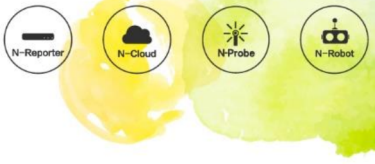
N-Partner

如何設定
Oracle 資料庫審核記錄

V010

2025/03/14



版權聲明

商標

目錄

前言 1

1 Red Hat 2

1.1 Red Hat 6 2

1.1.1 設定 Oracle Audit 2

1.1.2 設定 Rsyslog 4

1.2 Red Hat 7 5

1.2.1 設定 Oracle Audit 5

1.2.2 設定 Rsyslog 7

1.3 Red Hat 8 8

1.3.1 設定 Oracle Audit 8

1.3.2 設定 Rsyslog 10

2 Oracle Linux 11

2.1 Oracle Linux 6 11

2.1.1 設定 Oracle Audit 11

2.1.2 設定 Rsyslog 13

2.2 Oracle Linux 7 14

2.2.1 設定 Oracle Audit 14

2.2.2 設定 Rsyslog 17

2.3 Oracle Linux 8 18

2.3.1 設定 Oracle Audit 18

2.3.2 設定 Rsyslog 20

3 SUSE Linux 21

3.1 設定 Oracle Audit 21

3.2 設定 Rsyslog 23

4 AIX 24

4.1 設定 Oracle Audit 24

4.2 設定 Syslogd 26

5 Windows 27

5.1 NXLog 27

5.1.1 NXLog 安裝 27

5.1.2 NXLog 設定檔下載 30

5.1.3 NXLog 設定檔 31

5.1.4 NXLog 啟動服務 32

5.2 Oracle Database 33

5.2.1 Oracle 12c Audit 設定 33

5.2.2 Oracle 19c Audit 設定 36

6 Oracle RAC 39

6.1 Node 1 39

6.1.1 設定 Oracle Audit 39

6.1.2 設定 Rsyslog 44

6.2 Node 2 45

6.2.1 設定 Oracle Audit 45

6.2.2 設定 Rsyslog 49

7 N-Reporter 50

7.1 Linux/ AIX 52

7.2 Windows 55

8 問題排除 58

前言

本文件描述 N-Reporter 使用者在 Linux/ AIX 如何啟用資料庫審核，並使用 Rsyslog 或 Syslogd 方式設定 Oracle DataBase Audit Logs。

在 Windows 如何使用 Open Source 工具 NXLog 方式設定 Oracle audit 事件紀錄。

NXLog 工具將 Oracle audit 事件紀錄轉成 syslog，再傳送到 N-Reporter 做正規化、稽核與分析。

Oracle Security Guide:https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/introduction-to-auditing.html#GUID-94381464-53A3-421B-8F13-BD171C867405

Oracle Audit Syslog Level:https://docs.oracle.com/en/database/oracle/oracle-database/19/refrn/AUDIT_SYSLOG_LEVEL.html#GUID-EBBAD1D4-A4F8-49A4-9C4E-7CF6A085CB53

註：本文件僅做為如何將日誌吐出的設定參考，建議您仍應聯繫設備或是軟體原廠尋求日誌輸出方式之協助。

1 Red Hat

1.1 Red Hat 6

1.1.1 設定 Oracle Audit

(1) 切換 oracle 帳號

```
# su - oracle
```

(2) 登入 Oracle 資料庫

```
$ sqlplus / as sysdba
```

(3) 顯示審計參數

```
SQL> show parameter audit
```

(4) 顯示資料庫審計

```
SQL> show parameter audit_trail
```

(5) 顯示審計等級

```
SQL> show parameter audit_syslog_level
```

(6) 顯示 sysdba 特權用戶審計

```
SQL> show parameter audit_sys_operations
```

(7) 修改審計記錄到作業系統

```
SQL> alter system set audit_trail='OS' scope=spfile;
```

(8) 啟用 sysdba 特權用戶審計

```
SQL> alter system set audit_sys_operations=true scope=spfile;
```

(9) 修改審計紀錄 facility: local0 info 訊息

```
SQL> alter system set audit_syslog_level=local0.info' scope=spfile;
```

(10) 停止 Oracle 資料庫服務

```
SQL> shutdown immediate
```

(11) 啟動 Oracle 資料庫服務

```
SQL> startup
```

(12) 顯示審計參數

```
SQL> show parameter audit
```

(13) 離開 Oracle 資料庫

```
SQL> exit
```

1.1.2 設定 Rsyslog

(1) 編輯 Rsyslog 設定檔

```
# vi /etc/rsyslog.conf
```

(2) 將 Oracle log 傳送到 N-Reporter

```
# Send Oracle log to N-Reporter
local0.*                                @192.168.3.88
```

紅色文字部位請輸入 N-Reporter 系統 IP address

(3) 重啟 Rsyslog 服務和確認 Rsyslog 服務情形

```
# service rsyslog restart && service rsyslog status
```

1.2 Red Hat 7

1.2.1 設定 Oracle Audit

(1) 切換 oracle 帳號

```
# su - oracle
```

(2) 登入 Oracle 資料庫

```
$ sqlplus / as sysdba
```

(3) 顯示審計參數

```
SQL> show parameter audit
```

(4) 顯示資料庫審計

```
SQL> show parameter audit_trail
```

(5) 顯示審計等級

```
SQL> show parameter audit_syslog_level
```

(6) 顯示 sysdba 特權用戶審計

```
SQL> show parameter audit_sys_operations
```

(7) 修改審計記錄到作業系統

```
SQL> alter system set audit_trail='OS' scope=spfile;
```

(8) 啟用 sysdba 特權用戶審計

```
SQL> alter system set audit_sys_operations=true scope=spfile;
```

(9) 修改審計紀錄 facility: local0 info 訊息

```
SQL> alter system set audit_syslog_level=local0.info' scope=spfile;
```

(10) 停止 Oracle 資料庫服務

```
SQL> shutdown immediate
```

(11) 啟動 Oracle 資料庫服務

```
SQL> startup
```

(12) 顯示審計參數

```
SQL> show parameter audit
```

(13) 離開 Oracle 資料庫

```
SQL> exit
```

1.2.2 設定 Rsyslog

(1) 編輯 Rsyslog 設定檔

```
# vi /etc/rsyslog.conf
```

(2) 將 Oracle log 傳送到 N-Reporter

```
# Send Oracle log to N-Reporter
local0.*                                @192.168.3.88
```

紅色文字部位請輸入 N-Reporter 系統 IP address

(3) 重啟 Rsyslog 服務和確認 Rsyslog 服務情形

```
# systemctl restart rsyslog && systemctl status rsyslog
```

1.3 Red Hat 8

1.3.1 設定 Oracle Audit

(1) 切換 oracle 帳號

```
# su - oracle
```

(2) 登入 Oracle 資料庫

```
$ sqlplus / as sysdba
```

(3) 顯示審計參數

```
SQL> show parameter audit
```

(4) 顯示資料庫審計

```
SQL> show parameter audit_trail
```

(5) 顯示審計等級

```
SQL> show parameter audit_syslog_level
```

(6) 顯示 sysdba 特權用戶審計

```
SQL> show parameter audit_sys_operations
```

(7) 修改審計記錄到作業系統

```
SQL> alter system set audit_trail='OS' scope=spfile;
```

(8) 啟用 sysdba 特權用戶審計

```
SQL> alter system set audit_sys_operations=true scope=spfile;
```

(9) 修改審計紀錄 facility: local0 info 訊息

```
SQL> alter system set audit_syslog_level=local0.info' scope=spfile;
```

(10) 停止 Oracle 資料庫服務

```
SQL> shutdown immediate
```

(11) 啟動 Oracle 資料庫服務

```
SQL> startup
```

(12) 顯示審計參數

```
SQL> show parameter audit
```

(13) 離開 Oracle 資料庫

```
SQL> exit
```

1.3.2 設定 Rsyslog

(1) 編輯 Rsyslog 設定檔

```
# vi /etc/rsyslog.conf
```

(2) 將 Oracle log 傳送到 N-Reporter

```
# Send Oracle log to N-Reporter
local0.*                                @192.168.3.88
```

紅色文字部位請輸入 N-Reporter 系統 IP address

(3) 重啟 Rsyslog 服務和確認 Rsyslog 服務情形

```
# systemctl restart rsyslog && systemctl status rsyslog
```

2 Oracle Linux

2.1 Oracle Linux 6

2.1.1 設定 Oracle Audit

(1) 切換 oracle 帳號

```
# su - oracle
```

(2) 登入 Oracle 資料庫

```
$ sqlplus / as sysdba
```

(3) 顯示審計參數

```
SQL> show parameter audit
```

(4) 顯示資料庫審計

```
SQL> show parameter audit_trail
```

(5) 顯示審計等級

```
SQL> show parameter audit_syslog_level
```

(6) 顯示 sysdba 特權用戶審計

```
SQL> show parameter audit_sys_operations
```

(7) 修改審計記錄到作業系統

```
SQL> alter system set audit_trail='OS' scope=spfile;
```

(8) 啟用 sysdba 特權用戶審計

```
SQL> alter system set audit_sys_operations=true scope=spfile;
```

(9) 修改審計紀錄 facility: local0 info 訊息

```
SQL> alter system set audit_syslog_level=local0.info' scope=spfile;
```

(10) 停止 Oracle 資料庫服務

```
SQL> shutdown immediate
```

(11) 啟動 Oracle 資料庫服務

```
SQL> startup
```

(12) 顯示審計參數

```
SQL> show parameter audit
```

(13) 離開 Oracle 資料庫

```
SQL> exit
```

2.1.2 設定 Rsyslog

(1) 編輯 Rsyslog 設定檔

```
# vi /etc/rsyslog.conf
```

(2) 將 Oracle log 傳送到 N-Reporter

```
# Send Oracle log to N-Reporter
local0.*                                @192.168.3.88
```

紅色文字部位請輸入 N-Reporter 系統 IP address

(3) 重啟 Rsyslog 服務和確認 Rsyslog 服務情形

```
# service rsyslog restart && service rsyslog status
```

2.2 Oracle Linux 7

2.2.1 設定 Oracle Audit

(1) 切換 oracle 帳號

```
# su - oracle
```

(2) 登入 Oracle 資料庫

```
$ sqlplus / as sysdba
```

```
[oracle@oracle ~]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Jun 11 17:25:41 2021
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle.  All rights reserved.


Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0

SQL>
```

(3) 顯示審計參數

```
SQL> show parameter audit
```

```
SQL> show parameter audit

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
audit_file_dest                      string      /opt/oracle/admin/ORCLCDB/adum
                                                 p
audit_sys_operations                 boolean     TRUE
audit_syslog_level                   string
audit_trail                          string      DB
unified_audit_common_systemlog       string
unified_audit_sga_queue_size         integer     1048576
unified_audit_systemlog              string
SQL>
```

(4) 顯示資料庫審計

```
SQL> show parameter audit_trail
```

```
SQL> show parameter audit_trail

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
audit_trail                          string      DB
SQL>
```

(5) 修改審計記錄到作業系統

```
SQL> alter system set audit_trail='OS' scope=spfile;
```

```
SQL> alter system set audit_trail='OS' scope=spfile;

System altered.

SQL>
```

(6) 顯示審計等級

```
SQL> show parameter audit_syslog_level
```

```
SQL> show parameter audit_syslog_level

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
audit_syslog_level                   string
SQL>
```

(7) 修改審計紀錄 **facility: local0 info** 訊息

```
SQL> alter system set audit_syslog_level=local0.info' scope=spfile;
```

```
SQL> alter system set audit_syslog_level='local0.info' scope=spfile;

System altered.

SQL>
```

(8) 顯示 **sysdba** 特權用戶審計

```
SQL> show parameter audit_sys_operations
```

```
SQL> show parameter audit_sys_operations

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
audit_sys_operations                 boolean     TRUE
SQL>
```

(9) 啟用 **sysdba** 特權用戶審計

```
SQL> alter system set audit_sys_operations=true scope=spfile;
```

```
SQL> alter system set audit_sys_operations=true scope=spfile;

System altered.

SQL>
```

(10)　停止 Oracle 資料庫服務

```
SQL> shutdown immediate
```

```
SQL> shutdown immediate
Database closed.
Database dismounted.
ORACLE instance shut down.
SQL>
```

(11)　啟動 Oracle 資料庫服務

```
SQL> startup
```

```
SQL> startup
ORACLE instance started.

Total System Global Area 2.0200E+10 bytes
Fixed Size                  9145232 bytes
Variable Size            2483027968 bytes
Database Buffers         1.7650E+10 bytes
Redo Buffers               57962496 bytes
Database mounted.
Database opened.
SQL>
```

(12)　顯示審計參數

```
SQL> show parameter audit
```

```
SQL> show parameter audit

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
audit_file_dest                      string      /opt/oracle/admin/ORCLCDB/adum
                                                 p
audit_sys_operations                 boolean     TRUE
audit_syslog_level                   string      LOCAL0.INFO
audit_trail                          string      OS
unified_audit_common_systemlog       string
unified_audit_sga_queue_size         integer     1048576
unified_audit_systemlog              string
SQL>
```

(13)　離開 Oracle 資料庫

```
SQL> exit
```

```
SQL> exit
Disconnected from Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0
[oracle@oracle ~]$
```

2.2.2 設定 Rsyslog

(1) 編輯 Rsyslog 設定檔

```
# vi /etc/rsyslog.conf
```

(2) 將 Oracle log 傳送到 N-Reporter

```
# Send Oracle log to N-Reporter
local0.*                                @192.168.3.88
```

紅色文字部位請輸入 N-Reporter 系統 IP address

(3) 重啟 Rsyslog 服務和確認 Rsyslog 服務情形

```
# systemctl restart rsyslog && systemctl status rsyslog
```

2.3 Oracle Linux 8

2.3.1 設定 Oracle Audit

(1) 切換 oracle 帳號

```
# su - oracle
```

(2) 登入 Oracle 資料庫

```
$ sqlplus / as sysdba
```

(3) 顯示審計參數

```
SQL> show parameter audit
```

(4) 顯示資料庫審計

```
SQL> show parameter audit_trail
```

(5) 顯示審計等級

```
SQL> show parameter audit_syslog_level
```

(6) 顯示 sysdba 特權用戶審計

```
SQL> show parameter audit_sys_operations
```

(7) 修改審計記錄到作業系統

```
SQL> alter system set audit_trail='OS' scope=spfile;
```

(8) 啟用 sysdba 特權用戶審計

```
SQL> alter system set audit_sys_operations=true scope=spfile;
```

(9) 修改審計紀錄 facility: local0 info 訊息

```
SQL> alter system set audit_syslog_level=local0.info' scope=spfile;
```

(10) 停止 Oracle 資料庫服務

```
SQL> shutdown immediate
```

(11) 啟動 Oracle 資料庫服務

```
SQL> startup
```

(12) 顯示審計參數

```
SQL> show parameter audit
```

(13) 離開 Oracle 資料庫

```
SQL> exit
```

2.3.2 設定 Rsyslog

(1) 編輯 Rsyslog 設定檔

```
# vi /etc/rsyslog.conf
```

(2) 將 Oracle log 傳送到 N-Reporter

```
# Send Oracle log to N-Reporter
local0.*                                @192.168.3.88
```

紅色文字部位請輸入 N-Reporter 系統 IP address

(3) 重啟 Rsyslog 服務和確認 Rsyslog 服務情形

```
# systemctl restart rsyslog && systemctl status rsyslog
```

3 SUSE Linux

3.1 設定 Oracle Audit

(1) 切換 oracle 帳號

```
# su - oracle
```

(2) 登入 Oracle 資料庫

```
$ sqlplus / as sysdba
```

(3) 顯示審計參數

```
SQL> show parameter audit
```

(4) 顯示資料庫審計

```
SQL> show parameter audit_trail
```

(5) 顯示審計等級

```
SQL> show parameter audit_syslog_level
```

(6) 顯示 sysdba 特權用戶審計

```
SQL> show parameter audit_sys_operations
```

(7) 修改審計記錄到作業系統

```
SQL> alter system set audit_trail='OS' scope=spfile;
```

(8) 啟用 sysdba 特權用戶審計

```
SQL> alter system set audit_sys_operations=true scope=spfile;
```

(9) 修改審計紀錄 facility: local0 info 訊息

```
SQL> alter system set audit_syslog_level=local0.info' scope=spfile;
```

(10) 停止 Oracle 資料庫服務

```
SQL> shutdown immediate
```

(11) 啟動 Oracle 資料庫服務

```
SQL> startup
```

(12) 顯示審計參數

```
SQL> show parameter audit
```

(13) 離開 Oracle 資料庫

```
SQL> exit
```

3.2 設定 Rsyslog

(1) 編輯 Rsyslog 設定檔

```
# vi /etc/rsyslog.conf
```

(2) 將 Oracle log 傳送到 N-Reporter

```
# Send Oracle log to N-Reporter
local0.*                                @ 192.168.3.88
```

紅色文字部位請輸入 N-Reporter 系統 IP address

(3) 重啟 Rsyslog 服務和確認 Rsyslog 服務情形

```
# systemctl restart rsyslog && systemctl status rsyslog
```

4 AIX

4.1 設定 Oracle Audit

(1) 切換 oracle 帳號

```
# su - oracle
```

(2) 登入 Oracle 資料庫

```
$ sqlplus / as sysdba
```

(3) 顯示審計參數

```
SQL> show parameter audit;
```

(4) 顯示資料庫審計

```
SQL> show parameter audit_trail;
```

(5) 顯示審計等級

```
SQL> show parameter audit_syslog_level;
```

(6) 顯示 sysdba 特權用戶審計

```
SQL> show parameter audit_sys_operations;
```

(7) 修改審計記錄到作業系統

```
SQL> alter system set audit_trail='OS' scope=spfile;
```

(8) 啟用 sysdba 特權用戶審計

```
SQL> alter system set audit_sys_operations=true scope=spfile;
```

(9) 修改審計紀錄 facility: local0 info 訊息

```
SQL> alter system set audit_syslog_level=local0.info' scope=spfile;
```

(10) 停止 Oracle 資料庫服務

```
SQL> shutdown immediate;
```

(11) 啟動 Oracle 資料庫服務

```
SQL> startup;
```

(12) 顯示審計參數

```
SQL> show parameter audit;
```

(13) 離開 Oracle 資料庫

```
SQL> exit;
```

4.2 設定 Syslogd

(1) 編輯 syslog 設定檔

```
# vi /etc/rsyslog.conf
```

(2) 將 Oracle log 傳送到 N-Reporter

```
# Send Oracle log to N-Reporter
local0.*                                @ 192.168.3.88
```

紅色文字部位請輸入 N-Reporter 系統 IP address

(3) 停止 syslogd 服務和啟動 syslogd 服務

```
# stopsrc -s syslogd && startsrc -s syslogd
```

(4) 確認 syslogd 服務情形

```
# ps -ef | grep syslogd
```

5 Windows

5.1 NXLog

5.1.1 NXLog 安裝

(1) 下載 NXLog CE(Community Edition

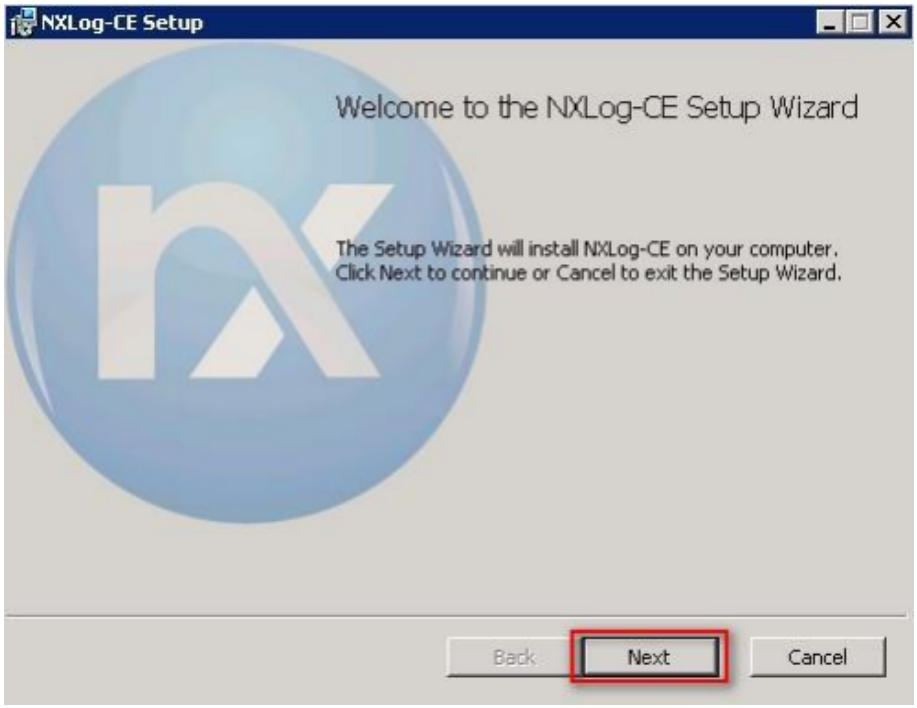
前往網址 https://nxlog.co/products/nxlog-community-edition/download

下載網址最新版 nxlog-ce-x.x.xxxx.msi，範例: nxlog-ce-3.0.2272.msi

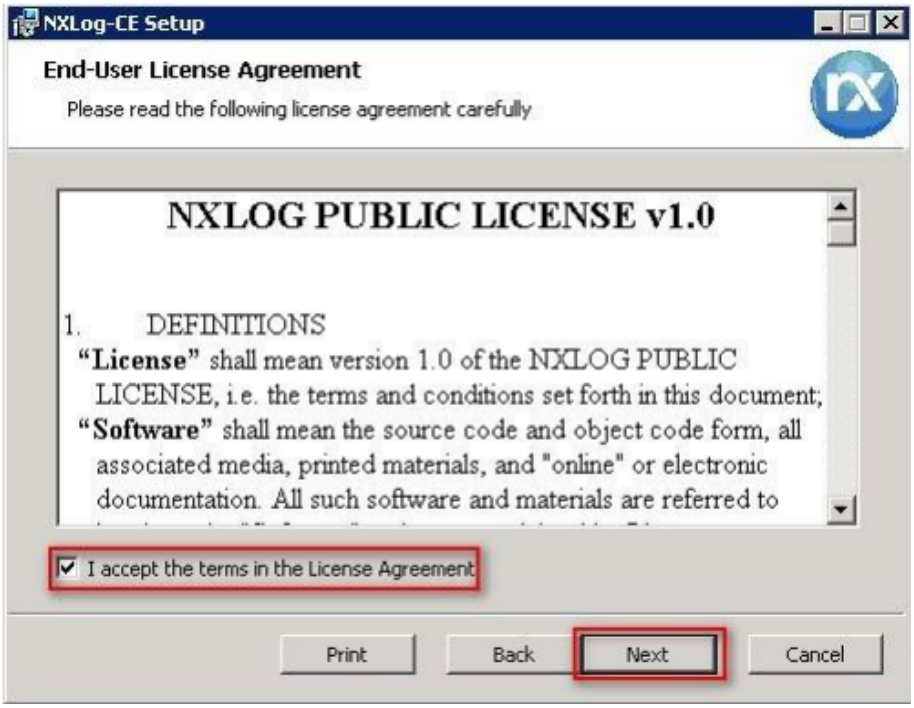
註：若需要下載 NXLog 32bit 版本，請與我們連繫。

(2) 安裝 NXLog

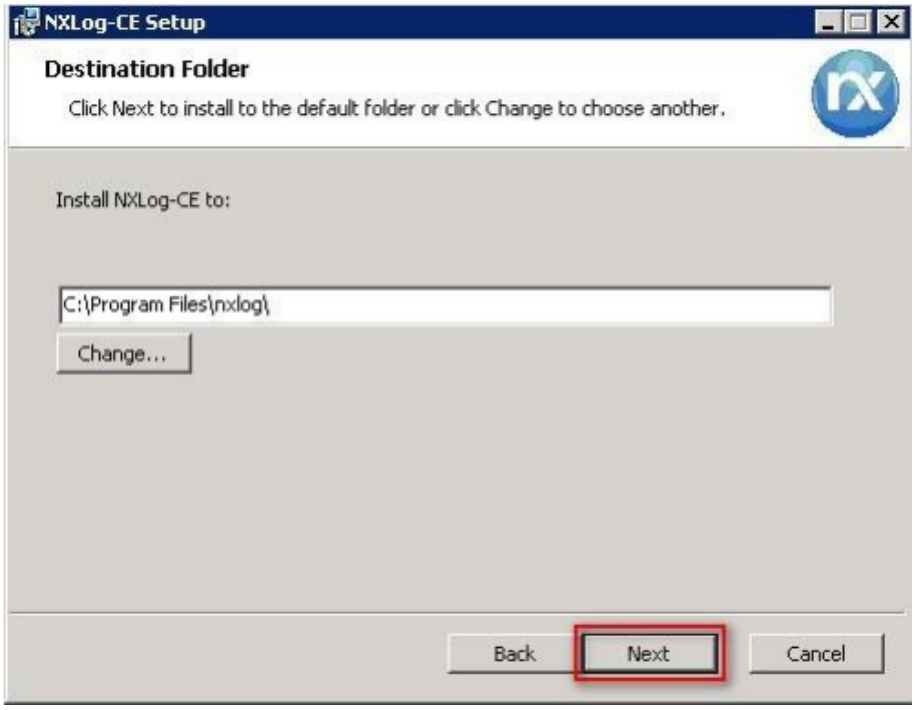
點擊 [nxlog-ce-3.2.2329.msi] -> 按 [Next].



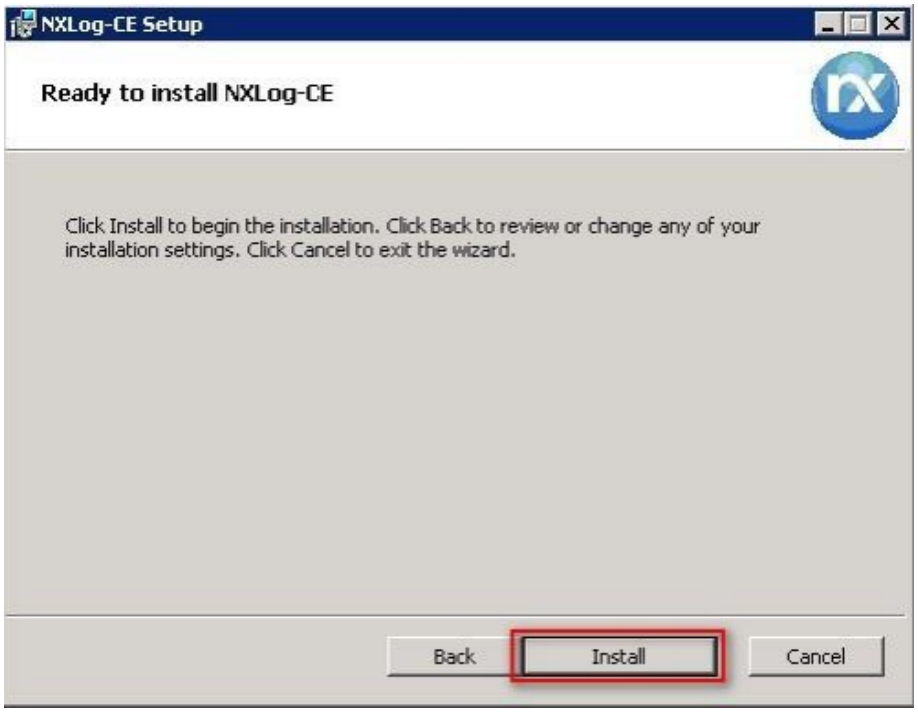
-> 勾選 [I accept the terms in the License Agreement], 按 [Next] .



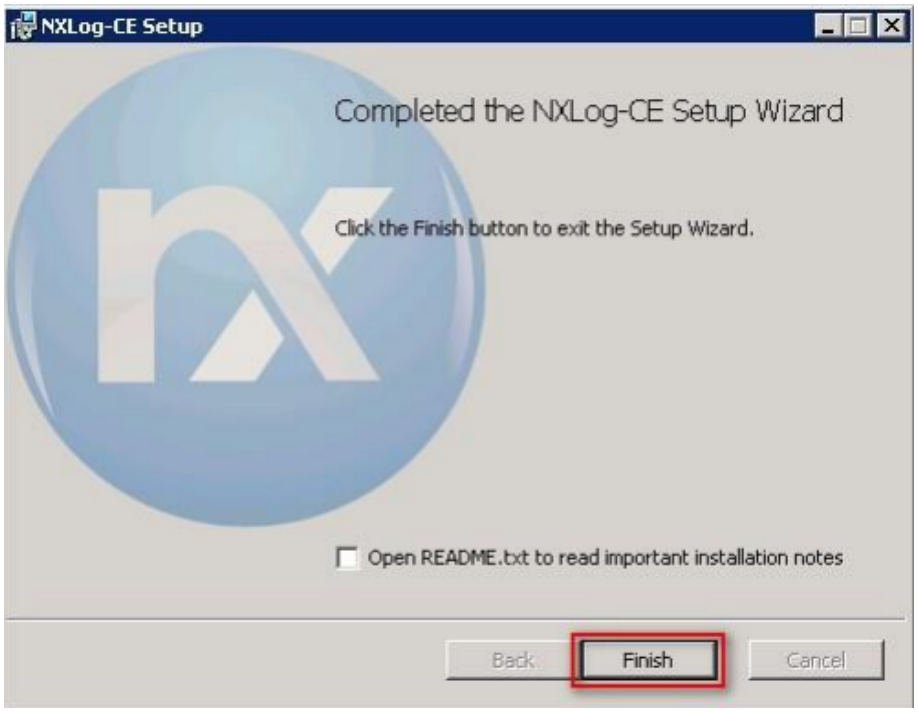
-> 按 [Next]. (預設安裝路徑為 C:\Program Files\nxlog\)



-> 按 [Install].



-> 按 [Finish].



5.1.2 NXLog 設定檔下載

(1) 開啟 [Windows PowerShell]

(2) 下載 nxlog_Oracle.conf 並覆蓋 NXLog 設定檔。

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

本文件範例是 64 位元作業系統，若作業系統是 32 位元，紅色文字部位請改以下設定 'C:\Program Files (x86)\nxlog\conf\nxlog.conf'

5.1.3 NXLog 設定檔

```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud  192.168.3.88
define ROOT  C:\Program Files\nxlog

Moduledir %ROOT%\modules
CacheDir %ROOT%\data
Pidfile %ROOT%\data\nxlog.pid
SpoolDir %ROOT%\data
LogFile %ROOT%\data\nxlog.log

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

## For Oracle event log file use the following:
<Input in_eventlog>
    Module    im_msvistalog
    ReadFromLast    TRUE
    SavePos    TRUE
    Query    <QueryList>\
               <Query Id="0">\
                   <Select Path="Application">*[System[(Provider[@Name='Oracle.orcl'])]]</Select>\
               </Query>\
             </QueryList>
</Input>

<Output out_eventlog>
    Module    om_udp
    Host    %NCloud%
    Port    514
    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>
```

藍色文字部位請輸入 N-Reporter 系統 IP address

```
define NCloud  192.168.3.88
```

本文件範例環境為 64bit 作業系統，若作業系統環境為 32bit 請改為以下設定

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

藍色文字部分請輸入 Oracle 執行個體名稱

```
@Name='Oracle.orcl'
```

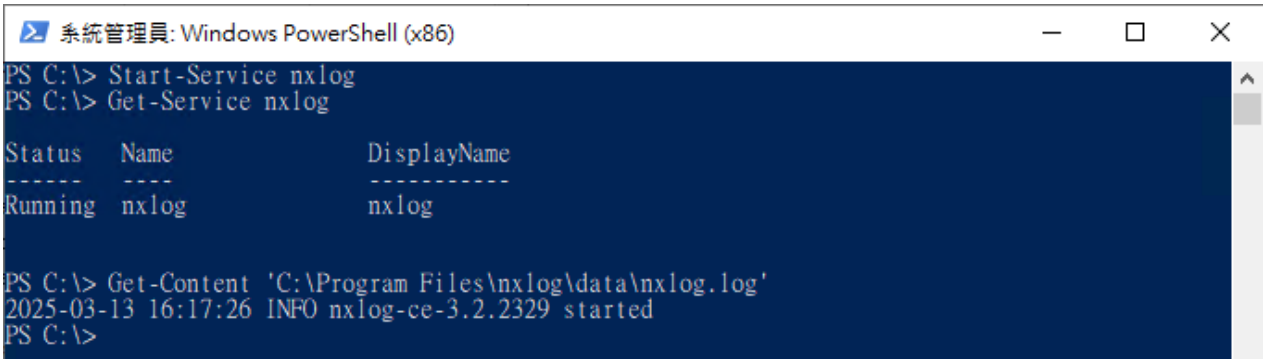
修改設定檔內容後需” 另存新檔” 覆蓋原本檔案，1. 存檔類型請選擇” 所有檔案 (*.*)”，2. 編碼請選擇”UTF-8” 以免編碼錯誤造成服務無法正常開啟。

5.1.4 NXLog 啟動服務

(1) 開啟 [Windows PowerShell]

(2) 重新啟動 NXLog 服務，檢查 NXLog 服務和確認 NXLog 沒有錯誤訊息

```
PS C:\> Start-Service nxlog
PS C:\> Get-Service nxlog
PS C:\> Get-Content 'C:\Program Files\nxlog\data\nxlog.log'
```



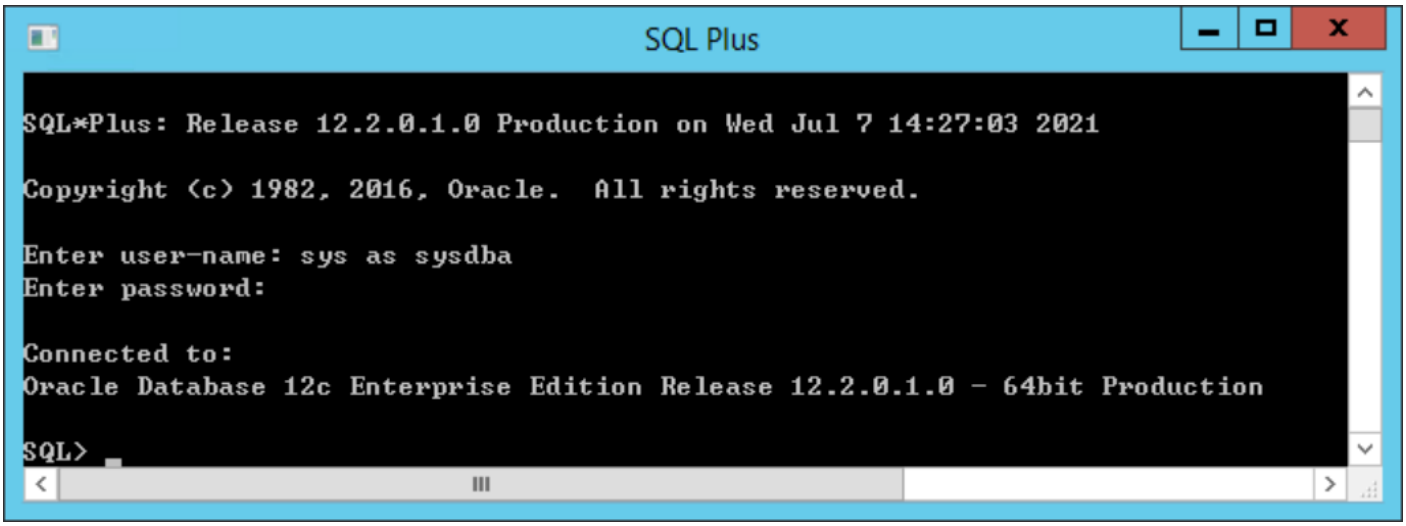
本文件範例是 NXLog 64bit 版本，若是 NXLog 32bit 版本，紅色文字部位請改以下設定 `'C:\Program Files (x86)\nxlog\conf\nxlog.conf'`

5.2 Oracle Database

5.2.1 Oracle 12c Audit 設定

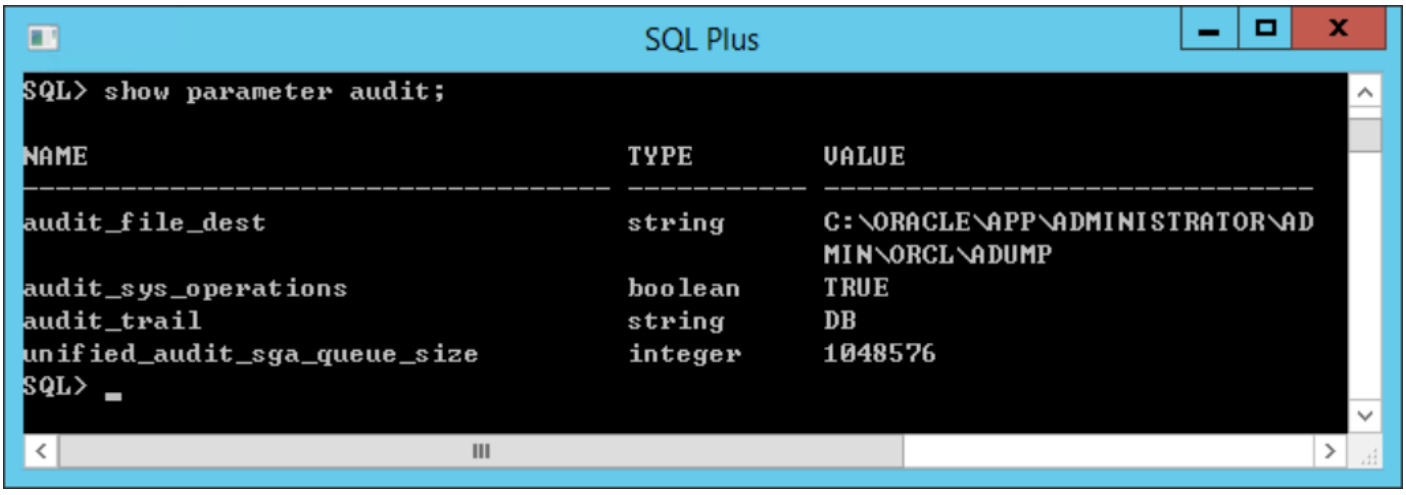
(1) 開啟 [SQL Plus]

(2) 輸入 `user-name:` 和 `password:`



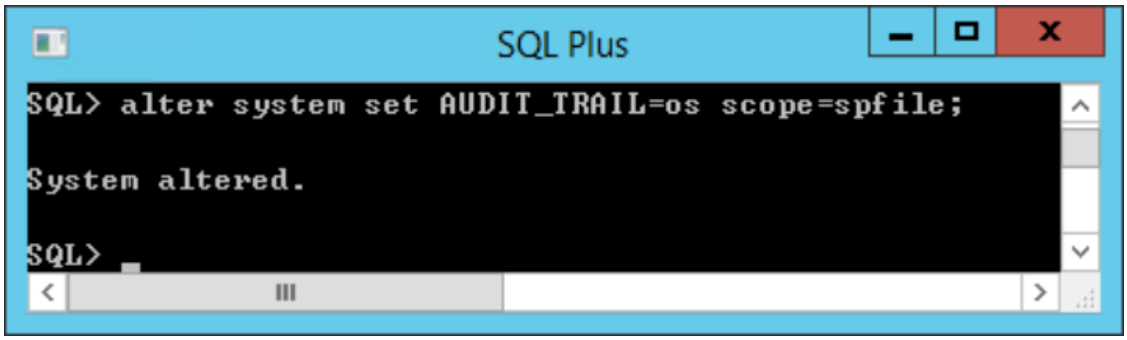
(3) 顯示審計參數

```
SQL> show parameter audit;
```



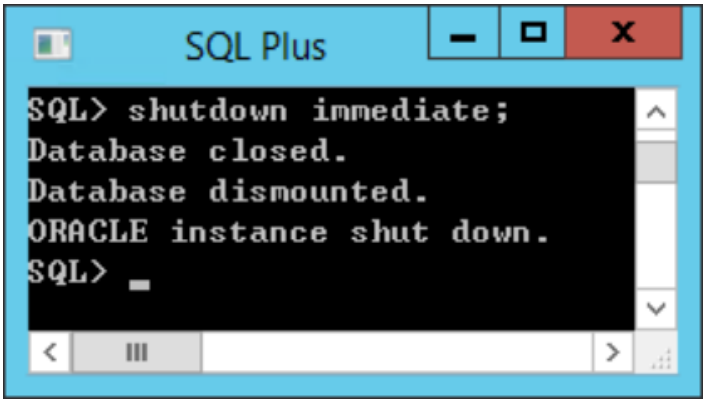
(4)　修改審計紀錄到作業系統

```
SQL>  alter system set AUDIT_TRAIL=os scope=spfile;
```



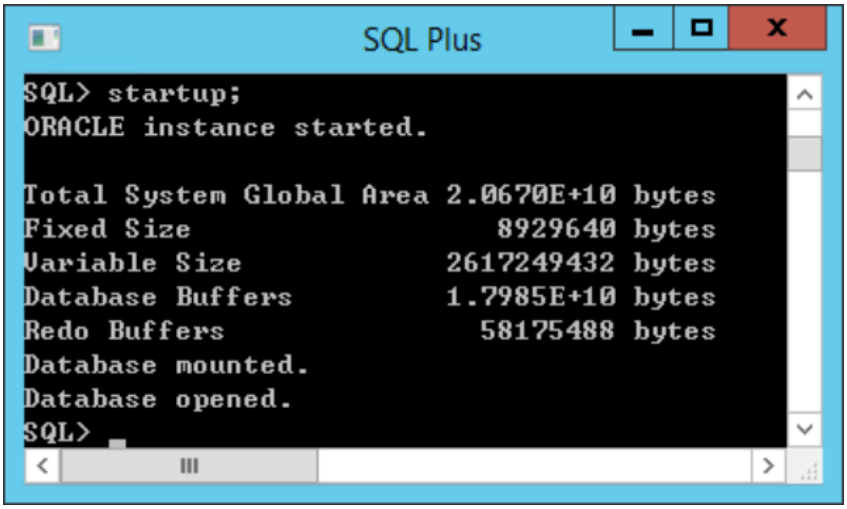
(5)　停止 Oracle 資料庫服務

```
SQL>  shutdown immediate;
```



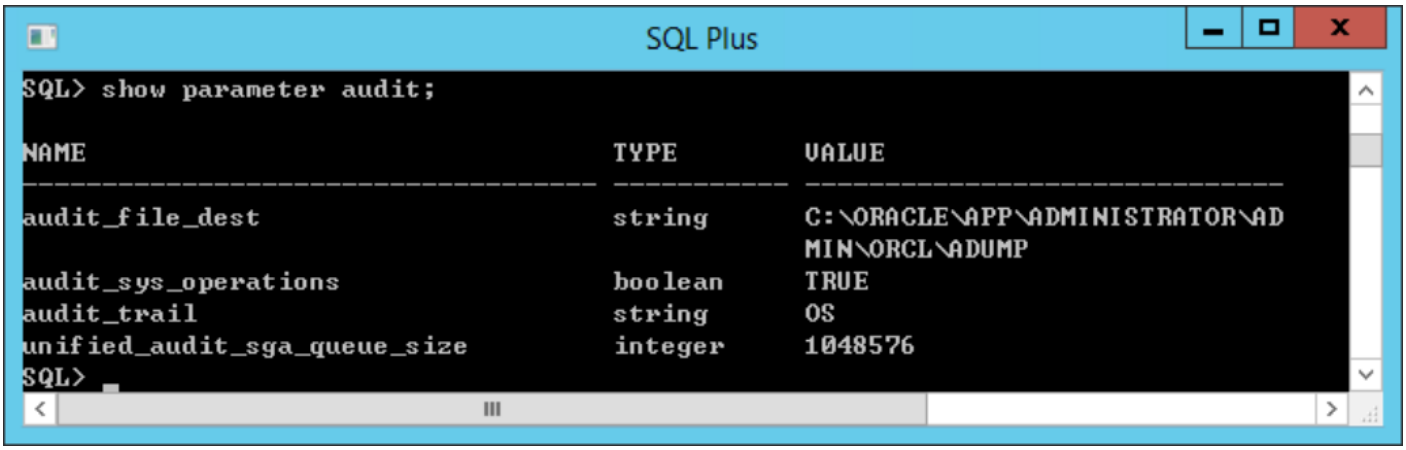
(6)　啟動 Oracle 資料庫服務

```
SQL>  startup;
```



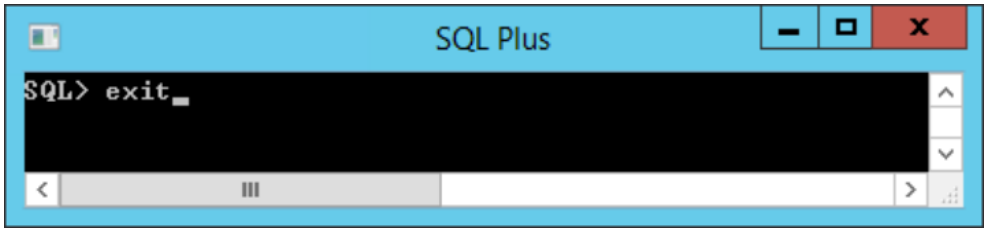
(7) 顯示審計參數

```
SQL>  show parameter audit;
```



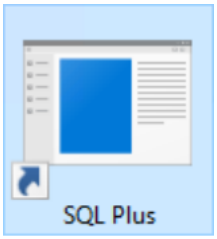
(8) 離開 [SQL Plus]

```
SQL>  exit;
```

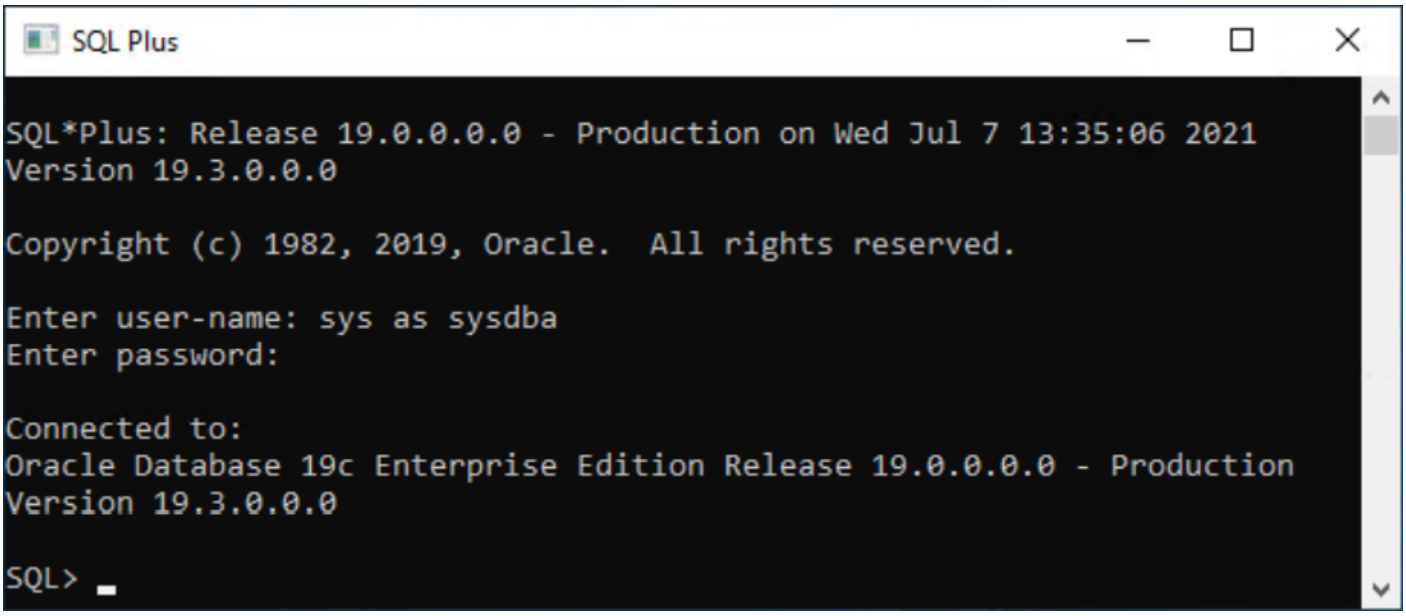


5.2.2 Oracle 19c Audit 設定

(1) 開啟 [SQL Plus]

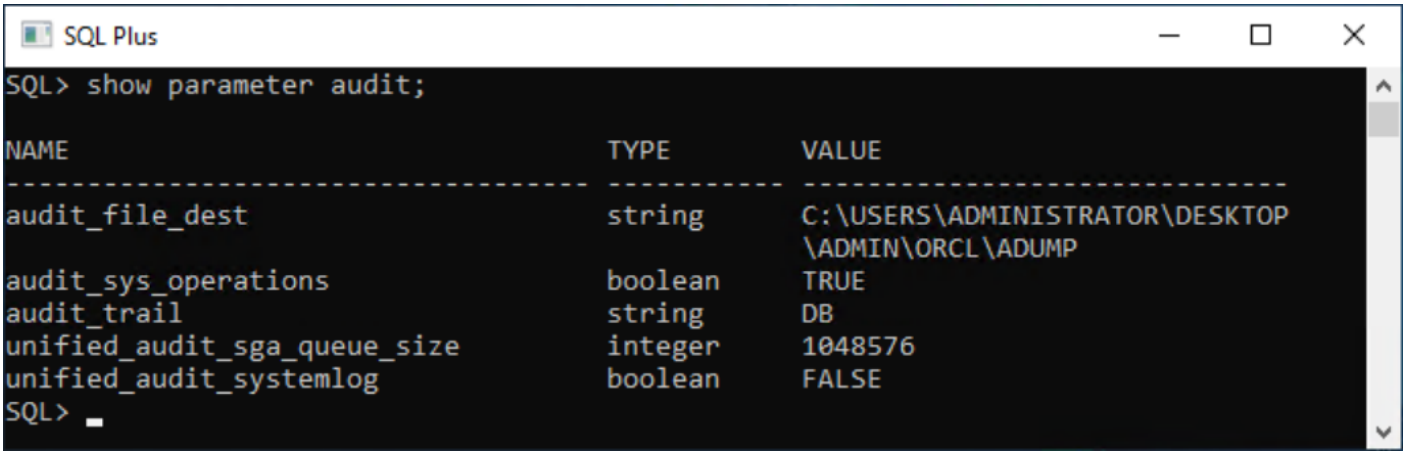


(2) 輸入 `user-name:` 和 `password:`



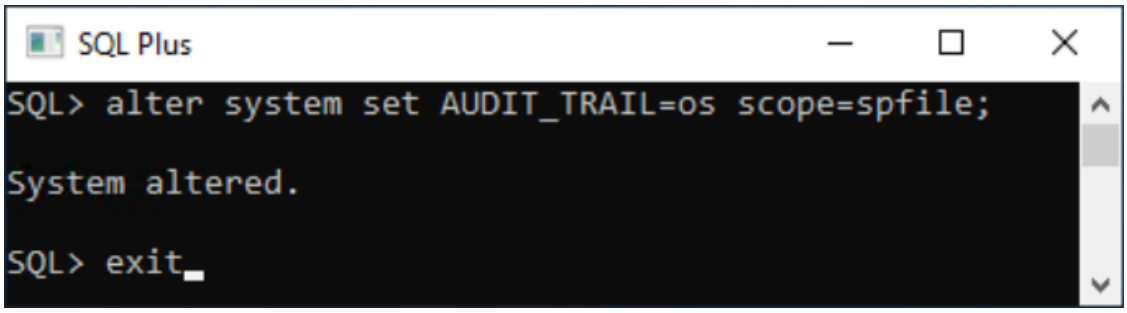
(3) 顯示審計參數

```
SQL> show parameter audit;
```



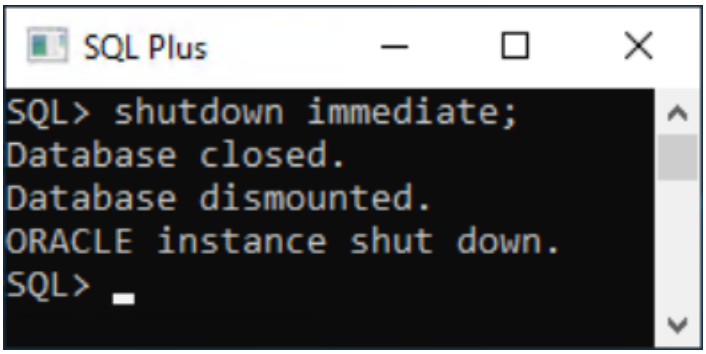
(4)　修改審計紀錄到作業系統

```
SQL>  alter system set AUDIT_TRAIL=os scope=spfile;
```



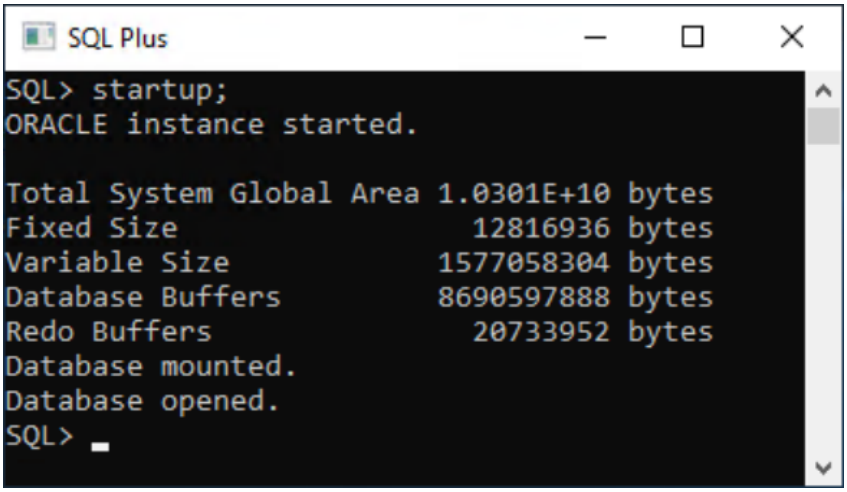
(5)　停止 Oracle 資料庫服務

```
SQL>  shutdown immediate;
```



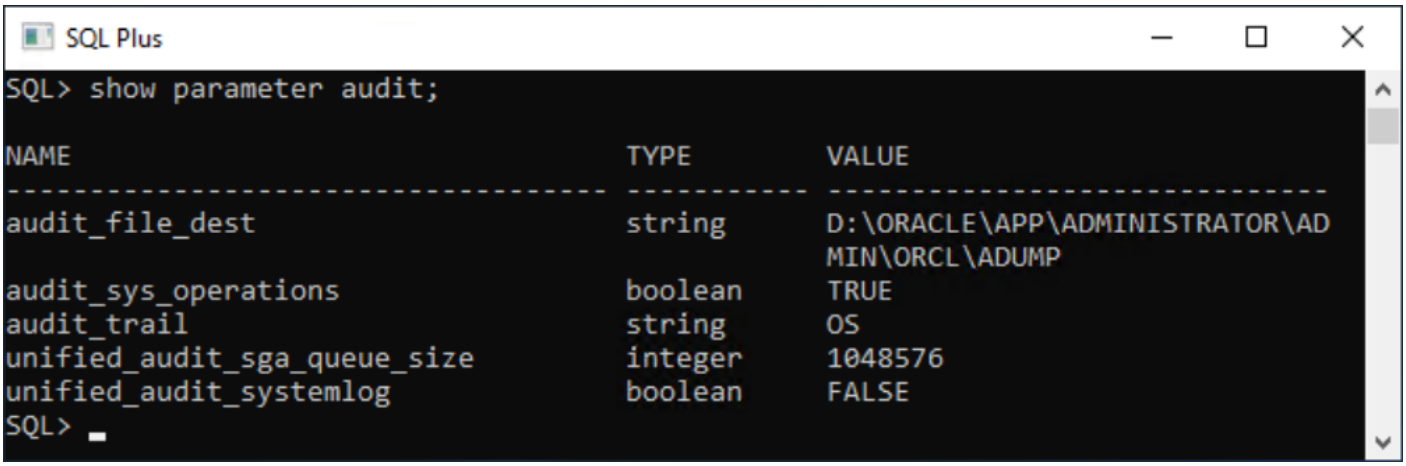
(6)　啟動 Oracle 資料庫服務

```
SQL>  startup;
```



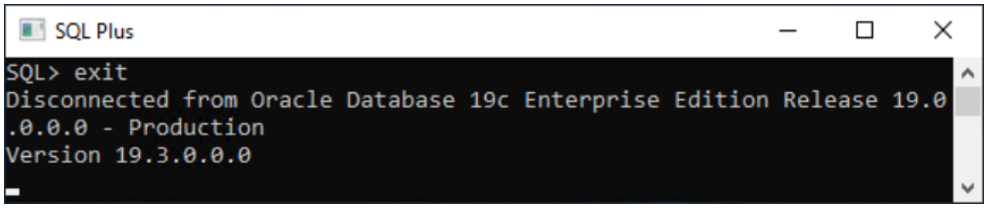
(7) 顯示審計參數

```
SQL>  show parameter audit;
```



(8) 離開 [SQL Plus]

```
SQL>  exit;
```



6 Oracle RAC

作業系統以 Oracle Linux 為範例。

6.1 Node 1

6.1.1 設定 Oracle Audit

(1) 切換 oracle 帳號

```
# su - oracle
```

(2) 登入 Oracle 資料庫

```
$ sqlplus / as sysdba
```

```
[oracle@oracle-rac1 ~]$ sqlplus / as sysdba

SQL*Plus: Release 12.2.0.1.0 Production on Wed Jul 7 10:43:39 2021

Copyright (c) 1982, 2016, Oracle.  All rights reserved.


Connected to:
Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 - 64bit Production

SQL>
```

(3) 查看當前資料庫的執行個體名稱

```
SQL>  SELECT inst_name FROM v$active_instances;
```

```
SQL> SELECT inst_name FROM v$active_instances;

INST_NAME
--------------------------------------------------------------------------------
oracle-rac1.localdomain:cdbrac1
oracle-rac2.localdomain:cdbrac2

SQL>
```

(4) 查看 Oracle SID

```
SQL>  select instance_name from V$instance;
```

```
SQL> select instance_name from V$instance;

INSTANCE_NAME
----------------
cdbrac1

SQL>
```

(5) 查看 Oracle spfile

```
SQL>  show parameter spfile;
```

```
SQL> show parameter spfile;

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
spfile                               string      +DATA/CDBRAC/PARAMETERFILE/spf
                                                 ile.309.1077273243
SQL>
```

(6) 顯示審計參數

```
SQL>  show parameter audit;
```

```
SQL> show parameter audit;

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
audit_file_dest                      string      /u01/app/oracle/admin/cdbrac/a
                                                 dump
audit_sys_operations                 boolean     TRUE
audit_syslog_level                   string
audit_trail                          string      DB
unified_audit_sga_queue_size         integer     1048576
SQL>
```

(7)　顯示資料庫審計

```
SQL>   show parameter audit_trail;
```

```
SQL> show parameter audit_trail;

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
audit_trail                          string      DB
SQL>
```

(8)　修改審計記錄到作業系統

```
SQL>   alter system set audit_trail='OS' scope=spfile;
```

```
SQL> alter system set audit_trail='OS' scope=spfile;

System altered.

SQL>
```

(9)　顯示審計等級

```
SQL>   show parameter audit_syslog_level;
```

```
SQL> show parameter audit_syslog_level;

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
audit_syslog_level                   string
SQL>
```

(10)　修改審計記錄 facility: local0 info 訊息

```
SQL>   alter system set audit_syslog_level='local0.info' scope=spfile;
```

```
SQL> alter system set audit_syslog_level='local0.info' scope=spfile;

System altered.

SQL>
```

(11)　顯示 sysdba 特權用戶審計

```
SQL>   show parameter audit_sys_operations;
```

```
SQL> show parameter audit_sys_operations;

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
audit_sys_operations                 boolean     TRUE
SQL>
```

(12)　啟用 sysdba 特權用戶審計

```
SQL>   alter system set audit_syslog_operations=true scope=spfile;
```

```
SQL> alter system set audit_sys_operations=true scope=spfile;

System altered.

SQL>
```

(13)　停止 Oracle 資料庫服務

```
SQL>   shutdown immediate;
```

```
SQL> shutdown immediate;
Database closed.
Database dismounted.
ORACLE instance shut down.
SQL>
```

(14)　啟動 Oracle 資料庫服務

```
SQL>   startup;
```

```
SQL> startup;
ORACLE instance started.

Total System Global Area 3707764736 bytes
Fixed Size                  8799320 bytes
Variable Size             905972648 bytes
Database Buffers         2785017856 bytes
Redo Buffers                7974912 bytes
Database mounted.
Database opened.
SQL>
```

(15) 顯示審計參數

```
SQL>   show parameter audit;
```

```
SQL> show parameter audit;

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
audit_file_dest                      string      /u01/app/oracle/admin/cdbrac/a
                                                 dump
audit_sys_operations                 boolean     TRUE
audit_syslog_level                   string      LOCAL0.INFO
audit_trail                          string      OS
unified_audit_sga_queue_size         integer     1048576
SQL>
```

(16) 離開 Oracle 資料庫

```
SQL>   exit;
```

```
SQL> exit;
Disconnected from Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 - 64bit Production
[oracle@oracle-rac1 ~]$
```

6.1.2 設定 Rsyslog

(1) 編輯 Rsyslog 設定檔

```
# vi /etc/rsyslog.conf
```

(2) 將 Oracle log 傳送到 N-Reporter

```
# Send Oracle log to N-Reporter
local0.*                                @192.168.3.88
```

紅色文字部位請輸入 N-Reporter 系統 IP address

(3) 重啟 Rsyslog 服務和確認 Rsyslog 服務情形

```
# systemctl restart rsyslog && systemctl status rsyslog
```

6.2 Node 2

6.2.1 設定 Oracle Audit

(1) 切換 oracle 帳號

```
# su - oracle
```

(2) 登入 Oracle 資料庫

```
$  sqlplus / as sysdba
```

```
[oracle@oracle-rac2 ~]$ sqlplus / as sysdba

SQL*Plus: Release 12.2.0.1.0 Production on Wed Jul 7 11:01:05 2021

Copyright (c) 1982, 2016, Oracle.  All rights reserved.


Connected to:
Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 - 64bit Production

SQL>
```

(3) 查看當前資料庫的執行個體名稱

```
SQL>  SELECT inst_name FROM v$active_instances;
```

```
SQL> SELECT inst_name FROM v$active_instances;

INST_NAME
------------------------------------------------------------------------------
oracle-rac1.localdomain:cdbrac1
oracle-rac2.localdomain:cdbrac2

SQL>
```

(4) 查看 Oracle SID

```
SQL>  select instance_name from V$instance;
```

```
SQL> select instance_name from V$instance;

INSTANCE_NAME
----------------
cdbrac2

SQL>
```

(5) 查看 Oracle spfile

```
SQL>  show parameter spfile;
```

```
SQL> show parameter spfile;

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
spfile                               string      +DATA/CDBRAC/PARAMETERFILE/spf
                                                 ile.309.1077273243

SQL>
```

(6) 顯示審計參數

```
SQL>  show parameter audit;
```

```
SQL> show parameter audit;

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
audit_file_dest                      string      /u01/app/oracle/admin/cdbrac/a
                                                 dump
audit_sys_operations                 boolean     TRUE
audit_syslog_level                   string
audit_trail                          string      DB
unified_audit_sga_queue_size         integer     1048576
SQL>
```

(7) 顯示資料庫審計

```
SQL>  show parameter audit_trail;
```

```
SQL> show parameter audit_trail;

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
audit_trail                          string      DB
SQL>
```

(8) 修改審計記錄到作業系統

```
SQL>  alter system set audit_trail='OS' scope=spfile;
```

```
SQL> alter system set audit_trail='OS' scope=spfile;

System altered.

SQL>
```

(9)　顯示審計等級

```
SQL>   show parameter audit_syslog_level;
```

```
SQL> show parameter audit_syslog_level;

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
audit_syslog_level                   string
SQL>
```

(10)　修改審計記錄 facility: local0 info 訊息

```
SQL>   alter system set audit_syslog_level='local0.info' scope=spfile;
```

```
SQL> alter system set audit_syslog_level='local0.info' scope=spfile;

System altered.

SQL>
```

(11)　顯示 sysdba 特權用戶審計

```
SQL>   show parameter audit_sys_operations;
```

```
SQL> show parameter audit_sys_operations;

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
audit_sys_operations                 boolean     TRUE
SQL>
```

(12)　啟用 sysdba 特權用戶審計

```
SQL>   alter system set audit_sys_operations=true scope=spfile;
```

```
SQL> alter system set audit_sys_operations=true scope=spfile;

System altered.

SQL>
```

(13)　停止 Oracle 資料庫服務

```
SQL>   shutdown immediate;
```

```
SQL> shutdown immediate;
Database closed.
Database dismounted.
ORACLE instance shut down.
SQL>
```

(14)　啟動 Oracle 資料庫服務

```
SQL>   startup;
```

```
SQL> startup;
ORACLE instance started.

Total System Global Area 3707764736 bytes
Fixed Size                  8799320 bytes
Variable Size             905972648 bytes
Database Buffers         2785017856 bytes
Redo Buffers                7974912 bytes
Database mounted.
Database opened.
SQL>
```

(15)　顯示審計參數

```
SQL>   show parameter audit;
```

```
SQL> show parameter audit;

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
audit_file_dest                      string      /u01/app/oracle/admin/cdbrac/a
                                                 dump
audit_sys_operations                 boolean     TRUE
audit_syslog_level                   string      LOCAL0.INFO
audit_trail                          string      OS
unified_audit_sga_queue_size         integer     1048576
SQL>
```

(16)　離開 Oracle 資料庫

```
SQL>   exit;
```

```
SQL> exit;
Disconnected from Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 - 64bit Production
[oracle@oracle-rac2 ~]$
```

6.2.2 設定 Rsyslog

(1) 編輯 Rsyslog 設定檔

```
# vi /etc/rsyslog.conf
```

(2) 將 Oracle log 傳送到 N-Reporter

```
# Send Oracle log to N-Reporter
local0.*                                @192.168.3.88
```

紅色文字部位請輸入 N-Reporter 系統 IP address

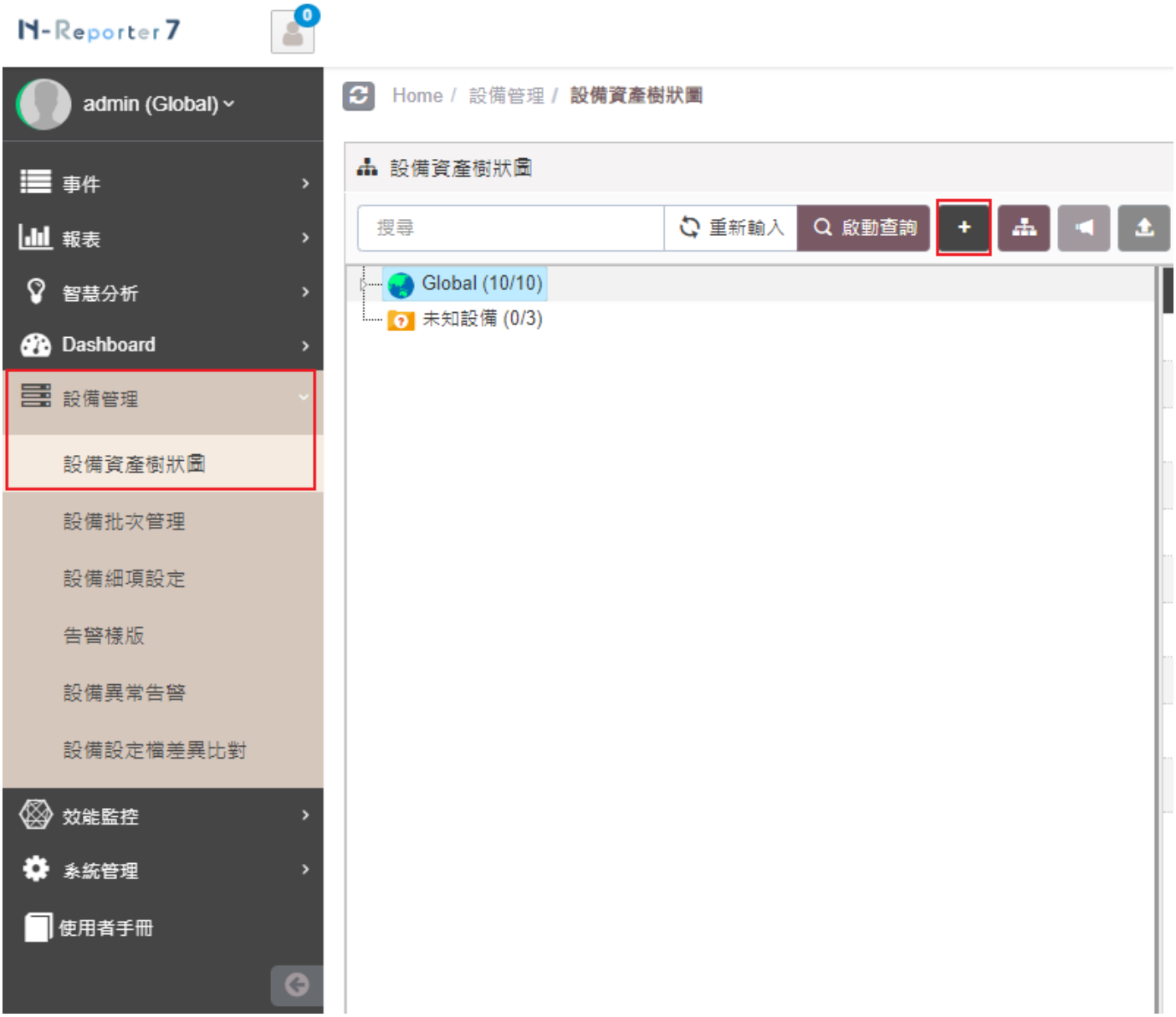
(3) 重啟 Rsyslog 服務和確認 Rsyslog 服務情形

```
# systemctl restart rsyslog && systemctl status rsyslog
```

7 N-Reporter

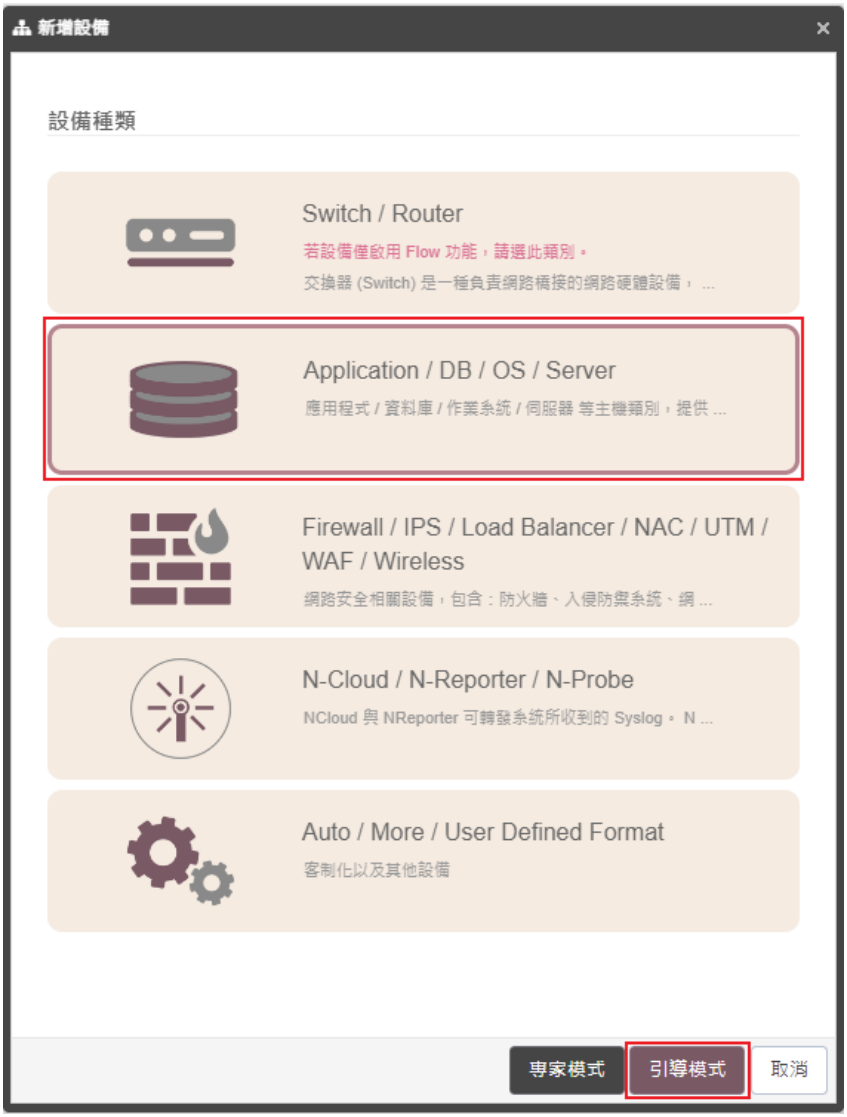
(1) 新增 Oracle Database 設備

[設備管理] -> [設備樹狀圖] -> 點選 [新增]



(2) 選擇設備種類

選擇 [Application/DB/OS/Server]-> 點選 [引導模式]



7.1 Linux/ AIX

(1) 設備基本設定

輸入設備名稱和IP->Syslog 資料格式選擇 [Oracle]-> 點選 [下一步]

(2) Syslog 相關設定

Facility 選擇 [(22) local use 6 (local6)]-> 點選 [下一步]

(若勾選 [Raw Data 保留]，則 [事件查詢] 顯示 Raw Data 資訊)

(3) 其他

設備 Icon 選擇 [Host]-> 接收狀態選擇 [啟用]-> 點選 [下一步]->[確認]

7.2 Windows

(1) 設備基本設定

輸入設備名稱和IP->Syslog 資料格式選擇 [Windows]-> 點選 [下一步]

(2) Syslog 相關設定

Facility 保持預設-> 點選 [下一步]

(若勾選 [Raw Data 保留]，則 [事件查詢] 顯示 Raw Data 資訊)

(3) 其他

設備 Icon 選擇 [Host]-> 接收狀態選擇 [啟用]-> 點選 [下一步]->[確認]

8 問題排除

(1) 查看 Oracle SID

```
SQL>  select instance_name from V$instance;
```

```
SQL> select instance_name from V$instance;

INSTANCE_NAME
----------------
ORCLCDB

SQL>
```

(2) 查看 Oracle DB 系統以 pfile 還是 spfile 啟動

```
SQL>  SELECT DECODE(value, NULL, 'PFILE', 'SPFILE') "Init File Type" FROM sys.v_$parameter
WHERE name ='spfile';
```

```
SQL> SELECT DECODE(value, NULL, 'PFILE', 'SPFILE') "Init File Type" FROM sys.v_$parameter WHERE name = 'spfile';

Init F
------
SPFILE

SQL>
```

(3) 查看 Oracle spfile

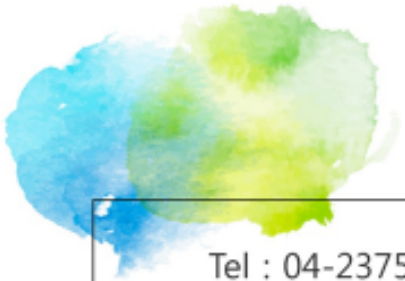
```
SQL>  show parameter spfile;
```

```
SQL> show parameter spfile;

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
spfile                               string      /opt/oracle/product/19c/dbhome
                                                 _1/dbs/spfileORCLCDB.ora
SQL>
```

(4) 查看 Oracle pfile

```
SQL>  show parameter pfile;
```

```
SQL> show parameter pfile;

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
spfile                               string      /opt/oracle/product/19c/dbhome
                                                 _1/dbs/spfileORCLCDB.ora
SQL>
```



Tel：04-23752865　Fax：04-23757458
業務詢問：sales@npartner.com
技術詢問：support@npartner.com