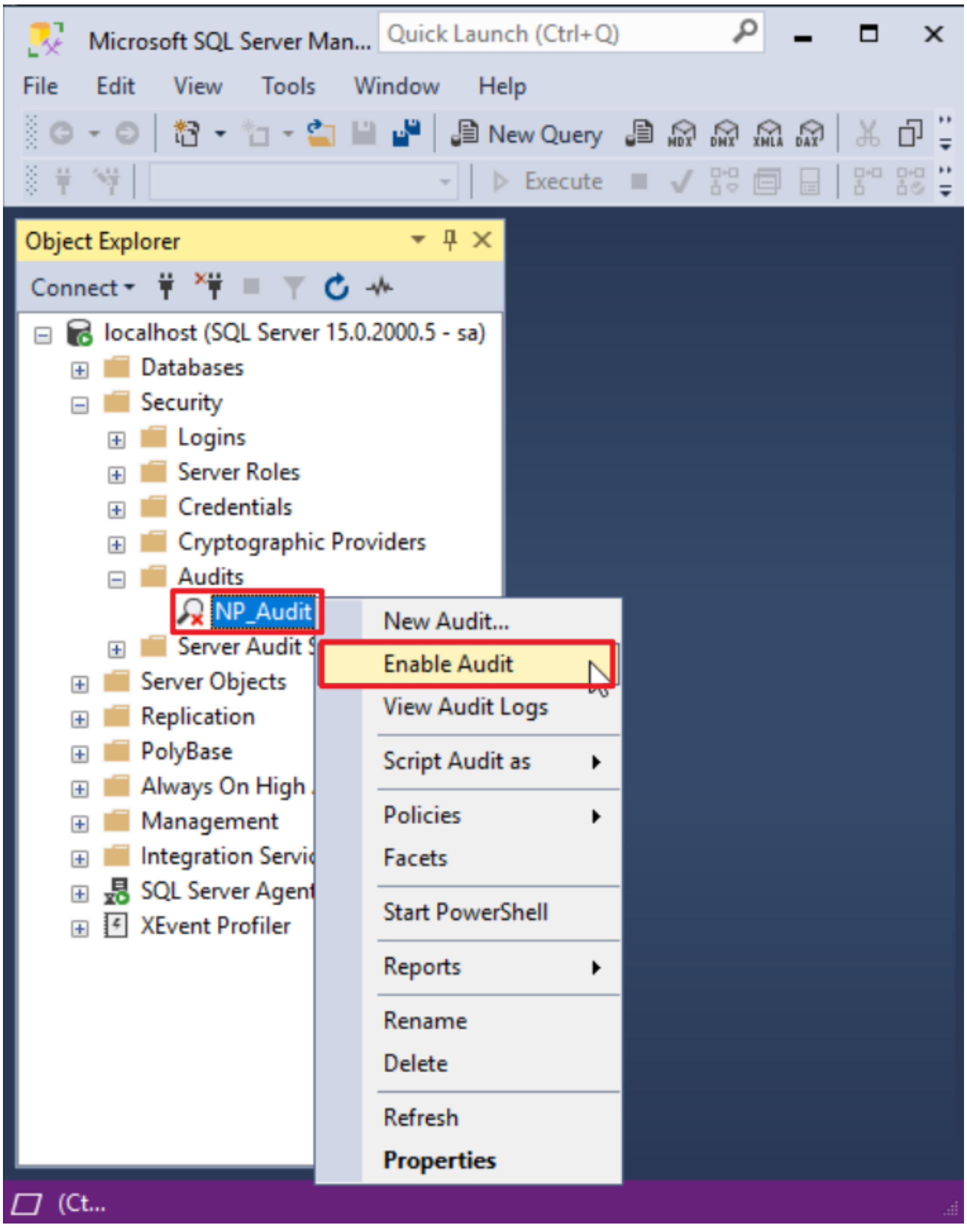
□ Reserve disk space

Connection
localhost [sa]

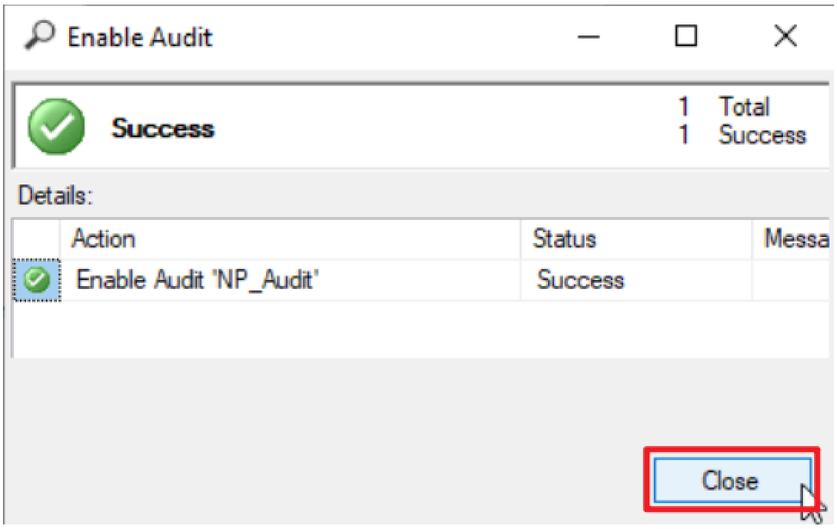
View connection properties

Progress
Ready

(5) In the audit list, right-click “NP_Audit” → select “Enable Audit.”



(6) Click “Close.”



Enable Audit

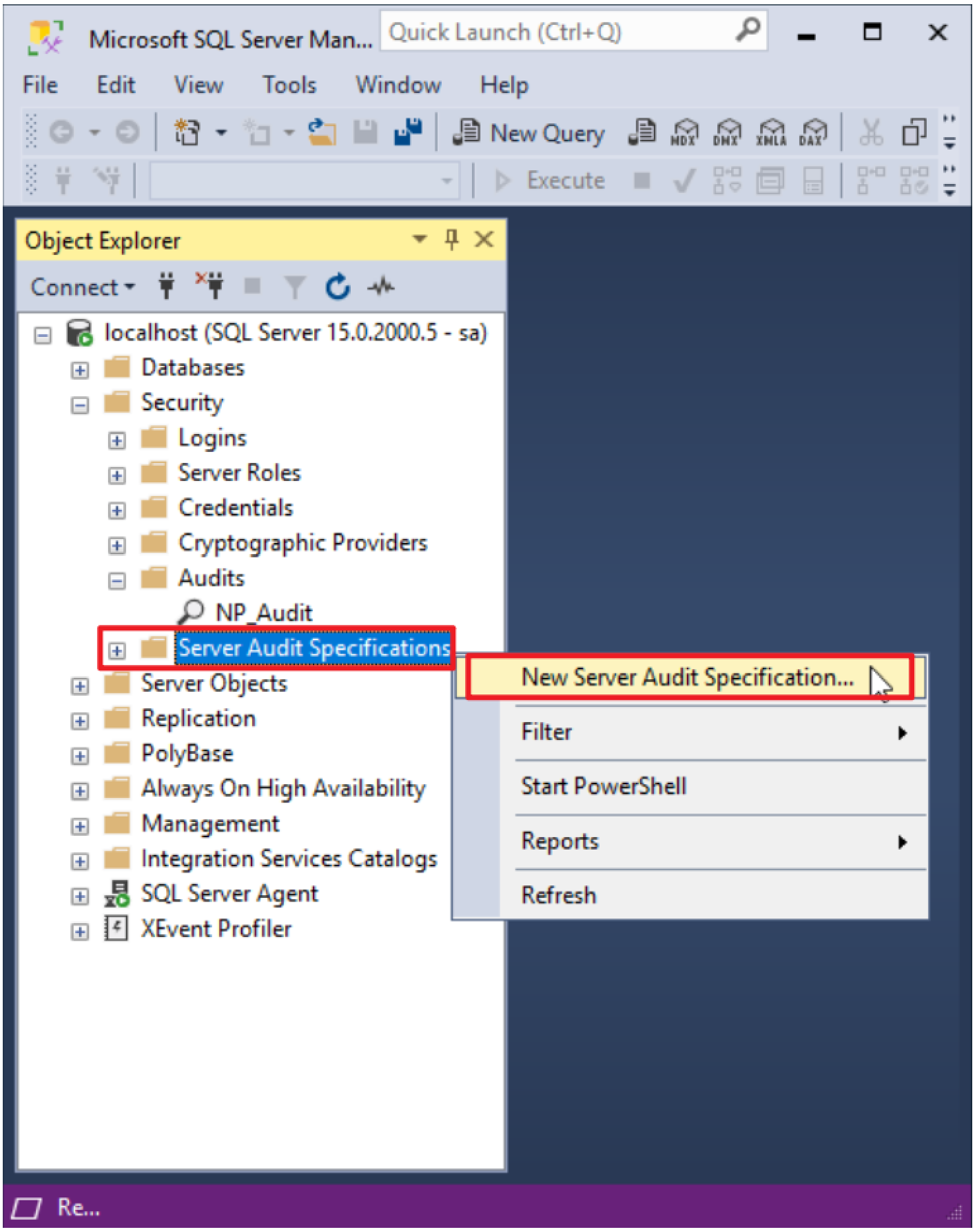
Success

1 Total
1 Success

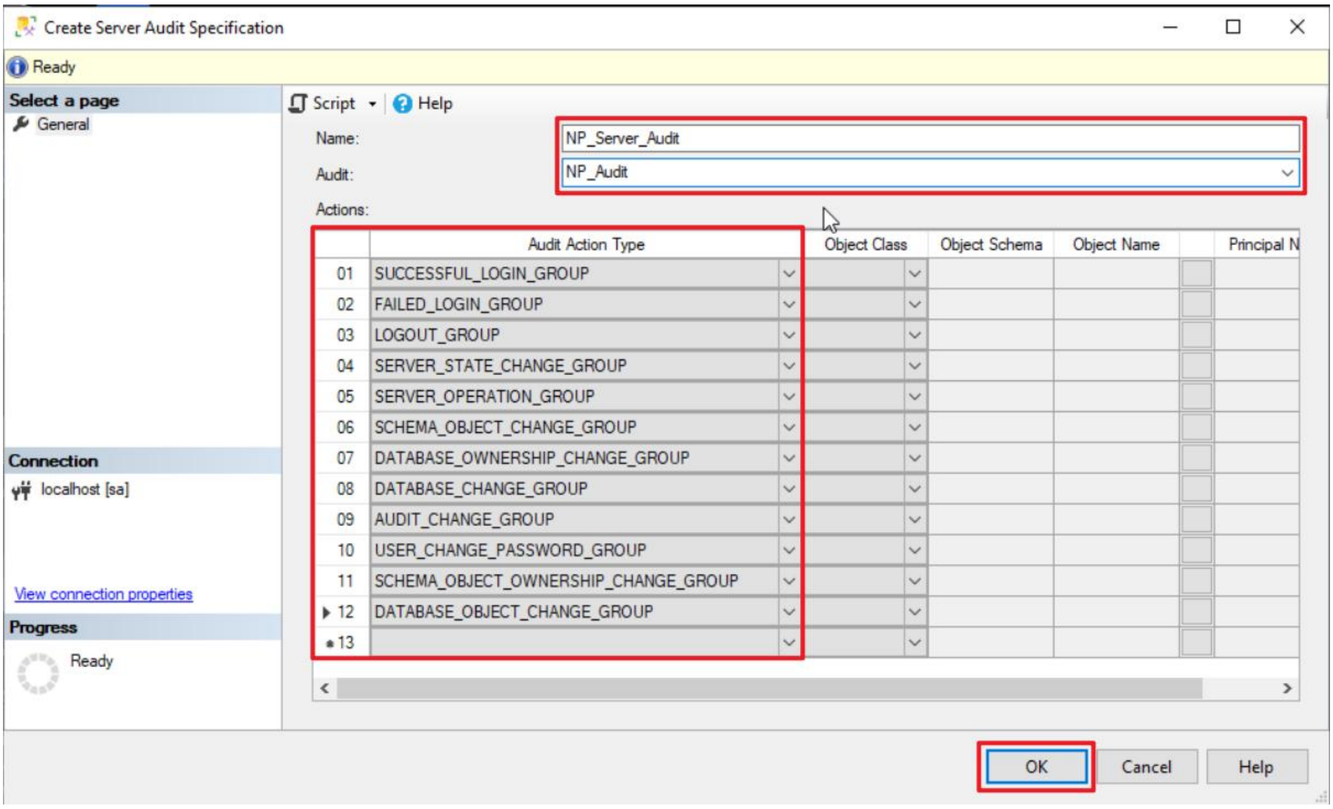
Details:

Action	Status	Messa
Enable Audit 'NP_Audit'	Success	

(7) Right-click “Server Audit Specifications,” → select “New Server Audit Specification...”



(8) Enter the specification name: (the example here is NP_Server_Audit) → select audit: NP_Audit → select action(s) (refer to the **SQL Server Audit Action Groups and Actions** in the references for details) → click "OK."



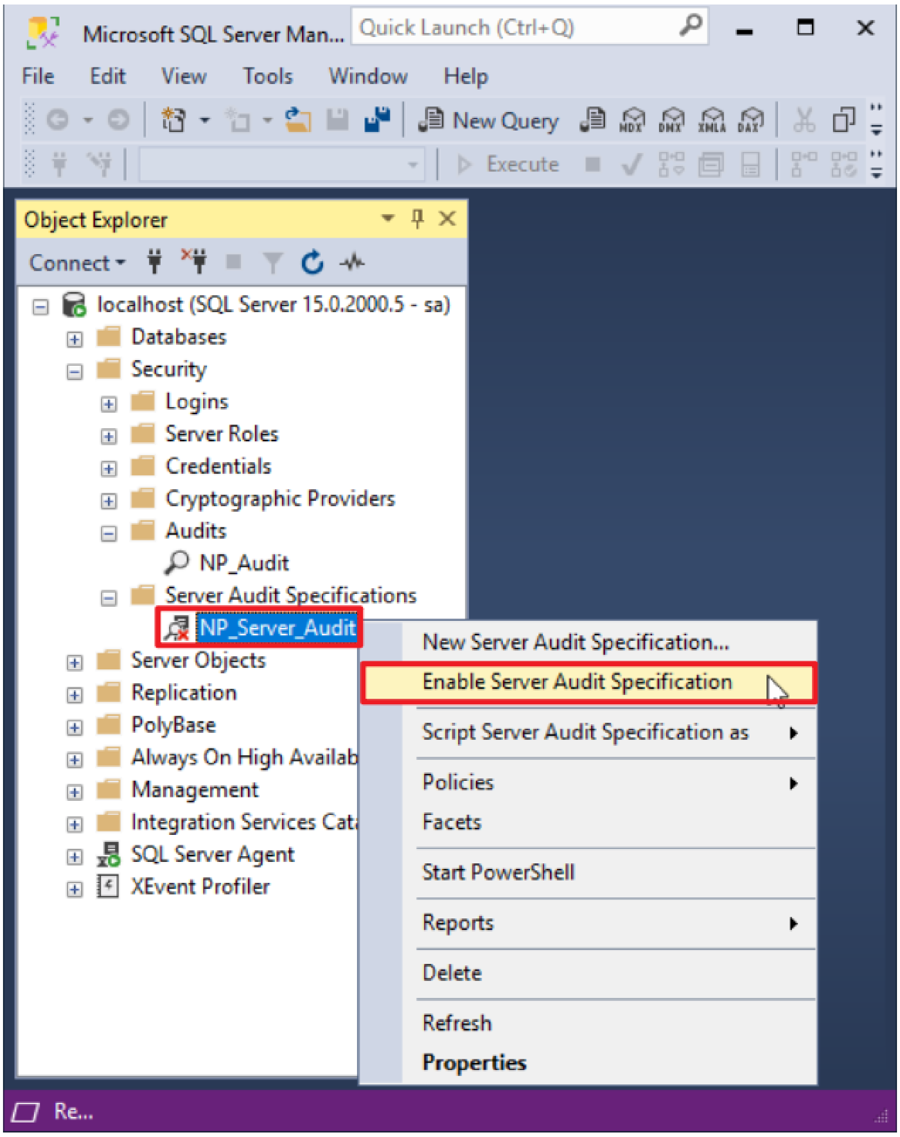
Name: NP_Server_Audit

Audit: NP_Audit

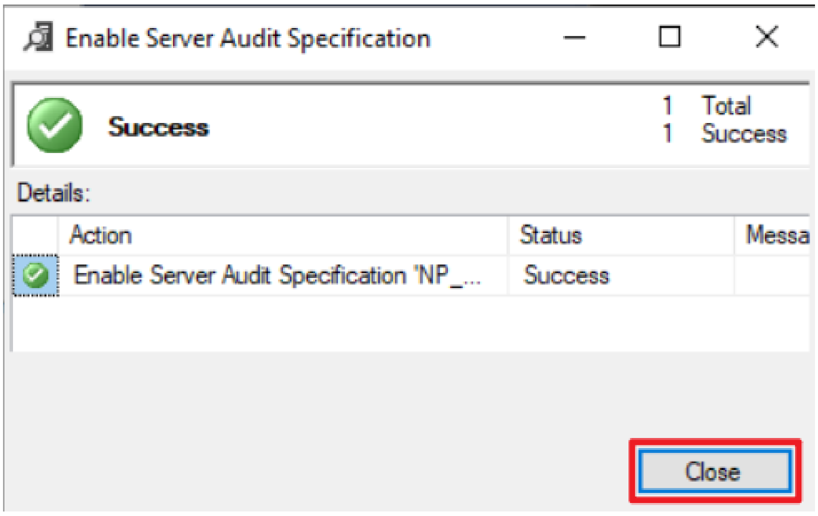
Actions:

	Audit Action Type	Object Class	Object Schema	Object Name	Principal N
01	SUCCESSFUL_LOGIN_GROUP				
02	FAILED_LOGIN_GROUP				
03	LOGOUT_GROUP				
04	SERVER_STATE_CHANGE_GROUP				
05	SERVER_OPERATION_GROUP				
06	SCHEMA_OBJECT_CHANGE_GROUP				
07	DATABASE_OWNERSHIP_CHANGE_GROUP				
08	DATABASE_CHANGE_GROUP				
09	AUDIT_CHANGE_GROUP				
10	USER_CHANGE_PASSWORD_GROUP				
11	SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP				
12	DATABASE_OBJECT_CHANGE_GROUP				
13					

(9) In the server audit specification list, right-click “NP_Server_Audit” → select “Enable Server Audit Specification.”



(10) Click “Close.”


Enable Server Audit Specification

Success

1 Total
1 Success

Details:

Action	Status	Messa
Enable Server Audit Specification 'NP_...	Success	

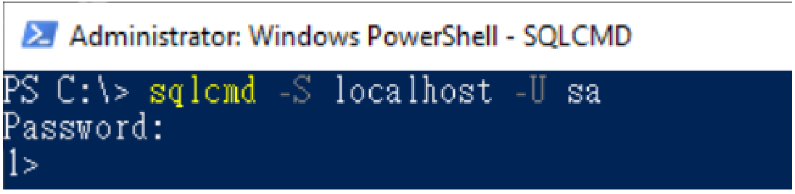
5.2.1.2 Configuring via Graphical User Interface (GUI)

(1) Open “Windows PowerShell.”

(2) Enter the command below to log in using either sa:

<2.1>Using sa account:

```
PS C:\> sqlcmd -S localhost -U sa
```



```
PS C:\> sqlcmd -S localhost -U sa
Password:
1>
```

Options:

-S [protocol:]server[instance_name][,port]

-U login_id

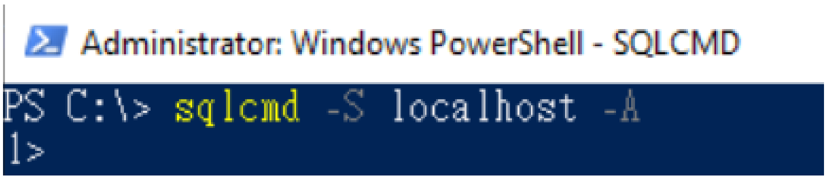
-P password

-A dedicated administrator connection

<2.2> Using Windows account:

Enter the command below to log in using Windows:

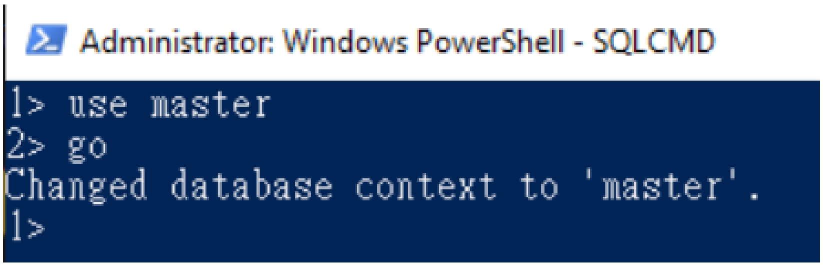
```
PS C:\> sqlcmd -S localhost -A
```



```
PS C:\> sqlcmd -S localhost -A
1>
```

(3) Enter the command below to switch to the **master** database:

```
1 > use master
2 > go
```

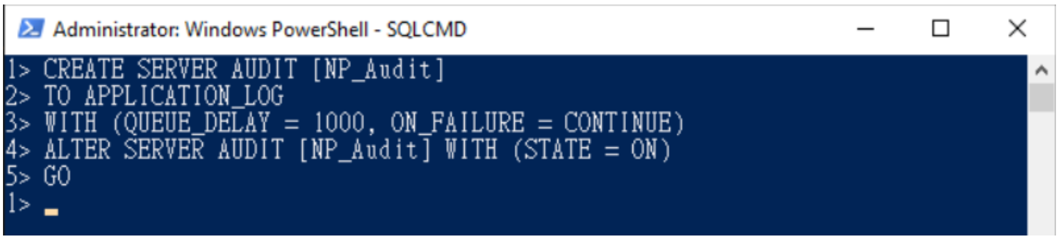


Administrator: Windows PowerShell - SQLCMD

```
1> use master
2> go
Changed database context to 'master'.
1>
```

(4) Enter the audit name: NP_Audit → select audit destination: Application Log (this stores MS SQL audit logs in the Windows Event Viewer Application Log) → click “OK.”

```
1 > CREATE SERVER AUDIT [ NP_Audit ]
2 > TO APPLICATION_LOG
3 > WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4 > ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5 > GO
```



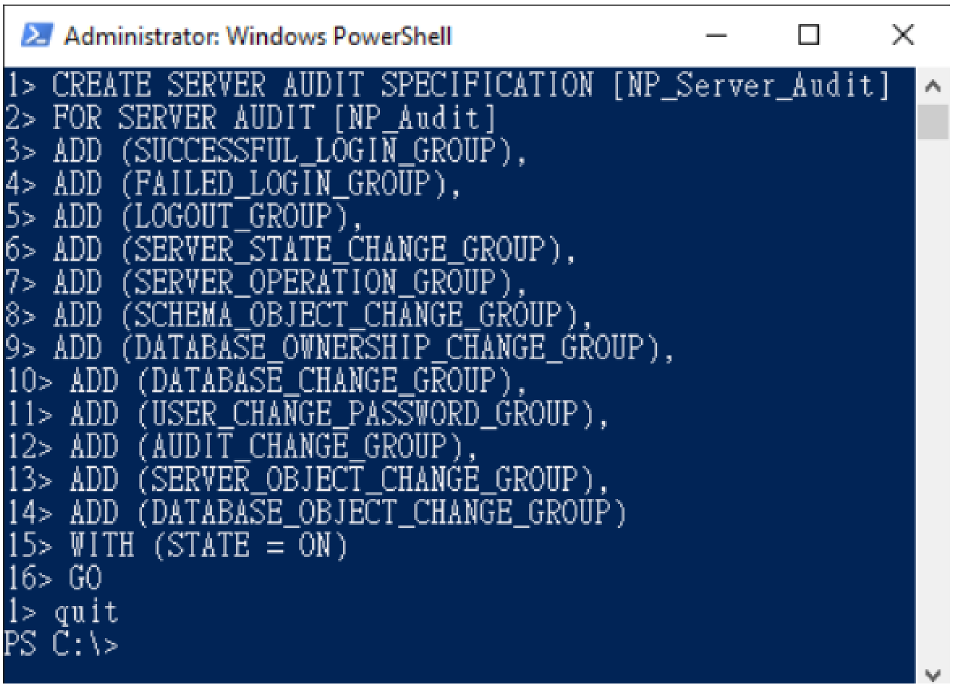
Administrator: Windows PowerShell - SQLCMD

```
1> CREATE SERVER AUDIT [NP_Audit]
2> TO APPLICATION_LOG
3> WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4> ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5> GO
1> _
```

(5) Enter the command below to configure the server audit and add actions. For detailed information, refer to the **SQL Server Audit Action Groups and Actions** in the references.

```
1 > CREATE SERVER AUDIT SPECIFICATION [ NP_Server_Audit ]
2 > FOR SERVER AUDIT [NP_Audit]
3 > ADD (SUCCESSFUL_LOGIN_GROUP),
4 > ADD (FAILED_LOGIN_GROUP),
5 > ADD (LOGOUT_GROUP),
6 > ADD (SERVER_STATE_CHANGE_GROUP),
7 > ADD (SERVER_OPERATION_GROUP),
8 > ADD (SCHEMA_OBJECT_CHANGE_GROUP),
9 > ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
10 > ADD (DATABASE_CHANGE_GROUP),
11 > ADD (DATABASE_OBJECT_CHANGE_GROUP),
12 > ADD (SERVER_OBJECT_CHANGE_GROUP),
13 > ADD (USER_CHANGE_PASSWORD_GROUP)
14 > ADD (AUDIT_CHANGE_GROUP)
```

```
15> WITH (STATE = ON)
16 > GO
1 > quit
```



```
1> CREATE SERVER AUDIT SPECIFICATION [NP_Server_Audit]
2> FOR SERVER AUDIT [NP_Audit]
3> ADD (SUCCESSFUL_LOGIN_GROUP),
4> ADD (FAILED_LOGIN_GROUP),
5> ADD (LOGOUT_GROUP),
6> ADD (SERVER_STATE_CHANGE_GROUP),
7> ADD (SERVER_OPERATION_GROUP),
8> ADD (SCHEMA_OBJECT_CHANGE_GROUP),
9> ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
10> ADD (DATABASE_CHANGE_GROUP),
11> ADD (USER_CHANGE_PASSWORD_GROUP),
12> ADD (AUDIT_CHANGE_GROUP),
13> ADD (SERVER_OBJECT_CHANGE_GROUP),
14> ADD (DATABASE_OBJECT_CHANGE_GROUP)
15> WITH (STATE = ON)
16> GO
1> quit
PS C:\>
```

Replace the text shown in red with the server audit specification name.

5.2.2 Database-Level Audit

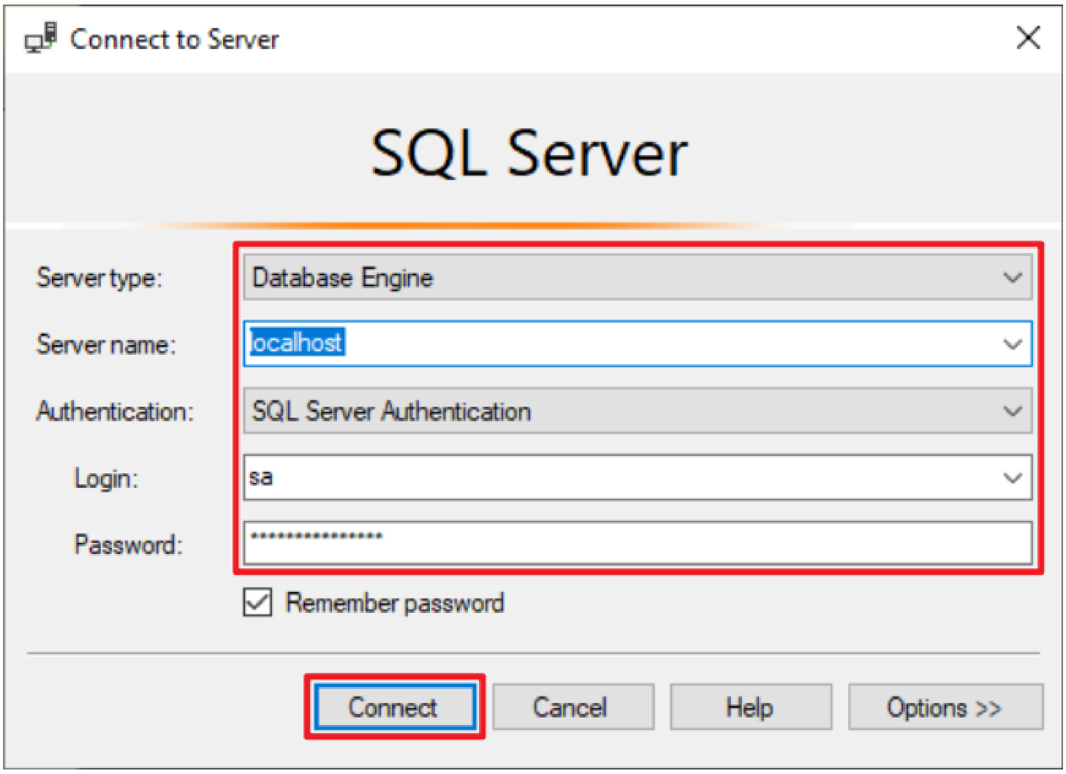
Enabling a database-level audit covers operations involving Data Manipulation Language (DML) and Data Definition Language (DDL) statements.

The following sections describe how to configure a database-level audit using the graphical user interface (GUI) and the command-line interface (CLI).

5.2.2.1 Configuring via Graphical User Interface (GUI)

(1) Open “SQL Server Management Studio (SSMS).”

(2) Enter the server’s name → select the authentication method → click “Connect.”


Connect to Server

SQL Server

Server type: Database Engine

Server name: localhost

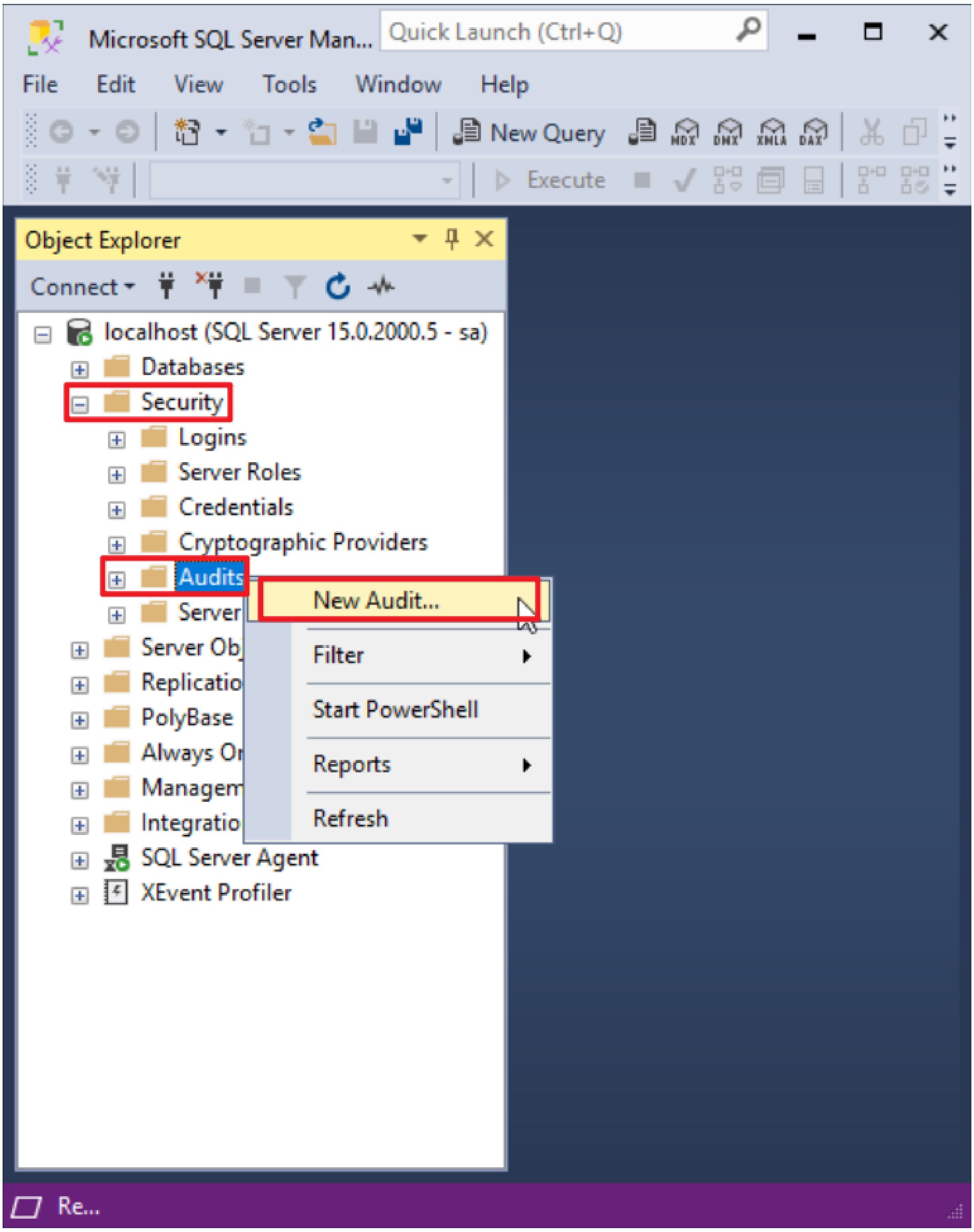
Authentication: SQL Server Authentication

Login: sa

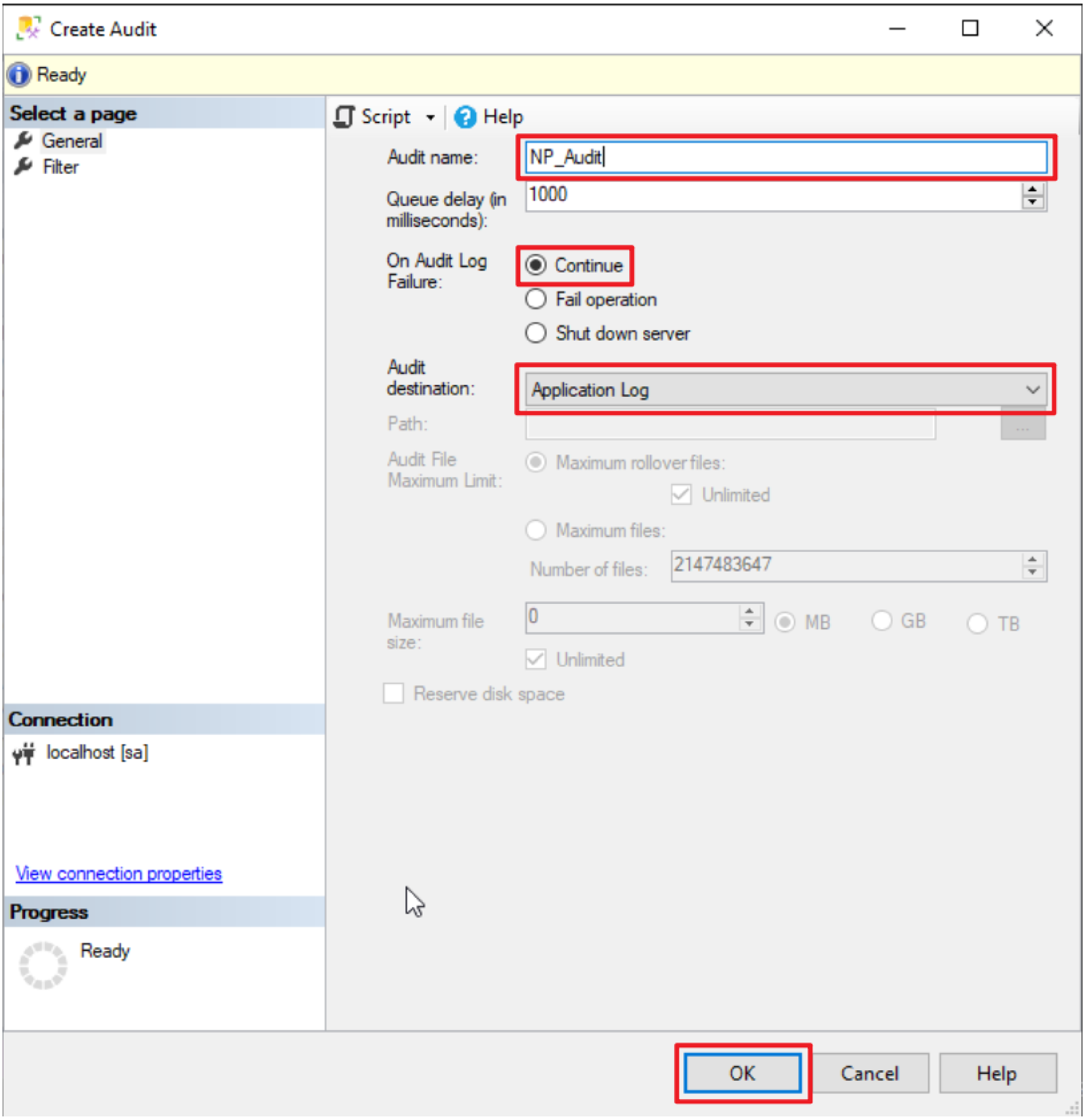
Password: ****************

☑ Remember password

(3) Expand "Security" → right-click "Audits" → select "New Audit..."



(4) Enter the audit name: (the example here is NP_Audit) → select “On audit log failure”: “Continue” → select audit destination: Application Log (this stores MS SQL audit logs in the Windows Event Viewer Application Log) → click “OK.”



Create Audit

Ready

Select a page
- General
- Filter

Script ▾ Help

Audit name: NP_Audit

Queue delay (in milliseconds): 1000

On Audit Log Failure:
- ● Continue
- ○ Fail operation
- ○ Shut down server

Audit destination: Application Log

Path:

Audit File Maximum Limit:
- ● Maximum rollover files:
  - ☑ Unlimited
- ○ Maximum files:

Number of files: 2147483647

Maximum file size: 0 ● MB ○ GB ○ TB

☑ Unlimited

□ Reserve disk space

Connection

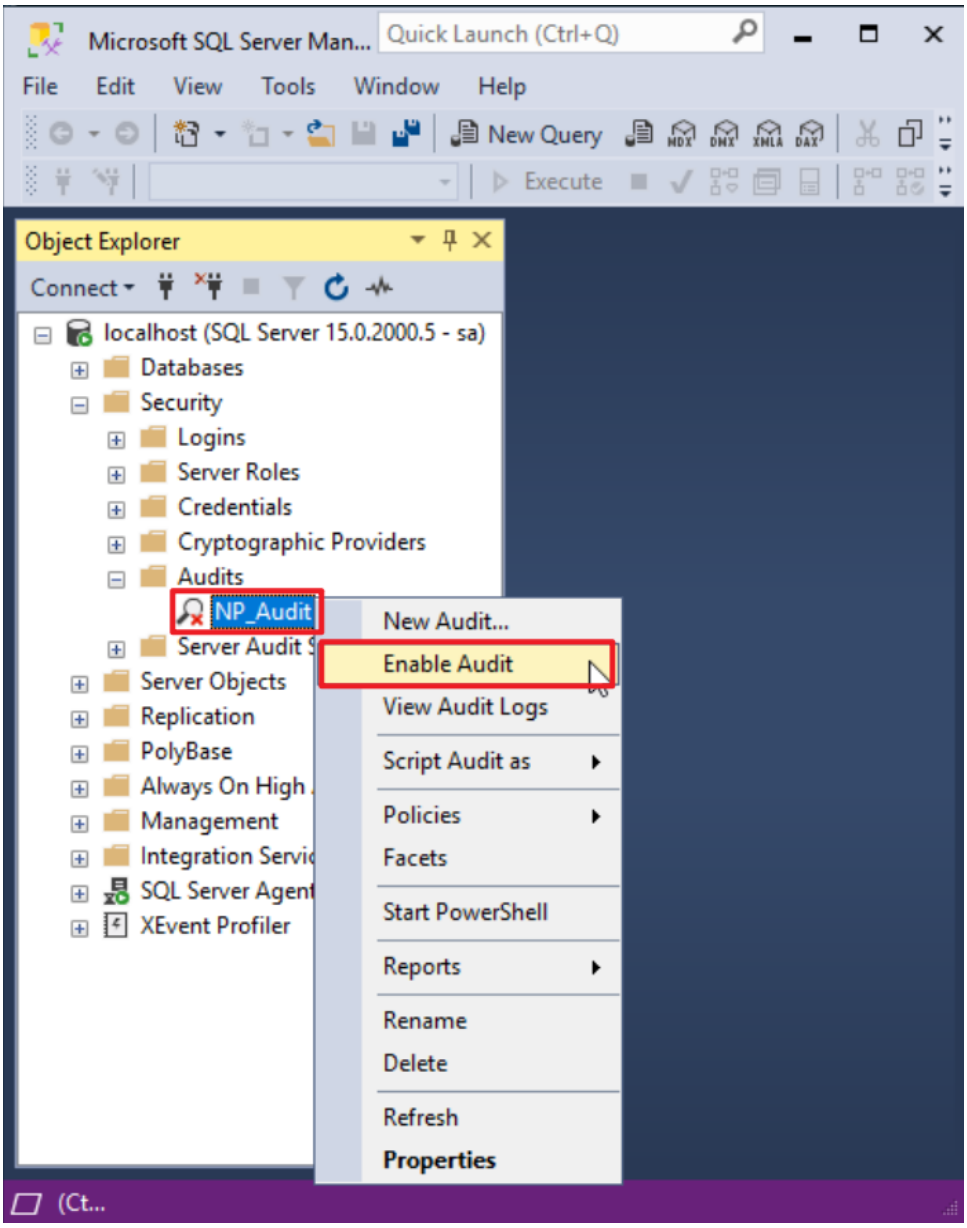
localhost [sa]

View connection properties

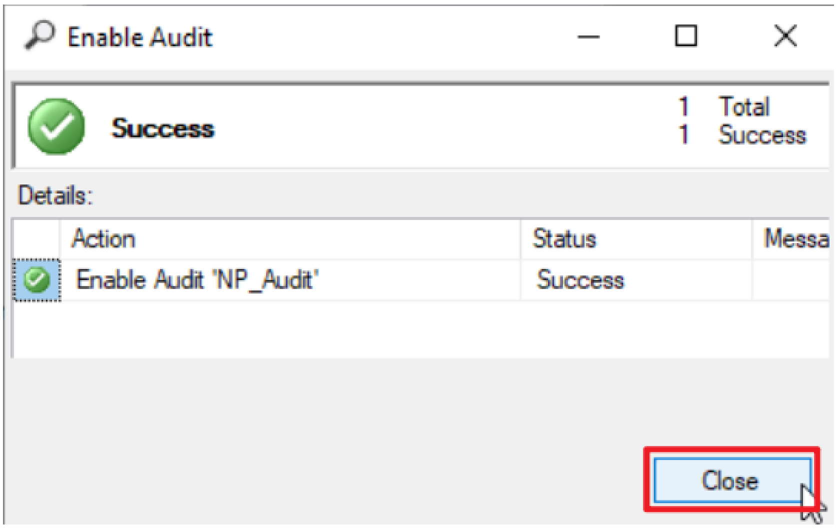
Progress

Ready

(5) In the audit list, right-click “NP_Audit” → select “Enable Audit.”



(6) Click “Close.”



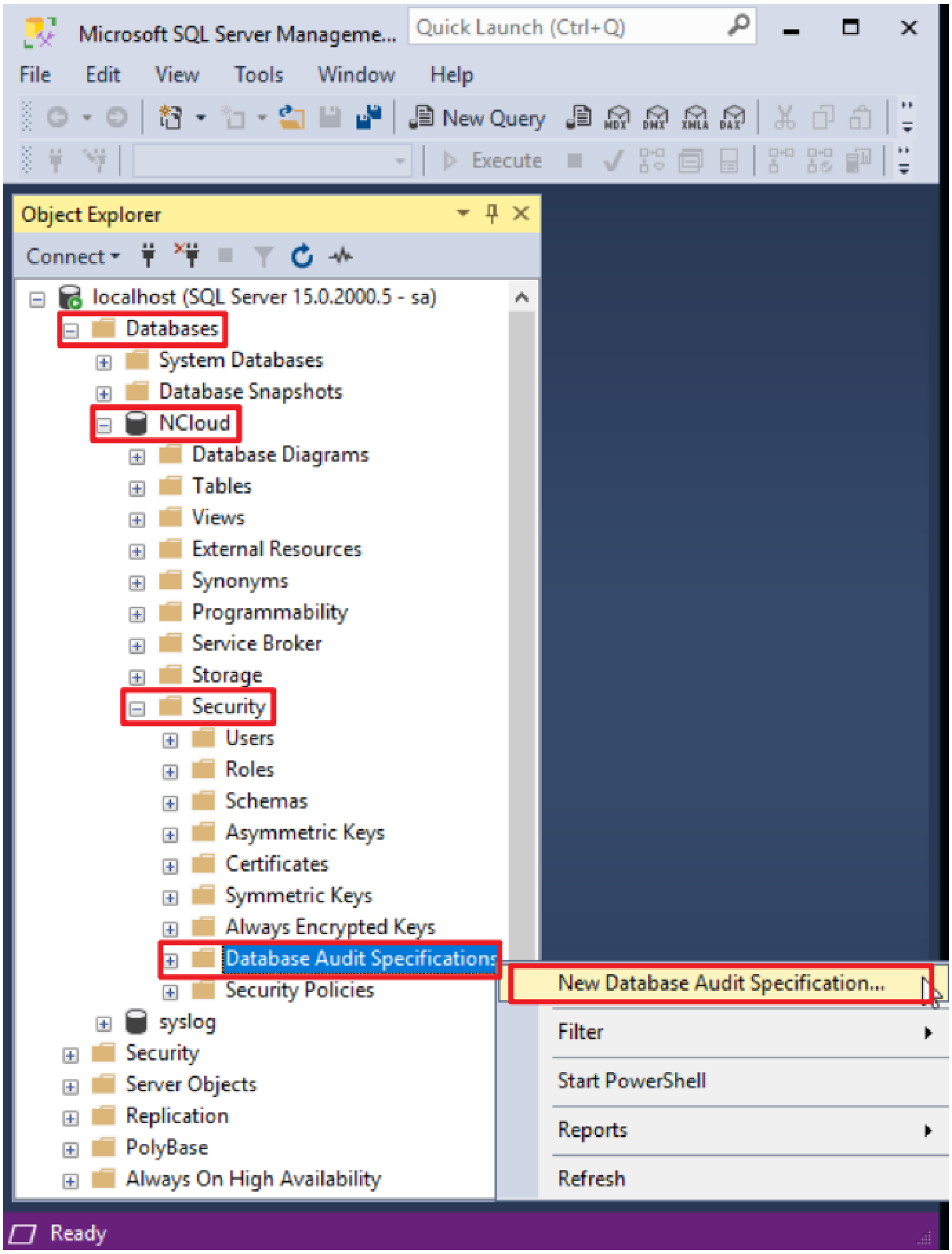
Success

1	Total
1	Success

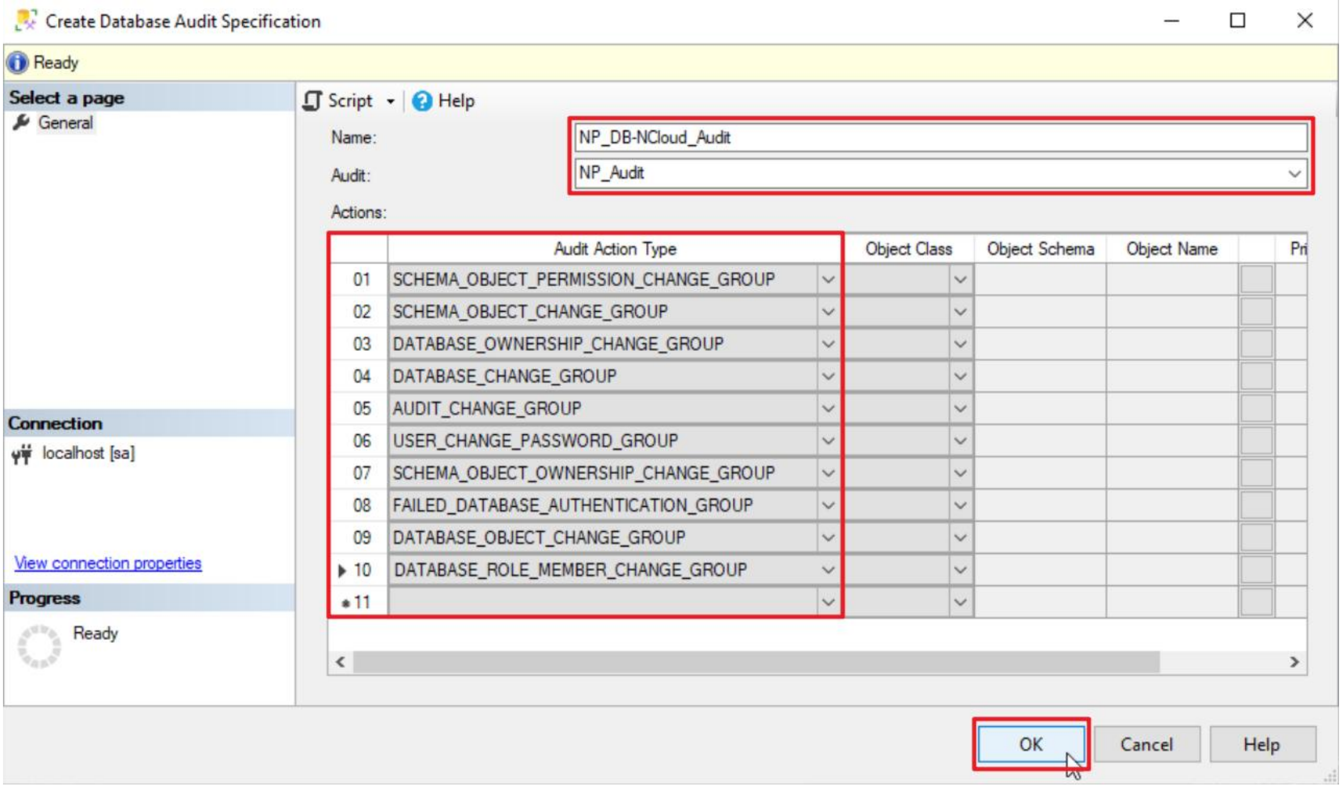
Details:

Action	Status	Messa
Enable Audit 'NP_Audit'	Success	

(7) In “Databases,” select the target database (the example here is : NCloud) → expand “Security” → right-click “Database Audit Specifications” → select "New Database Audit Specification...”



(8) Enter the specification name: (the example here is NP_DB-NCloud_Audit) → select audit: NP_Audit and action(s) → select action(s) (refer to the **SQL Server Audit Action Groups and Actions** in the references for details) → click "OK."



Create Database Audit Specification

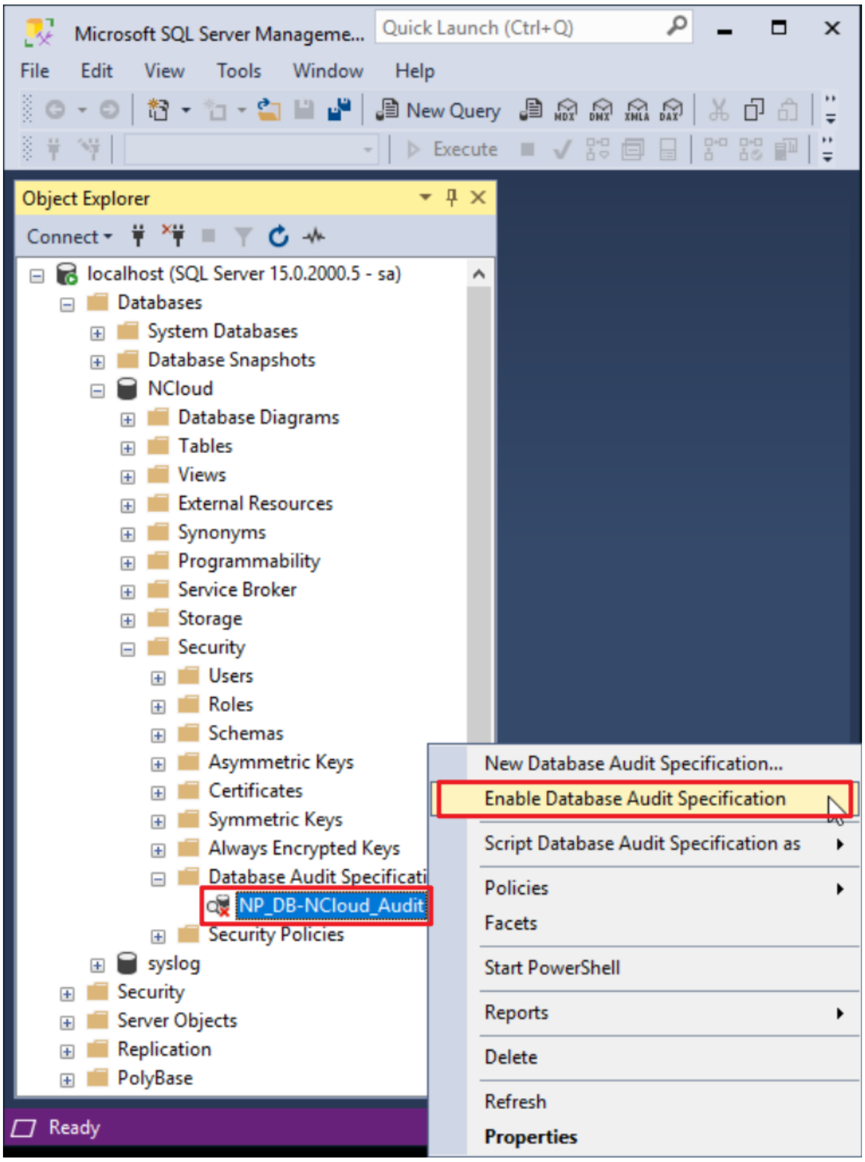
Name: NP_DB-NCloud_Audit

Audit: NP_Audit

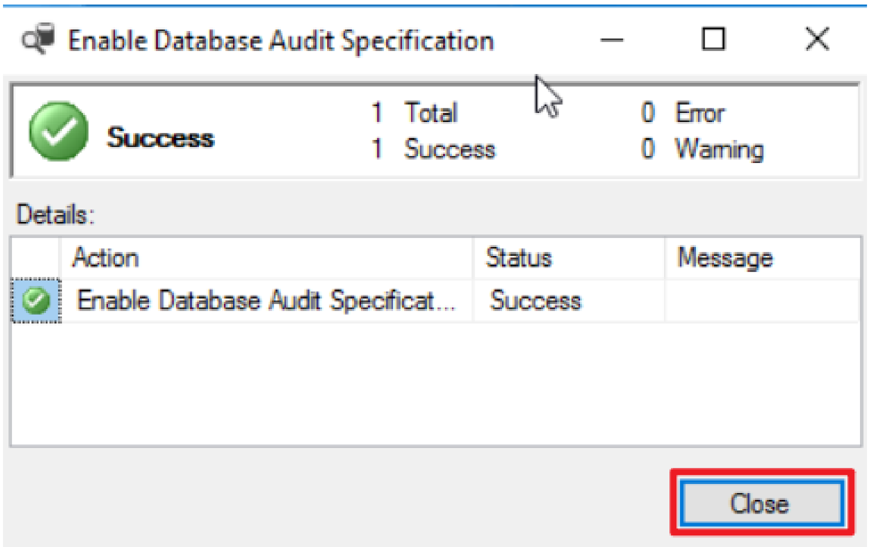
Actions:

	Audit Action Type	Object Class	Object Schema	Object Name	Pri
01	SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP				
02	SCHEMA_OBJECT_CHANGE_GROUP				
03	DATABASE_OWNERSHIP_CHANGE_GROUP				
04	DATABASE_CHANGE_GROUP				
05	AUDIT_CHANGE_GROUP				
06	USER_CHANGE_PASSWORD_GROUP				
07	SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP				
08	FAILED_DATABASE_AUTHENTICATION_GROUP				
09	DATABASE_OBJECT_CHANGE_GROUP				
10	DATABASE_ROLE_MEMBER_CHANGE_GROUP				
11					

(9) In the database audit specification list, right-click “NP_DB-NCloud_Audit” → select “Enable Server Audit Specification.”



(10) Click “Close.”



Success

1	Total	0	Error
1	Success	0	Warning

Details:

	Action	Status	Message
✓	Enable Database Audit Specificat...	Success	

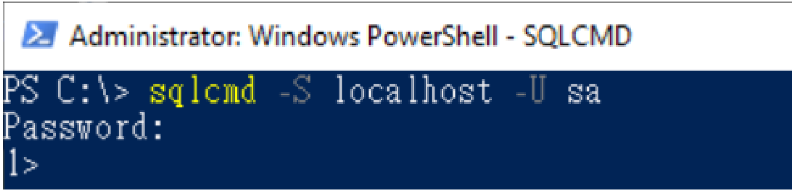
5.2.2.2 Configuring via Graphical User Interface (GUI)

(1) Open “Windows PowerShell.”

(2) Enter the command below to log in using either sa:

<2.1>Using sa account:

```
PS C:\> sqlcmd -S localhost -U sa
```



```
PS C:\> sqlcmd -S localhost -U sa
Password:
1>
```

Options:

-S [protocol:]server[instance_name][,port]

-U login_id

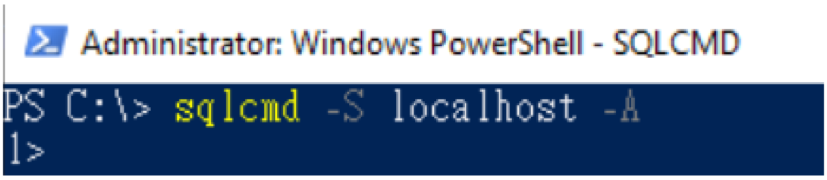
-P password

-A dedicated administrator connection

<2.2> Using Windows account:

Enter the command below to log in using Windows account:

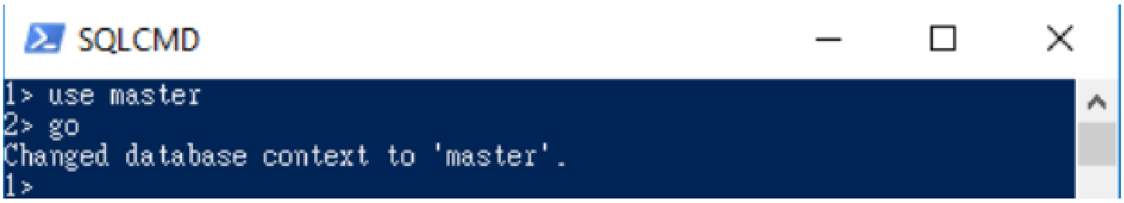
```
PS C:\> sqlcmd -S localhost -A
```



```
PS C:\> sqlcmd -S localhost -A
1>
```

(3) Enter the command below to switch to the **master** database:

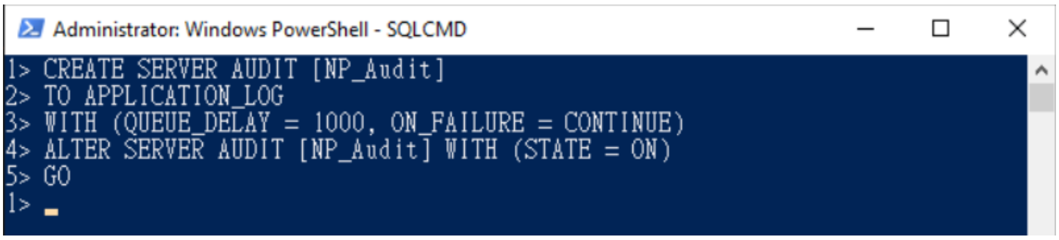
```
1 > use master
2 > go
```



```
1> use master
2> go
Changed database context to 'master'.
1>
```

(4) Enter the audit name: NP_Audit → select audit destination: Application Log (this stores MS SQL audit logs in the Windows Event Viewer Application Log) → click “OK.”

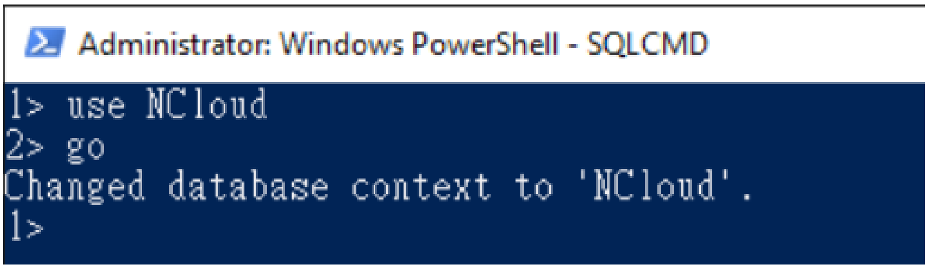
```
1 > CREATE SERVER AUDIT [ NP_Audit ]
2 > TO APPLICATION_LOG
3 > WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4 > ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5 > GO
```



```
1> CREATE SERVER AUDIT [NP_Audit]
2> TO APPLICATION_LOG
3> WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4> ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5> GO
1> _
```

(5) Enter the command below to switch to the target audit database (the example here is: NCloud).

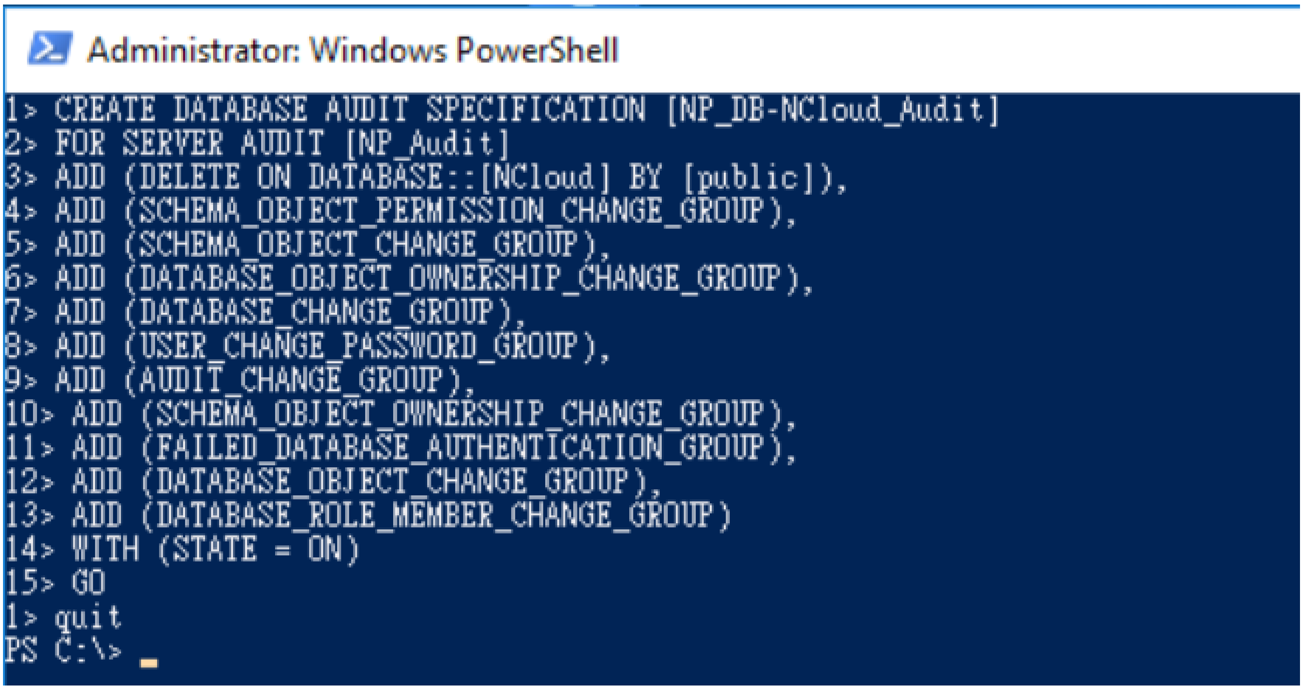
```
1 > use NCloud
2 > go
```



```
1> use NCloud
2> go
Changed database context to 'NCloud'.
1>
```

(6) Enter the command below to configure the audit for the database and add actions. For detailed information, refer to the **SQL Server Audit Action Groups and Actions** in the references.

```
1 > CREATE DATABASE AUDIT SPECIFICATION [ NP_DB-NCloud_Audit ]
2 > FOR SERVER AUDIT [NP_Audit]
3 > ADD (DELETE ON DATABASE::[ NCloud ] BY [public]),
4 > ADD (SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP),
5 > ADD (SCHEMA_OBJECT_CHANGE_GROUP),
6 > ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
7 > ADD (DATABASE _CHANGE_GROUP),
8 > ADD (AUDIT_CHANGE_GROUP),
9 > ADD (USER_CHANGE_PASSWORD_GROUP),
10 > ADD (SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP),
11 > ADD (FAILED_DATABASE_AUTHENTICATION_GROUP),
12 > ADD (DATABASE_OBJECT_CHANGE_GROUP),
13 > ADD (DATABASE_ROLE_MEMBER_CHANGE_GROUP)
14 > WITH (STATE = ON)
15 > GO
1 > quit
```



```
1> CREATE DATABASE AUDIT SPECIFICATION [NP_DB-NCloud_Audit]
2> FOR SERVER AUDIT [NP_Audit]
3> ADD (DELETE ON DATABASE::[NCloud] BY [public]),
4> ADD (SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP),
5> ADD (SCHEMA_OBJECT_CHANGE_GROUP),
6> ADD (DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP),
7> ADD (DATABASE_CHANGE_GROUP),
8> ADD (USER_CHANGE_PASSWORD_GROUP),
9> ADD (AUDIT_CHANGE_GROUP),
10> ADD (SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP),
11> ADD (FAILED_DATABASE_AUTHENTICATION_GROUP),
12> ADD (DATABASE_OBJECT_CHANGE_GROUP),
13> ADD (DATABASE_ROLE_MEMBER_CHANGE_GROUP)
14> WITH (STATE = ON)
15> GO
1> quit
PS C:\> _
```

Replace the text shown in red with the database audit specification name.

```
1 > CREATE DATABASE AUDIT SPECIFICATION [NP_DB-NCloud_Audit]
```

Replace the text shown in red with the target database name.

```
3 > ADD (DELETE ON DATABASE::[NCloud] BY [public])
```

5.3 Event Log Configuration

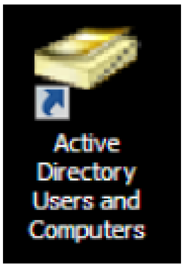
This is an optional configuration.

The following sections describe configuration methods for Domain and Workgroup environments.

5.3.1 Domain

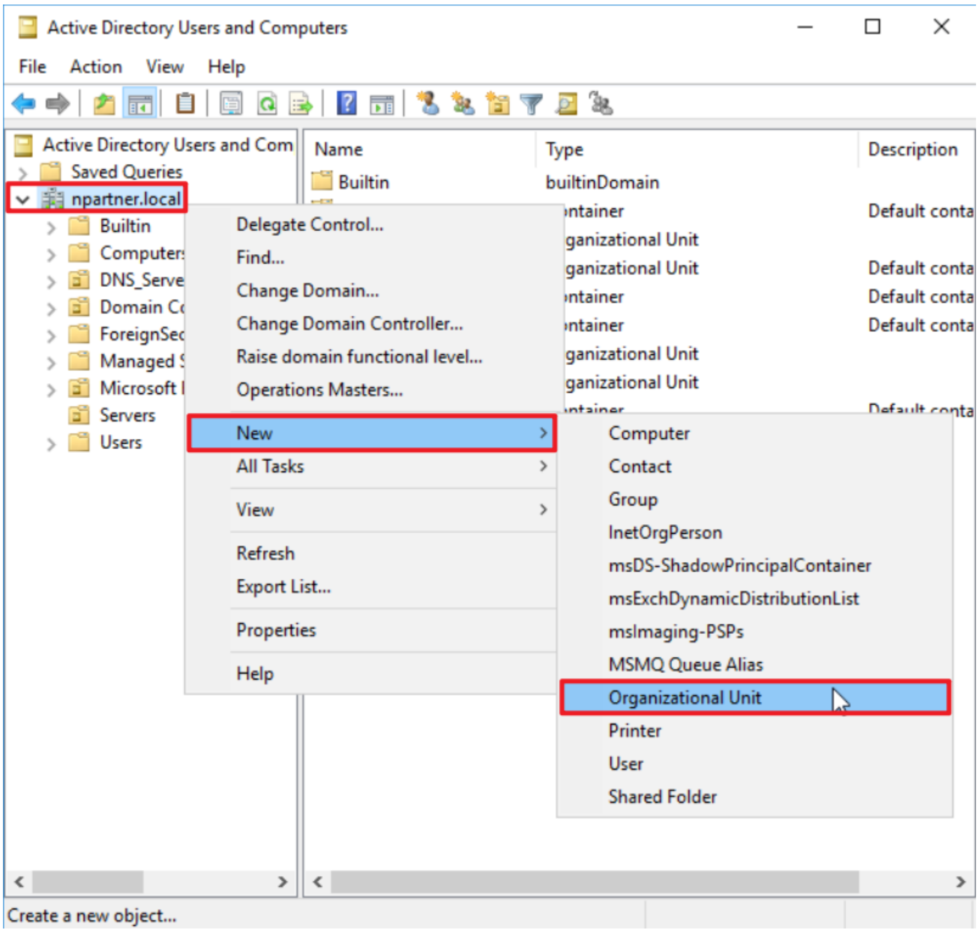
5.3.1.1 Organizational Unit (OU) Configuration

(1) Click “Active Directory Users and Computers.”



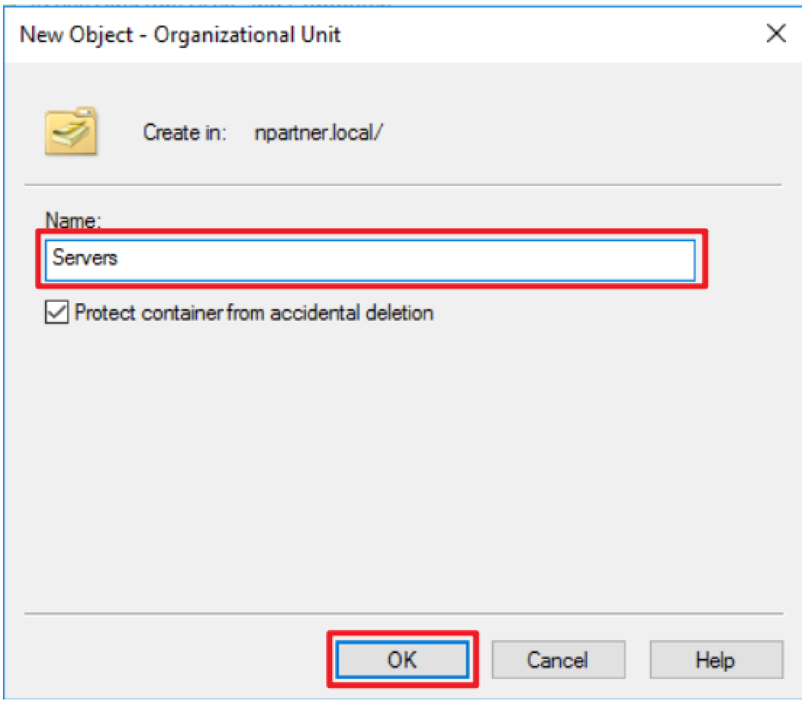
(2) Add an Organizational Unit

Right-click on “Domain Controllers, select “New,” and click “Organizational Unit.”



(3) Enter your Organizational Unit name: (in this example, it is “Servers”)

Note: Please create the organizational unit name according to the customer's environment. → click “OK.”



New Object - Organizational Unit

Create in: npartner.local/

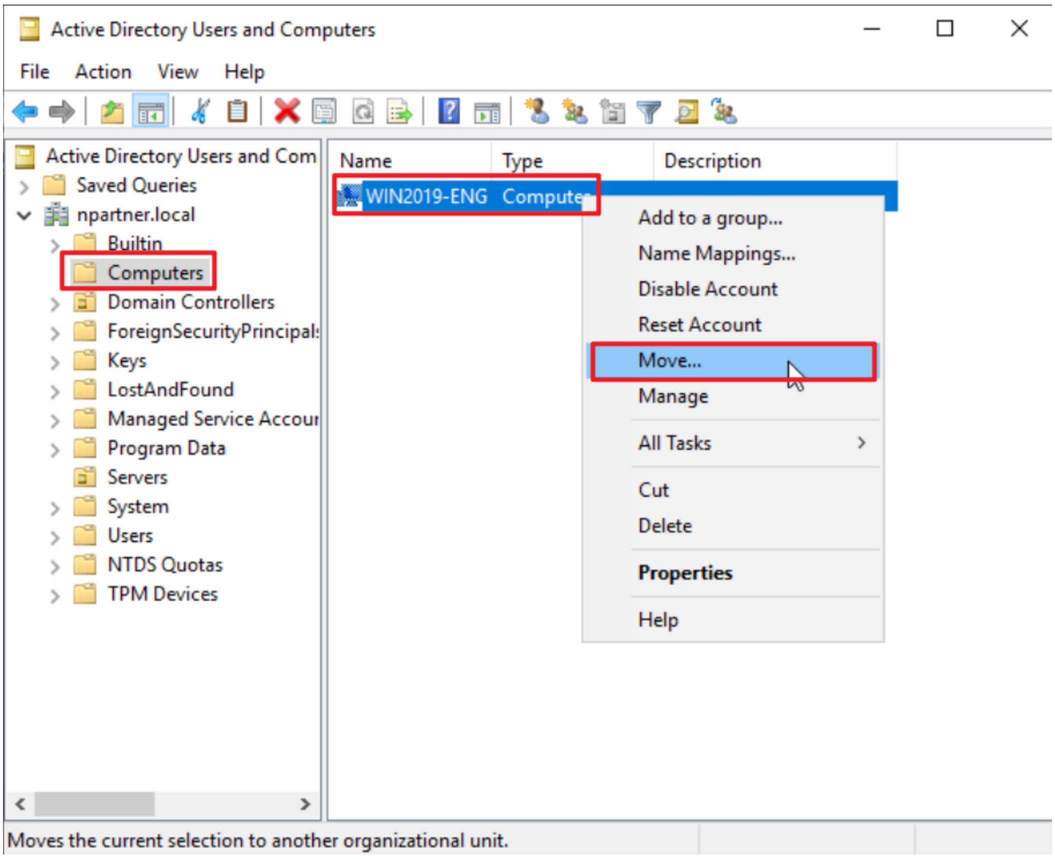
Name: Servers

☑ Protect container from accidental deletion

(4) Move the Server to your New Organizational Unit:

Select your organizational unit in “Domain Controllers” -> Right-click on the “WIN2019-ENG” server.

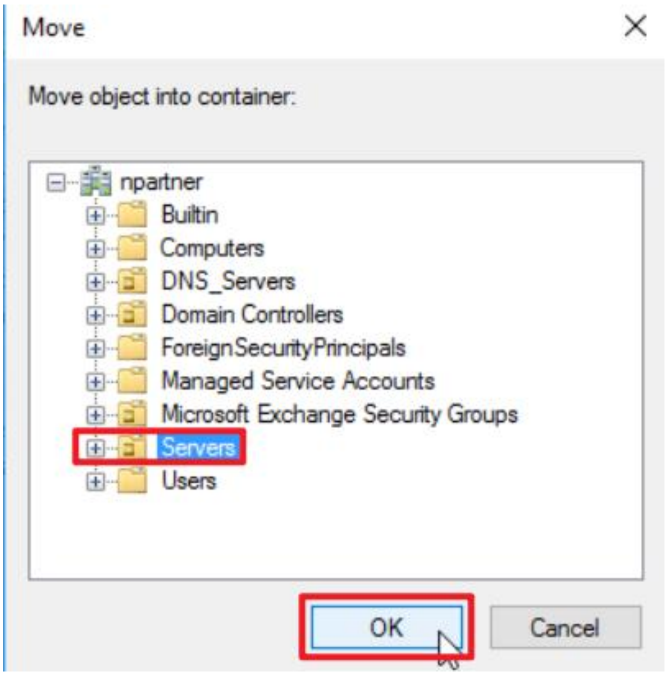
Note: Please select the MS SQL server according to the actual environment. → click “Move.”



Moves the current selection to another organizational unit.

(5) Select your Organizational Unit:

Select your organizational unit (in this example, it is “Servers”) → click “OK.”



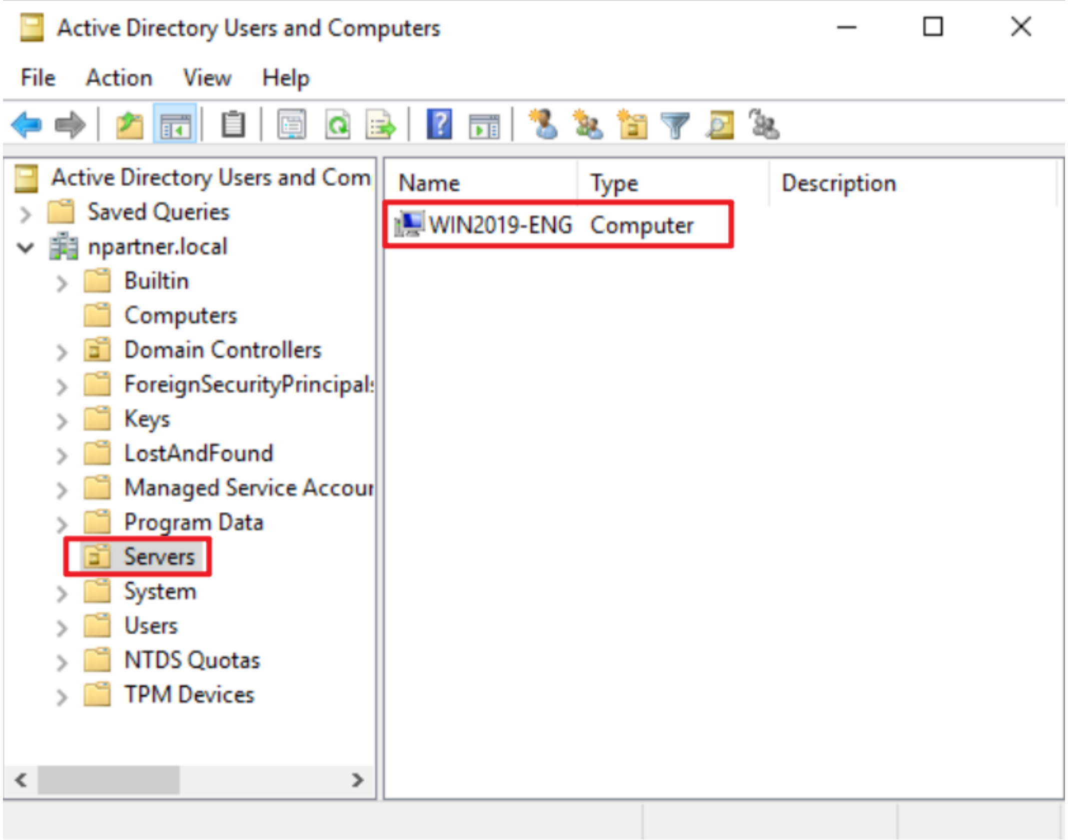
Move

Move object into container:

- npartner
  - Builtin
  - Computers
  - DNS_Servers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - Managed Service Accounts
  - Microsoft Exchange Security Groups
  - Servers
  - Users

(6) Verify the Server Has Been Moved to your New Organizational Unit:

Expand your organizational unit folder (in this example, it is “Servers”) and confirm that the “WIN2019-ENG” server has been moved.



Active Directory Users and Computers

- Active Directory Users and Com
  - Saved Queries
  - npartner.local
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipal:
    - Keys
    - LostAndFound
    - Managed Service Accour
    - Program Data
    - Servers
    - System
    - Users
    - NTDS Quotas
    - TPM Devices

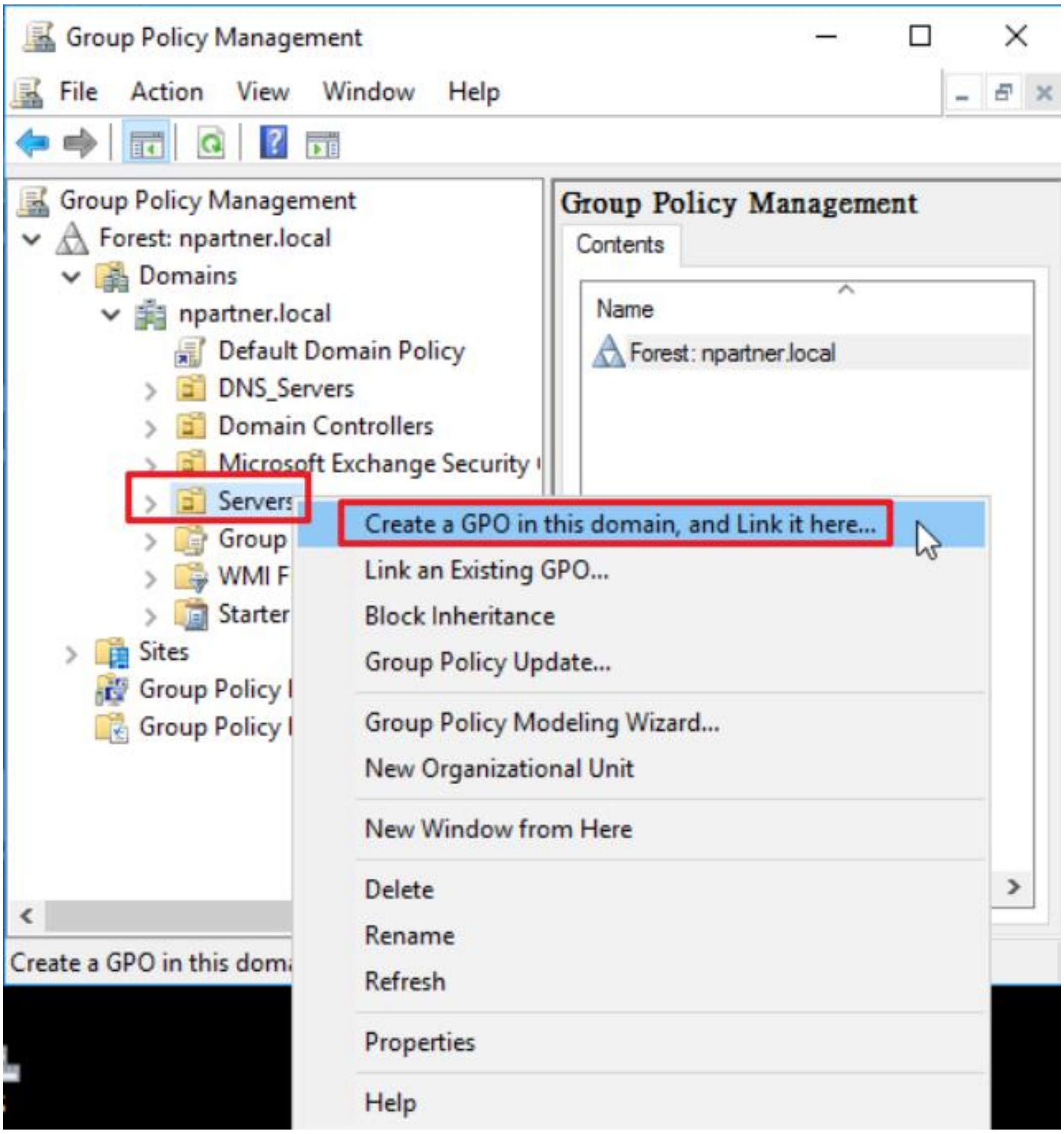
Name	Type	Description
WIN2019-ENG	Computer	

5.3.1.2 Group Policy Settings

(1) Click “Group Policy Management.”

(2) In the Servers organizational unit (OU), create a new Group Policy Object (GPO):

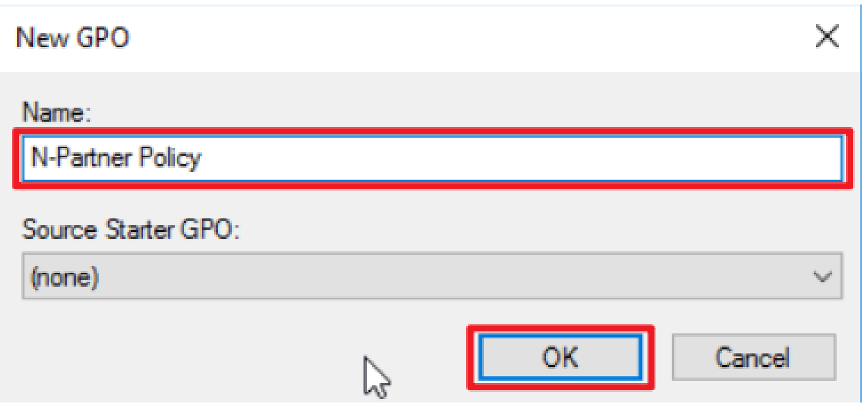
Right-click the [Servers] organizational unit → select “Create a GPO in this domain, and Link it here...”



(3) Edit your Group Policy Object

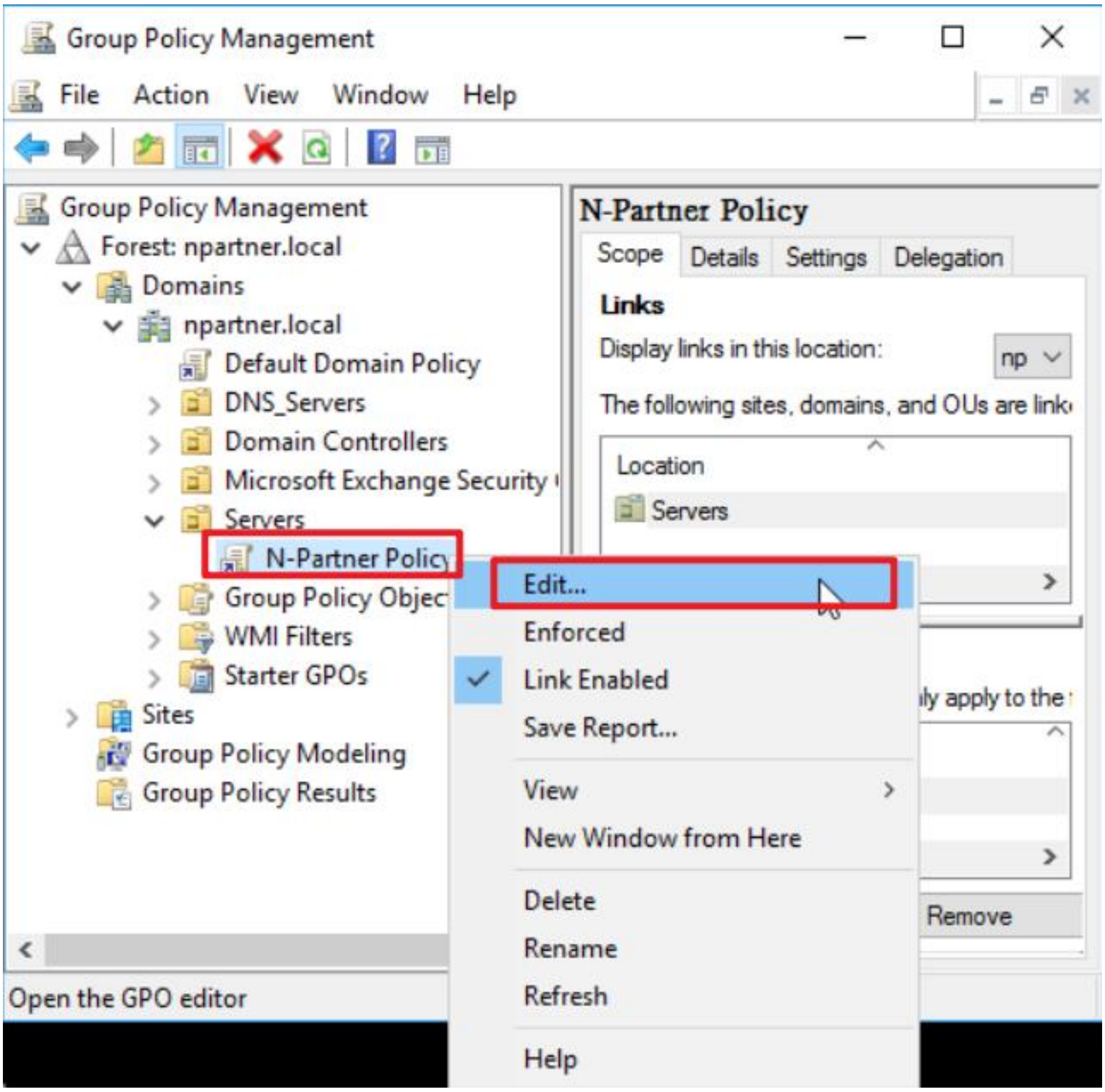
Enter your Group Policy Object name. (in this example, it is “N-Partner Policy”)

Note: Create your GPO name according to the actual environment. Then click “Edit.”



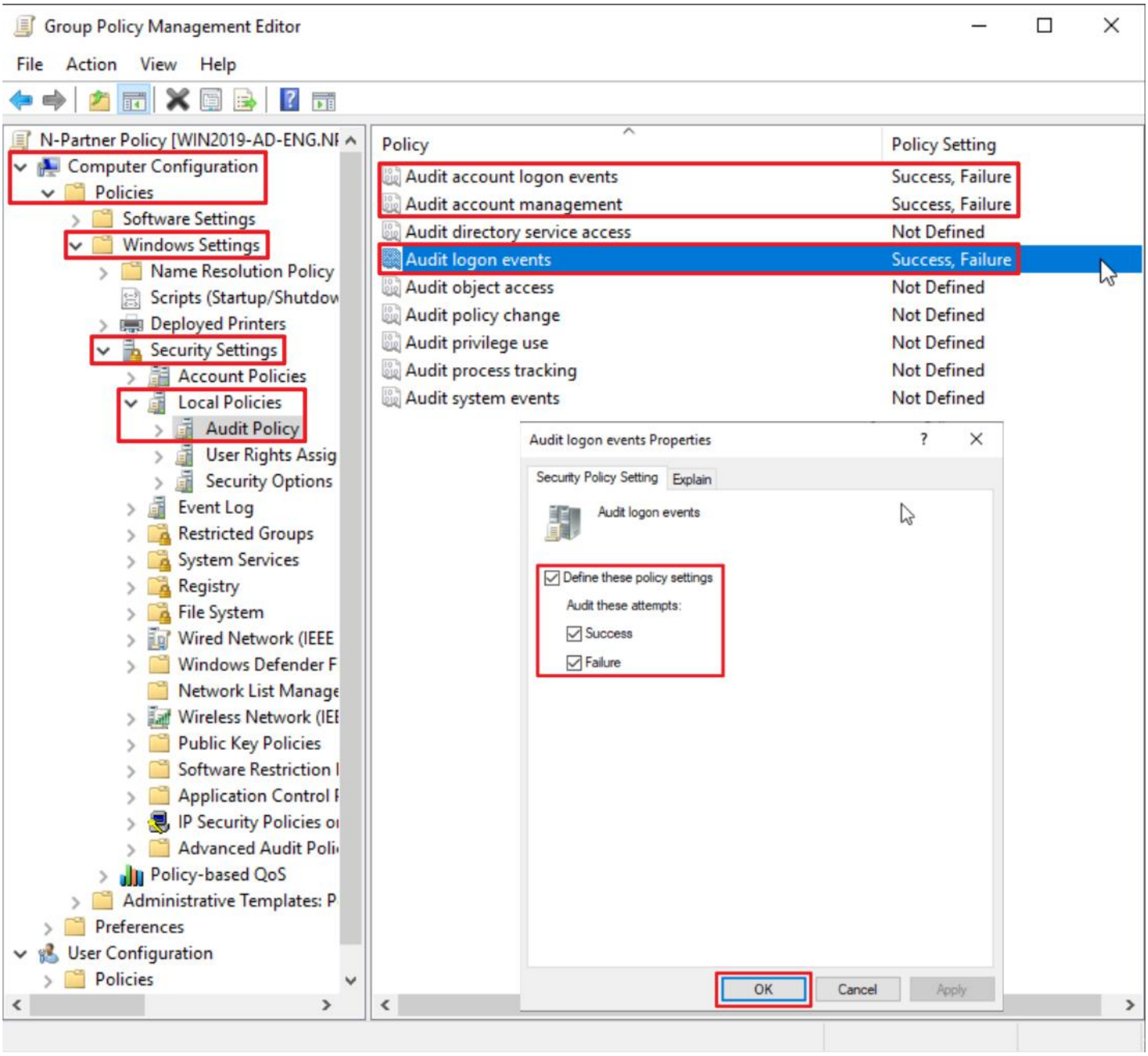
(4) Edit your Group Policy Object

In your group policy object, (in this example, it is “N-Partner Policy”)
right-click and select “Edit.”



(5) Local Group Policies: Audit Policy

Expand folder “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Local Policies” → “Audit Policy.” And click on “Audit account logon events,” “Audit account management,” and “Audit logon events,” → check “Define these policy settings”: Success, Failure. → click “OK.”


Group Policy Management Editor

Policy	Policy Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Not Defined
Audit logon events	Success, Failure
Audit object access	Not Defined
Audit policy change	Not Defined
Audit privilege use	Not Defined
Audit process tracking	Not Defined
Audit system events	Not Defined

Audit logon events Properties

Audit logon events

☑ Define these policy settings

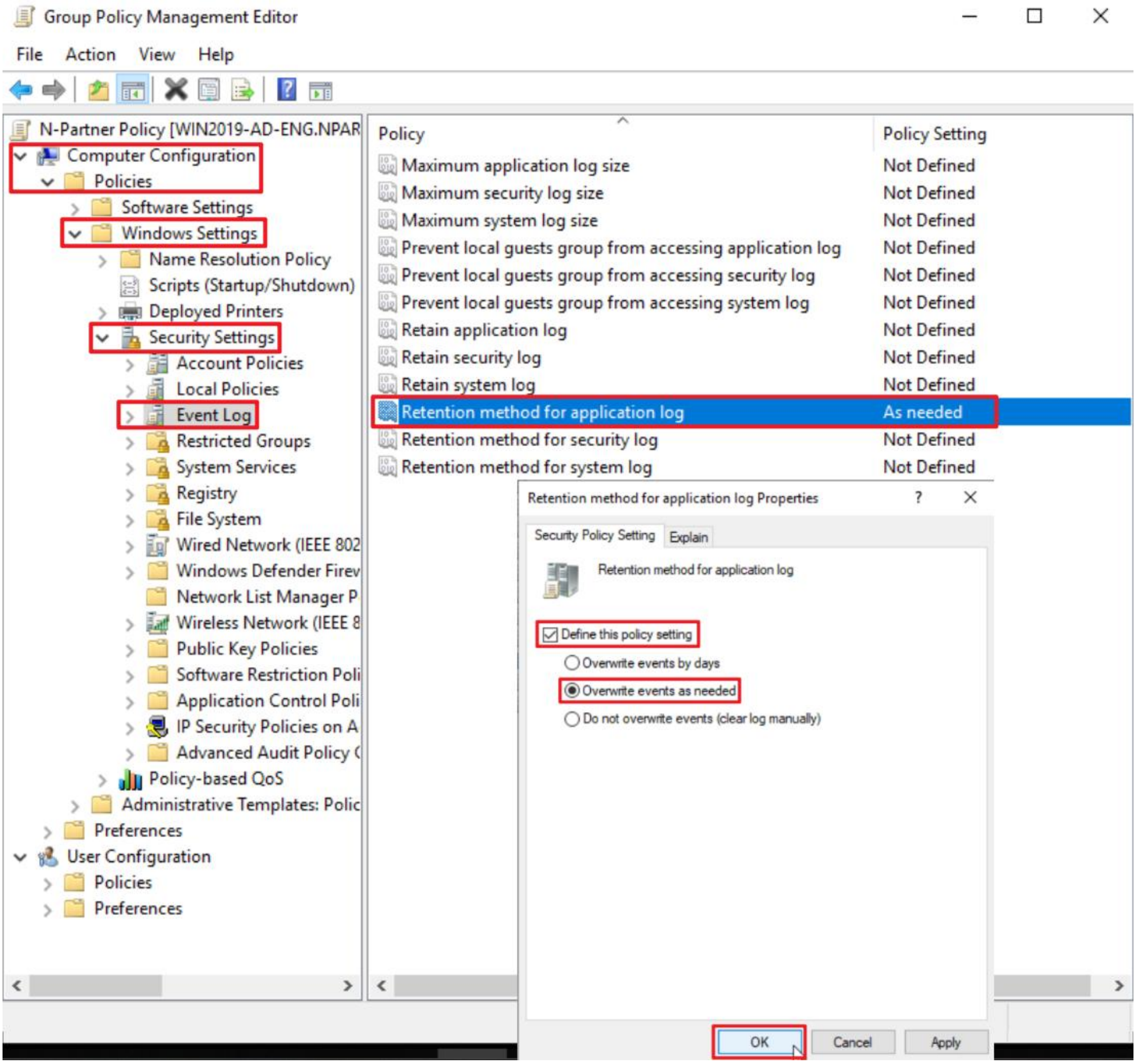
Audit these attempts:

☑ Success

☑ Failure

(6) Event Log: Application Log Retention Method

Expand “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” → select “Retention method for application log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



Policy	Policy Setting
Maximum application log size	Not Defined
Maximum security log size	Not Defined
Maximum system log size	Not Defined
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	As needed
Retention method for security log	Not Defined
Retention method for system log	Not Defined

Retention method for application log Properties

Security Policy Setting | Explain

Retention method for application log

☑ Define this policy setting

○ Overwrite events by days

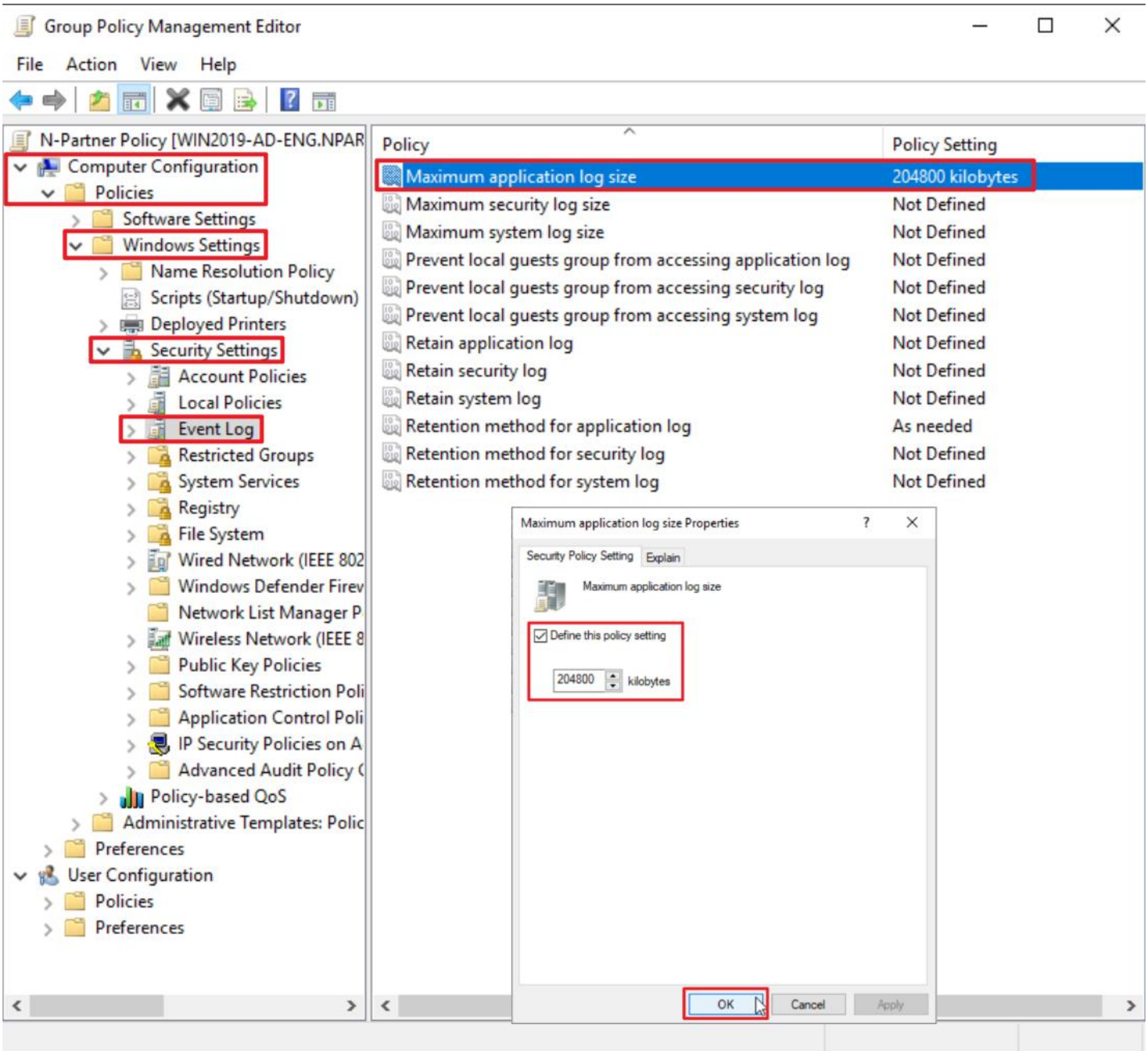
● Overwrite events as needed

○ Do not overwrite events (clear log manually)

(7) Event Logs: Maximum Size of Security Log

Expand folder “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” →And click on “Maximum application log size” → Check “Define this policy setting” → enter 204800 KB

Note: Please adjust the number based on the actual environment. → click “OK.”



Policy	Policy Setting
Maximum application log size	204800 kilobytes
Maximum security log size	Not Defined
Maximum system log size	Not Defined
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	As needed
Retention method for security log	Not Defined
Retention method for system log	Not Defined

Maximum application log size

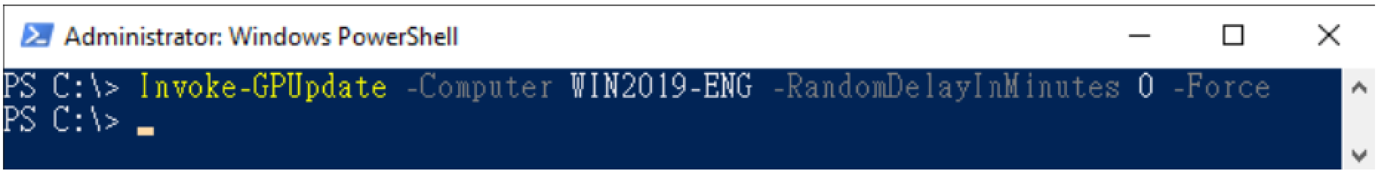
☑ Define this policy setting

204800 kilobytes

(8) On the AD domain server, open “Windows PowerShell.”

(9) Enter the command below to refresh group policy.

```
PS C:\> Invoke-GPUpdate -Computer WIN2019-ENG -RandomDelayInMinutes 0 -Force
```

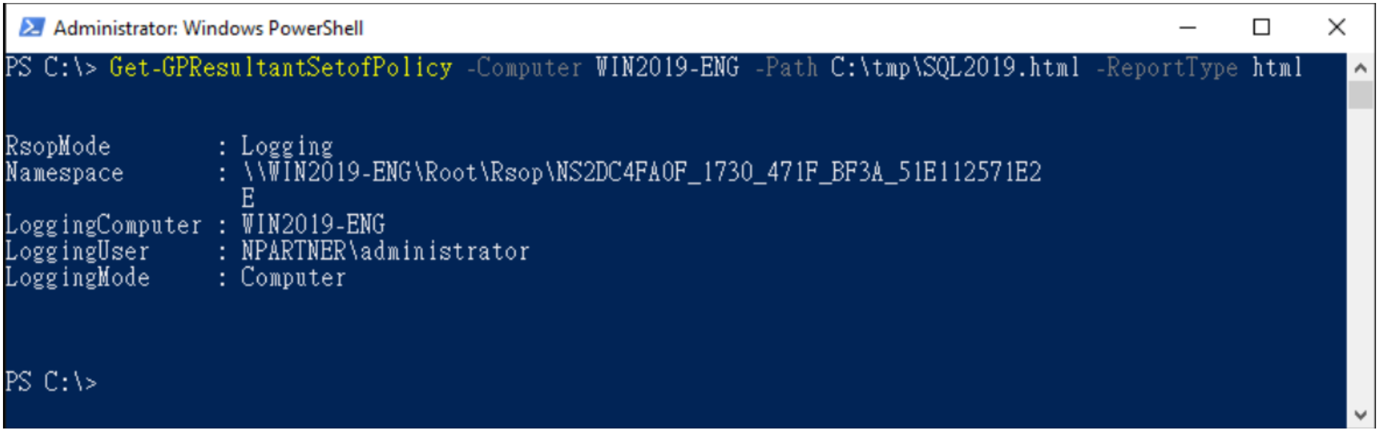


```
PS C:\> Invoke-GPUpdate -Computer WIN2019-ENG -RandomDelayInMinutes 0 -Force
PS C:\> _
```

Replace the text shown in red with the MS SQL server name.

(10) Enter the command below to generate server group policy report.

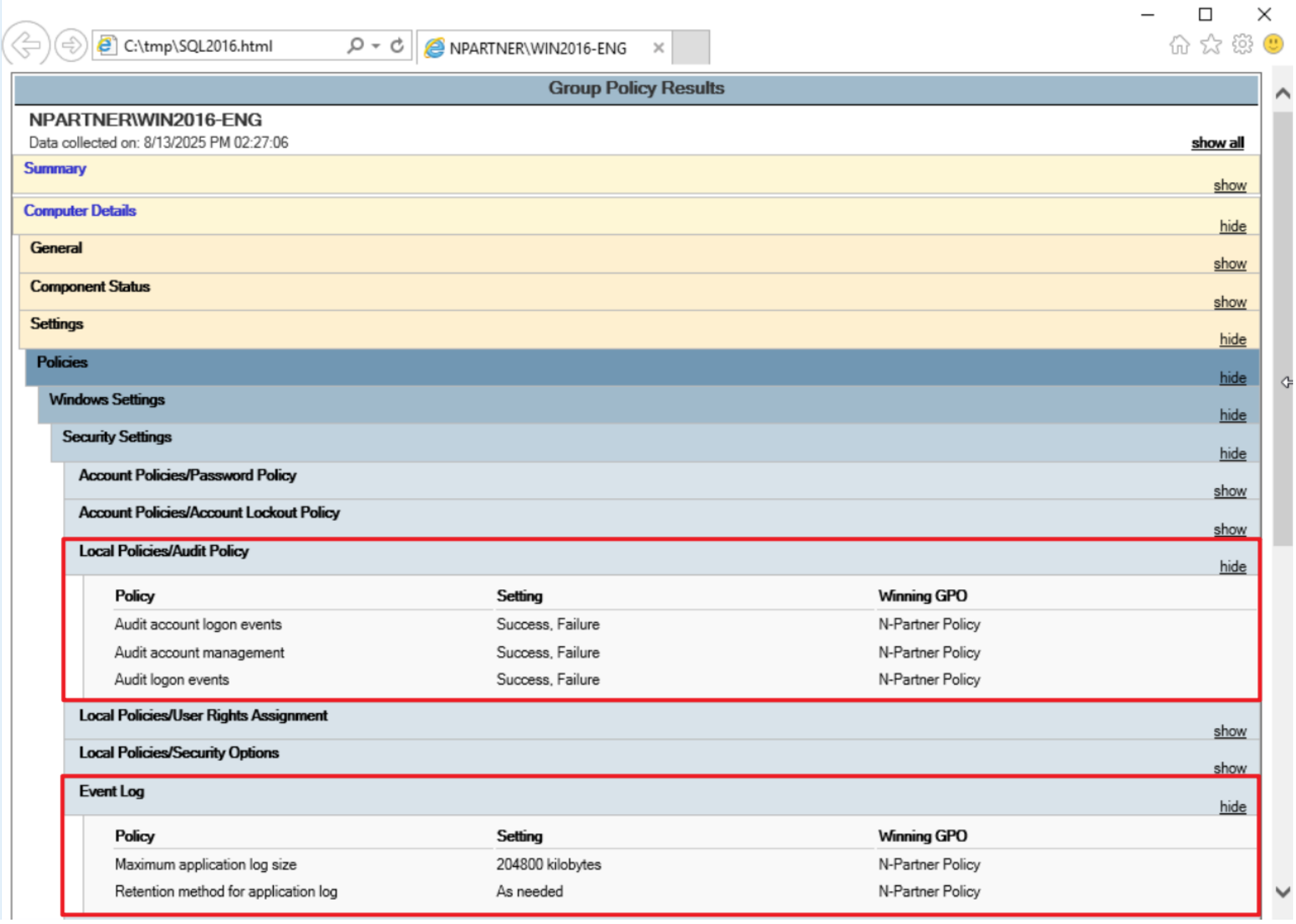
```
PS C:\> Get-GPResultantSetofPolicy -Computer WIN2019-ENG -Path C:\tmp\SQL2019.htnl -ReportType.html
```



```
PS C:\> Get-GPResultantSetofPolicy -Computer WIN2019-ENG -Path C:\tmp\SQL2019.html -ReportType html


RsopMode        : Logging
Namespace       : \\WIN2019-ENG\Root\Rsop\NS2DC4FA0F_1730_471F_BF3A_51E112571E2
                  E
LoggingComputer : WIN2019-ENG
LoggingUser     : NPARTNER\administrator
LoggingMode     : Computer



PS C:\>
```

For the red text , please enter the MS SQL server name and the folder path/file name.

(11) Open the report and verify that your MS SQL server is applying the N-Partner Policy Group Policy.



Group Policy Results

NPARTNER\WIN2016-ENG
Data collected on: 8/13/2025 PM 02:27:06 show all

Summary show

Computer Details hide

General show

Component Status show

Settings hide

Policies hide

Windows Settings hide

Security Settings hide

Account Policies/Password Policy show

Account Policies/Account Lockout Policy show

Local Policies/Audit Policy hide

Policy	Setting	Winning GPO
Audit account logon events	Success, Failure	N-Partner Policy
Audit account management	Success, Failure	N-Partner Policy
Audit logon events	Success, Failure	N-Partner Policy

Local Policies/User Rights Assignment show

Local Policies/Security Options show

Event Log hide

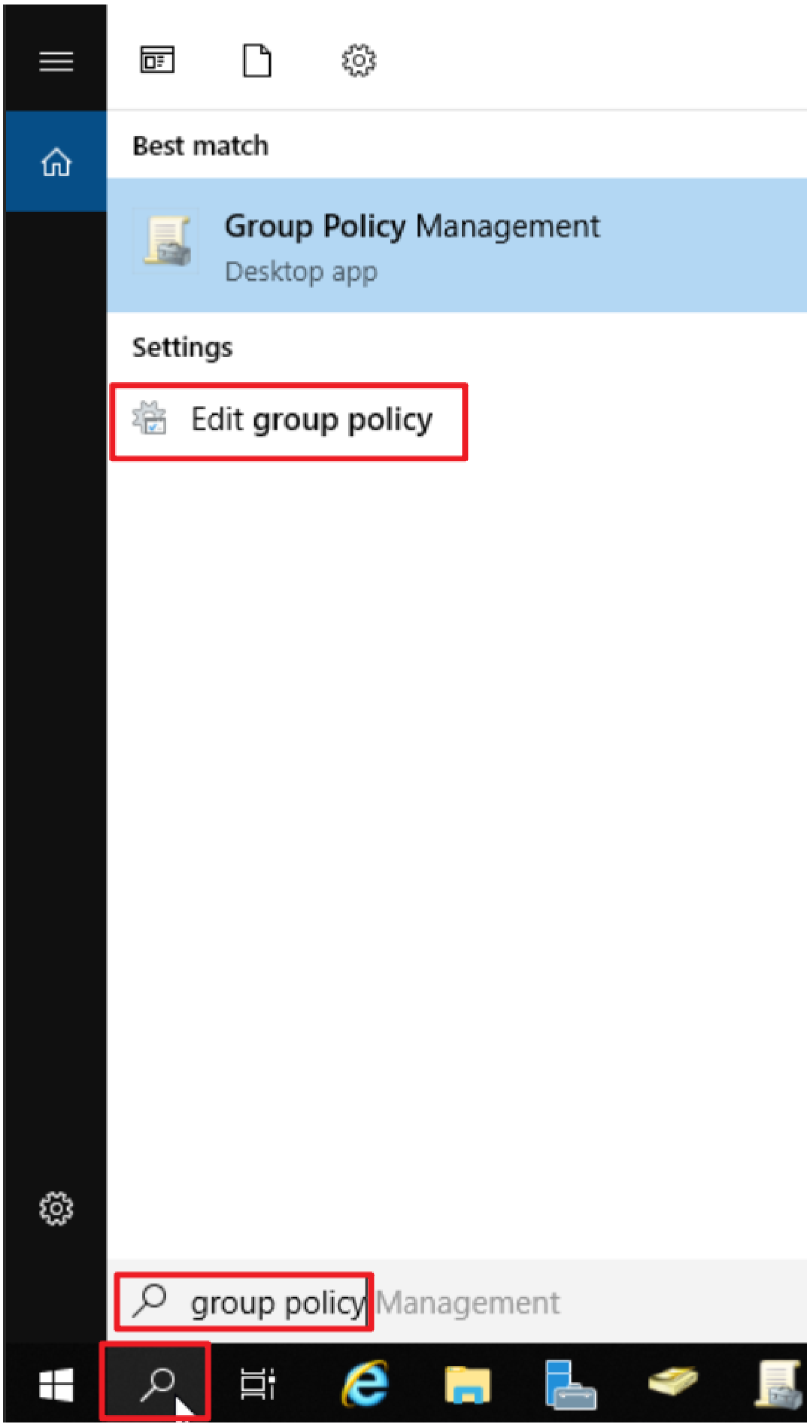
Policy	Setting	Winning GPO
Maximum application log size	204800 kilobytes	N-Partner Policy
Retention method for application log	As needed	N-Partner Policy

5.3.2 Workgroup

5.3.2.1 Audit Policy Configuration

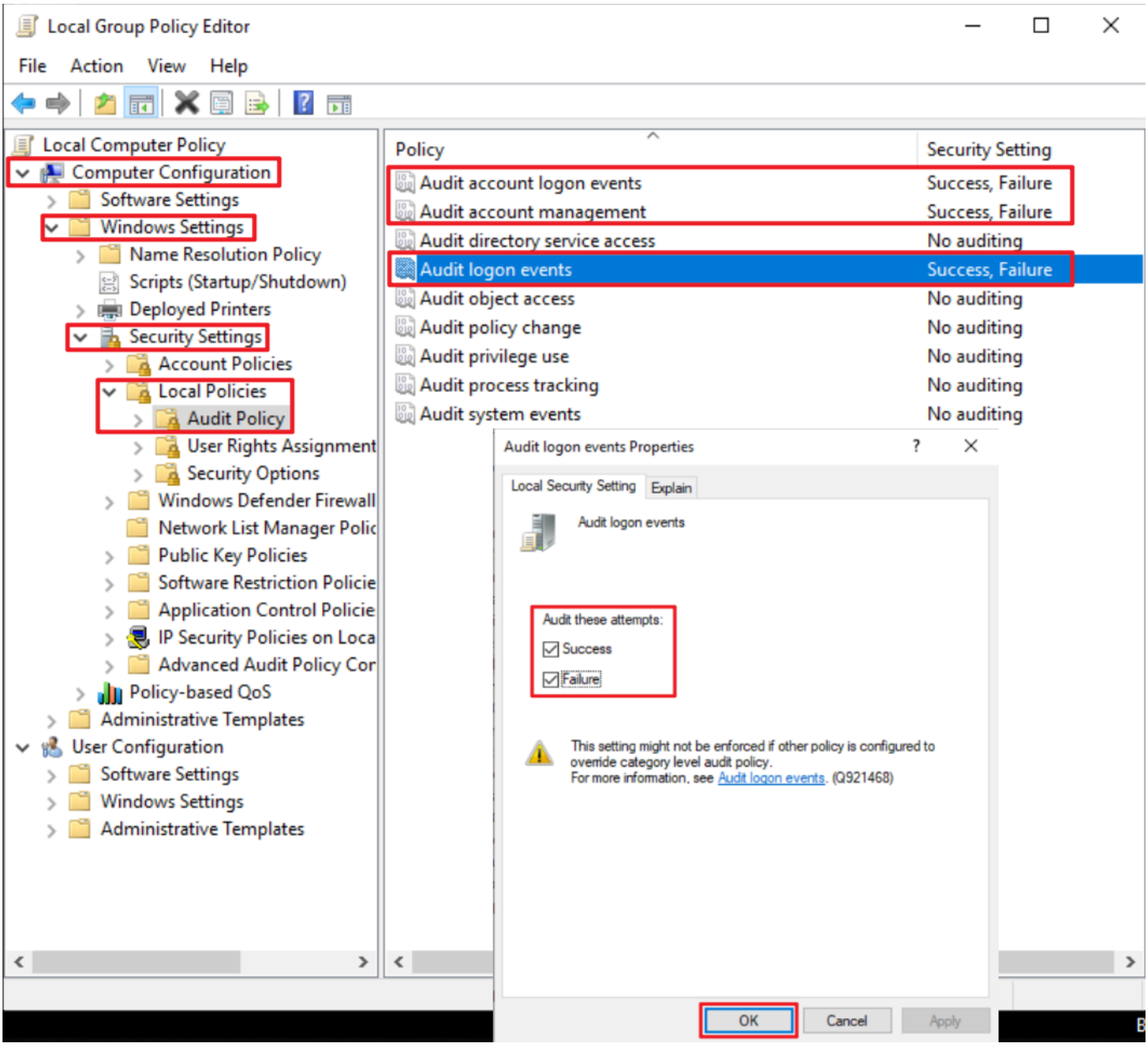
(1) Open Local Group Policy Editor

Click on “Start” → enter “group policy” to search → click on “Edit Group Policy.”



(2) Local Group Policies: Audit Policy

Expand folder “Computer Configuration” → “Windows Settings” → “Security Settings” -> “Local Policies” → “Audit Policy.” And click on “Audit account logon events,” “Audit account management,” and “Audit logon events” items → check “Define these policy settings”: Success, Failure. → click “OK.”



Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	No auditing
Audit logon events	Success, Failure
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

Audit logon events Properties

Local Security Setting | Explain

Audit logon events

Audit these attempts:

☑ Success

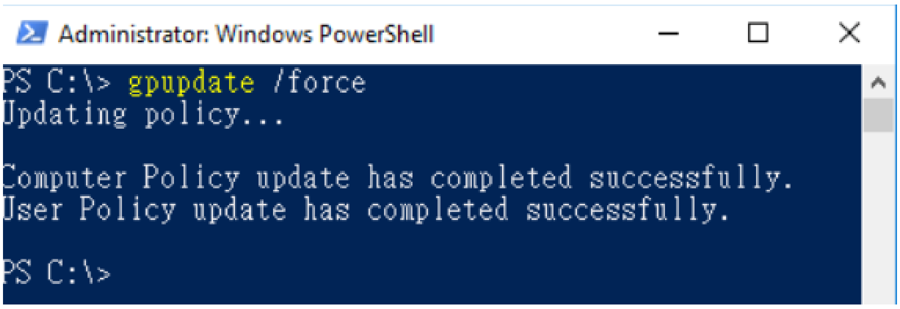
☑ Failure

This setting might not be enforced if other policy is configured to override category level audit policy.
For more information, see Audit logon events. (Q921468)

(3) Open “Windows PowerShell.”

(4) Enter the command below to refresh group policy.

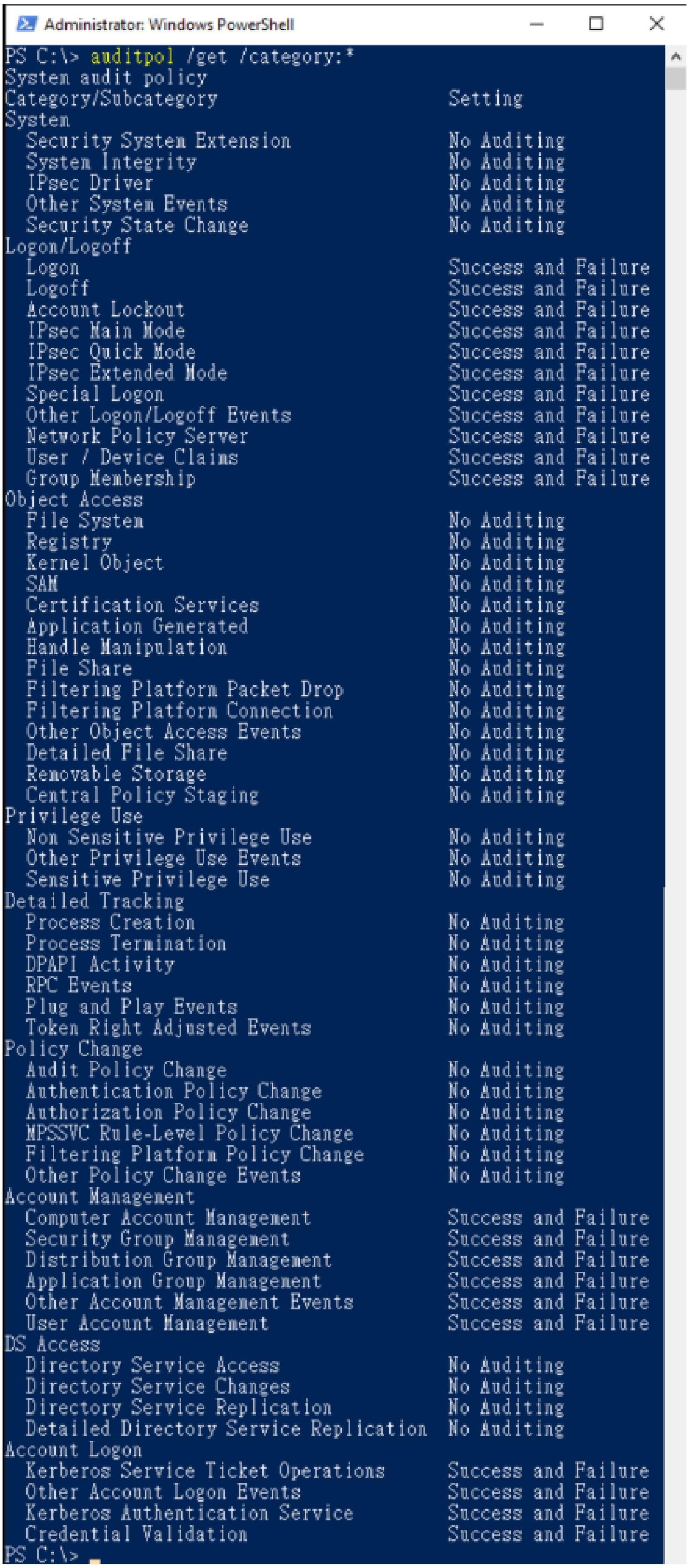
```
PS C:\> gpupdate /force
```



```
PS C:\> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

PS C:\>
```

(5) Enter the command below to view group policy applied status.

```
PS C: \> auditpol /get /category:*
```

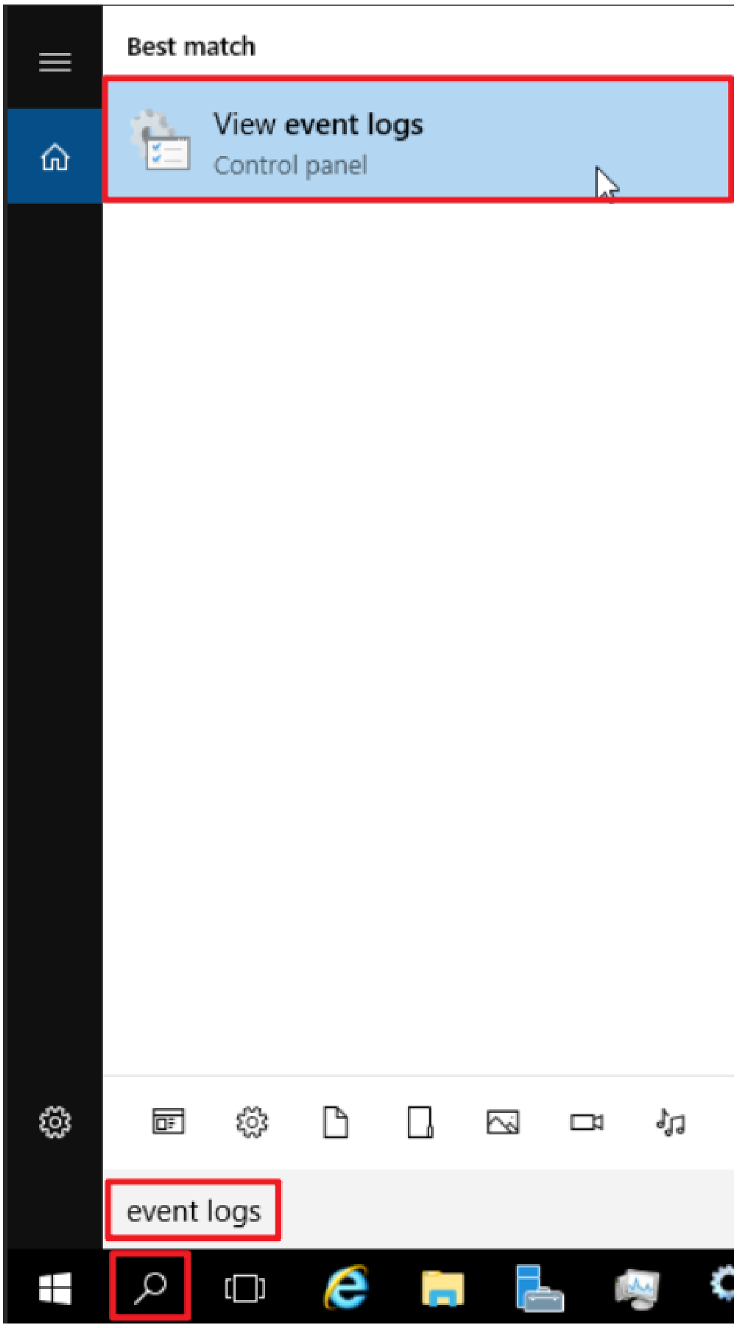


```
PS C:\> auditpol /get /category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               No Auditing
  System Integrity                        No Auditing
  IPsec Driver                            No Auditing
  Other System Events                     No Auditing
  Security State Change                   No Auditing
Logon/Logoff
  Logon                                   Success and Failure
  Logoff                                  Success and Failure
  Account Lockout                         Success and Failure
  IPsec Main Mode                         Success and Failure
  IPsec Quick Mode                        Success and Failure
  IPsec Extended Mode                     Success and Failure
  Special Logon                           Success and Failure
  Other Logon/Logoff Events               Success and Failure
  Network Policy Server                   Success and Failure
  User / Device Claims                    Success and Failure
  Group Membership                        Success and Failure
Object Access
  File System                             No Auditing
  Registry                                No Auditing
  Kernel Object                           No Auditing
  SAM                                     No Auditing
  Certification Services                  No Auditing
  Application Generated                   No Auditing
  Handle Manipulation                     No Auditing
  File Share                              No Auditing
  Filtering Platform Packet Drop          No Auditing
  Filtering Platform Connection           No Auditing
  Other Object Access Events              No Auditing
  Detailed File Share                     No Auditing
  Removable Storage                       No Auditing
  Central Policy Staging                  No Auditing
Privilege Use
  Non Sensitive Privilege Use             No Auditing
  Other Privilege Use Events              No Auditing
  Sensitive Privilege Use                 No Auditing
Detailed Tracking
  Process Creation                        No Auditing
  Process Termination                     No Auditing
  DPAPI Activity                          No Auditing
  RPC Events                              No Auditing
  Plug and Play Events                    No Auditing
  Token Right Adjusted Events             No Auditing
Policy Change
  Audit Policy Change                     No Auditing
  Authentication Policy Change            No Auditing
  Authorization Policy Change             No Auditing
  MPSSVC Rule-Level Policy Change         No Auditing
  Filtering Platform Policy Change        No Auditing
  Other Policy Change Events              No Auditing
Account Management
  Computer Account Management             Success and Failure
  Security Group Management               Success and Failure
  Distribution Group Management           Success and Failure
  Application Group Management             Success and Failure
  Other Account Management Events         Success and Failure
  User Account Management                 Success and Failure
DS Access
  Directory Service Access                No Auditing
  Directory Service Changes               No Auditing
  Directory Service Replication           No Auditing
  Detailed Directory Service Replication  No Auditing
Account Logon
  Kerberos Service Ticket Operations      Success and Failure
  Other Account Logon Events              Success and Failure
  Kerberos Authentication Service         Success and Failure
  Credential Validation                   Success and Failure
PS C:\>
```

5.3.2.2 Event Log Settings

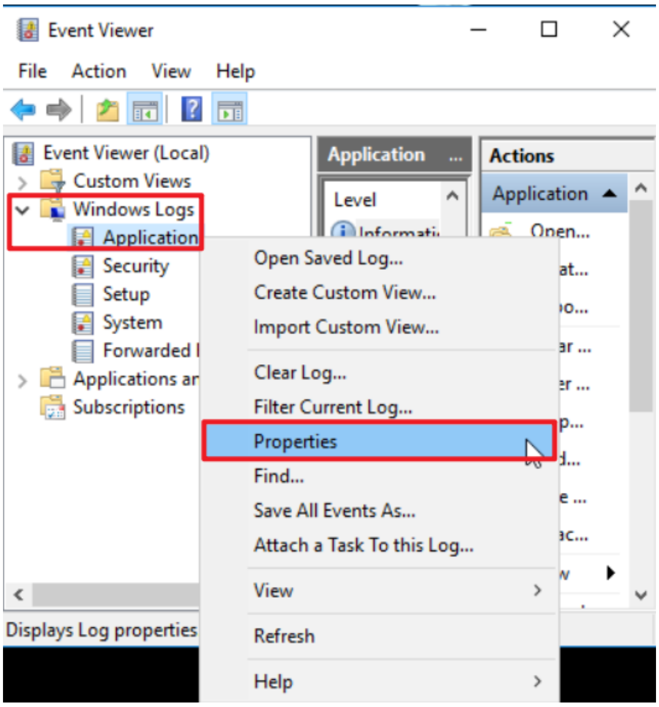
(1) Search for “Event Viewer”

Enter “Event Viewer” to search → click on “Event Viewer” in the search results.



(2) Edit Security Log

Expand folder “Windows Logs” → right-click on “Application” → And click on “Properties.”

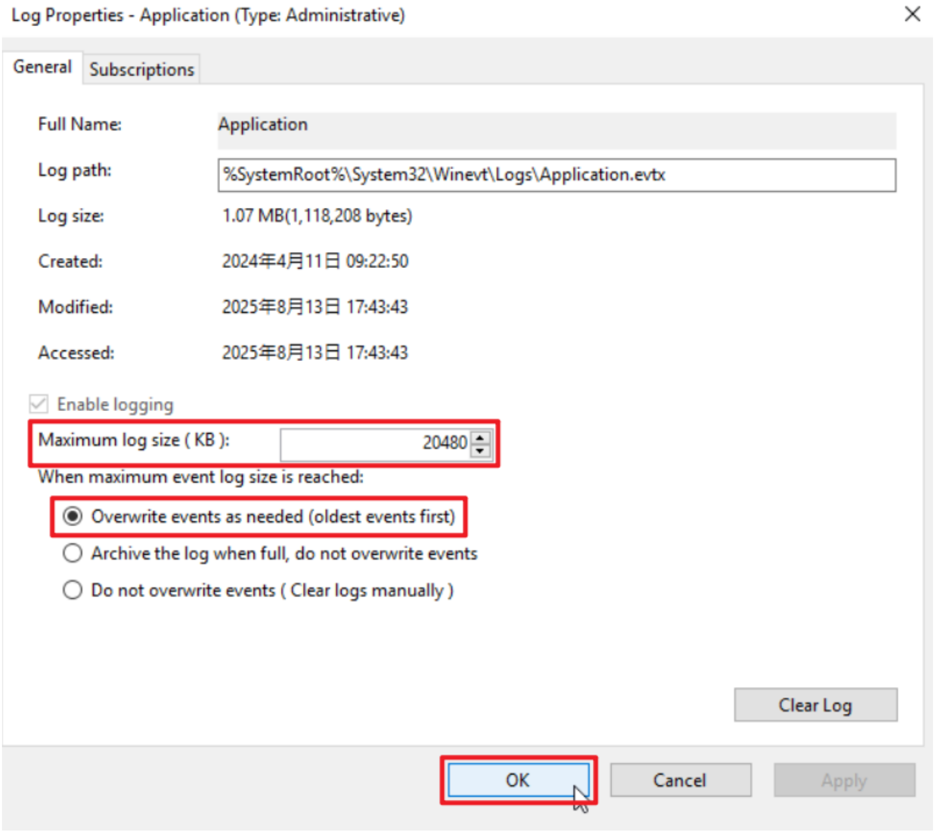


(3) Configure Security Log

Enter maximum log file size: 204800 KB

Note: Please adjust the number according to the actual environment.

→ click on “Overwrite events as needed (oldest events first)” → click “OK.”


Log Properties - Application (Type: Administrative)

General | Subscriptions

Full Name: Application

Log path: %SystemRoot%\System32\Winevt\Logs\Application.evtx

Log size: 1.07 MB(1,118,208 bytes)

Created: 2024年4月11日 09:22:50

Modified: 2025年8月13日 17:43:43

Accessed: 2025年8月13日 17:43:43

☑ Enable logging

Maximum log size (KB): 20480

When maximum event log size is reached:

● Overwrite events as needed (oldest events first)

○ Archive the log when full, do not overwrite events

○ Do not overwrite events (Clear logs manually)

6. SQL Server 2022

6.1 Login Auditing

Enable login auditing to monitor SQL Server Database Engine login activities.

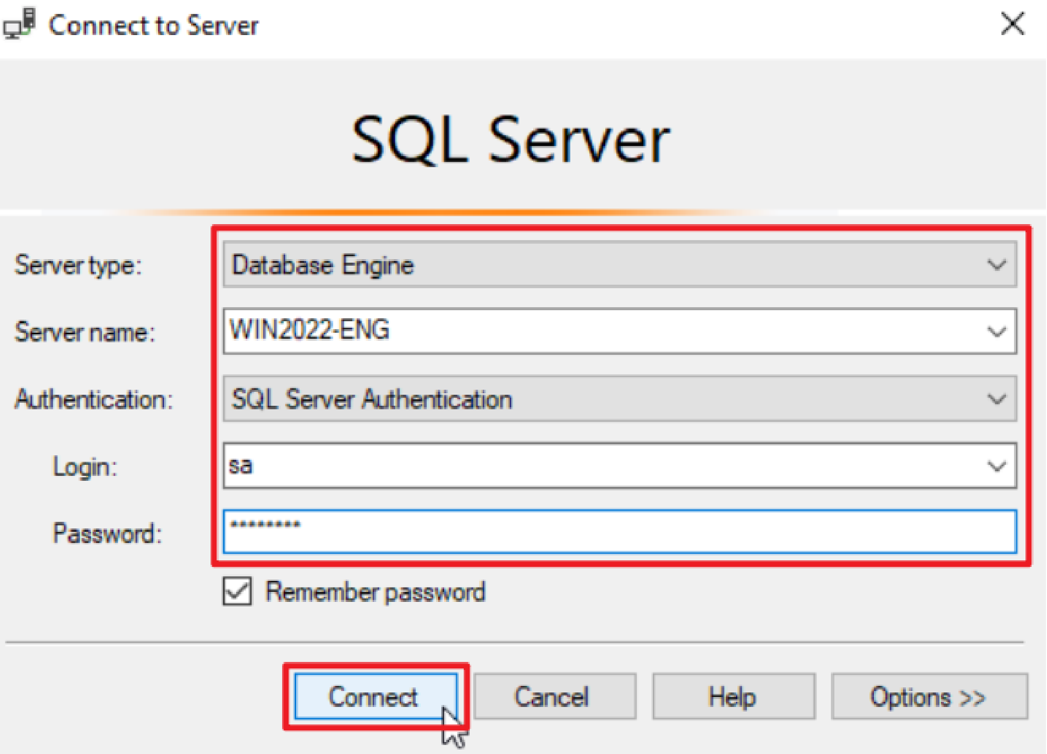
After configuration, the MS SQL Server service must be **restarted**.

The following sections describe how to configure login auditing using both the graphical user interface (GUI) and command-line interface (CLI).

6.1.1 Configuring via Graphical User Interface (GUI)

(1) Open “SQL Server Management Studio (SSMS).”

(2) Enter the server’s name → select the authentication method → click “Connect.”



Server type: Database Engine

Server name: WIN2022-ENG

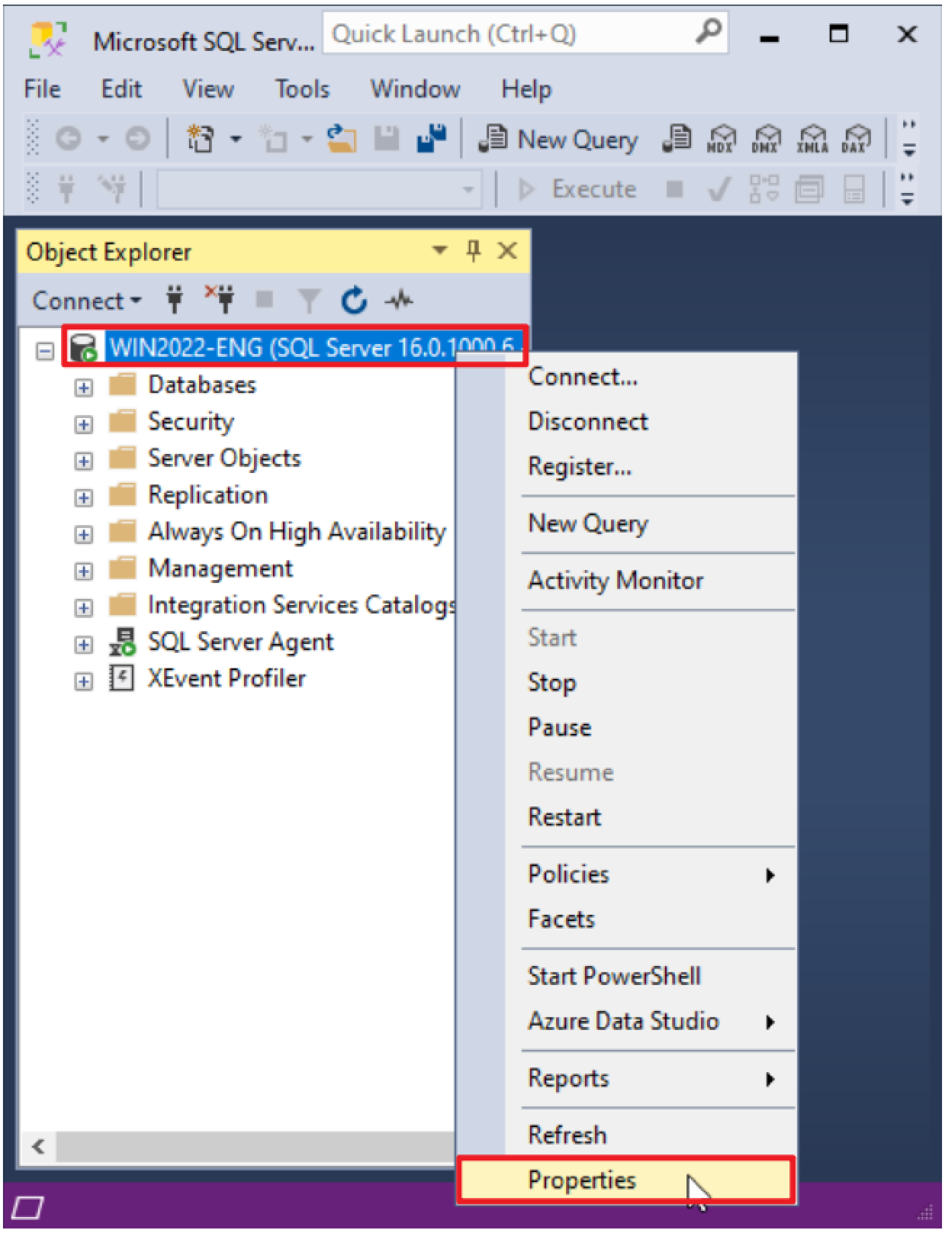
Authentication: SQL Server Authentication

Login: sa

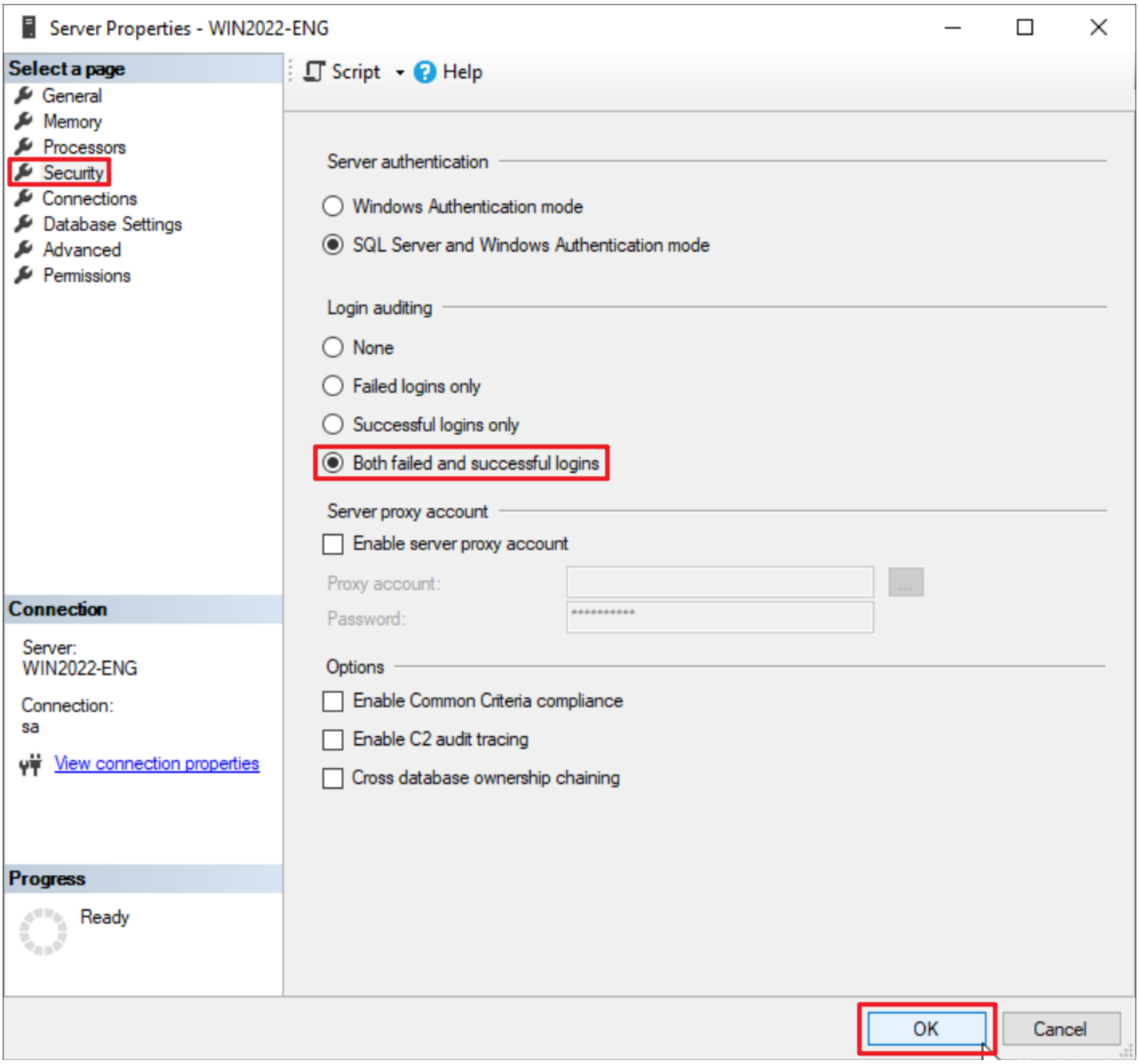
Password: ********

☑ Remember password

(3) In [Server Name] (the example here is WIN2022-ENG), right-click and select “Properties.”



(4) On the Security page, under Login auditing, select “Both failed and successful logins” → click “OK”.



Server Properties - WIN2022-ENG

Server authentication

○ Windows Authentication mode

● SQL Server and Windows Authentication mode

Login auditing

○ None

○ Failed logins only

○ Successful logins only

● Both failed and successful logins

Server proxy account

□ Enable server proxy account

Proxy account:

Password: ***********

Options

□ Enable Common Criteria compliance

□ Enable C2 audit tracing

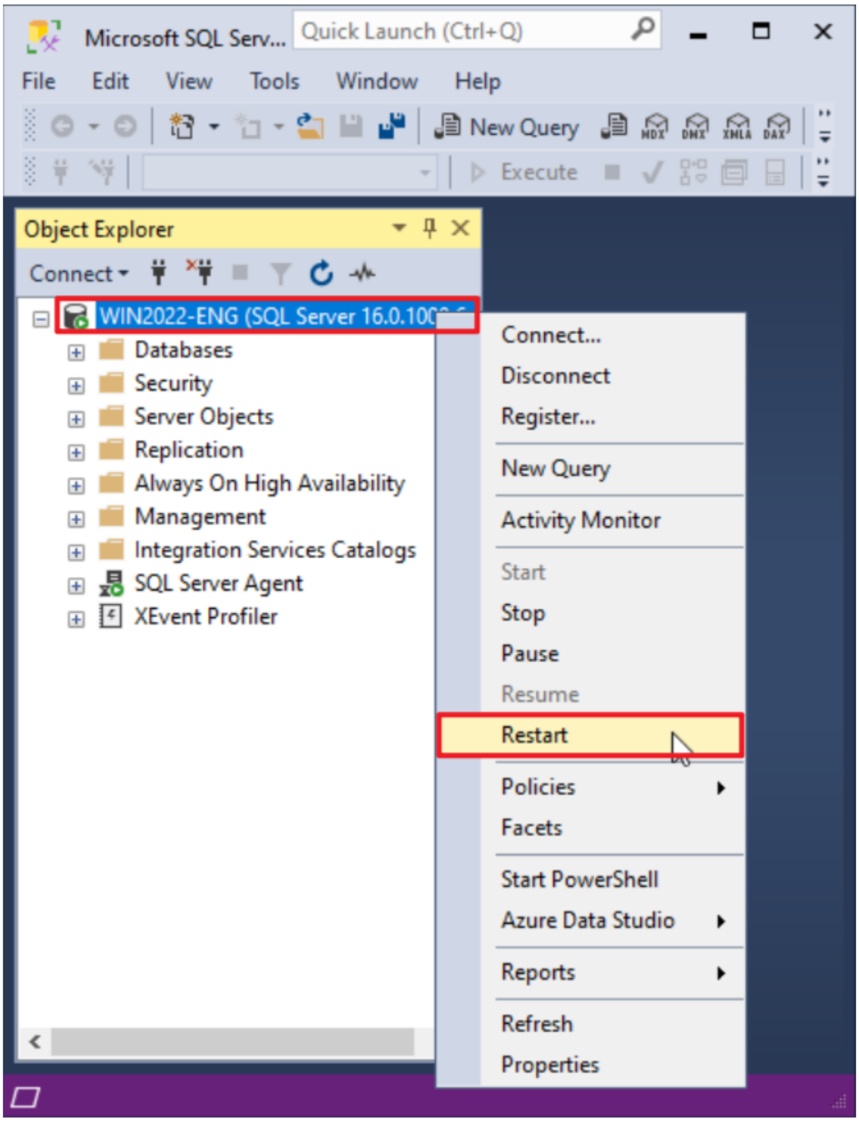
□ Cross database ownership chaining

Connection

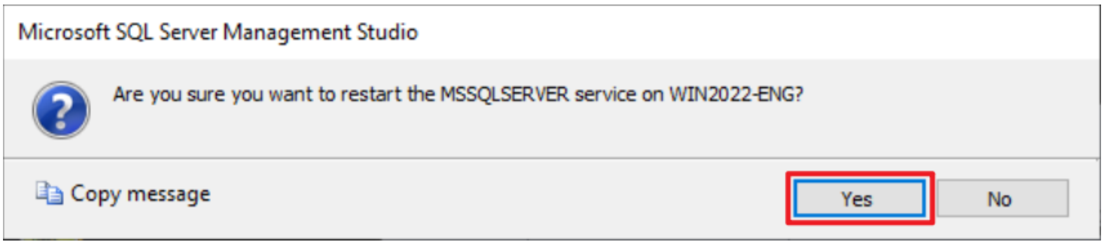
Server:
WIN2022-ENG

Connection:
sa

(5) Restart the MS SQL Server service: right-click [Server Name] (the example here is WIN2022-ENG) → select "Restart."



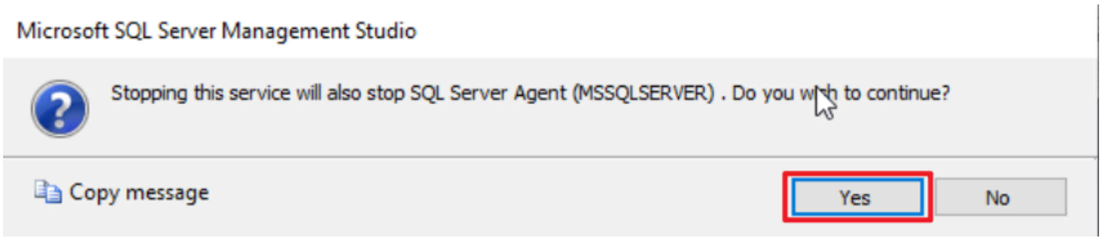
(6) Click "Yes" to restart the MS SQL Server service.



Microsoft SQL Server Management Studio

Are you sure you want to restart the MSSQLSERVER service on WIN2022-ENG?

(7) Click "Yes" again to stop the SQL Server Agent service. =.



Microsoft SQL Server Management Studio

Stopping this service will also stop SQL Server Agent (MSSQLSERVER) . Do you wish to continue?

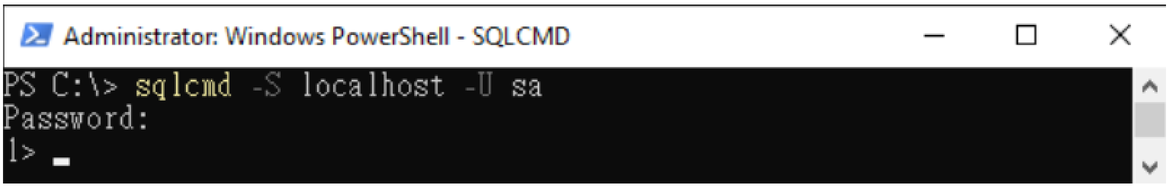
6.1.2 Configuring via Command-Line Interface (CLI)

(1) Open “Windows PowerShell.”

(2) Enter the command below to log in using sa:

<2.1>Using sa account:

```
PS C:\> sqlcmd -S localhost -U sa
```



```
PS C:\> sqlcmd -S localhost -U sa
Password:
1> _
```

Options:

-S [protocol:]server[instance_name][,port]

-U login_id

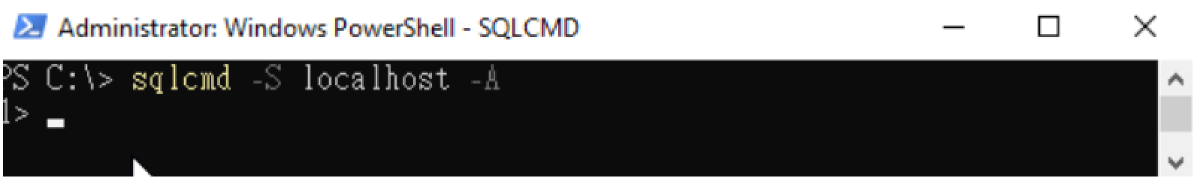
-P password

-A dedicated administrator connection

<2.2> Using Windows account:

Enter the command below to log in using Windows:

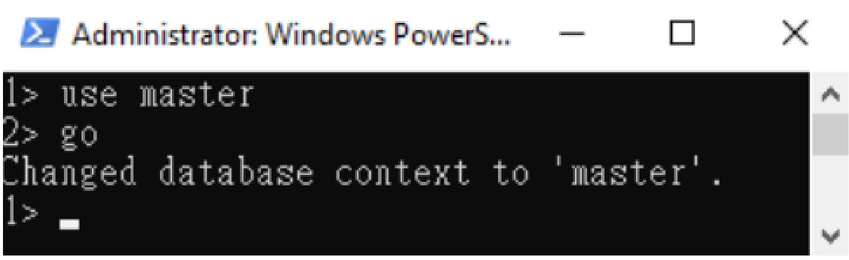
```
PS C:\> sqlcmd -S localhost -A
```



```
PS C:\> sqlcmd -S localhost -A
1> _
```

(3) Enter the command below to switch to the **master** database:

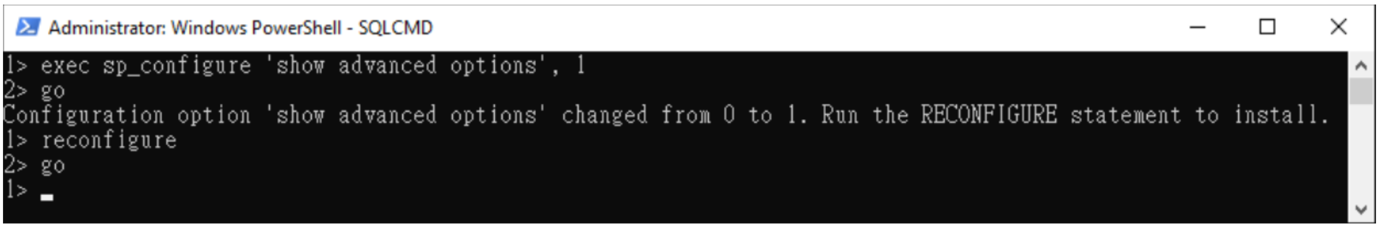
```
1 > use master
2 > go
```



```
1> use master
2> go
Changed database context to 'master'.
1>
```

(4) Enter the command below to enable advanced options:

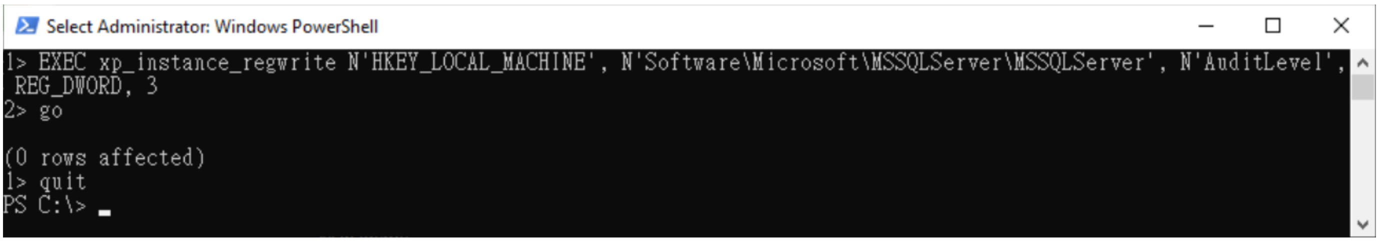
```
1 > exec sp_configure 'show advanced options', 1
2 > go
1 > reconfigure
2 > go
```



```
1> exec sp_configure 'show advanced options', 1
2> go
Configuration option 'show advanced options' changed from 0 to 1. Run the RECONFIGURE statement to install.
1> reconfigure
2> go
1>
```

(5) Enter the command below to enable auditing for both failed and successful logins:

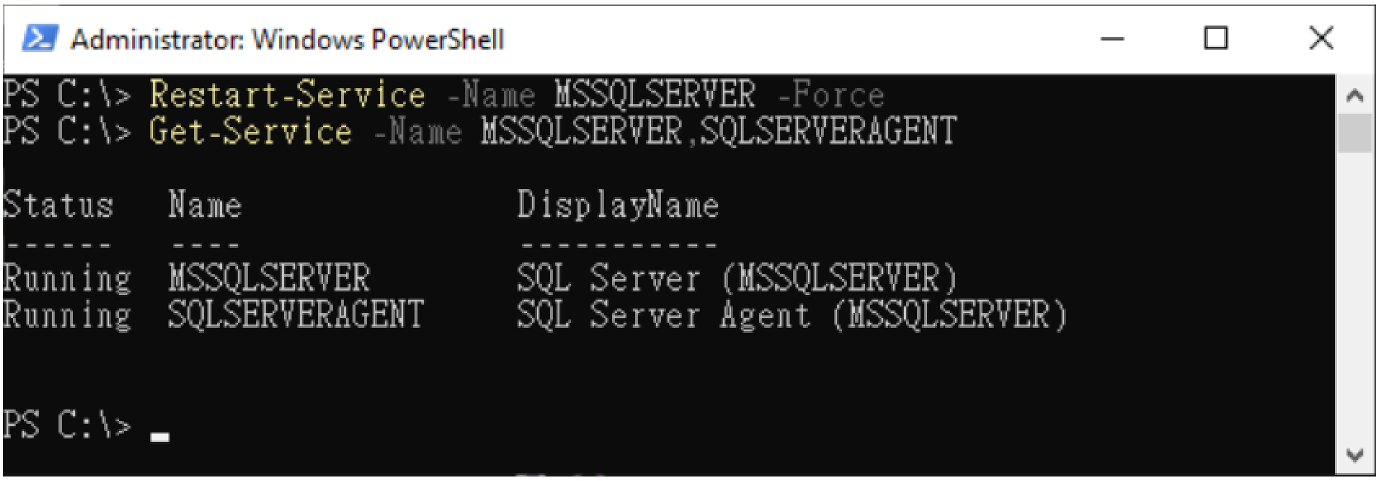
```
1 > EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE',
N'Software\Microsoft\MSSQLServer\MSSQLServer', N'AuditLevel', REG_DWORD, 3
2 > go
```



```
1> EXEC xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'Software\Microsoft\MSSQLServer\MSSQLServer', N'AuditLevel',
 REG_DWORD, 3
2> go

(0 rows affected)
1> quit
PS C:\>
```

(6) Enter the command below to restart the MS SQL Server services:

```
PS C:\> Restart-Service -Name MSSQLSERVER -Force
PS C:\> Get-Service -Name MSSQLSERVER,SQLSERVERAGENT
```



```
PS C:\> Restart-Service -Name MSSQLSERVER -Force
PS C:\> Get-Service -Name MSSQLSERVER,SQLSERVERAGENT

Status   Name               DisplayName
------   ----               -----------
Running  MSSQLSERVER        SQL Server (MSSQLSERVER)
Running  SQLSERVERAGENT     SQL Server Agent (MSSQLSERVER)


PS C:\> _
```

6.2 Configuring Auditing

6.2.1 Server-Level Audit

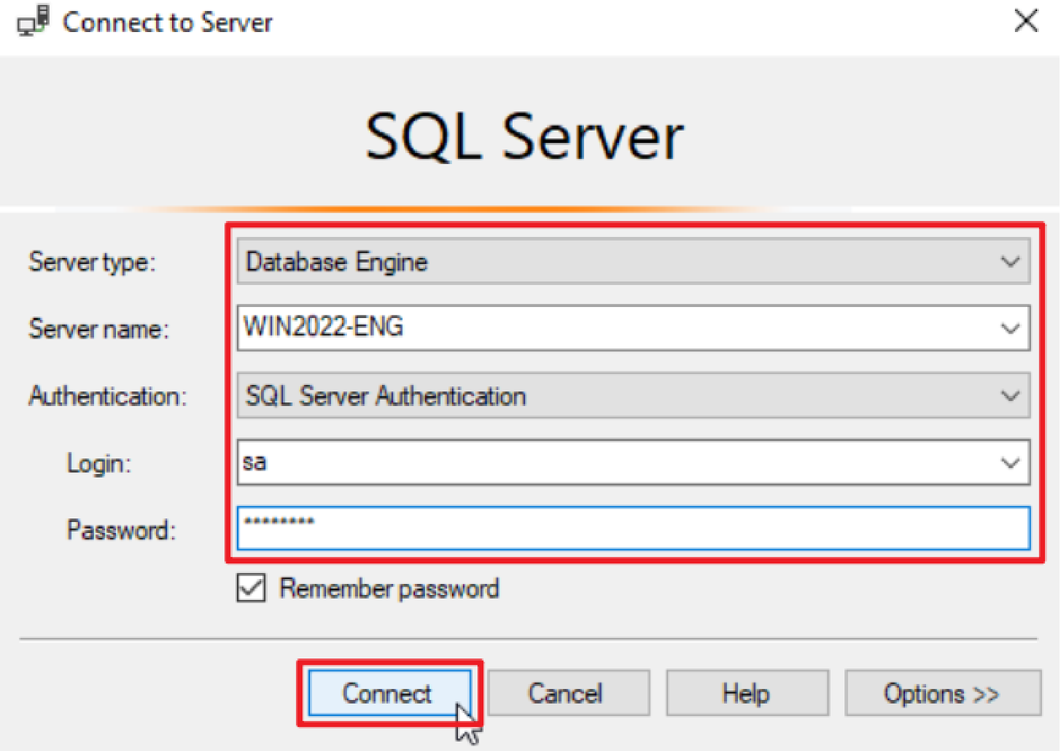
Enabling a server-level audit covers server operations such as administrative changes, login, and logout activities.

The following sections describe how to configure a server-level audit using the graphical user interface (GUI) and the command-line interface (CLI).

6.2.1.1 Configuring via Graphical User Interface (GUI)

(1) Open “SQL Server Management Studio (SSMS).”

(2) Enter the server’s name → select the authentication method → click “Connect.”



Server type: Database Engine

Server name: WIN2022-ENG

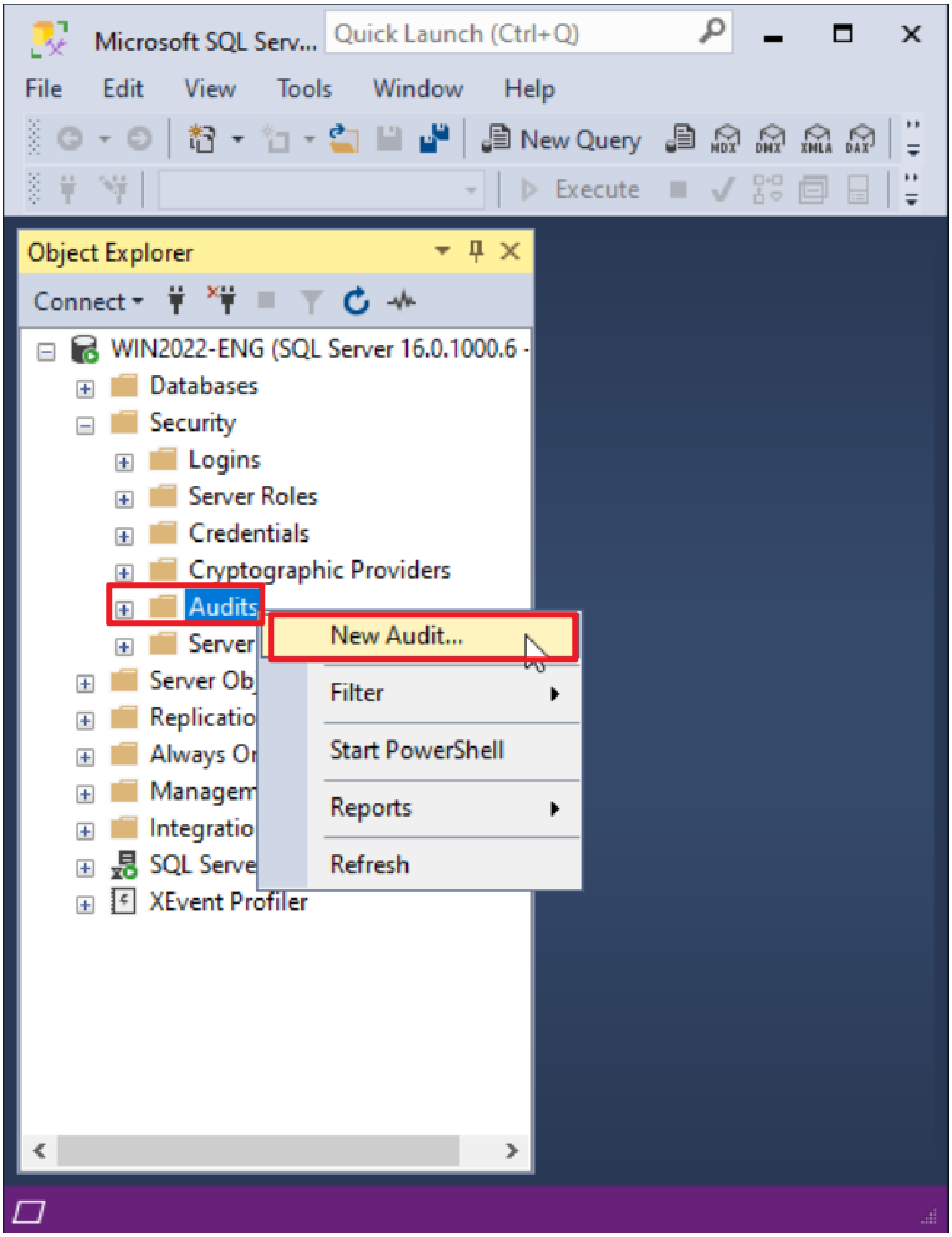
Authentication: SQL Server Authentication

Login: sa

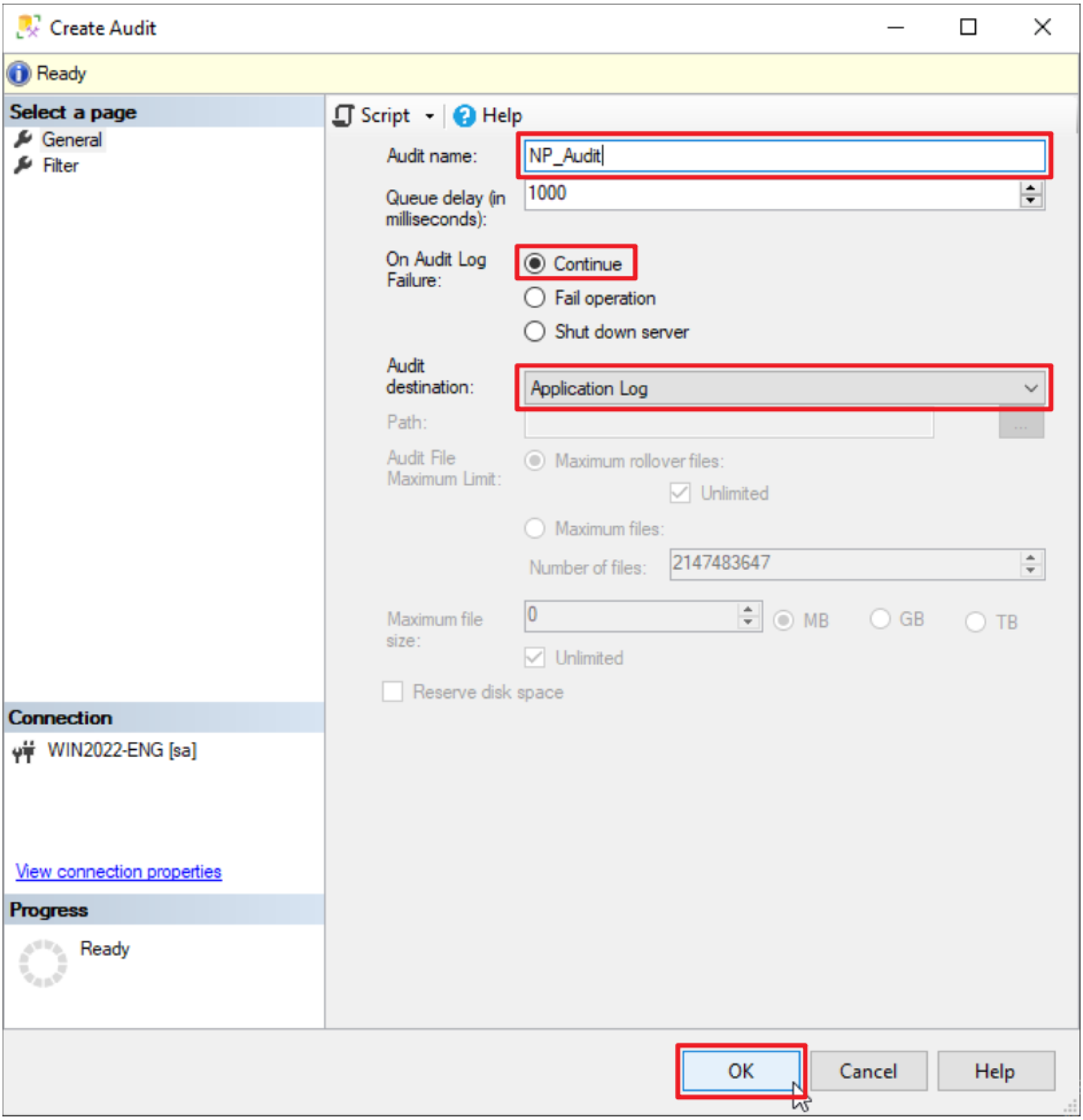
Password: ********

☑ Remember password

(3) Expand “Security” → right-click “Audits” → select “New Audit...”



(4) Enter the audit name: (the example here is NP_Audit) → select “On audit log failure”: “Continue” → select audit destination: Application Log (this stores MS SQL audit logs in the Windows Event Viewer Application Log) → click “OK.”



Create Audit

Ready

Audit name: NP_Audit

Queue delay (in milliseconds): 1000

On Audit Log Failure:
● Continue
○ Fail operation
○ Shut down server

Audit destination: Application Log

Path:

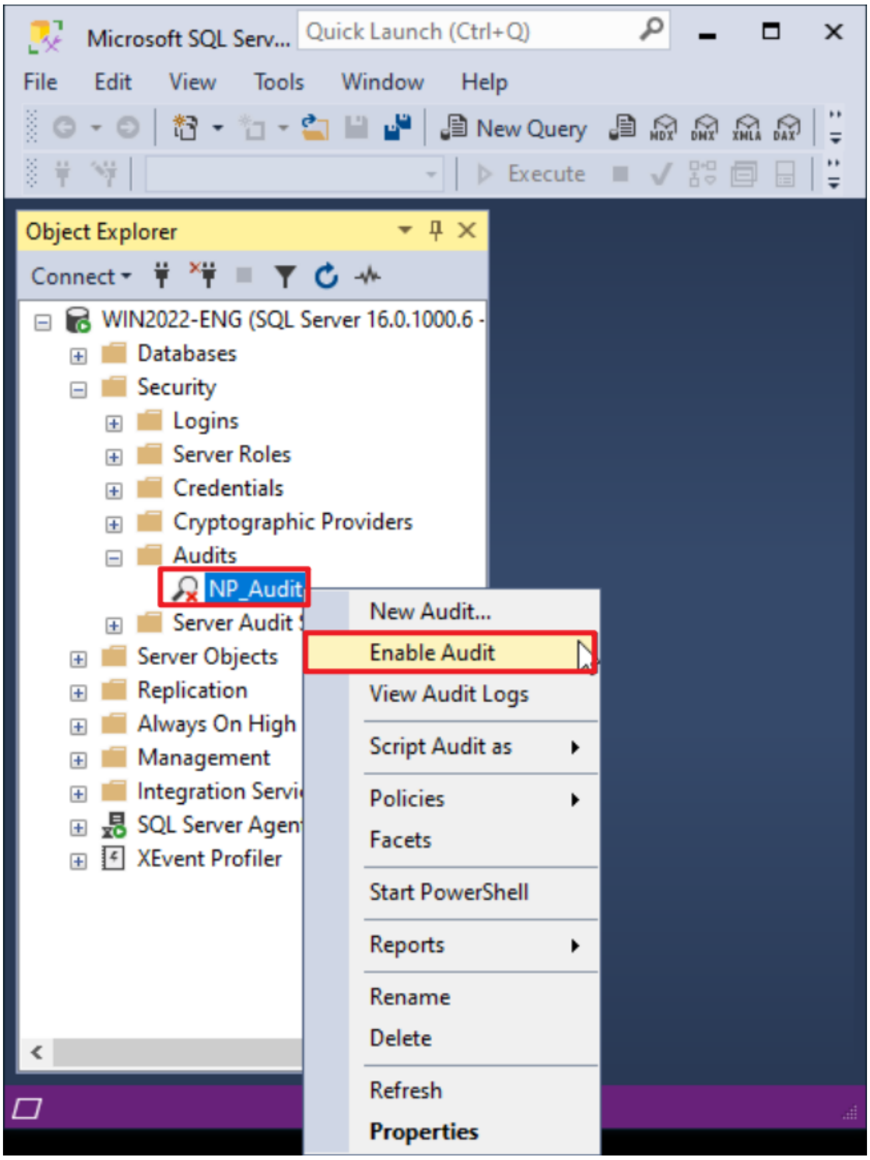
Audit File Maximum Limit:
● Maximum rollover files:
☑ Unlimited
○ Maximum files:
Number of files: 2147483647

Maximum file size: 0 ● MB ○ GB ○ TB
☑ Unlimited

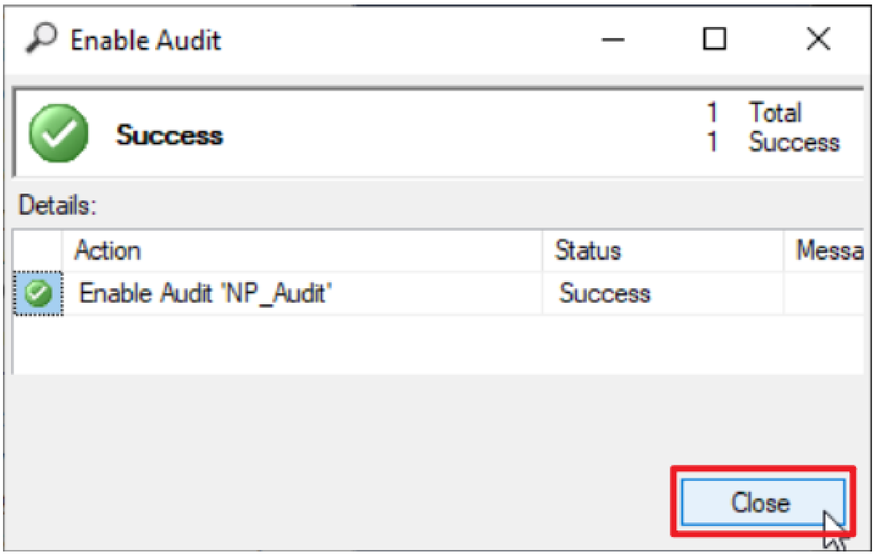
☐ Reserve disk space

Connection
WIN2022-ENG [sa]

(5) In the audit list, right-click “NP_Audit” → select “Enable Audit.”



(6) Click “Close.”



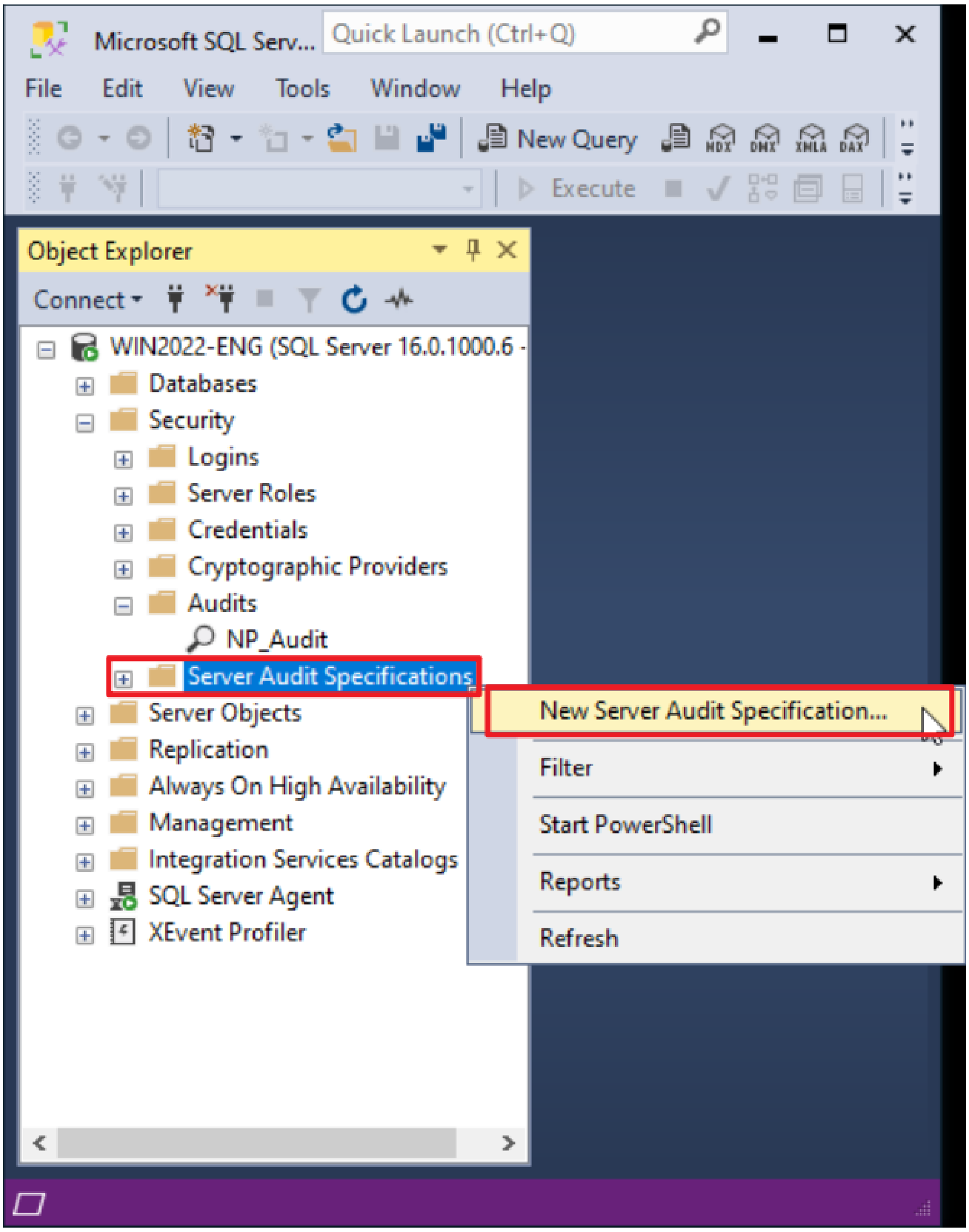
Success

1 Total
1 Success

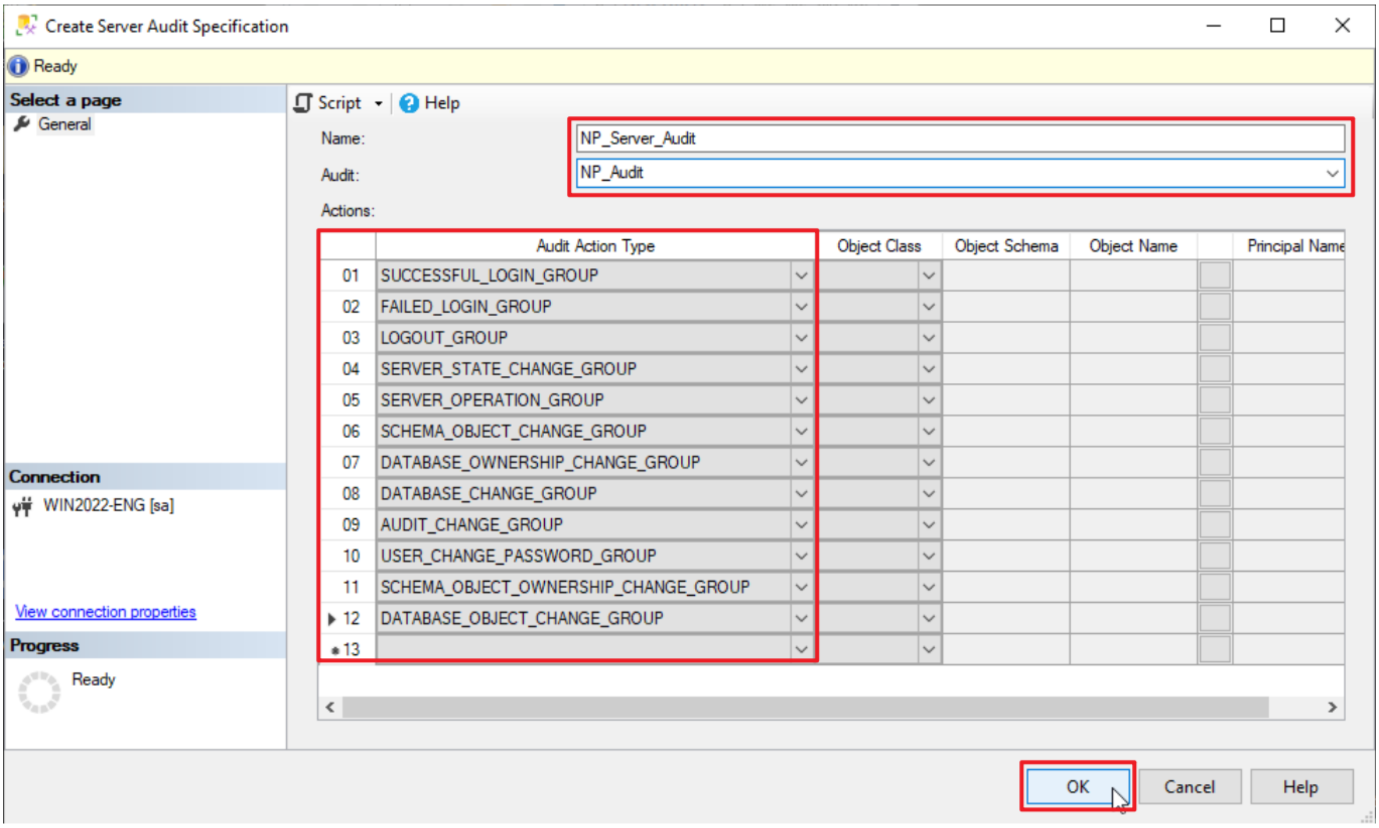
Details:

	Action	Status	Messa
✓	Enable Audit 'NP_Audit'	Success	

(7) Right-click “Server Audit Specifications,” → select “New Server Audit Specification...”



(8) Enter the specification name: (the example here is NP_Server_Audit) → select audit: NP_Audit → select action(s) (refer to the **SQL Server Audit Action Groups and Actions** in the references for details) → click "OK."



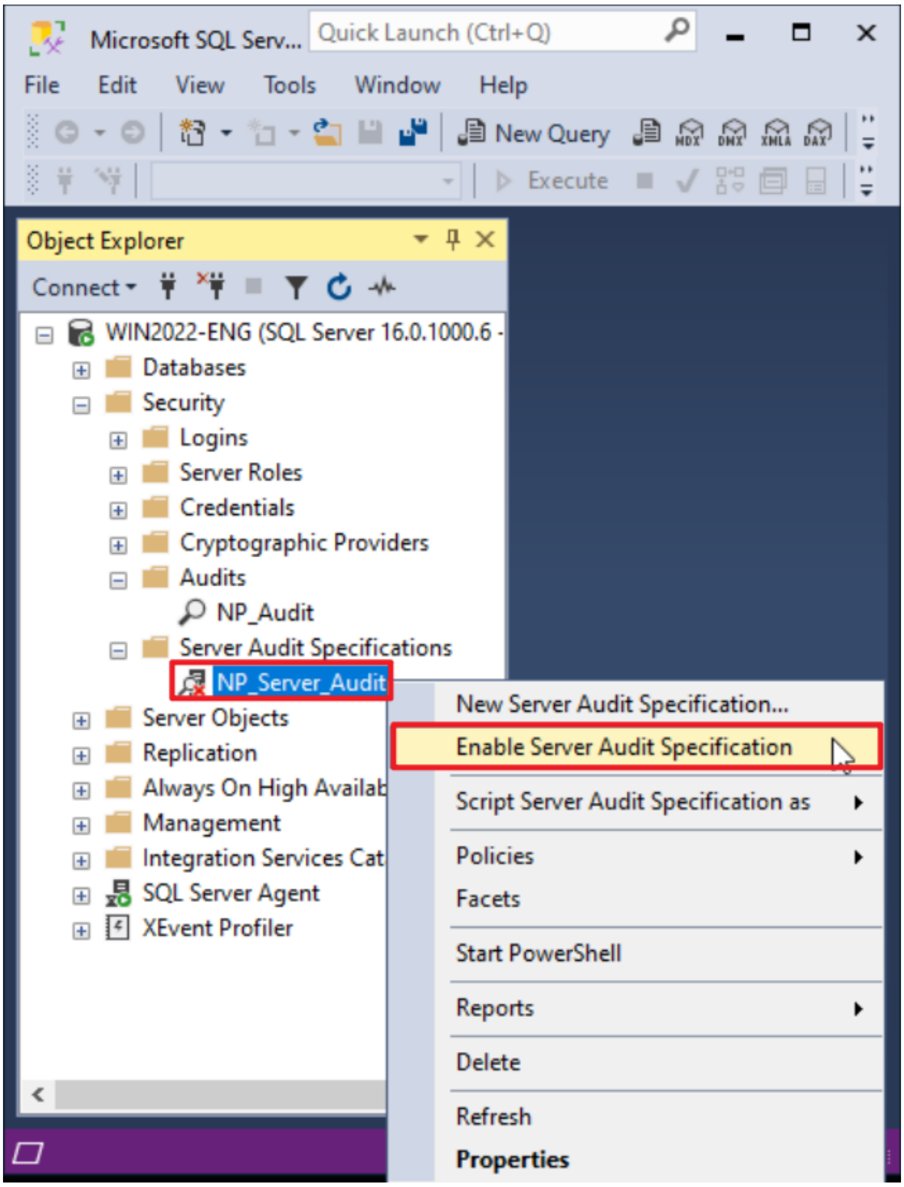
Name: NP_Server_Audit

Audit: NP_Audit

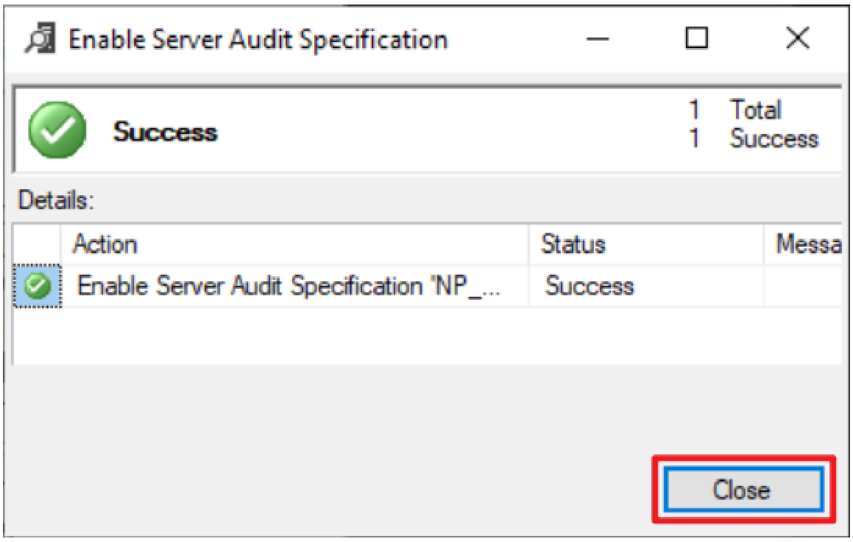
Actions:

	Audit Action Type	Object Class	Object Schema	Object Name	Principal Name
01	SUCCESSFUL_LOGIN_GROUP				
02	FAILED_LOGIN_GROUP				
03	LOGOUT_GROUP				
04	SERVER_STATE_CHANGE_GROUP				
05	SERVER_OPERATION_GROUP				
06	SCHEMA_OBJECT_CHANGE_GROUP				
07	DATABASE_OWNERSHIP_CHANGE_GROUP				
08	DATABASE_CHANGE_GROUP				
09	AUDIT_CHANGE_GROUP				
10	USER_CHANGE_PASSWORD_GROUP				
11	SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP				
12	DATABASE_OBJECT_CHANGE_GROUP				
13					

(9) In the server audit specification list, right-click “NP_Server_Audit” → select “Enable Server Audit Specification.”



(10) Click “Close.”



Action	Status	Messa
Enable Server Audit Specification 'NP_...	Success	

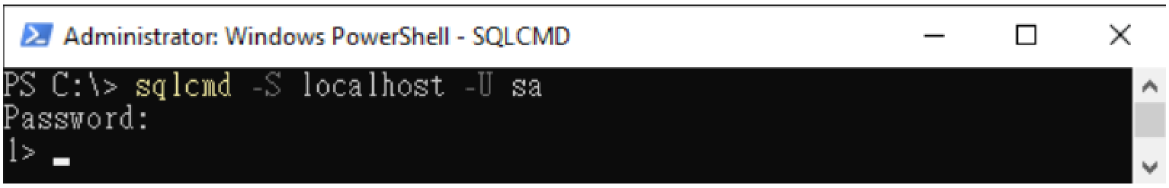
6.2.1.2 Configuring via Graphical User Interface (GUI)

(1) Open “Windows PowerShell.”

(2) Enter the command below to log in using either sa:

<2.1>Using sa account:

```
PS C:\> sqlcmd -S localhost -U sa
```



```
PS C:\> sqlcmd -S localhost -U sa
Password:
1> _
```

Options:

-S [protocol:]server[instance_name][,port]

-U login_id

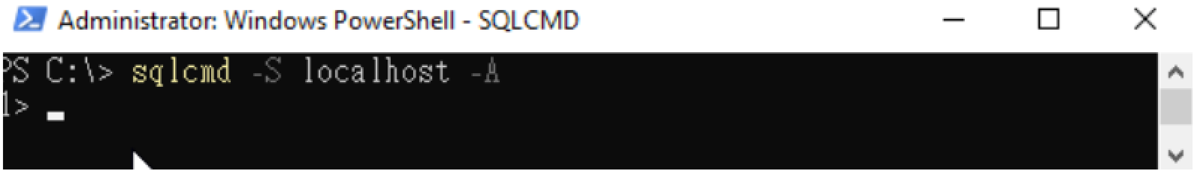
-P password

-A dedicated administrator connection

<2.2> Using Windows account:

Enter the command below to log in using Windows:

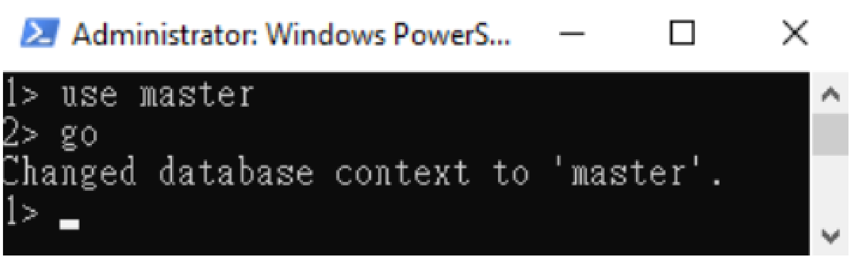
```
PS C:\> sqlcmd -S localhost -A
```



```
PS C:\> sqlcmd -S localhost -A
1> _
```

(3) Enter the command below to switch to the **master** database:

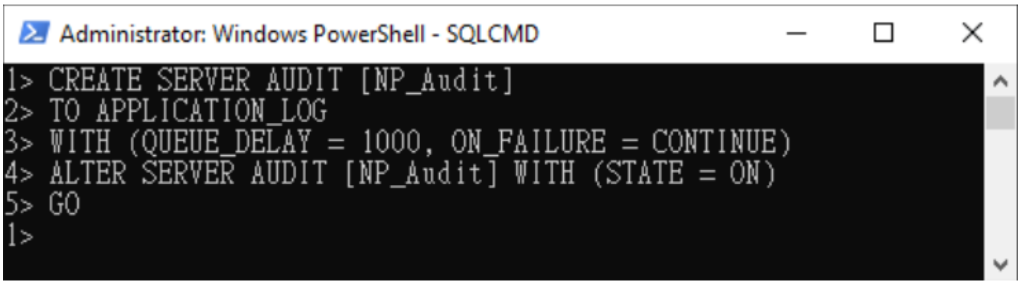
```
1 > use master
2 > go
```



```
1> use master
2> go
Changed database context to 'master'.
1> _
```

(4) Enter the audit name: NP_Audit → select audit destination: Application Log (this stores MS SQL audit logs in the Windows Event Viewer Application Log) → click "OK."

```
1 > CREATE SERVER AUDIT [ NP_Audit ]
2 > TO APPLICATION_LOG
3 > WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4 > ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5 > GO
```

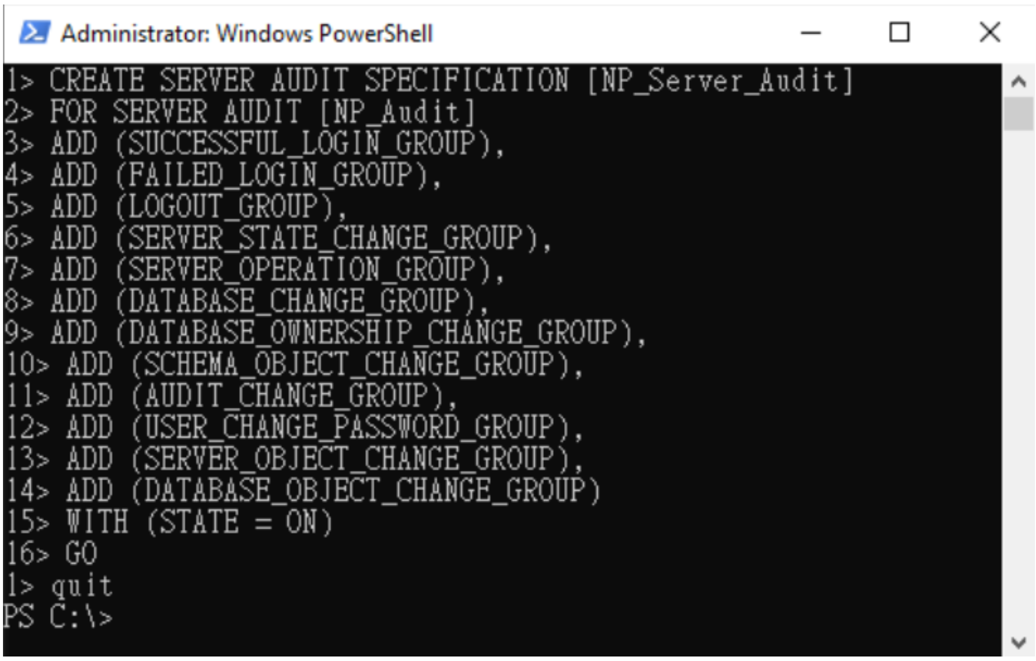


```
1> CREATE SERVER AUDIT [NP_Audit]
2> TO APPLICATION_LOG
3> WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4> ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5> GO
1>
```

(5) Enter the command below to configure the server audit and add actions. For detailed information, refer to the **SQL Server Audit Action Groups and Actions** in the references.

```
1 > CREATE SERVER AUDIT SPECIFICATION [ NP_Server_Audit ]
2 > FOR SERVER AUDIT [NP_Audit]
3 > ADD (SUCCESSFUL_LOGIN_GROUP),
4 > ADD (FAILED_LOGIN_GROUP),
5 > ADD (LOGOUT_GROUP),
6 > ADD (SERVER_STATE_CHANGE_GROUP),
7 > ADD (SERVER_OPERATION_GROUP),
8 > ADD (SCHEMA_OBJECT_CHANGE_GROUP),
9 > ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
10 > ADD (DATABASE_CHANGE_GROUP),
11 > ADD (DATABASE_OBJECT_CHANGE_GROUP),
12 > ADD (SERVER_OBJECT_CHANGE_GROUP),
13 > ADD (USER_CHANGE_PASSWORD_GROUP)
```

```
14 > ADD (AUDIT_CHANGE_GROUP)

15> WITH (STATE = ON)

16 > GO

1 > quit
```



```
1> CREATE SERVER AUDIT SPECIFICATION [NP_Server_Audit]
2> FOR SERVER AUDIT [NP_Audit]
3> ADD (SUCCESSFUL_LOGIN_GROUP),
4> ADD (FAILED_LOGIN_GROUP),
5> ADD (LOGOUT_GROUP),
6> ADD (SERVER_STATE_CHANGE_GROUP),
7> ADD (SERVER_OPERATION_GROUP),
8> ADD (DATABASE_CHANGE_GROUP),
9> ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
10> ADD (SCHEMA_OBJECT_CHANGE_GROUP),
11> ADD (AUDIT_CHANGE_GROUP),
12> ADD (USER_CHANGE_PASSWORD_GROUP),
13> ADD (SERVER_OBJECT_CHANGE_GROUP),
14> ADD (DATABASE_OBJECT_CHANGE_GROUP)
15> WITH (STATE = ON)
16> GO
1> quit
PS C:\>
```

Replace the text shown in red with the server audit specification name.

6.2.2 Database-Level Audit

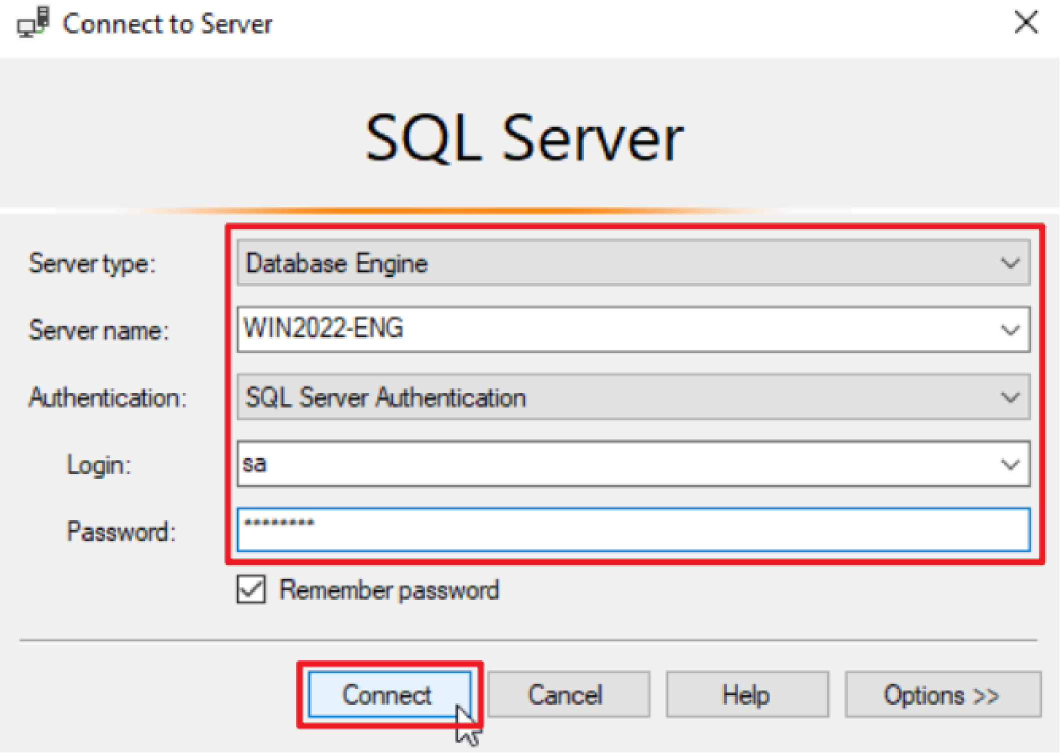
Enabling a database-level audit covers operations involving Data Manipulation Language (DML) and Data Definition Language (DDL) statements.

The following sections describe how to configure a database-level audit using the graphical user interface (GUI) and the command-line interface (CLI).

6.2.2.1 Configuring via Graphical User Interface (GUI)

(1) Open “SQL Server Management Studio (SSMS).”

(2) Enter the server’s name → select the authentication method → click “Connect.”


Connect to Server

SQL Server

Server type: Database Engine

Server name: WIN2022-ENG

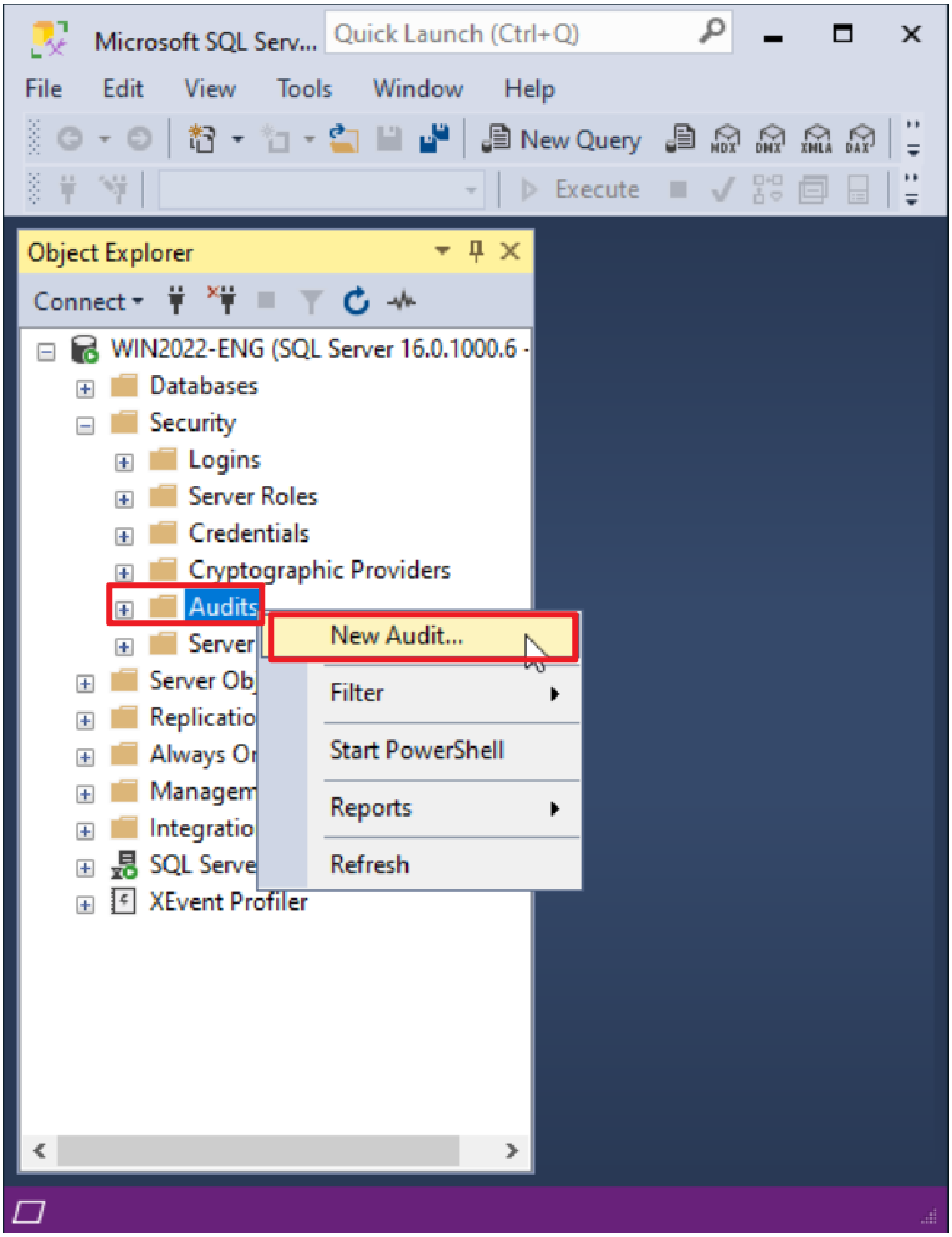
Authentication: SQL Server Authentication

Login: sa

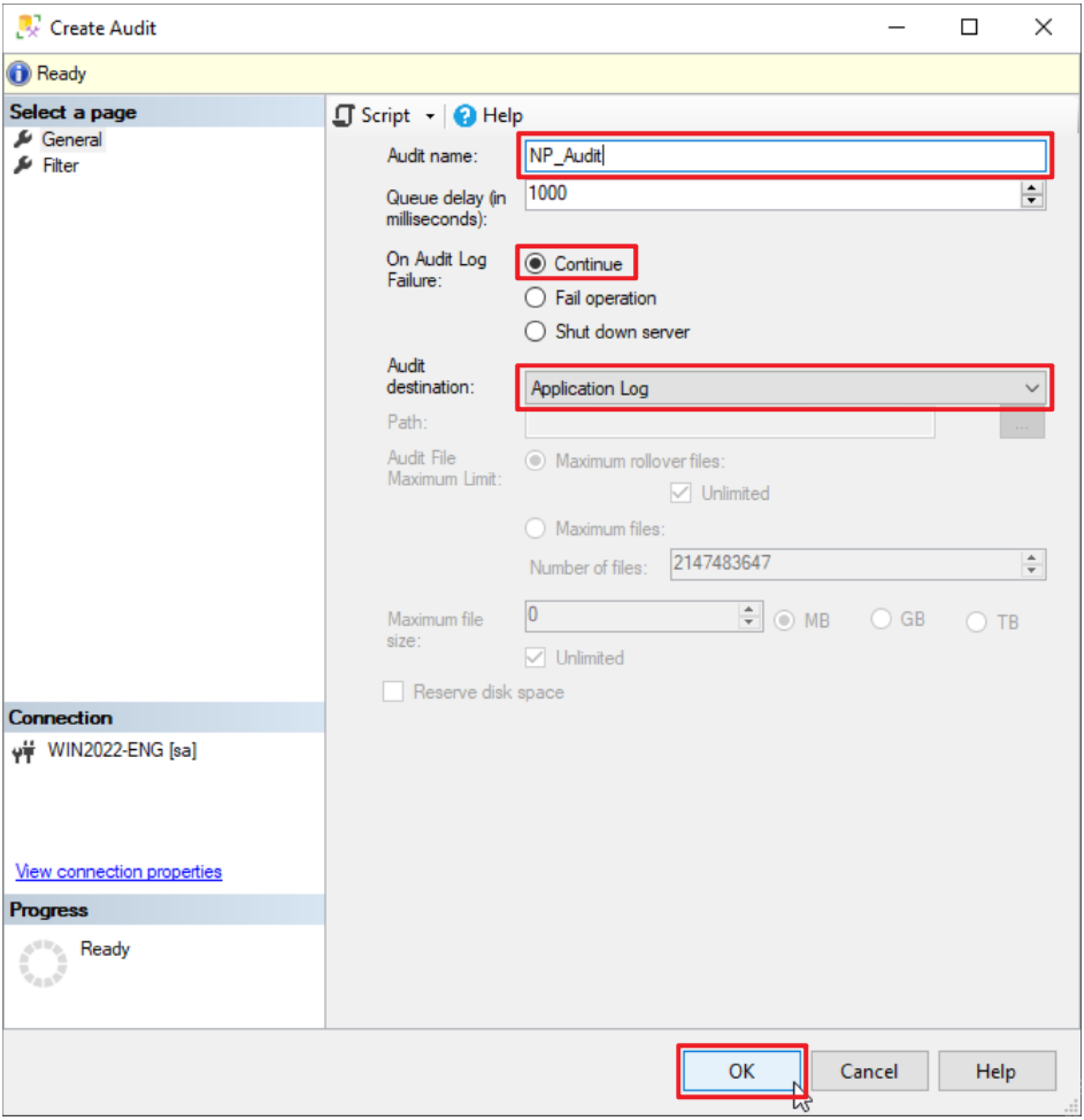
Password: ********

☑ Remember password

(3) Expand “Security” → right-click “Audits” → select “New Audit...”



(4) Enter the audit name: (the example here is NP_Audit) → select "On audit log failure": "Continue" → select audit destination: Application Log (this stores MS SQL audit logs in the Windows Event Viewer Application Log) → click "OK."



Create Audit

Ready

Select a page
- General
- Filter

Script ▾ | Help

Audit name: NP_Audit

Queue delay (in milliseconds): 1000

On Audit Log Failure:
- ● Continue
- ○ Fail operation
- ○ Shut down server

Audit destination: Application Log

Path:

Audit File Maximum Limit:
- ● Maximum rollover files:
  - ☑ Unlimited
- ○ Maximum files:
  - Number of files: 2147483647

Maximum file size: 0 ● MB ○ GB ○ TB

☑ Unlimited

□ Reserve disk space

Connection

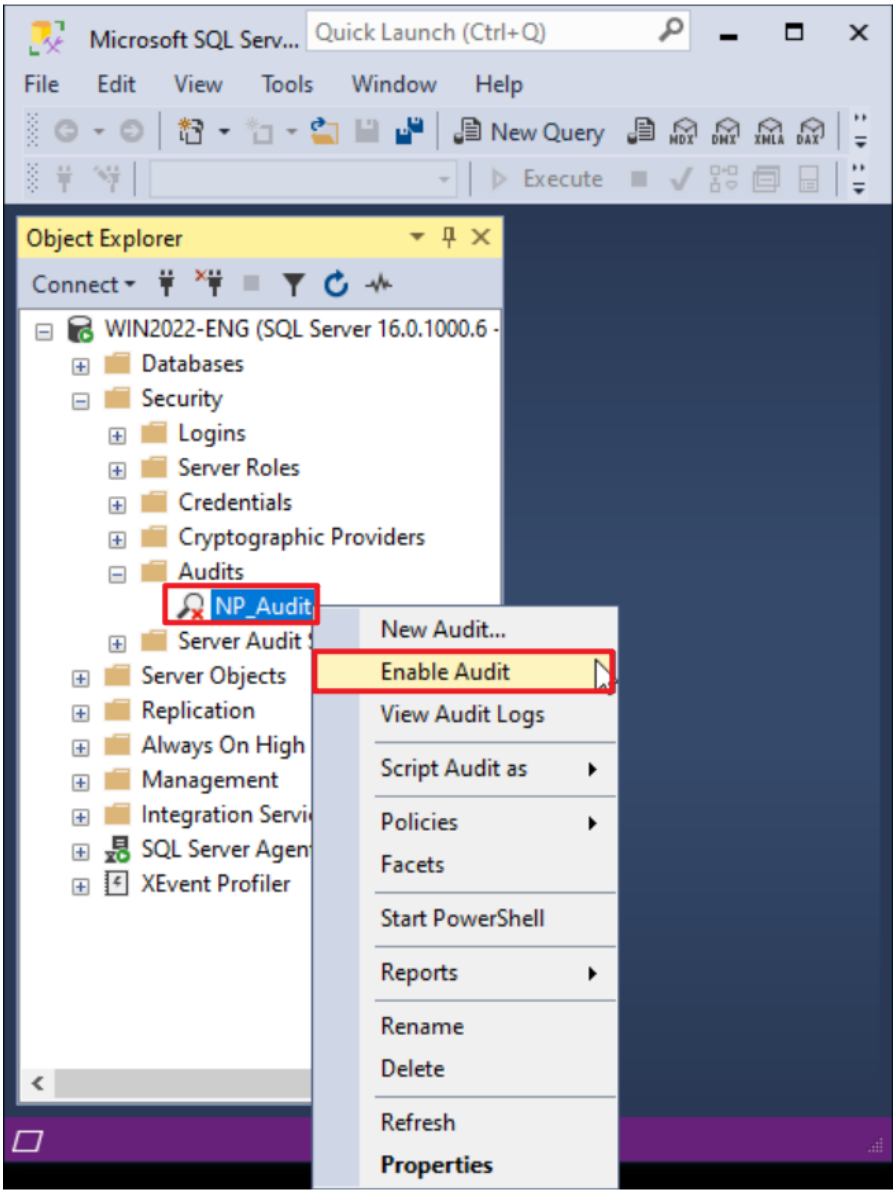
WIN2022-ENG [sa]

View connection properties

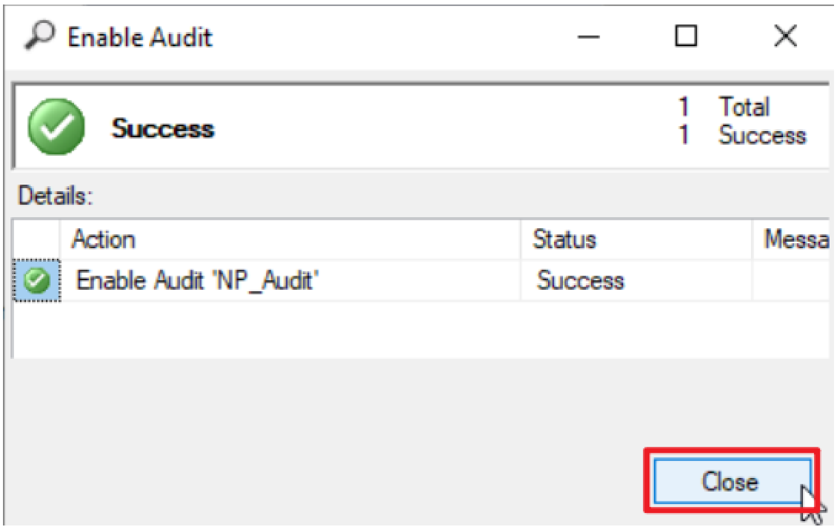
Progress

Ready

(5) In the audit list, right-click "NP_Audit" → select "Enable Audit."



(6) Click "Close."



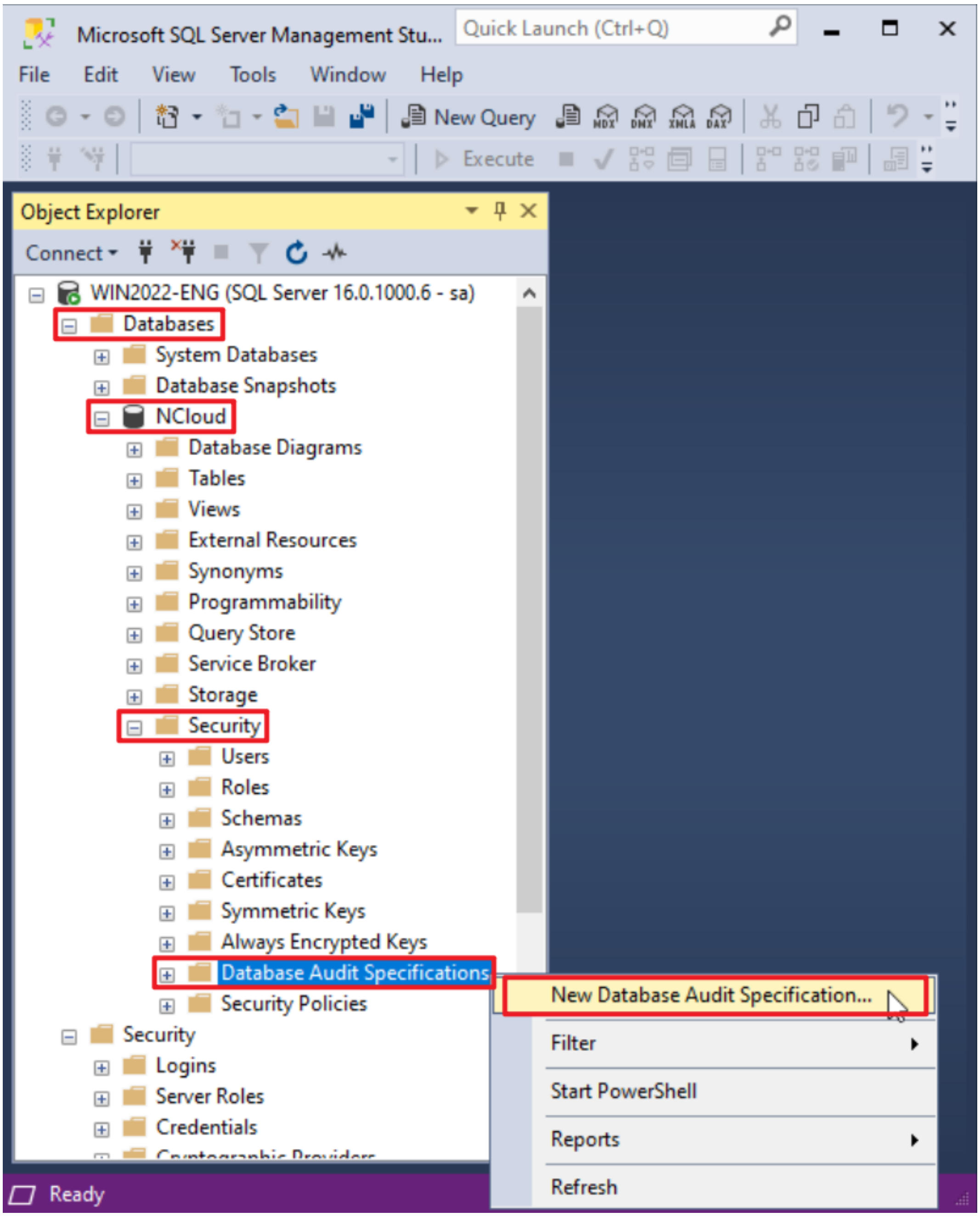
Success

1 Total
1 Success

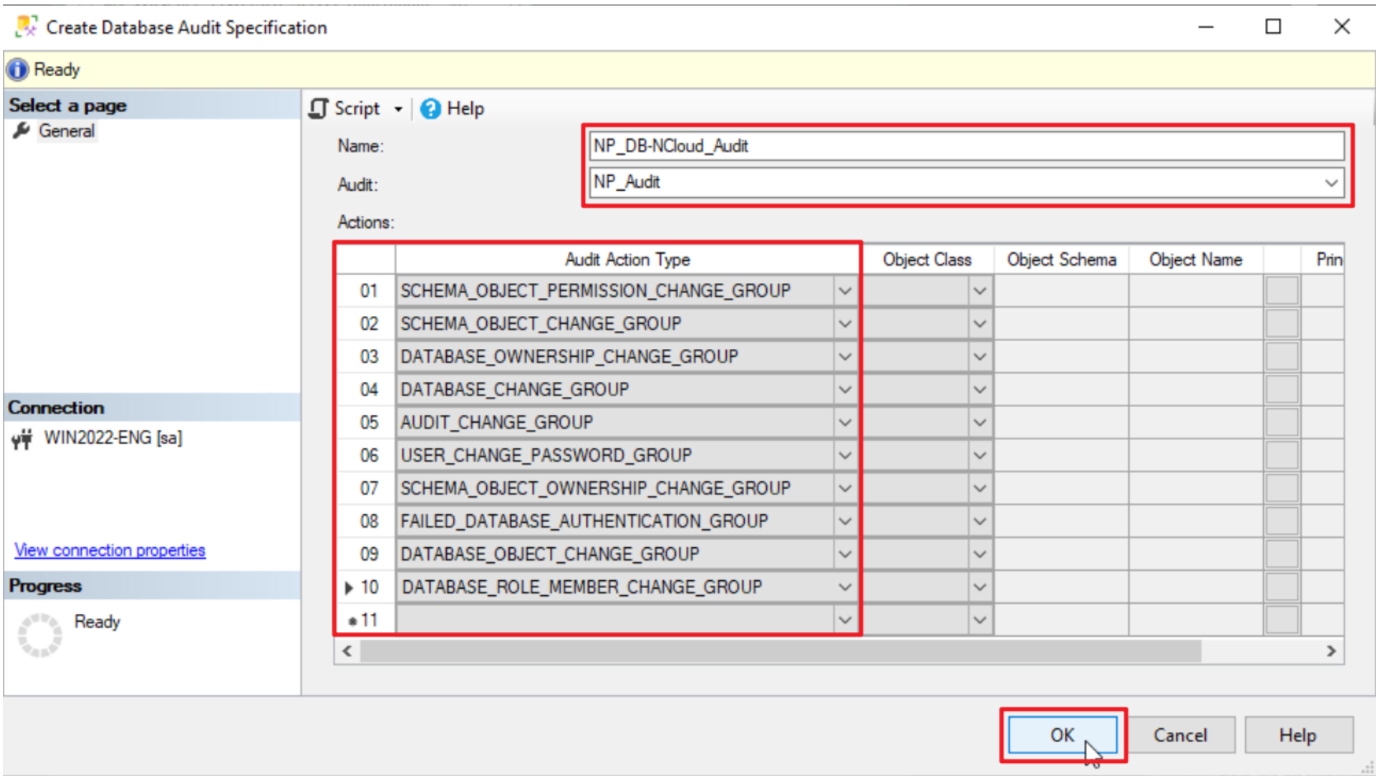
Details:

	Action	Status	Messa
✓	Enable Audit 'NP_Audit'	Success	

(7) In “Databases,” select the target database (the example here is : NCloud) → expand “Security” → right-click “Database Audit Specifications” → select "New Database Audit Specification...”



(8) Enter the specification name: (the example here is NP_DB-NCloud_Audit) → select audit: NP_Audit and action(s) → select action(s) (refer to the **SQL Server Audit Action Groups and Actions** in the references for details) → click "OK."



Create Database Audit Specification

Ready

Name: NP_DB-NCloud_Audit

Audit: NP_Audit

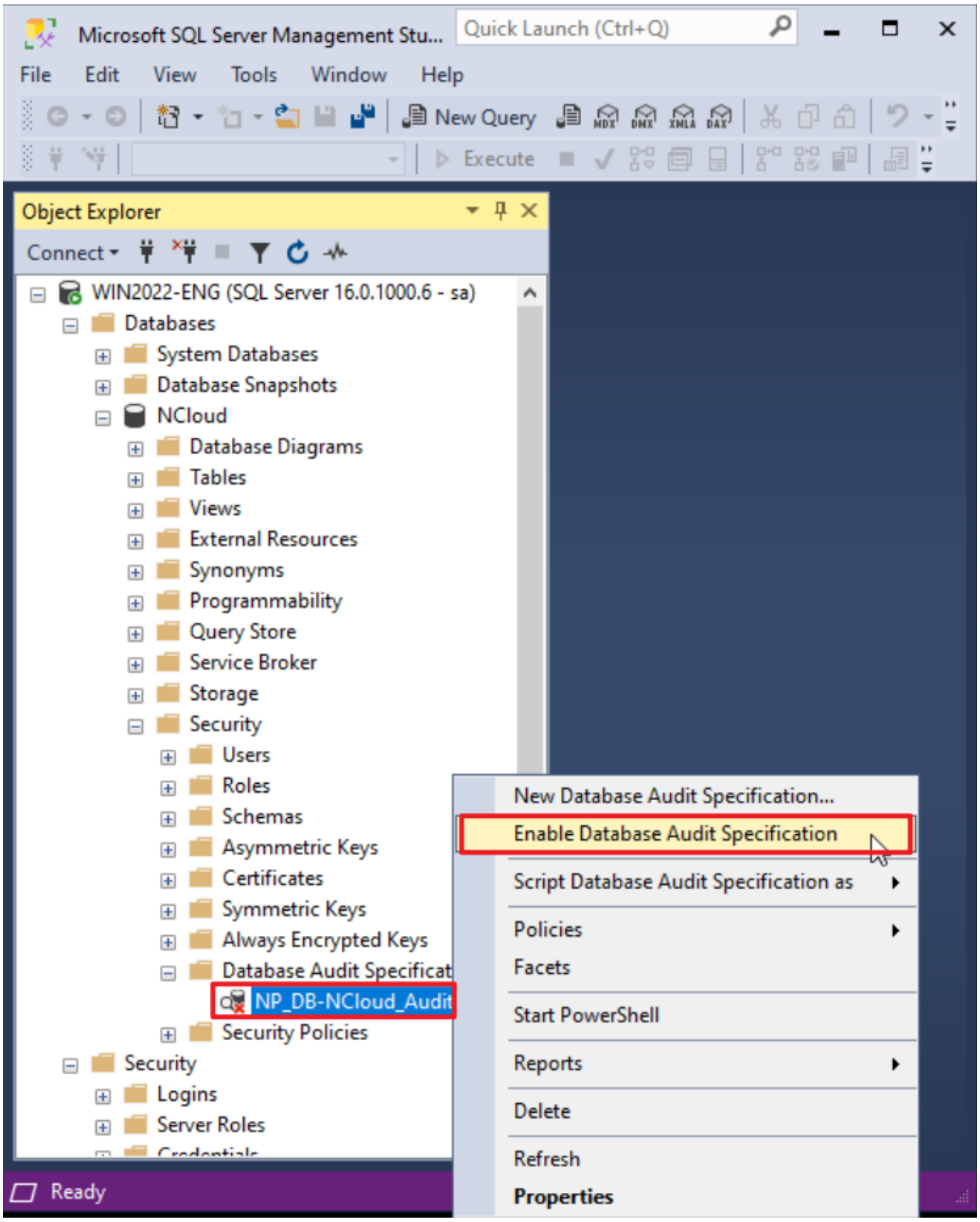
Actions:

	Audit Action Type	Object Class	Object Schema	Object Name	Prin
01	SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP				
02	SCHEMA_OBJECT_CHANGE_GROUP				
03	DATABASE_OWNERSHIP_CHANGE_GROUP				
04	DATABASE_CHANGE_GROUP				
05	AUDIT_CHANGE_GROUP				
06	USER_CHANGE_PASSWORD_GROUP				
07	SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP				
08	FAILED_DATABASE_AUTHENTICATION_GROUP				
09	DATABASE_OBJECT_CHANGE_GROUP				
▸ 10	DATABASE_ROLE_MEMBER_CHANGE_GROUP				
* 11					

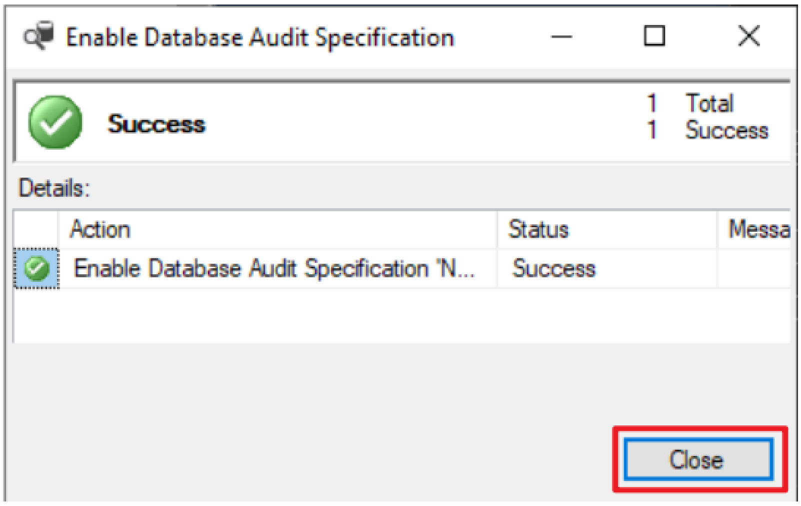
Connection: WIN2022-ENG [sa]

Progress: Ready

(9) In the database audit specification list, right-click “NP_DB-NCloud_Audit” → select “Enable Server Audit Specification.”



(10) Click “Close.”


Enable Database Audit Specification
Success
1 Total
1 Success
Details:
Action
Status
Messa
Enable Database Audit Specification 'N...
Success
Close

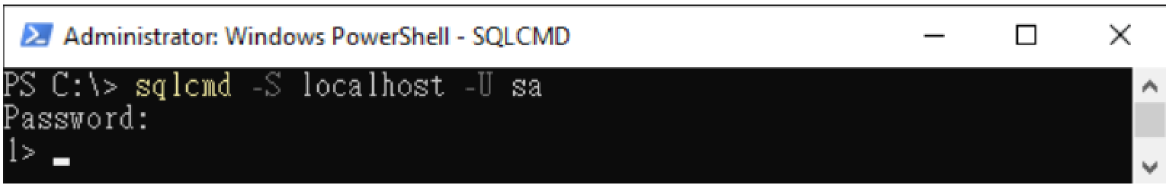
6.2.2.2 Configuring via Graphical User Interface (GUI)

(1) Open “Windows PowerShell.”

(2) Enter the command below to log in using either sa:

<2.1>Using sa account:

```
PS C:\> sqlcmd -S localhost -U sa
```



```
PS C:\> sqlcmd -S localhost -U sa
Password:
1> _
```

Options:

-S [protocol:]server[instance_name][,port]

-U login_id

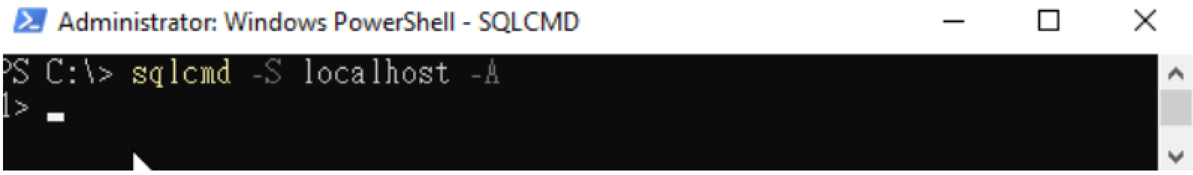
-P password

-A dedicated administrator connection

<2.2> Using Windows account:

Enter the command below to log in using Windows account:

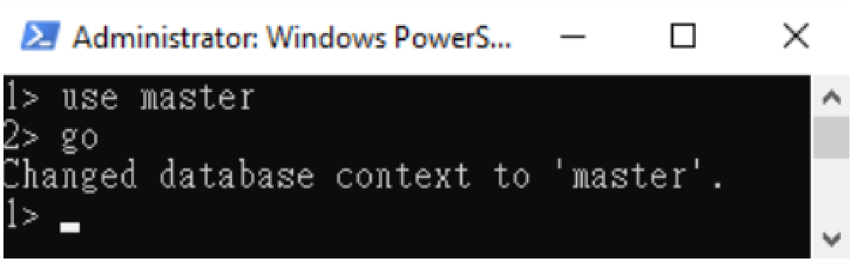
```
PS C:\> sqlcmd -S localhost -A
```



```
PS C:\> sqlcmd -S localhost -A
1> _
```

(3) Enter the command below to switch to the **master** database:

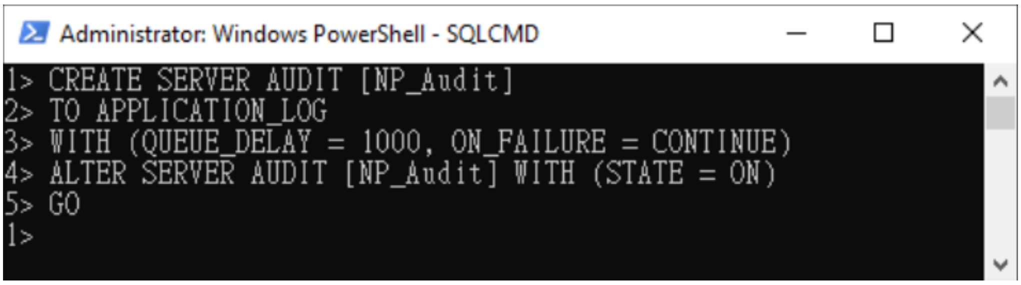
```
1 > use master
2 > go
```



```
1> use master
2> go
Changed database context to 'master'.
1> _
```

(4) Enter the audit name: NP_Audit → select audit destination: Application Log (this stores MS SQL audit logs in the Windows Event Viewer Application Log) → click "OK."

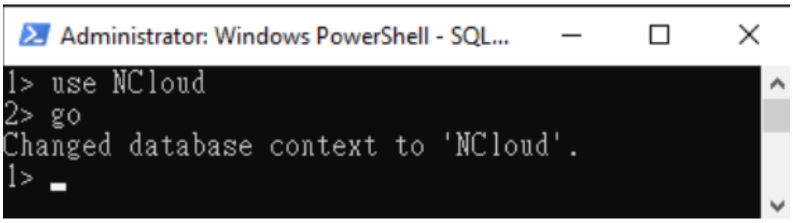
```
1 > CREATE SERVER AUDIT [ NP_Audit ]
2 > TO APPLICATION_LOG
3 > WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4 > ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5 > GO
```



```
1> CREATE SERVER AUDIT [NP_Audit]
2> TO APPLICATION_LOG
3> WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
4> ALTER SERVER AUDIT [NP_Audit] WITH (STATE = ON)
5> GO
1>
```

(5) Enter the command below to switch to the target audit database (the example here is: NCloud).

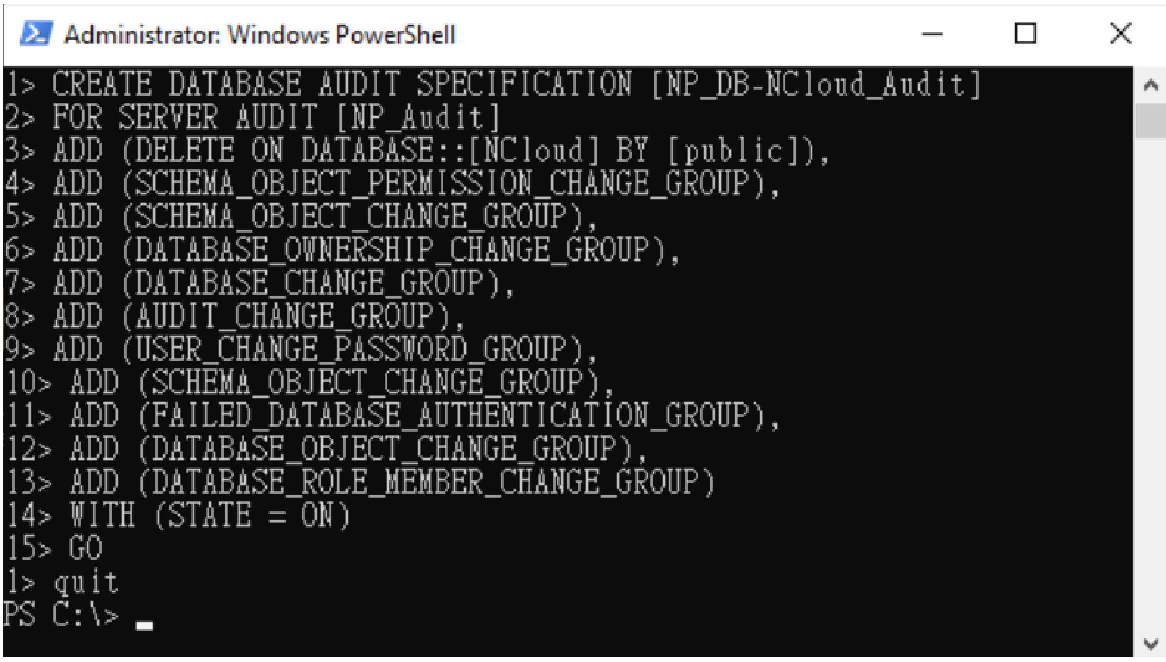
```
1 > use NCloud
2 > go
```



```
1> use NCloud
2> go
Changed database context to 'NCloud'.
1> _
```

(6) Enter the command below to configure the audit for the database and add actions. For detailed information, refer to the **SQL Server Audit Action Groups and Actions** in the references.

```
1 > CREATE DATABASE AUDIT SPECIFICATION [ NP_DB-NCloud_Audit ]
2 > FOR SERVER AUDIT [NP_Audit]
3 > ADD (DELETE ON DATABASE::[ NCloud ] BY [public]),
4 > ADD (SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP),
5 > ADD (SCHEMA_OBJECT_CHANGE_GROUP),
6 > ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
7 > ADD (DATABASE _CHANGE_GROUP),
8 > ADD (AUDIT_CHANGE_GROUP),
9 > ADD (USER_CHANGE_PASSWORD_GROUP),
10 > ADD (SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP),
11 > ADD (FAILED_DATABASE_AUTHENTICATION_GROUP),
12 > ADD (DATABASE_OBJECT_CHANGE_GROUP),
13 > ADD (DATABASE_ROLE_MEMBER_CHANGE_GROUP)
14 > WITH (STATE = ON)
15 > GO
1 > quit
```



```
1> CREATE DATABASE AUDIT SPECIFICATION [NP_DB-NCloud_Audit]
2> FOR SERVER AUDIT [NP_Audit]
3> ADD (DELETE ON DATABASE::[NCloud] BY [public]),
4> ADD (SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP),
5> ADD (SCHEMA_OBJECT_CHANGE_GROUP),
6> ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
7> ADD (DATABASE_CHANGE_GROUP),
8> ADD (AUDIT_CHANGE_GROUP),
9> ADD (USER_CHANGE_PASSWORD_GROUP),
10> ADD (SCHEMA_OBJECT_CHANGE_GROUP),
11> ADD (FAILED_DATABASE_AUTHENTICATION_GROUP),
12> ADD (DATABASE_OBJECT_CHANGE_GROUP),
13> ADD (DATABASE_ROLE_MEMBER_CHANGE_GROUP)
14> WITH (STATE = ON)
15> GO
1> quit
PS C:\> _
```

Replace the text shown in red with the database audit specification name.

```
1 > CREATE DATABASE AUDIT SPECIFICATION [NP_DB-NCloud_Audit]
```

Replace the text shown in red with the target database name.

```
3 > ADD (DELETE ON DATABASE::[NCloud] BY [public])
```

6.3 Event Log Configuration

This is an optional configuration.

The following sections describe configuration methods for Domain and Workgroup environments.

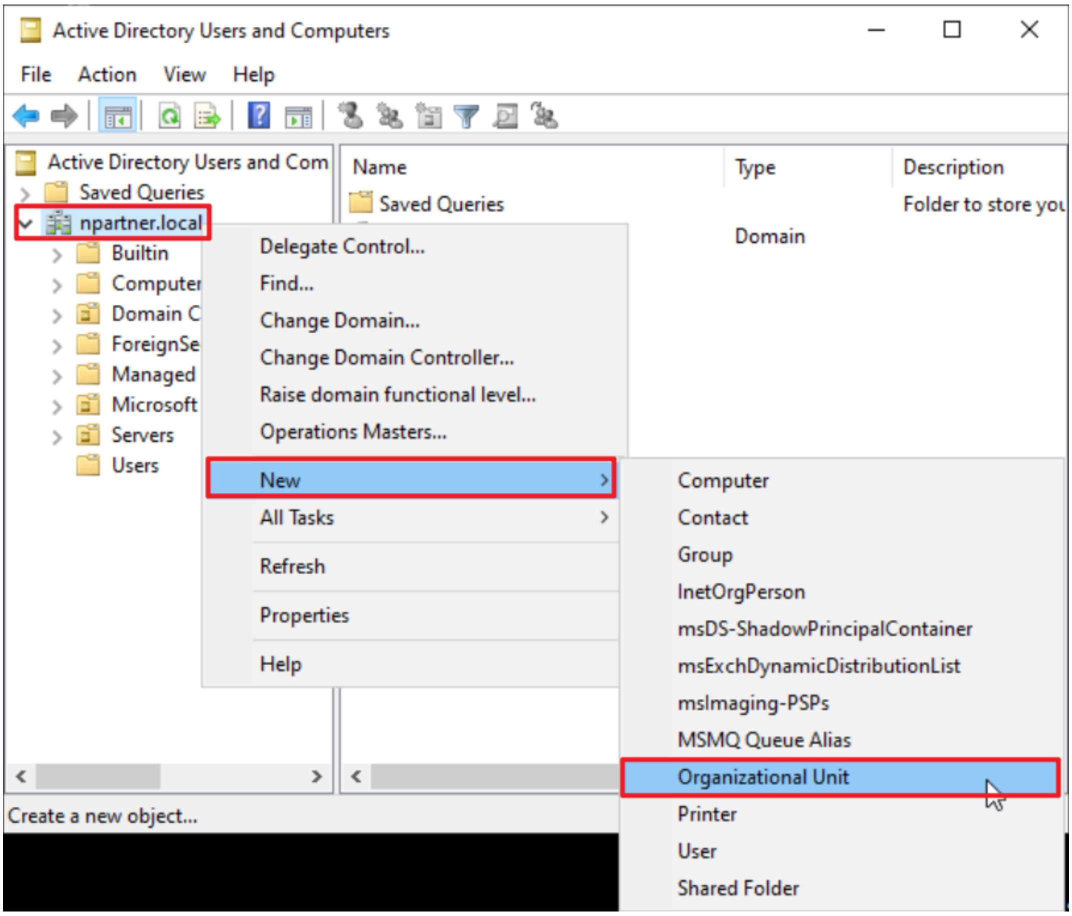
6.3.1 Domain

6.3.1.1 Organizational Unit (OU) Configuration

(1) Click “Active Directory Users and Computers.”

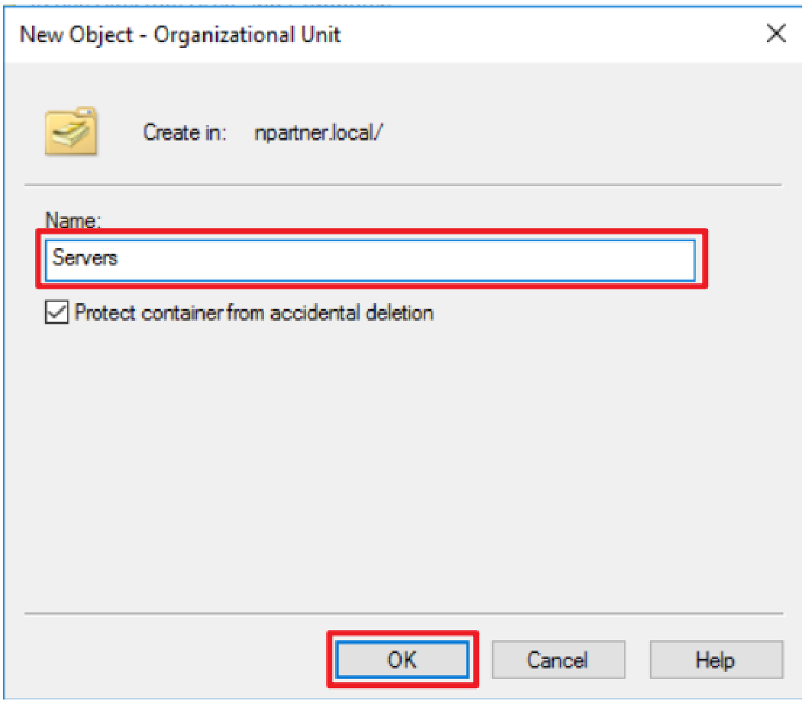
(2) Add an Organizational Unit

Right-click on “Domain Controllers, select “New,” and click “Organizational Unit.”



(3) Enter your Organizational Unit name: (in this example, it is “Servers”)

Note: Please create the organizational unit name according to the customer's environment. → click “OK.”



New Object - Organizational Unit

Create in: npartner.local/

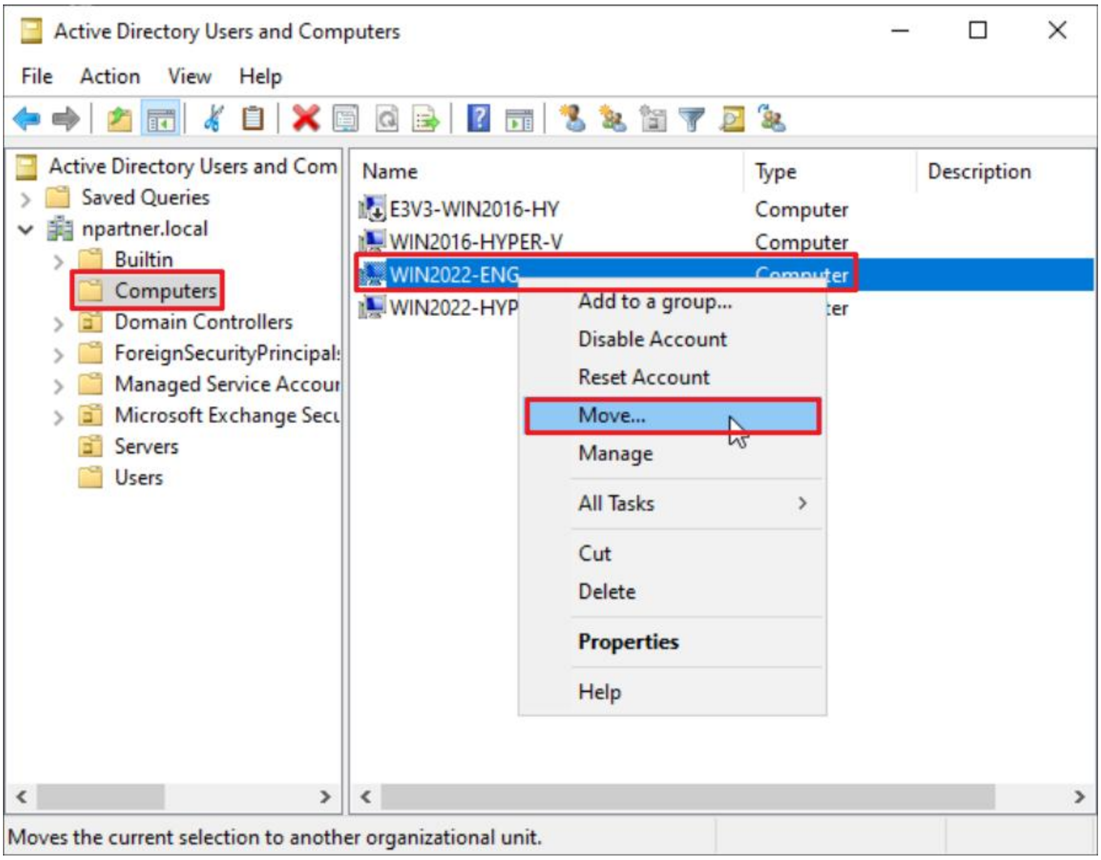
Name: Servers

☑ Protect container from accidental deletion

(4) Move the Server to your New Organizational Unit:

Select your organizational unit in “Domain Controllers” -> Right-click on the “WIN2022-ENG” server.

Note: Please select the MS SQL server according to the actual environment. → click “Move.”



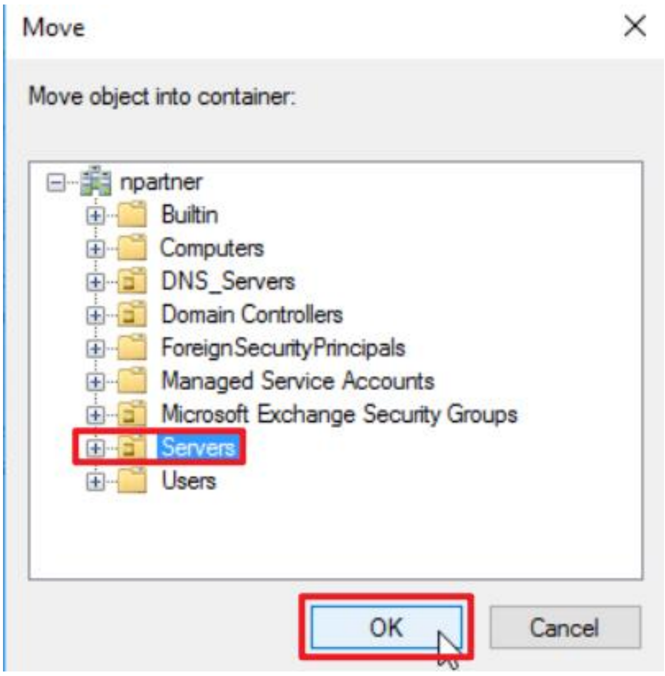
Active Directory Users and Computers

Name	Type	Description
E3V3-WIN2016-HY	Computer	
WIN2016-HYPER-V	Computer	
WIN2022-ENG	Computer	
WIN2022-HYP	ter	

Moves the current selection to another organizational unit.

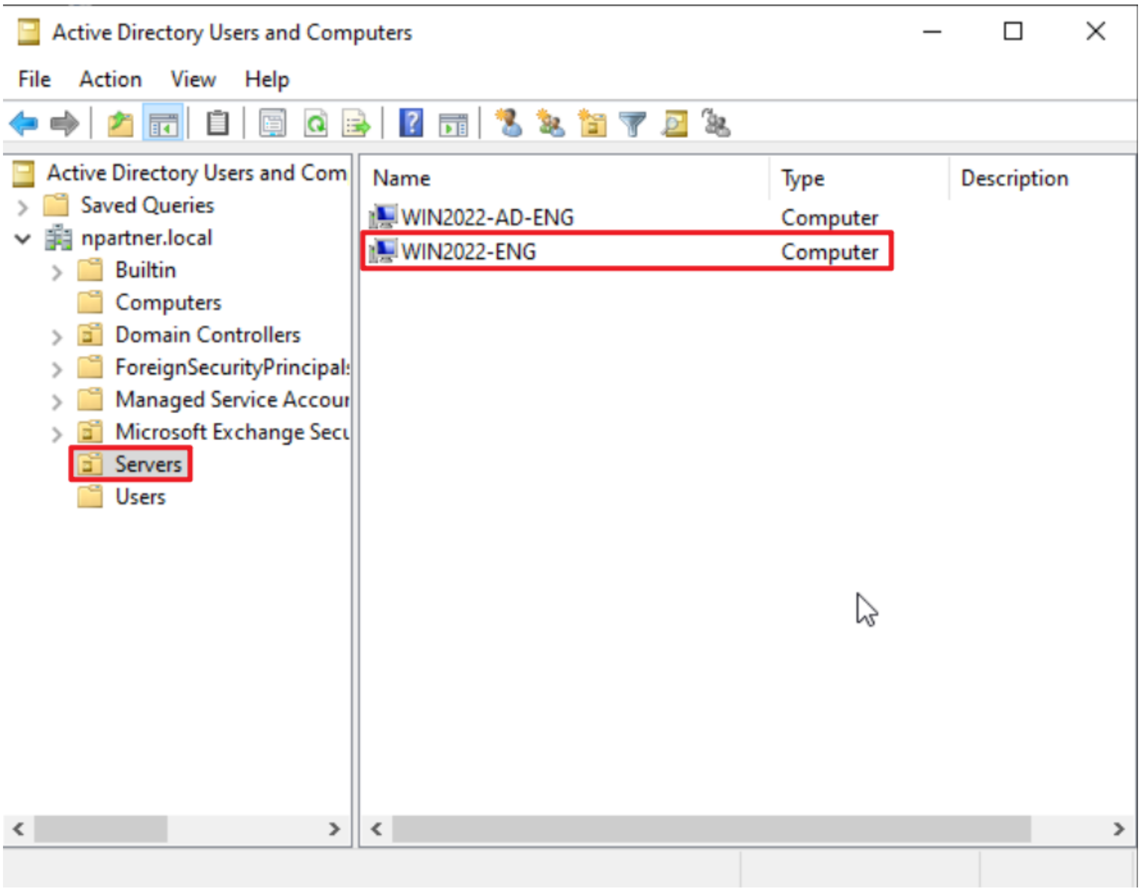
(5) Select your Organizational Unit:

Select your organizational unit (in this example, it is “Servers”) → click “OK.”



(6) Verify the Server Has Been Moved to your New Organizational Unit:

Expand your organizational unit folder (in this example, it is “Servers”) and confirm that the “WIN2022-ENG” server has been moved.



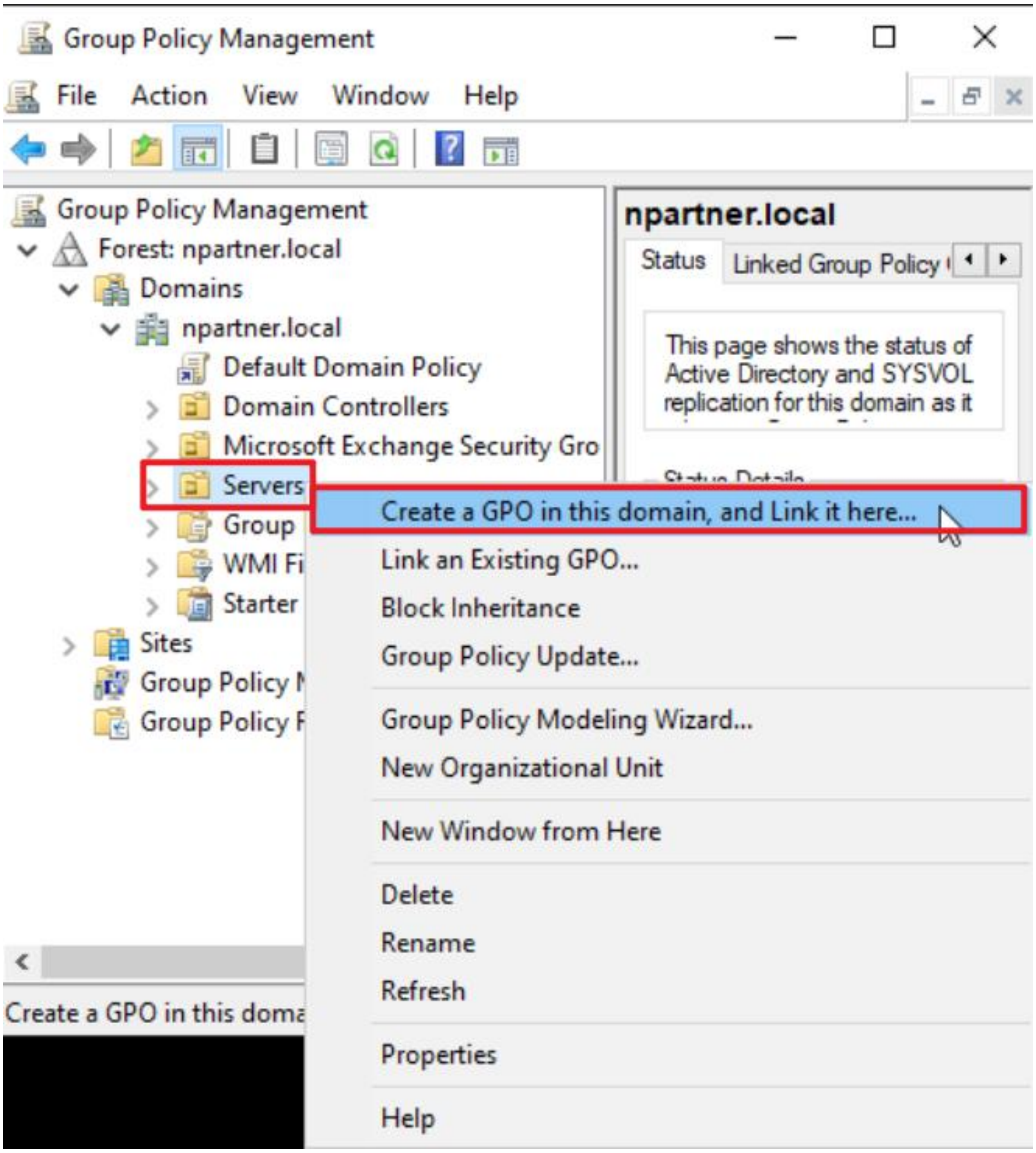
Name	Type	Description
WIN2022-AD-ENG	Computer	
WIN2022-ENG	Computer	

6.3.1.2 Group Policy Settings

(1) Click “Group Policy Management.”

(2) In the Servers organizational unit (OU), create a new Group Policy Object (GPO):

Right-click the [Servers] organizational unit → select “Create a GPO in this domain, and Link it here...”

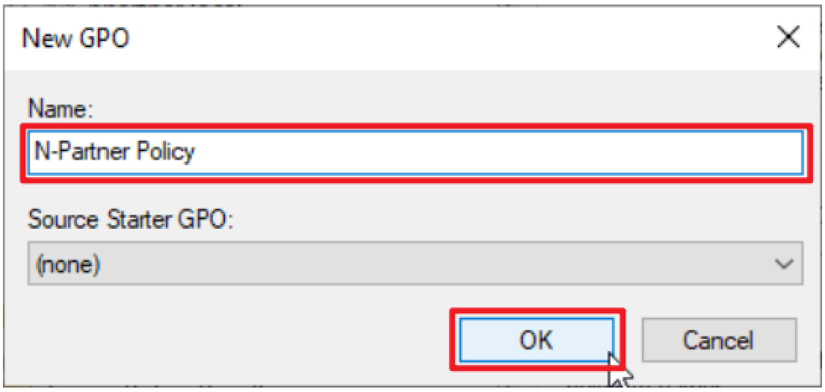


This page shows the status of Active Directory and SYSVOL replication for this domain as it

(3) Edit your Group Policy Object

Enter your Group Policy Object name. (in this example, it is “N-Partner Policy”)

Note: Create your GPO name according to the actual environment. Then click “Edit.”



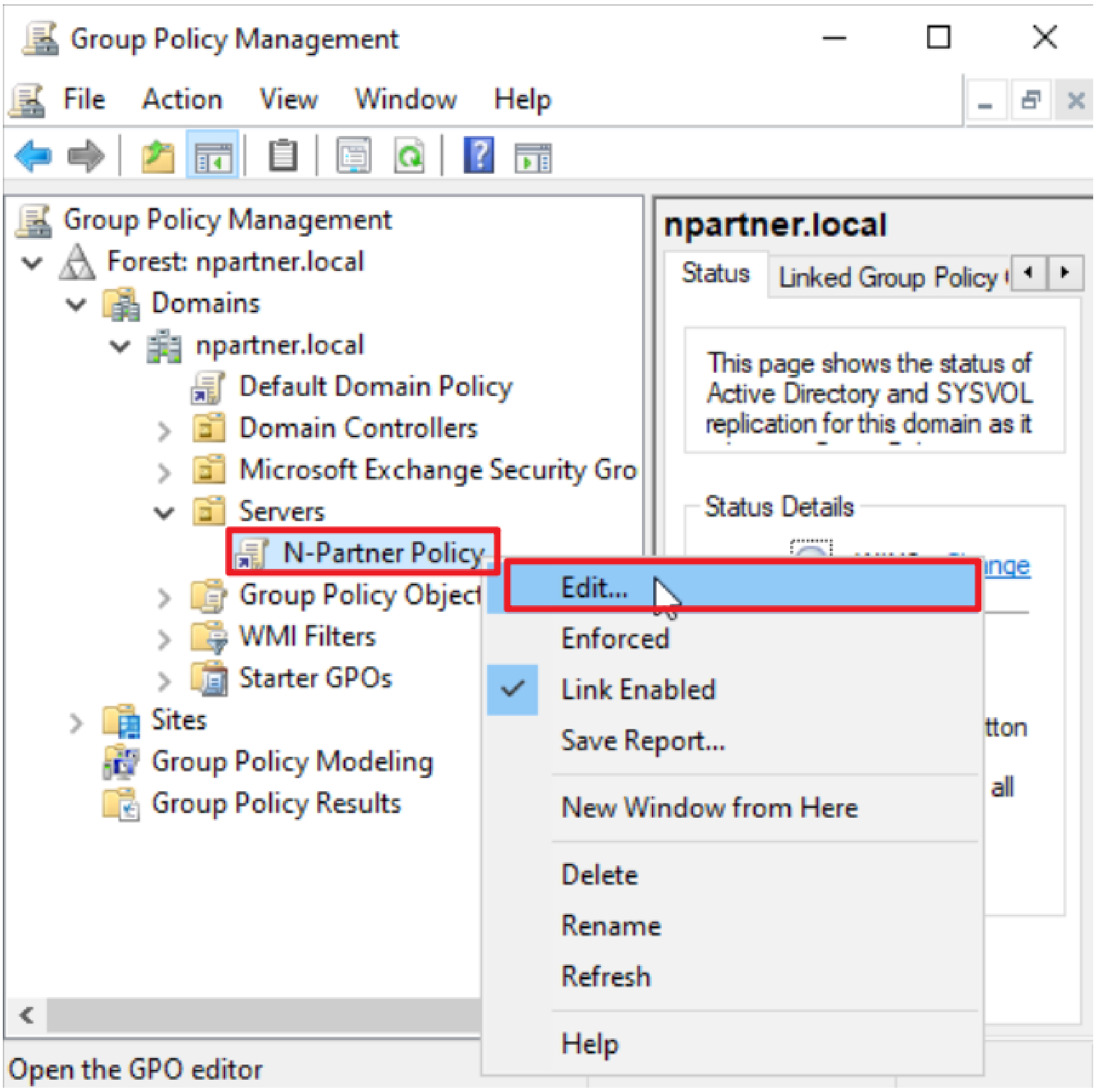
New GPO

Name: N-Partner Policy

Source Starter GPO: (none)

(4) Edit your Group Policy Object

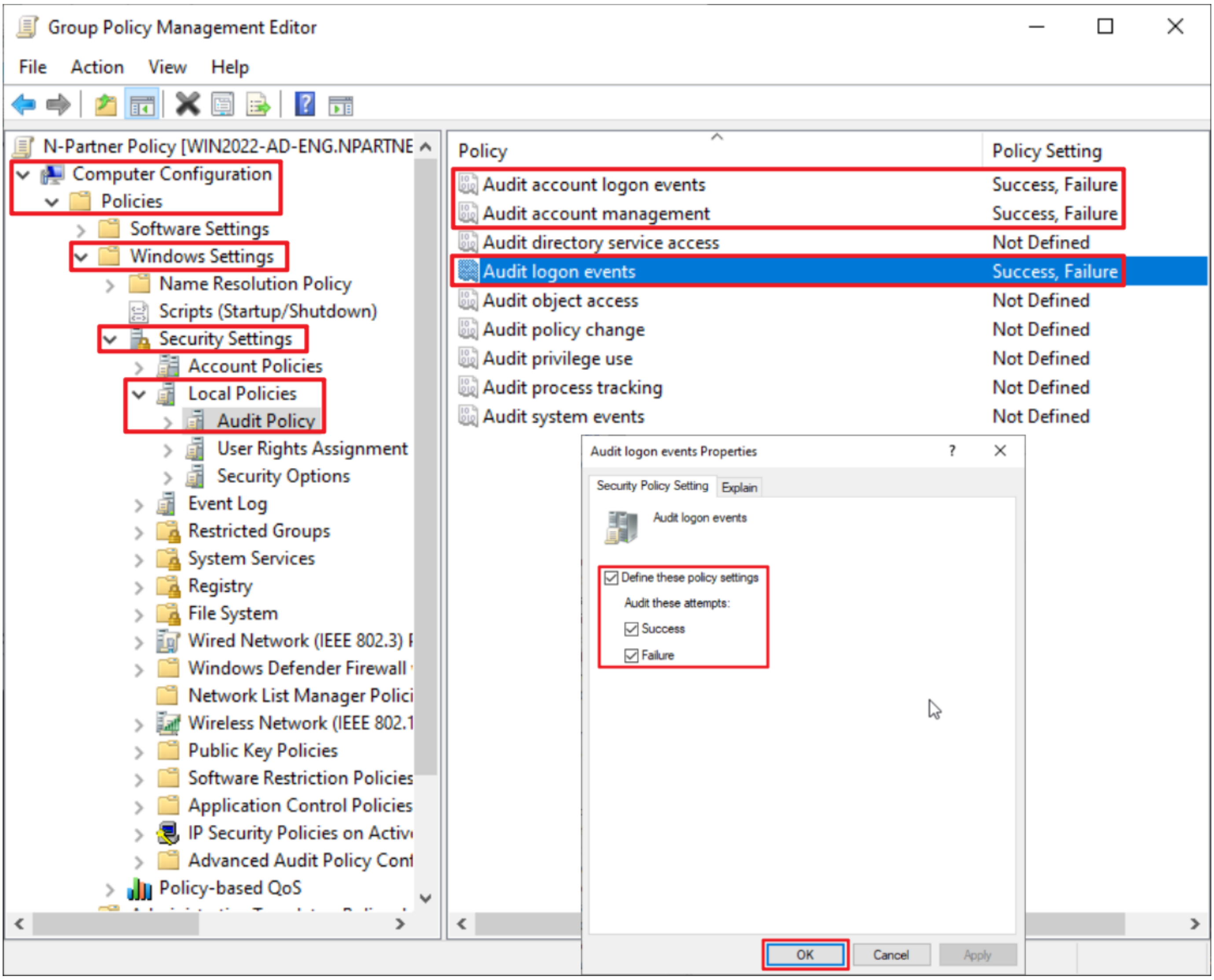
In your group policy object, (in this example, it is “N-Partner Policy”) right-click and select “Edit.”



This page shows the status of Active Directory and SYSVOL replication for this domain as it

(5) Local Group Policies: Audit Policy

Expand folder “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Local Policies” → “Audit Policy.” And click on “Audit account logon events,” “Audit account management,” and “Audit logon events,” → check “Define these policy settings”: Success, Failure. → click “OK.”



Group Policy Management Editor

Policy	Policy Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Not Defined
Audit logon events	Success, Failure
Audit object access	Not Defined
Audit policy change	Not Defined
Audit privilege use	Not Defined
Audit process tracking	Not Defined
Audit system events	Not Defined

Audit logon events Properties

Audit logon events

☑ Define these policy settings

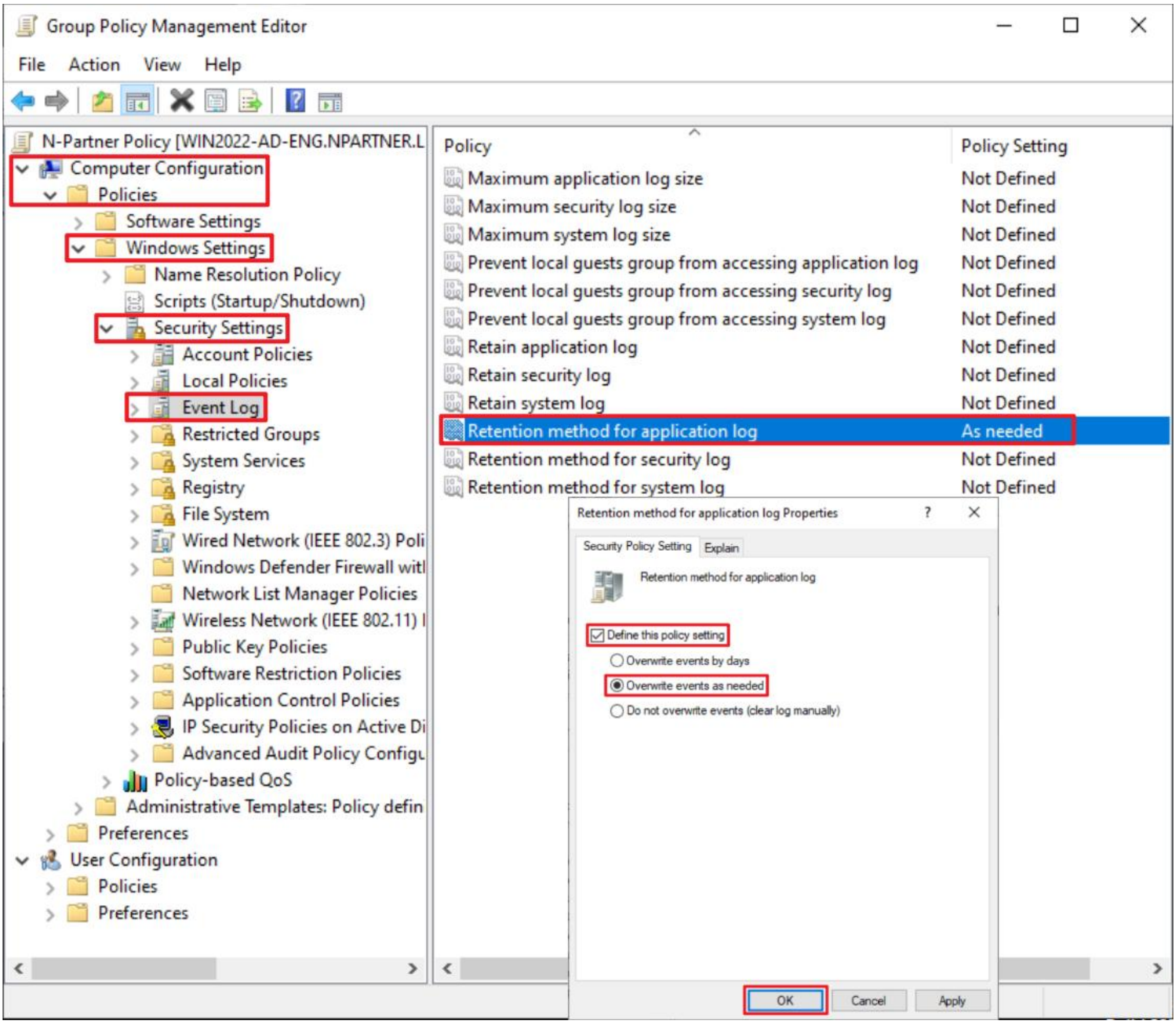
Audit these attempts:

☑ Success

☑ Failure

(6) Event Log: Application Log Retention Method

Expand “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” → select “Retention method for application log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



Group Policy Management Editor
File
Action
View
Help
N-Partner Policy [WIN2022-AD-ENG.NPARTNER.L
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Poli
Windows Defender Firewall witl
Network List Manager Policies
Wireless Network (IEEE 802.11) I
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Di
Advanced Audit Policy Configu
Policy-based QoS
Administrative Templates: Policy defin
Preferences
User Configuration
Policies
Preferences

Policy	Policy Setting
Maximum application log size	Not Defined
Maximum security log size	Not Defined
Maximum system log size	Not Defined
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	As needed
Retention method for security log	Not Defined
Retention method for system log	Not Defined

Retention method for application log Properties

Retention method for application log

☑ Define this policy setting

○ Overwrite events by days

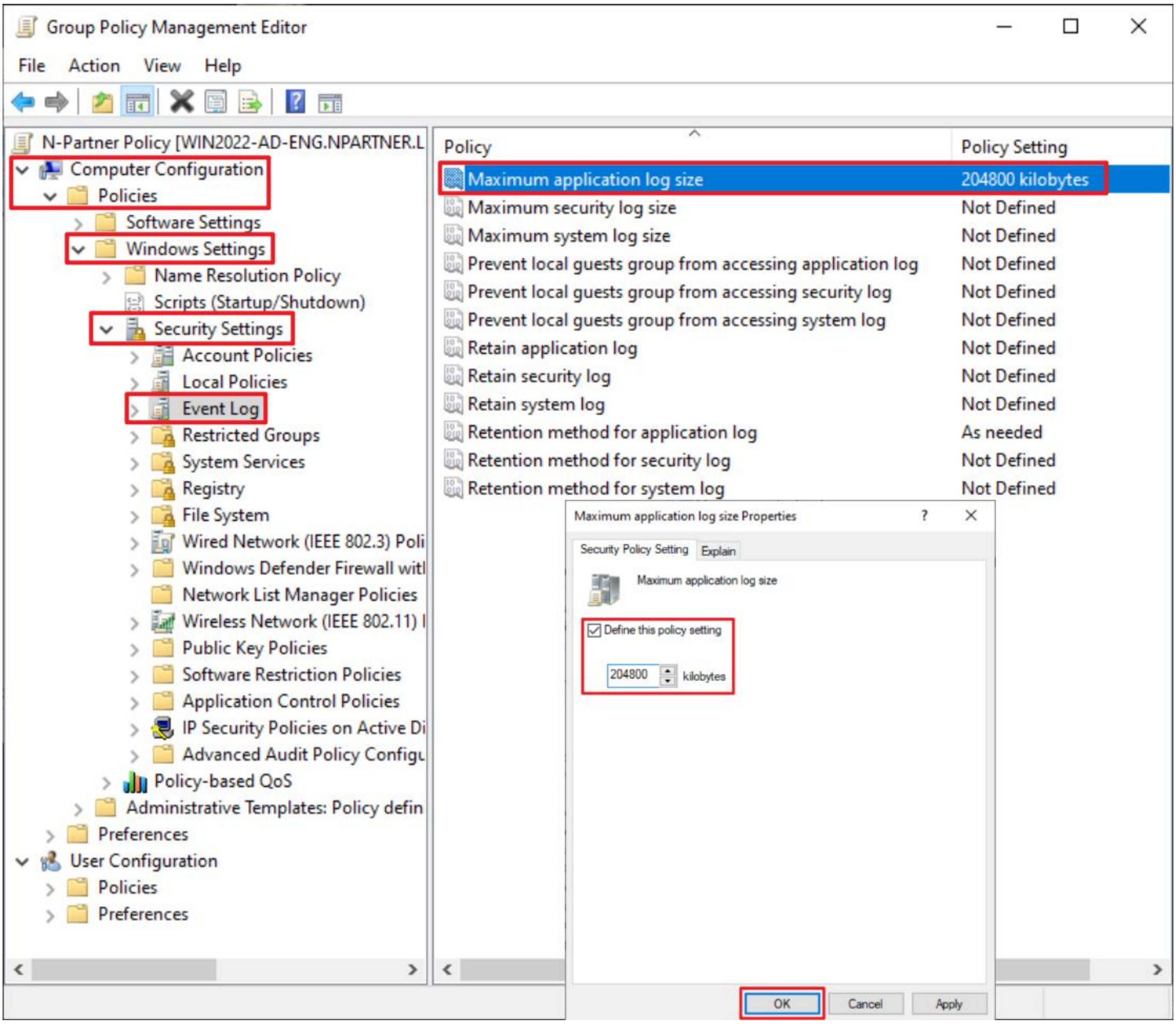
● Overwrite events as needed

○ Do not overwrite events (clear log manually)

(7) Event Logs: Maximum Size of Security Log

Expand folder “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” →And click on “Maximum application log size” → Check “Define this policy setting” → enter 204800 KB

Note: Please adjust the number based on the actual environment. → click “OK.”



Group Policy Management Editor
File Action View Help
N-Partner Policy [WIN2022-AD-ENG.NPARTNER.L
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Poli
Windows Defender Firewall witl
Network List Manager Policies
Wireless Network (IEEE 802.11) I
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Di
Advanced Audit Policy Configu
Policy-based QoS
Administrative Templates: Policy defin
Preferences
User Configuration
Policies
Preferences

Policy	Policy Setting
Maximum application log size	204800 kilobytes
Maximum security log size	Not Defined
Maximum system log size	Not Defined
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	As needed
Retention method for security log	Not Defined
Retention method for system log	Not Defined

Maximum application log size Properties

Security Policy Setting | Explain

Maximum application log size

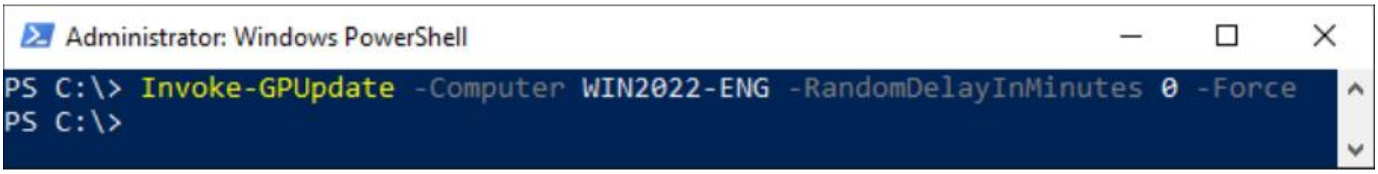
☑ Define this policy setting

204800 kilobytes

(8) On the AD domain server, open “Windows PowerShell.”

(9) Enter the command below to refresh group policy.

```
PS C:\> Invoke-GPUpdate -Computer WIN2022-ENG -RandomDelayInMinutes 0 -Force
```

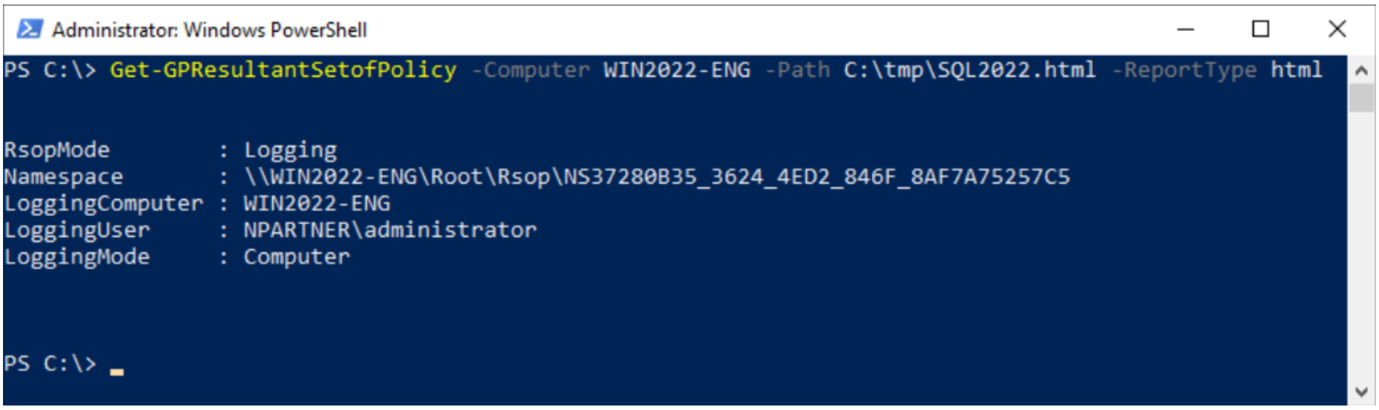


```
PS C:\> Invoke-GPUpdate -Computer WIN2022-ENG -RandomDelayInMinutes 0 -Force
PS C:\>
```

Replace the text shown in red with the MS SQL server name.

(10) Enter the command below to generate server group policy report.

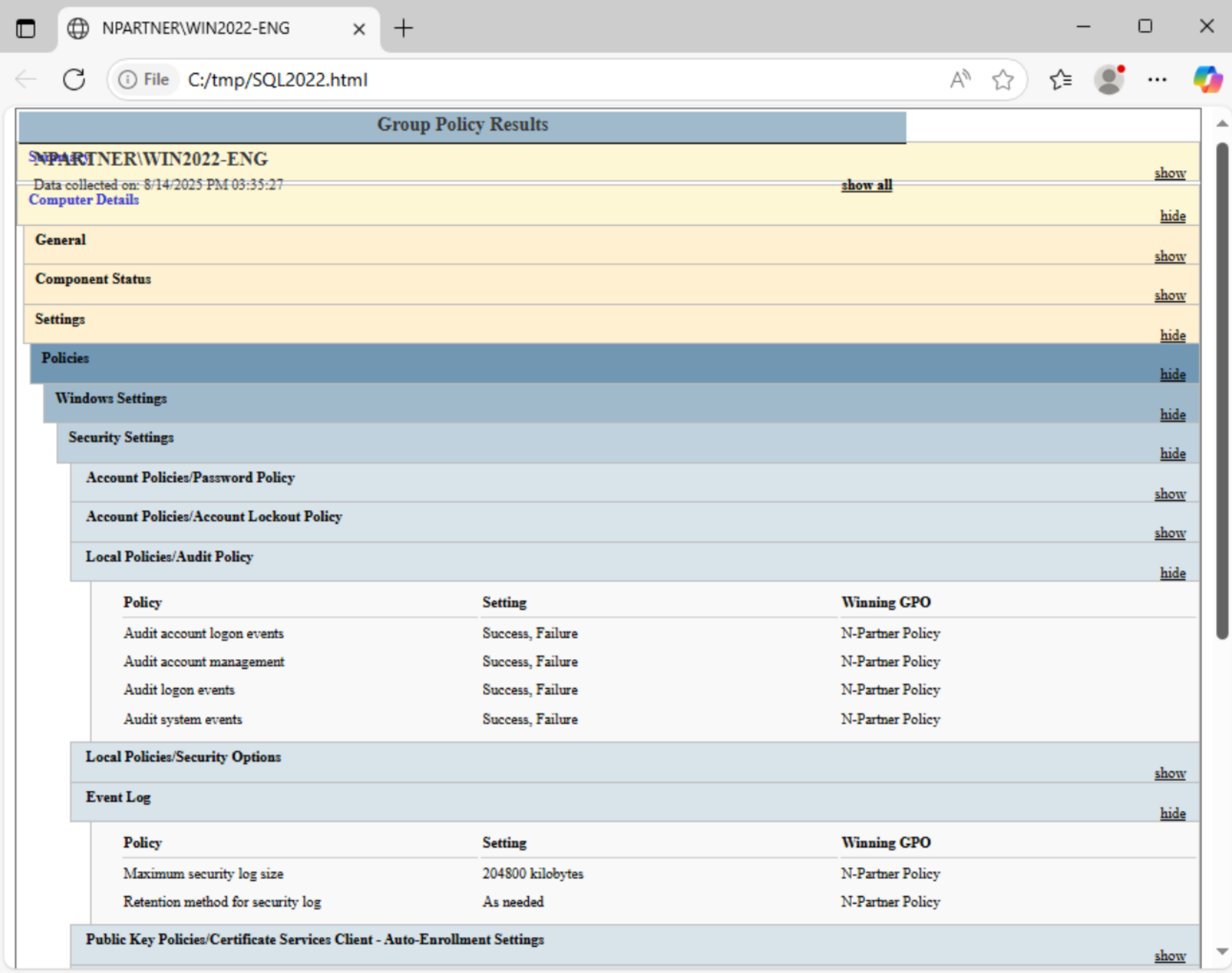
```
PS C:\> Get-GPResultantSetofPolicy -Computer WIN2022-ENG -Path C:\tmp\SQL2022.html -ReportType
html
```



```
PS C:\> Get-GPResultantSetofPolicy -Computer WIN2022-ENG -Path C:\tmp\SQL2022.html -ReportType html


RsopMode        : Logging
Namespace       : \\WIN2022-ENG\Root\Rsop\NS37280B35_3624_4ED2_846F_8AF7A75257C5
LoggingComputer : WIN2022-ENG
LoggingUser     : NPARTNER\administrator
LoggingMode     : Computer



PS C:\> _
```

For the red text , please enter the MS SQL server name and the folder path/file name.

(11) Open the report and verify that your MS SQL server is applying the N-Partner Policy Group Policy.



Group Policy Results

NPARTNER\WIN2022-ENG

Data collected on: 8/14/2025 PM 03:35:27

Summary show

show all

Computer Details hide

General show

Component Status show

Settings hide

Policies hide

Windows Settings hide

Security Settings hide

Account Policies/Password Policy show

Account Policies/Account Lockout Policy show

Local Policies/Audit Policy hide

Policy	Setting	Winning GPO
Audit account logon events	Success, Failure	N-Partner Policy
Audit account management	Success, Failure	N-Partner Policy
Audit logon events	Success, Failure	N-Partner Policy
Audit system events	Success, Failure	N-Partner Policy

Local Policies/Security Options show

Event Log hide

Policy	Setting	Winning GPO
Maximum security log size	204800 kilobytes	N-Partner Policy
Retention method for security log	As needed	N-Partner Policy

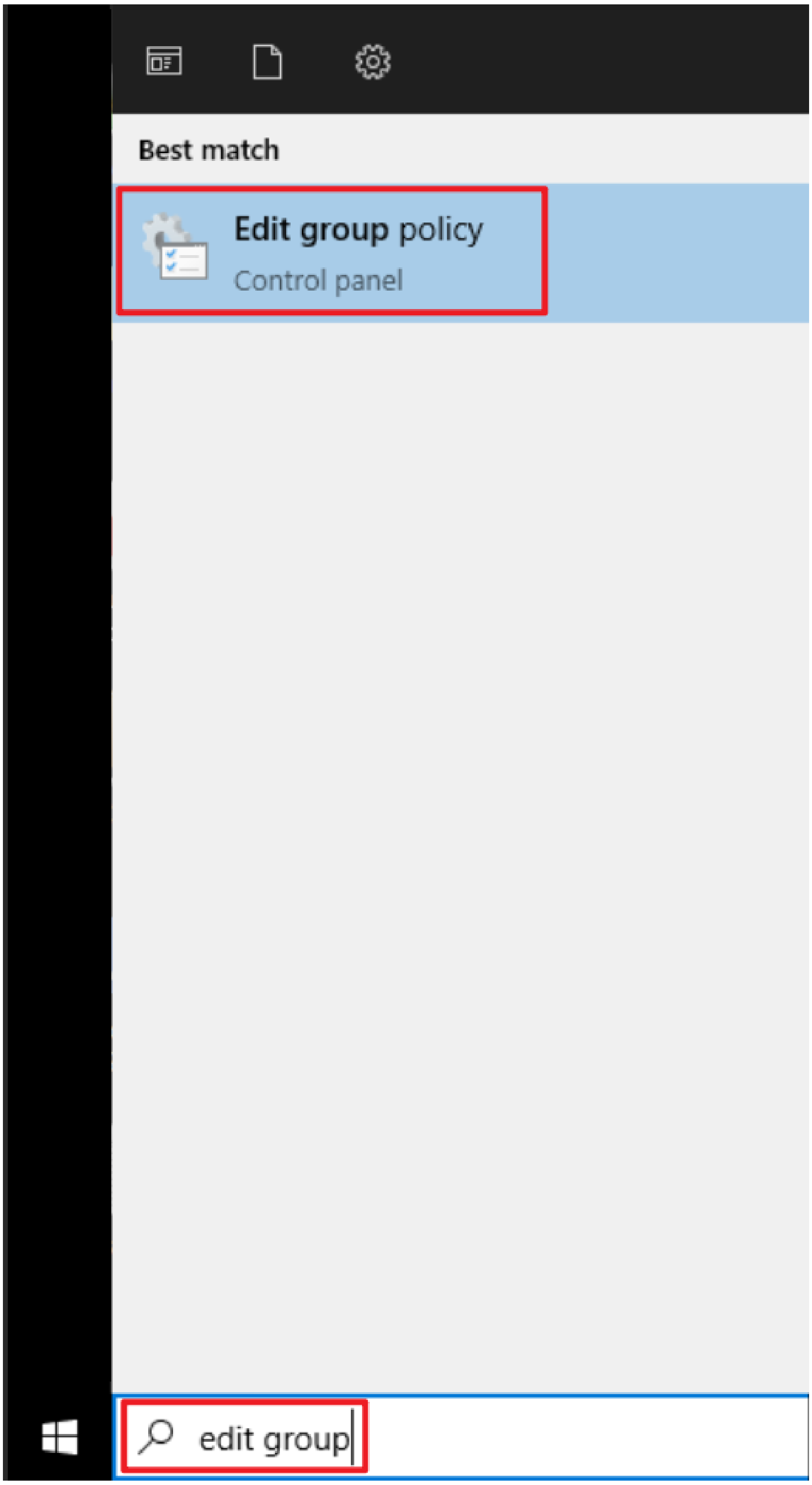
Public Key Policies/Certificate Services Client - Auto-Enrollment Settings show

6.3.2 Workgroup

6.3.2.1 Audit Policy Configuration

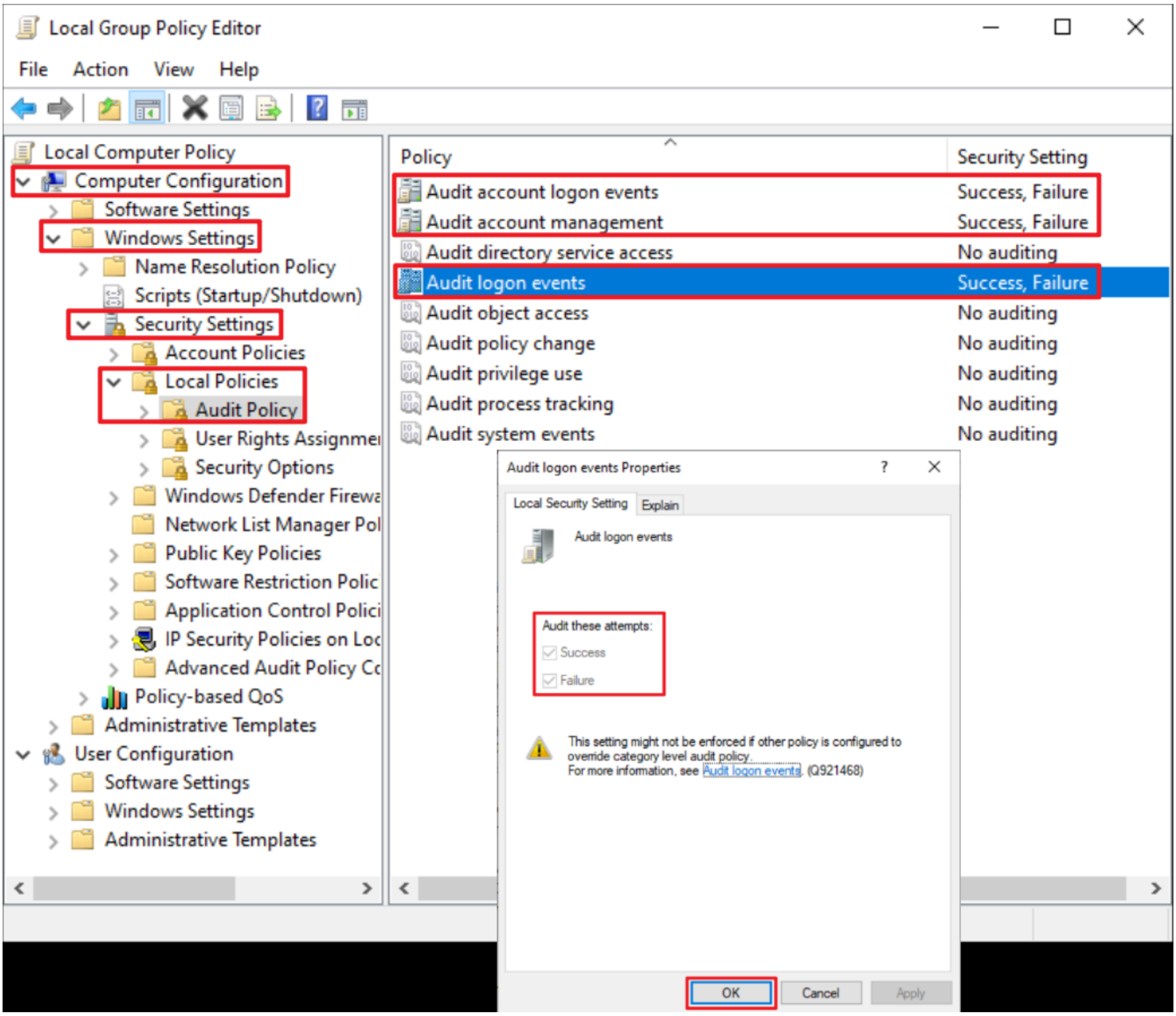
(1) Open Local Group Policy Editor

Click on “Start” → enter “group policy” to search → click on “Edit Group Policy.”



(2) Local Group Policies: Audit Policy

Expand folder “Computer Configuration” → “Windows Settings” → “Security Settings” -> “Local Policies” → “Audit Policy.” And click on “Audit account logon events,” “Audit account management,” and “Audit logon events” items → check “Define these policy settings”: Success, Failure. → click “OK.”



Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	No auditing
Audit logon events	Success, Failure
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

Audit logon events Properties

Local Security Setting | Explain

Audit logon events

Audit these attempts:

☑ Success

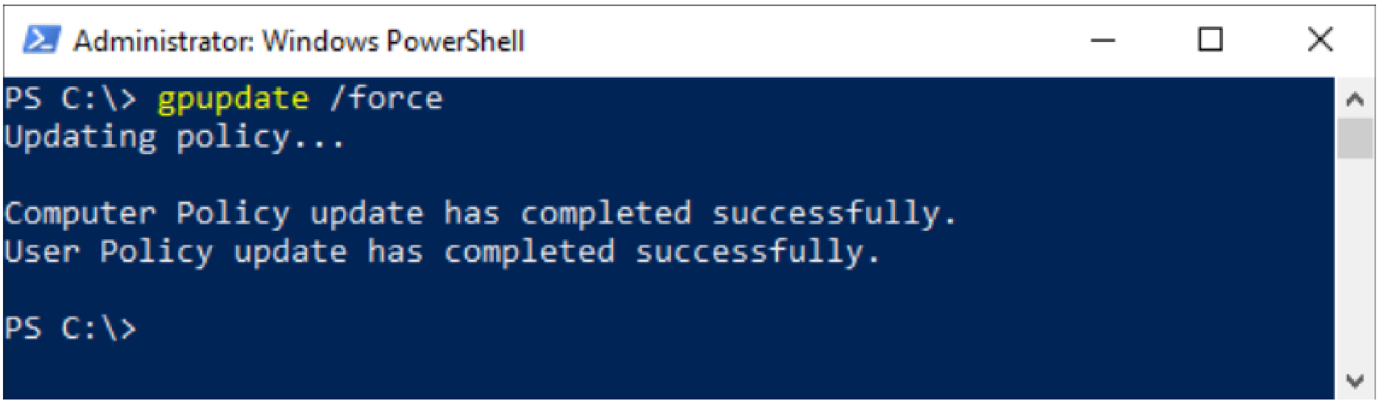
☑ Failure

This setting might not be enforced if other policy is configured to override category level audit policy.
For more information, see Audit logon events. (Q921468)

(3) Open “Windows PowerShell.”

(4) Enter the command below to refresh group policy.

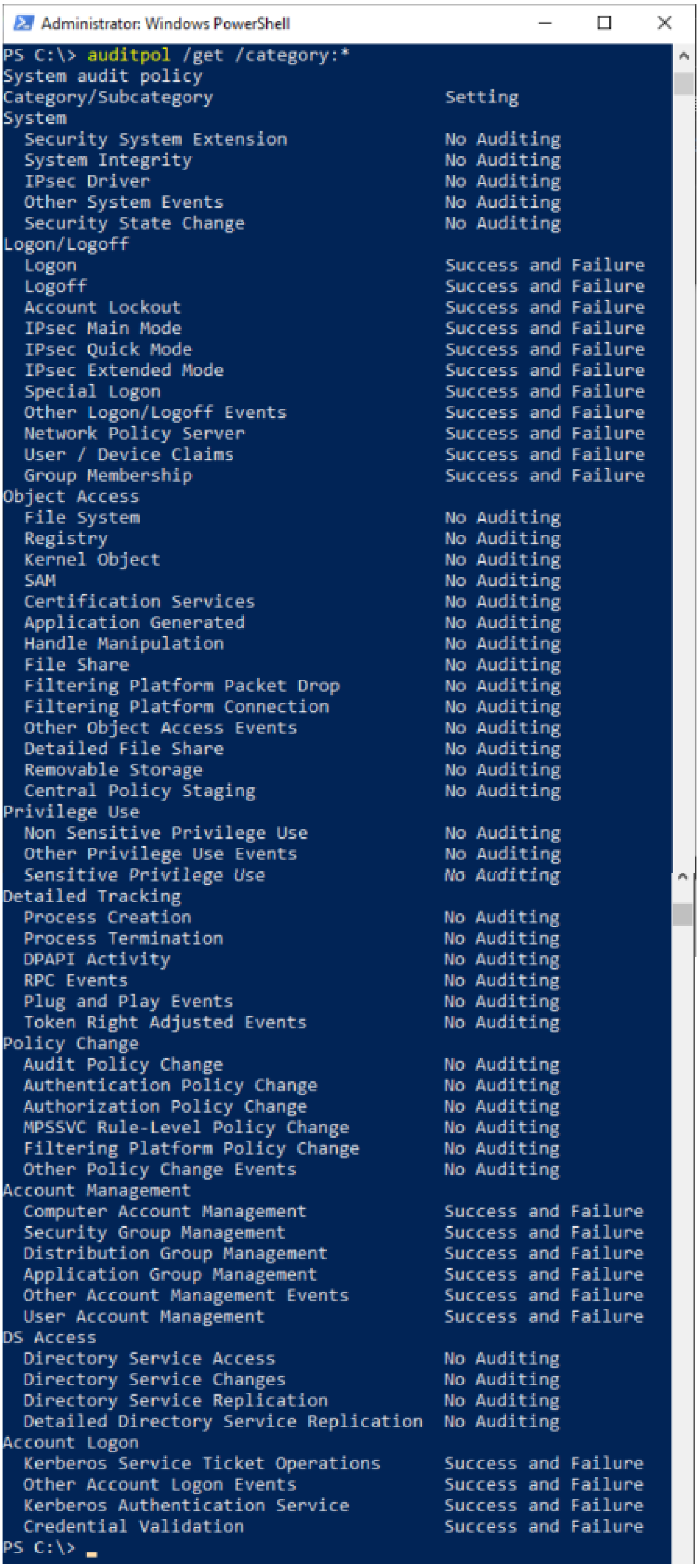
```
PS C:\> gpupdate /force
```



```
PS C:\> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

PS C:\>
```

(5) Enter the command below to view group policy applied status.

```
PS C: \> auditpol /get /category:*
```

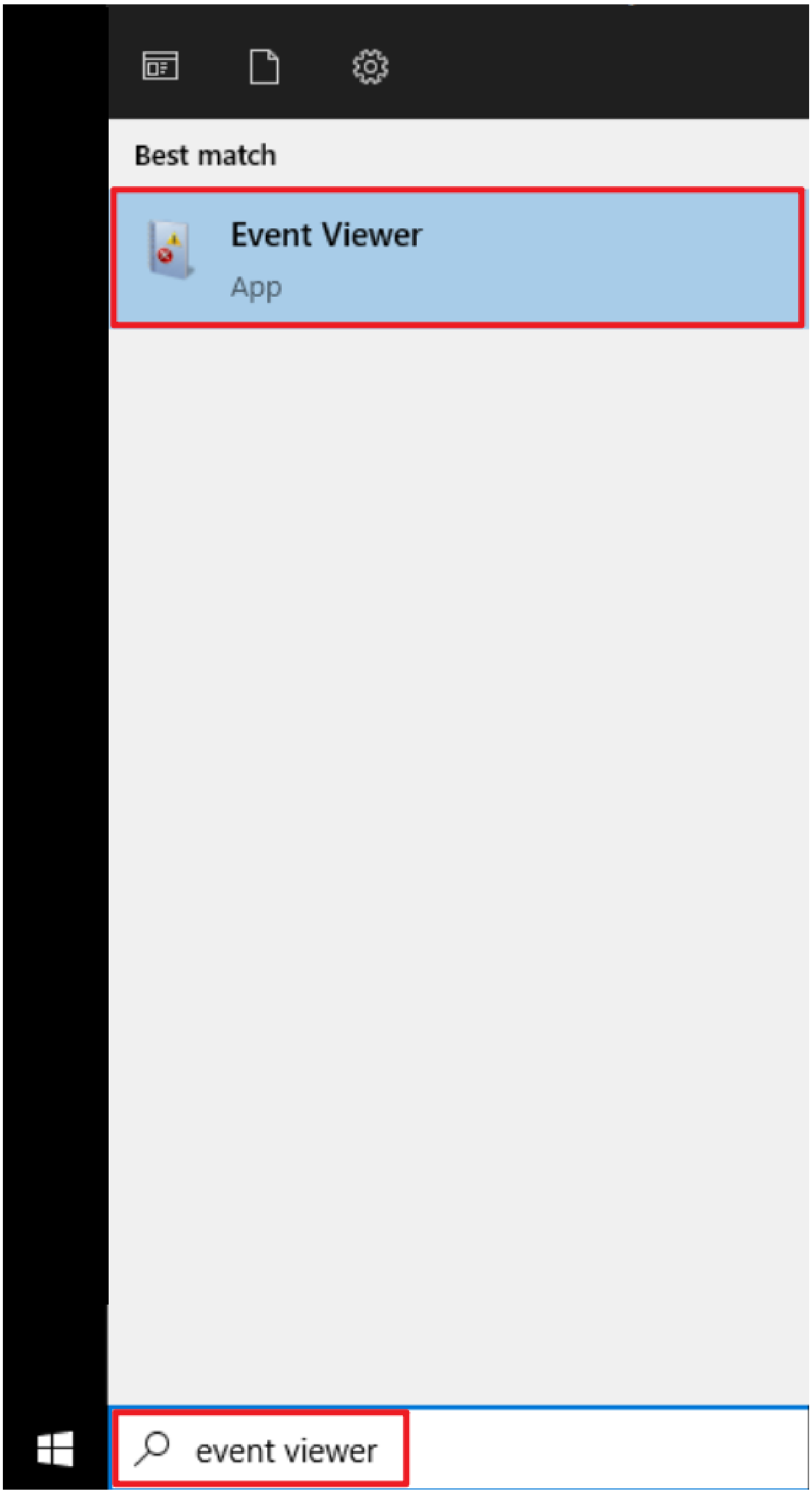


```
PS C:\> auditpol /get /category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               No Auditing
  System Integrity                        No Auditing
  IPsec Driver                            No Auditing
  Other System Events                     No Auditing
  Security State Change                   No Auditing
Logon/Logoff
  Logon                                   Success and Failure
  Logoff                                  Success and Failure
  Account Lockout                         Success and Failure
  IPsec Main Mode                         Success and Failure
  IPsec Quick Mode                        Success and Failure
  IPsec Extended Mode                     Success and Failure
  Special Logon                           Success and Failure
  Other Logon/Logoff Events               Success and Failure
  Network Policy Server                   Success and Failure
  User / Device Claims                    Success and Failure
  Group Membership                        Success and Failure
Object Access
  File System                             No Auditing
  Registry                                No Auditing
  Kernel Object                           No Auditing
  SAM                                     No Auditing
  Certification Services                  No Auditing
  Application Generated                   No Auditing
  Handle Manipulation                     No Auditing
  File Share                              No Auditing
  Filtering Platform Packet Drop          No Auditing
  Filtering Platform Connection           No Auditing
  Other Object Access Events              No Auditing
  Detailed File Share                     No Auditing
  Removable Storage                       No Auditing
  Central Policy Staging                  No Auditing
Privilege Use
  Non Sensitive Privilege Use             No Auditing
  Other Privilege Use Events              No Auditing
  Sensitive Privilege Use                 No Auditing
Detailed Tracking
  Process Creation                        No Auditing
  Process Termination                     No Auditing
  DPAPI Activity                          No Auditing
  RPC Events                              No Auditing
  Plug and Play Events                    No Auditing
  Token Right Adjusted Events             No Auditing
Policy Change
  Audit Policy Change                     No Auditing
  Authentication Policy Change            No Auditing
  Authorization Policy Change             No Auditing
  MPSSVC Rule-Level Policy Change         No Auditing
  Filtering Platform Policy Change        No Auditing
  Other Policy Change Events              No Auditing
Account Management
  Computer Account Management             Success and Failure
  Security Group Management               Success and Failure
  Distribution Group Management           Success and Failure
  Application Group Management            Success and Failure
  Other Account Management Events         Success and Failure
  User Account Management                 Success and Failure
DS Access
  Directory Service Access                No Auditing
  Directory Service Changes               No Auditing
  Directory Service Replication           No Auditing
  Detailed Directory Service Replication  No Auditing
Account Logon
  Kerberos Service Ticket Operations      Success and Failure
  Other Account Logon Events              Success and Failure
  Kerberos Authentication Service         Success and Failure
  Credential Validation                   Success and Failure
PS C:\> _
```

6.3.2.2 Event Log Settings

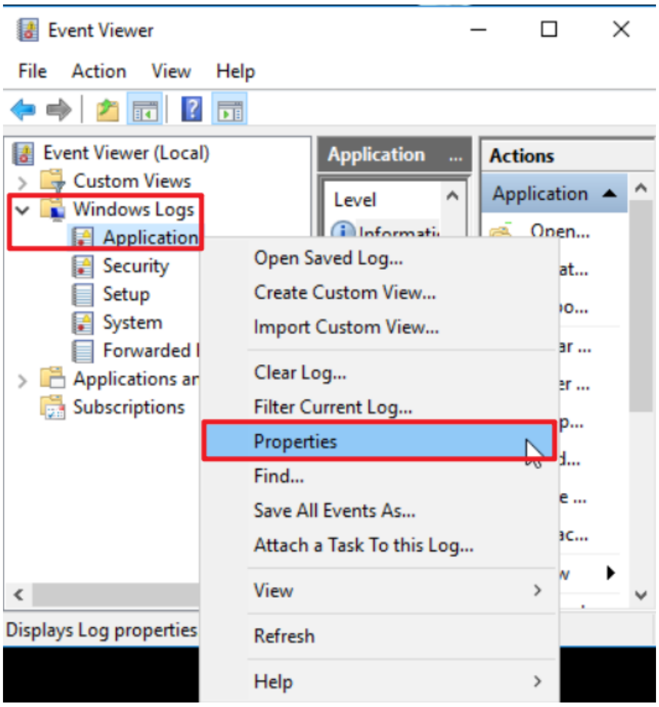
(1) Search for “Event Viewer”

Enter “Event Viewer” to search → click on “Event Viewer” in the search results.



(2) Edit Security Log

Expand folder “Windows Logs” → right-click on “Application” → And click on “Properties.”

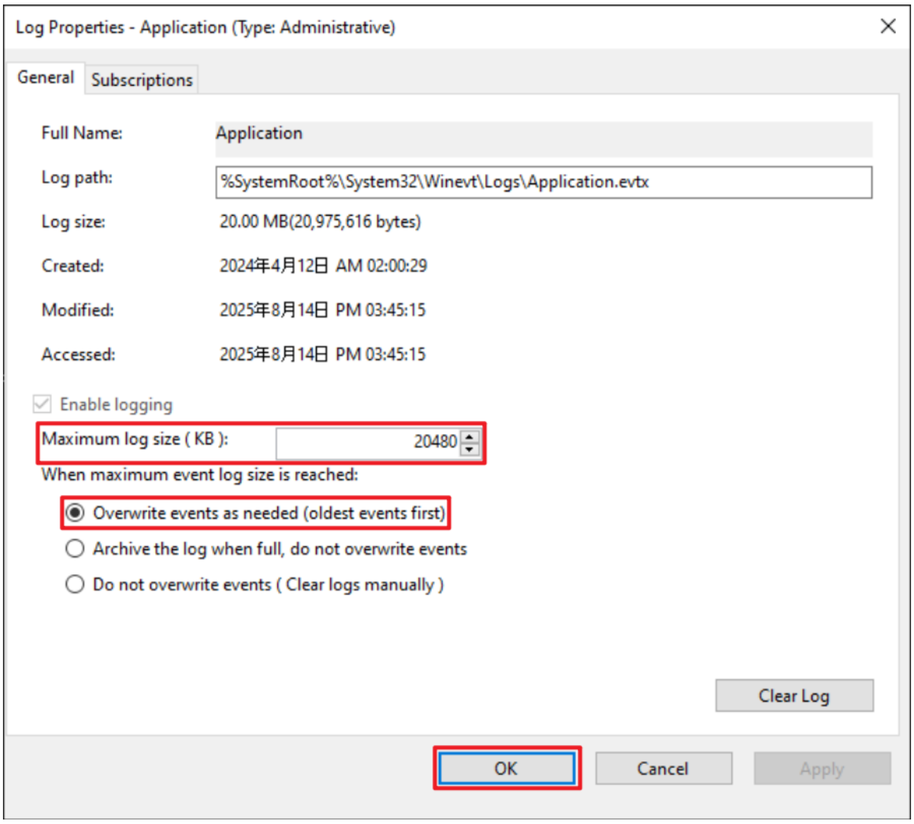


(3) Configure Security Log

Enter maximum log file size: 204800 KB

Note: Please adjust the number according to the actual environment.

→ click on “Overwrite events as needed (oldest events first) → click “OK.”



Log Properties - Application (Type: Administrative)

General | Subscriptions

Full Name: Application

Log path: %SystemRoot%\System32\Winevt\Logs\Application.evtx

Log size: 20.00 MB(20,975,616 bytes)

Created: 2024年4月12日 AM 02:00:29

Modified: 2025年8月14日 PM 03:45:15

Accessed: 2025年8月14日 PM 03:45:15

☑ Enable logging

Maximum log size (KB): 20480

When maximum event log size is reached:

● Overwrite events as needed (oldest events first)

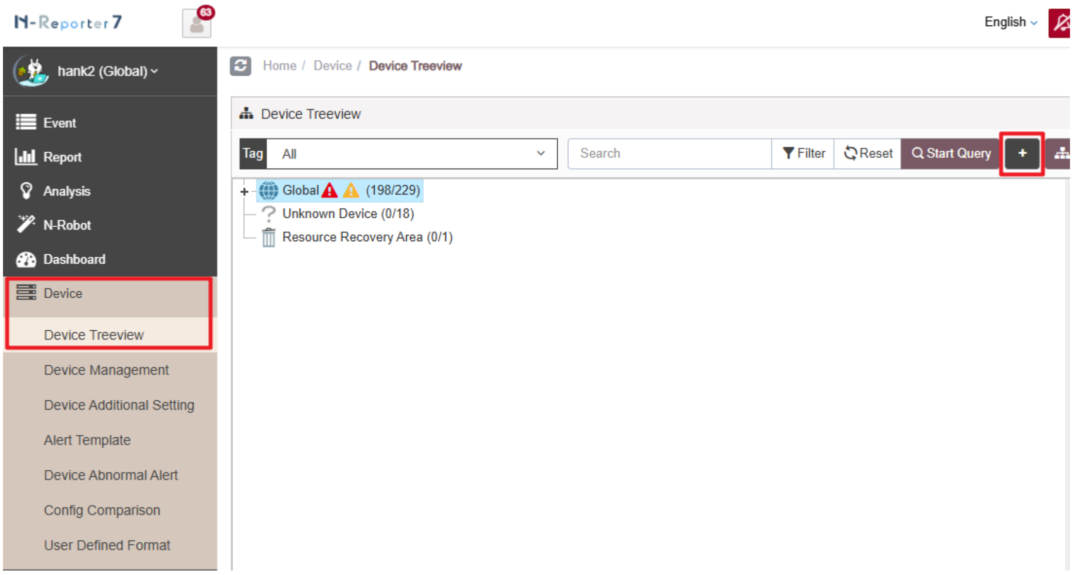
○ Archive the log when full, do not overwrite events

○ Do not overwrite events (Clear logs manually)

7. N-Reporter

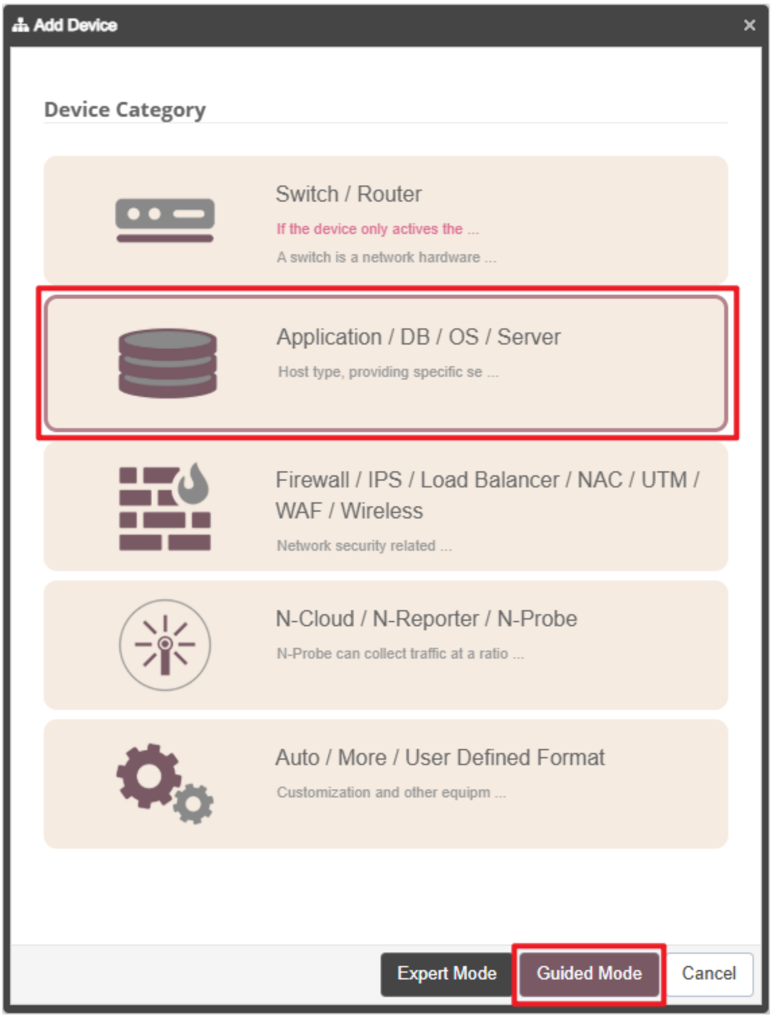
(1) Add a Windows MS SQL device:

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



(2) Select the device type:

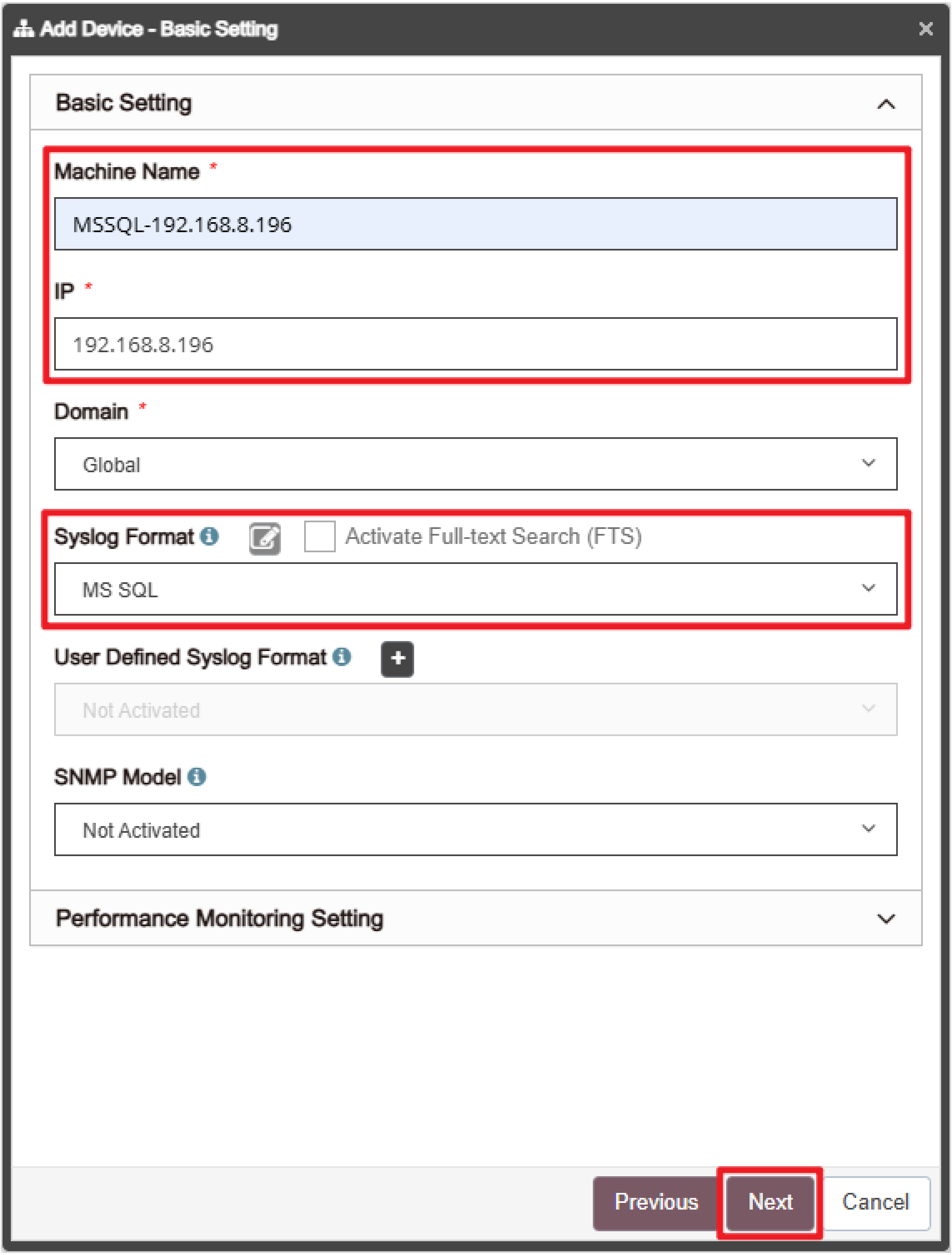
Choose “Application/DB/OS/Server” → click “Guided Mode.”


Add Device
×
Device Category
Switch / Router
If the device only actives the ...
A switch is a network hardware ...
Application / DB / OS / Server
Host type, providing specific se ...
Firewall / IPS / Load Balancer / NAC / UTM / WAF / Wireless
Network security related ...
N-Cloud / N-Reporter / N-Probe
N-Probe can collect traffic at a ratio ...
Auto / More / User Defined Format
Customization and other equipm ...
Expert Mode
Guided Mode
Cancel

7.1 MS SQL Server Event Log

(1) Basic Device Settings:

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



Add Device - Basic Setting

Basic Setting

Machine Name *

MSSQL-192.168.8.196

IP *

192.168.8.196

Domain *

Global

Syslog Format □ Activate Full-text Search (FTS)

MS SQL

User Defined Syslog Format

Not Activated

SNMP Model

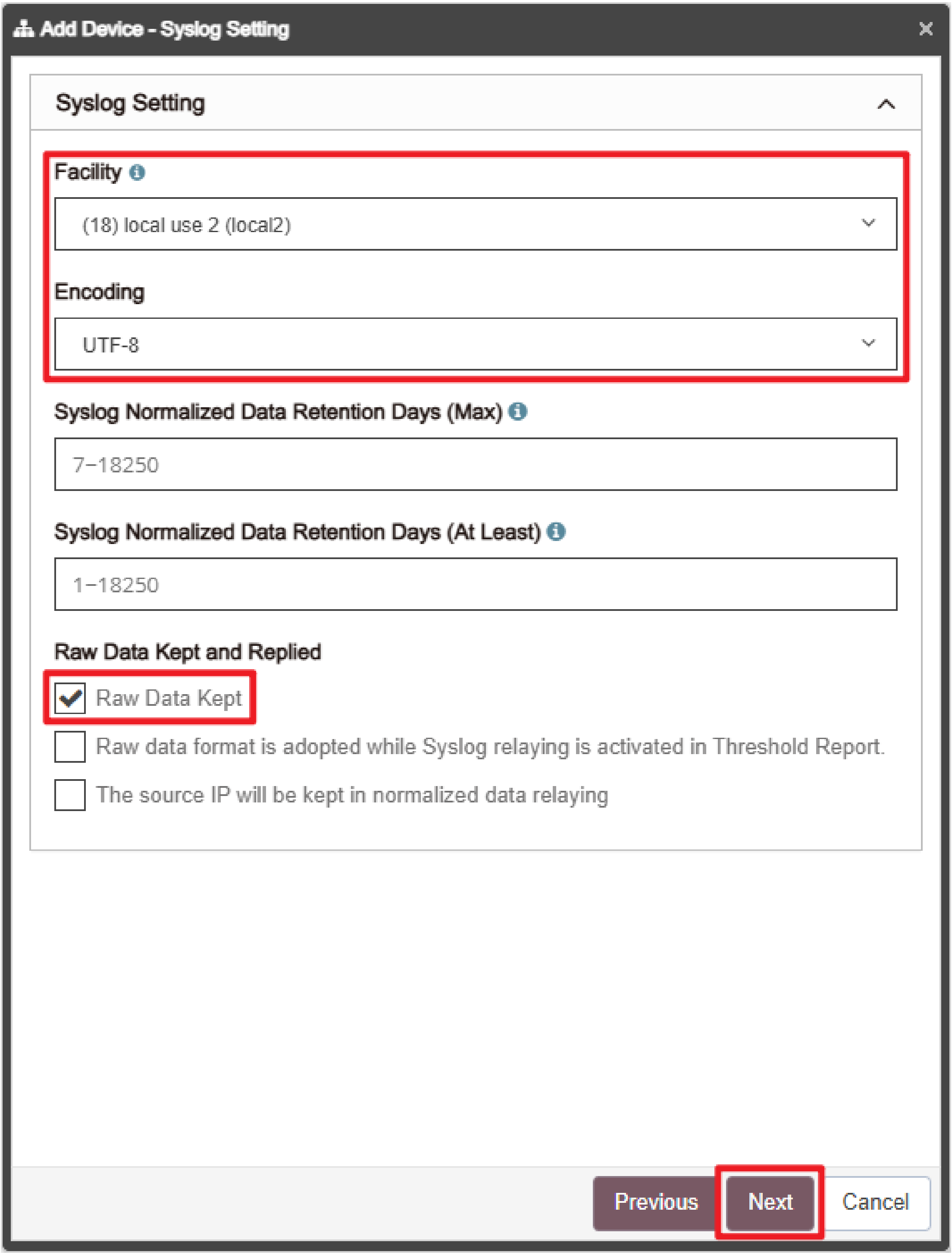
Not Activated

Performance Monitoring Setting

(2) Syslog Settings

Set “Facility” to “(18) local use 2 (local2)” → click “Next.”

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



Add Device - Syslog Setting

Syslog Setting

Facility: (18) local use 2 (local2)

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

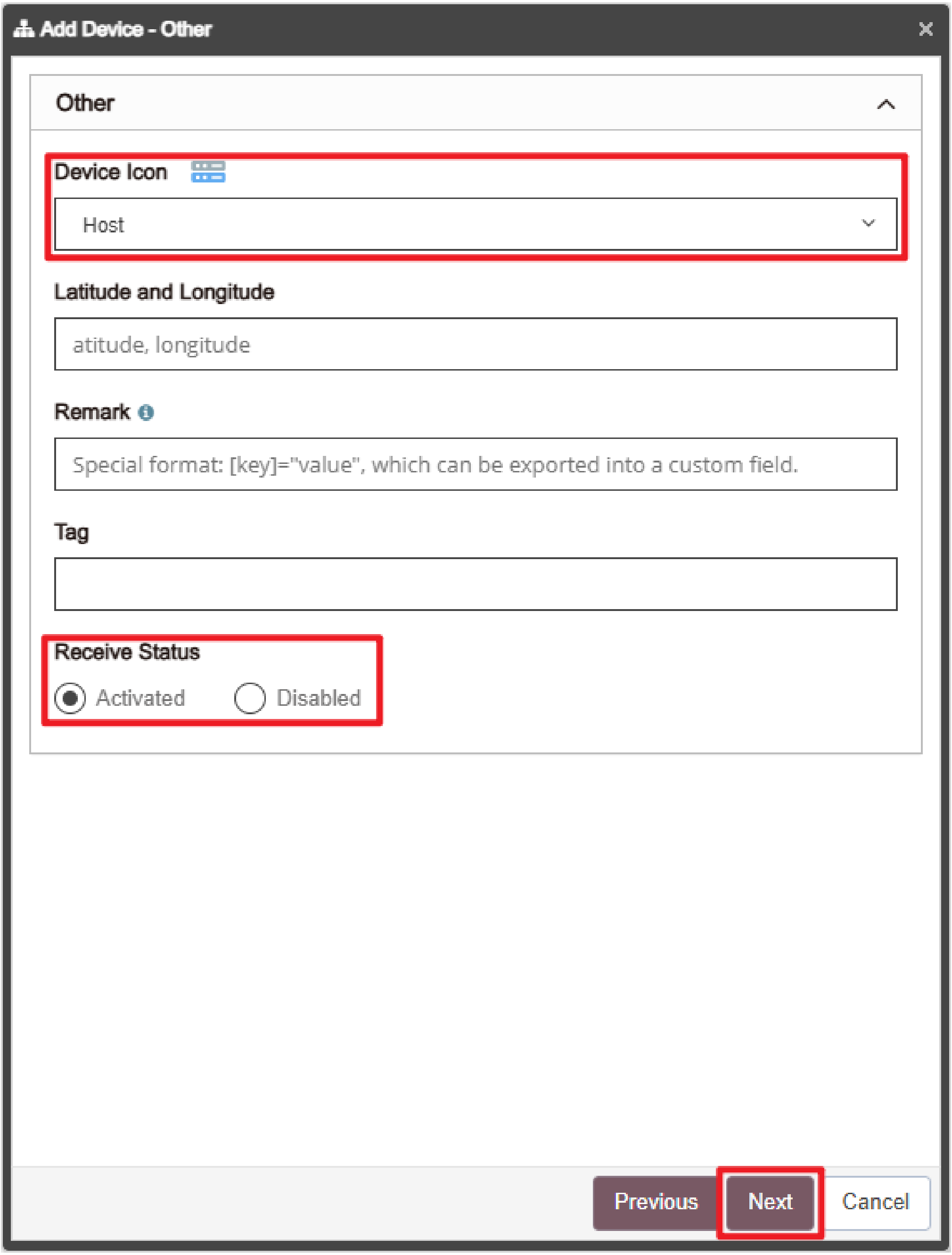
☑ Raw Data Kept

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

□ The source IP will be kept in normalized data relaying

(3) Others

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



Add Device - Other

Other

Device Icon

Host

Latitude and Longitude

atitude, longitude

Remark

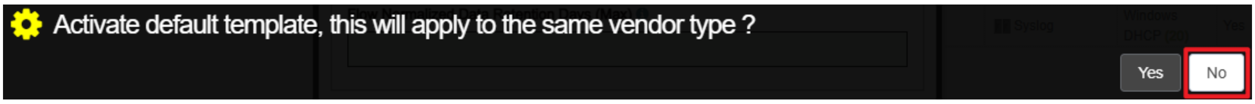
Special format: [key]="value", which can be exported into a custom field.

Tag

Receive Status

● Activated ○ Disabled

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

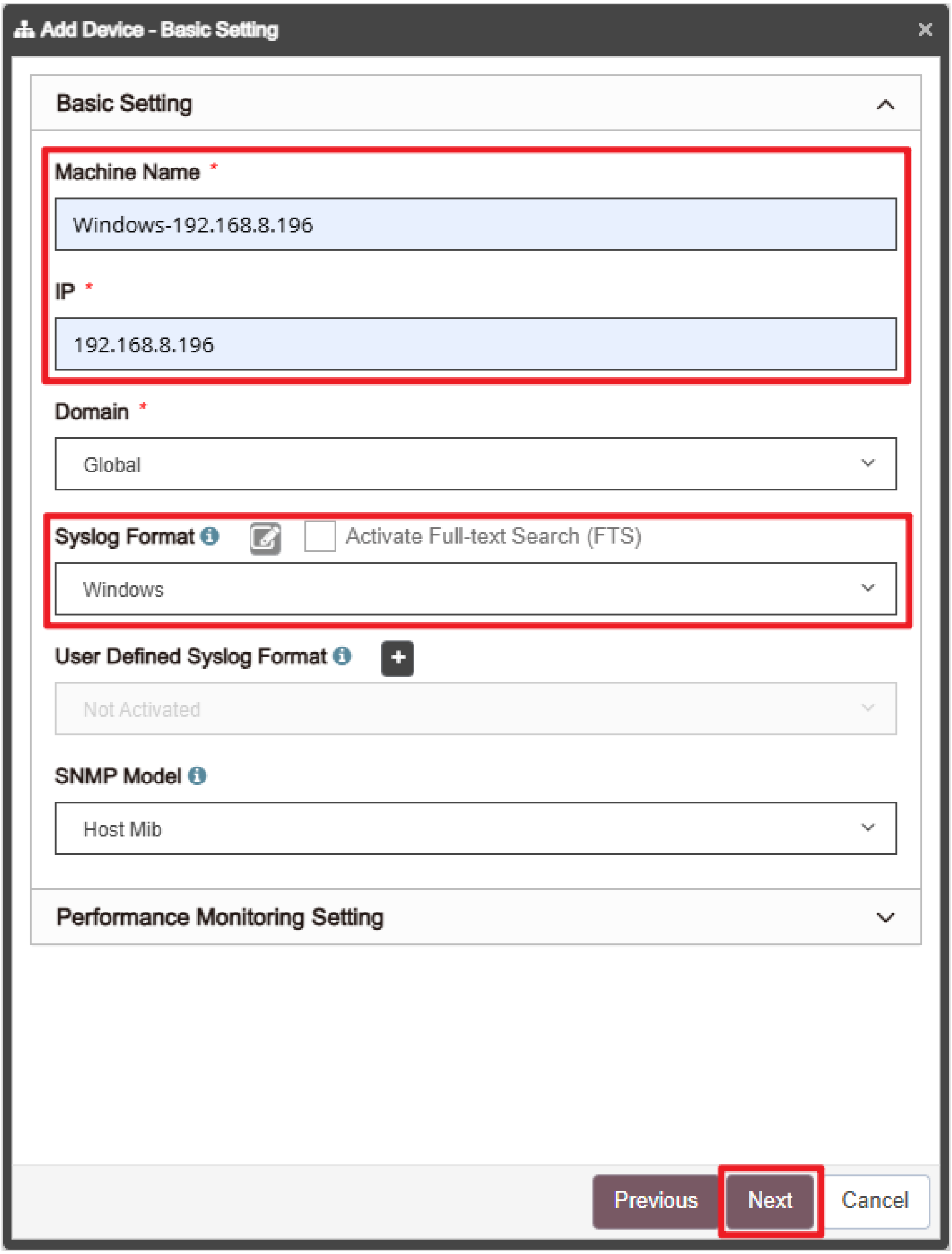


Activate default template, this will apply to the same vendor type ?

7.2 Windows Event Log

(1) Device Basic Settings

Enter the device name and IP → Select “Windows” for the Syslog data format → Click “Next.”



Add Device - Basic Setting

Basic Setting

Machine Name *

Windows-192.168.8.196

IP *

192.168.8.196

Domain *

Global

Syslog Format □ Activate Full-text Search (FTS)

Windows

User Defined Syslog Format

Not Activated

SNMP Model

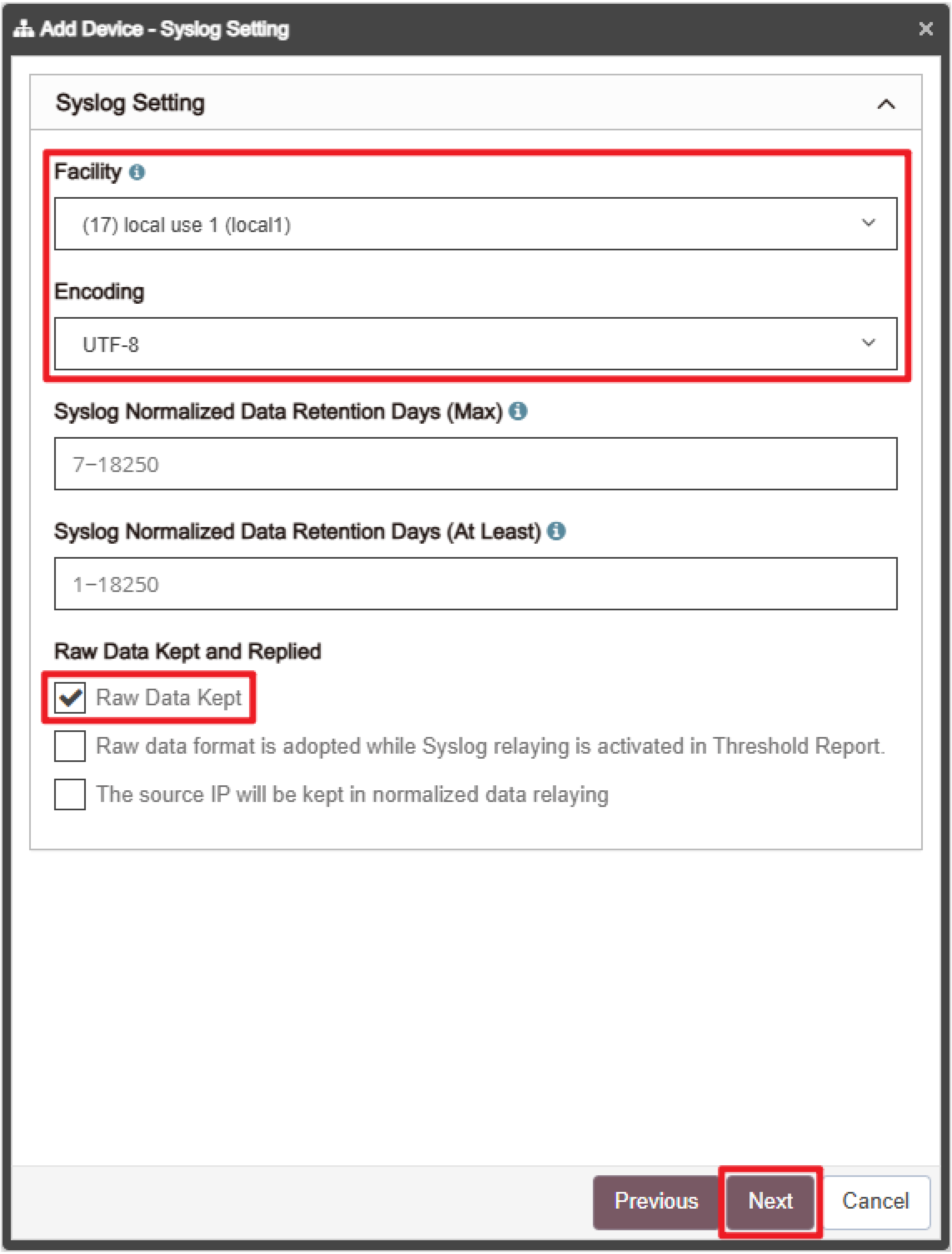
Host Mib

Performance Monitoring Setting

(2) Syslog Settings

Set “Facility” to “(17) local use 1 (local1)” → click “Next.”

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



Add Device - Syslog Setting

Syslog Setting

Facility: (17) local use 1 (local1)

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

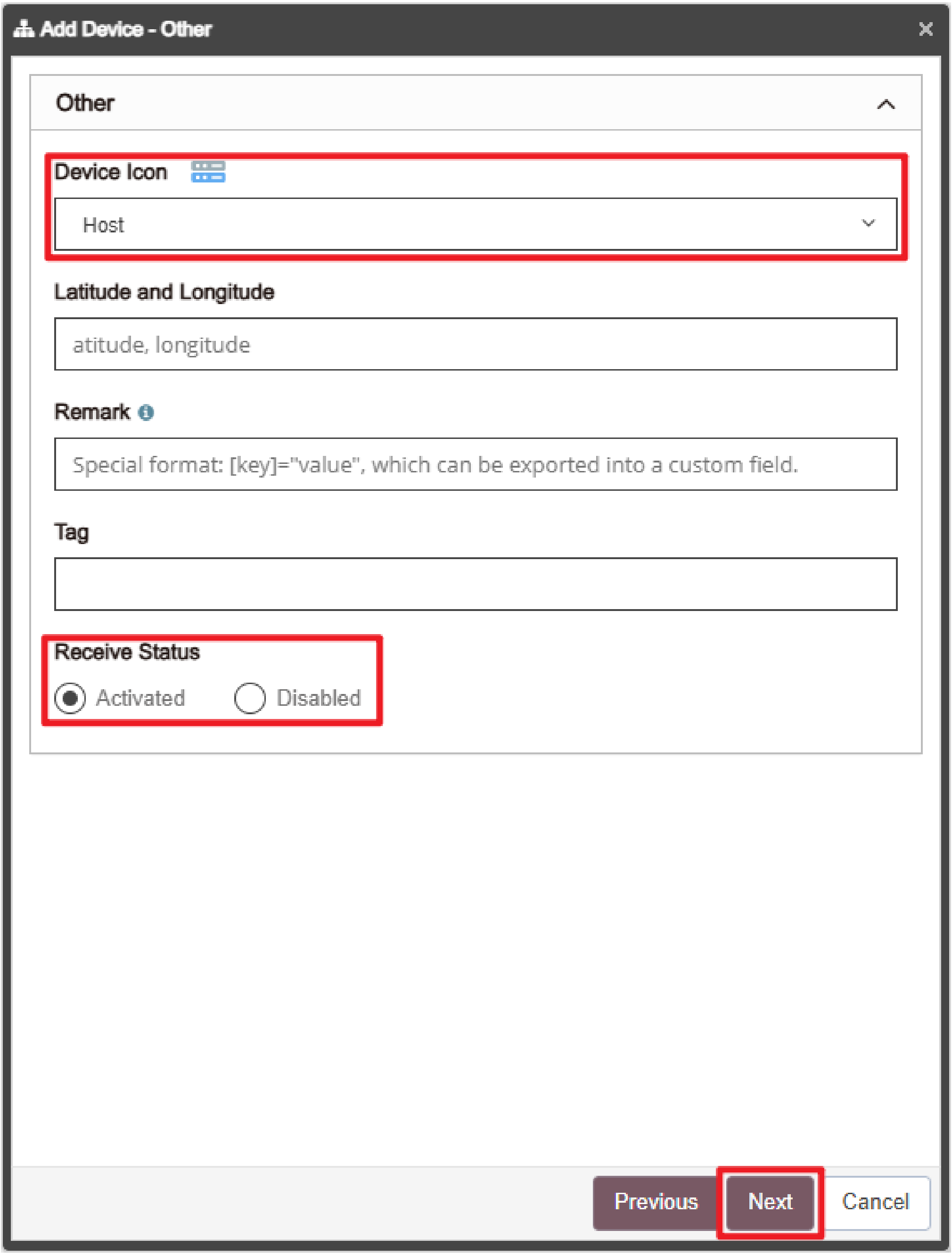
☑ Raw Data Kept

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

□ The source IP will be kept in normalized data relaying

(3) Others

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



Add Device - Other

Other

Device Icon

Host

Latitude and Longitude

atitude, longitude

Remark

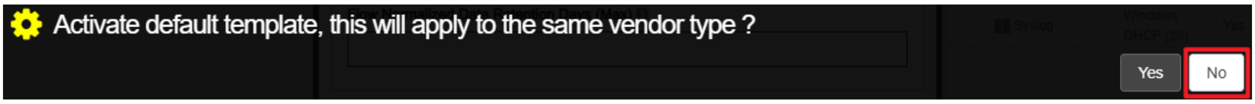
Special format: [key]="value", which can be exported into a custom field.

Tag

Receive Status

● Activated ○ Disabled

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

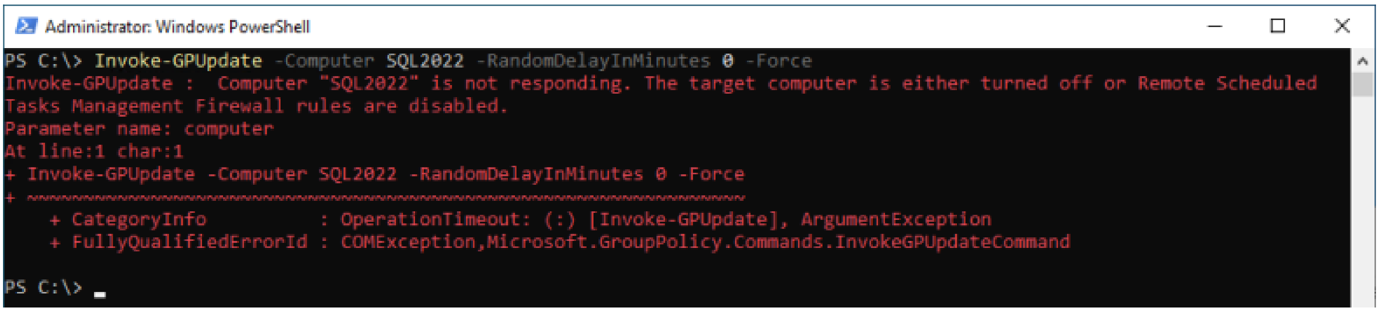


Activate default template, this will apply to the same vendor type ?

8. Troubleshooting

8.1 Invoke-GPUpdate Error

(1) On the AD domain server, run Invoke-GPUpdate to update the Windows Server Group Policy. An error message may appear.



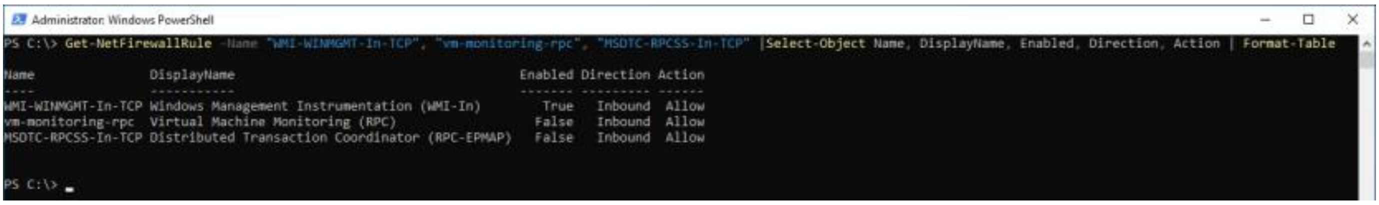
Administrator: Windows PowerShell

```
PS C:\> Invoke-GPUpdate -Computer SQL2022 -RandomDelayInMinutes 0 -Force
Invoke-GPUpdate :  Computer "SQL2022" is not responding. The target computer is either turned off or Remote Scheduled
Tasks Management Firewall rules are disabled.
Parameter name: computer
At line:1 char:1
+ Invoke-GPUpdate -Computer SQL2022 -RandomDelayInMinutes 0 -Force
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : OperationTimeout: (:) [Invoke-GPUpdate], ArgumentException
    + FullyQualifiedErrorId : COMException,Microsoft.GroupPolicy.Commands.InvokeGPUpdateCommand

PS C:\> _
```

(2) On the Windows Server, open "Windows PowerShell."

(3) Enter the following command to check the Windows Firewall rules for **WMI-WINMGMT-In-TCP**, **vm-monitoring-rpc**, and **MSDTC-RPCSS-In-TCP**:

```
PS C:\> Get-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" | Select-Object Name, DisplayName, Enabled, Direction, Action | Format-Table
```

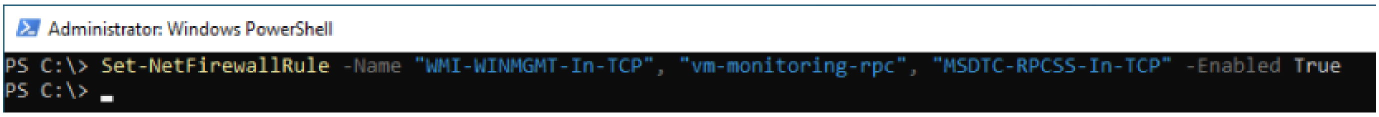


Administrator: Windows PowerShell

```
PS C:\> Get-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" |Select-Object Name, DisplayName, Enabled, Direction, Action | Format-Table

Name               DisplayName                                      Enabled Direction Action
----               -----------                                      ------- --------- ------
WMI-WINMGMT-In-TCP Windows Management Instrumentation (WMI-In)         True   Inbound  Allow
vm-monitoring-rpc  Virtual Machine Monitoring (RPC)                   False   Inbound  Allow
MSDTC-RPCSS-In-TCP Distributed Transaction Coordinator (RPC-EPMAP)    False   Inbound  Allow


PS C:\> _
```

(4) Enter the following command to enable the Windows Firewall rules **WMI-WINMGMT-In-TCP**, **vm-monitoring-rpc**, and **MSDTC-RPCSS-In-TCP**:

```
PS C:\> Set-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" -Enabled True
```

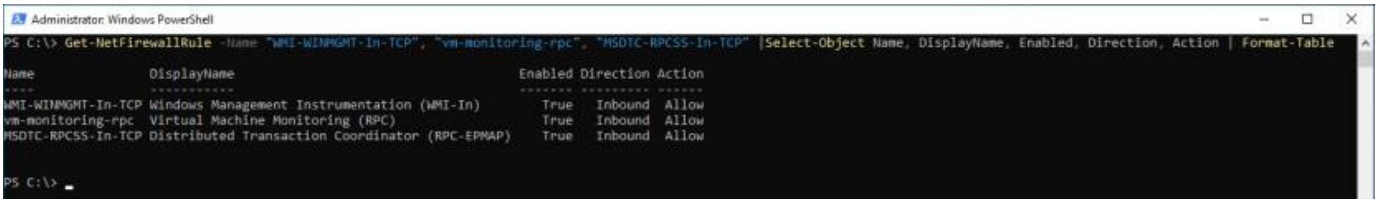


Administrator: Windows PowerShell

```
PS C:\> Set-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" -Enabled True
PS C:\> _
```

(5) Enter the following command to verify the Windows Firewall rules **WMI-WINMGMT-In-TCP, vm-monitoring-rpc, MSDTC-RPCSS-In-TCP** again:

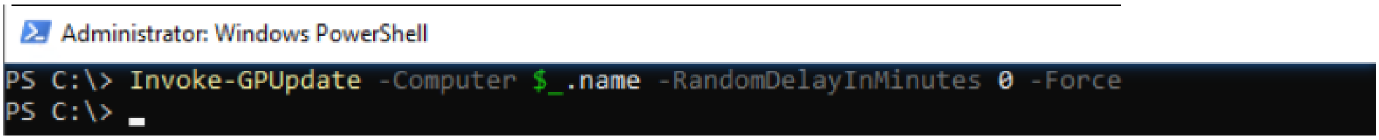
```
PS C:\> Get-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" | Select-Object Name, DisplayName, Enabled, Direction, Action | Format-Table
```



```
PS C:\> Get-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" |Select-Object Name, DisplayName, Enabled, Direction, Action | Format-Table

Name               DisplayName                                   Enabled Direction Action
----               -----------                                   ------- --------- ------
WMI-WINMGMT-In-TCP Windows Management Instrumentation (WMI-In)      True   Inbound  Allow
vm-monitoring-rpc  Virtual Machine Monitoring (RPC)                 True   Inbound  Allow
MSDTC-RPCSS-In-TCP Distributed Transaction Coordinator (RPC-EPMAP)  True   Inbound  Allow


PS C:\> _
```

(6) On the **AD domain server**, enter the following command to update the Windows Server Group Policy:

```
PS C:\> Invoke-GPUpdate -Computer Win2019 -RandomDelayInMinutes 0 -Force
```



```
PS C:\> Invoke-GPUpdate -Computer $_.name -RandomDelayInMinutes 0 -Force
PS C:\> _
```

Note: Replace the text shown in red with the Windows Server name.

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

Sales Information：sales@npartner.com

Technical Support：support@npartner.com