

Partner

如何設定

Oracle 資料庫審核記錄

V009

2021/07/07



版權聲明

N-Partner Technologies Co.版權所有。未經 N-Partner Technologies Co.書面許可，不得以任何形式仿製、拷貝、謄抄或轉譯本手冊的任何內容。由於產品一直在更新中， N-Partner Technologies Co. 保留不告知變動的權利。

商標

本手冊內所提到的任何的公司產品、名稱及註冊商標，均屬其合法註冊公司所有。

目錄

前言	2	7.1 Linux / AIX	49
1. Red Hat	3	7.2 Windows	50
1.1 Red Hat 6	3	8. 問題排除.....	51
1.1.1 設定 Oracle Audit	3		
1.1.2 設定 Rsyslog	5		
1.2 Red Hat 7	6		
1.2.1 設定 Oracle Audit	6		
1.2.2 設定 Rsyslog	8		
1.3 Red Hat 8	9		
1.3.1 設定 Oracle Audit	9		
1.3.2 設定 Rsyslog	11		
2. Oracle Linux	12		
2.1 Oracle Linux 6	12		
2.1.1 設定 Oracle Audit	12		
2.1.2 設定 Rsyslog	14		
2.2 Oracle Linux 7	15		
2.2.1 設定 Oracle Audit	15		
2.2.2 設定 Rsyslog	18		
2.3 Oracle Linux 8	19		
2.3.1 設定 Oracle Audit	19		
2.3.2 設定 Rsyslog	21		
3. SUSE Linux.....	22		
3.1 設定 Oracle Audit.....	22		
3.2 設定 Rsyslog	24		
4. AIX.....	25		
4.1 設定 Oracle Audit.....	25		
4.2 設定 Syslog	27		
5. Windows	28		
5.1 NXLog	28		
5.1.1 NXLog 安裝	28		
5.1.2 NXLog 設定檔下載	29		
5.1.3 NXLog 設定檔	30		
5.1.4 NXLog 啟動服務.....	31		
5.2 Oracle Database.....	32		
5.2.1 Oracle 12c Audit 設定.....	32		
5.2.2 Oracle 19c Audit 設定.....	35		
6. Oracle RAC	38		
6.1 Node 1	38		
6.1.1 設定 Oracle Audit	38		
6.1.2 設定 Rsyslog	42		
6.2 Node 2	43		
6.2.1 設定 Oracle Audit	43		
6.2.2 設定 Rsyslog	47		
7. N-Reporter	48		

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 事件記錄。

NXLog 工具將 Oracle audit 事件記錄轉成 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
```

(6) 顯示審計等級

```
SQL> show parameter audit_syslog_level
```

(7) 顯示 sysdba 特權用戶審計

```
SQL> show parameter audit_sys_operations
```

(8) 修改審計記錄到作業系統

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

(9) 啟用 sysdba 特權用戶審計

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

(10) 修改審計記錄 facility: local0 info 訊息

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

(11) 停止 Oracle 資料庫服務

```
SQL> shutdown immediate
```

(12) 啟動 Oracle 資料庫服務

```
SQL> startup
```

(13) 顯示審計參數

```
SQL> show parameter audit
```

(14) 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.* @192.168.8.184
```

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
```

(6) 顯示審計等級

```
SQL> show parameter audit_syslog_level
```

(7) 顯示 sysdba 特權用戶審計

```
SQL> show parameter audit_sys_operations
```

(8) 修改審計記錄到作業系統

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

(9) 啟用 sysdba 特權用戶審計

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

(10) 修改審計記錄 facility: local0 info 訊息

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

(11) 停止 Oracle 資料庫服務

```
SQL> shutdown immediate
```


(12) 啟動 Oracle 資料庫服務

```
SQL> startup
```

(13) 顯示審計參數

```
SQL> show parameter audit
```

(14) 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.*
```

```
@ 192.168.8.184
```

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
```

(6) 顯示審計等級

```
SQL> show parameter audit_syslog_level
```

(7) 顯示 sysdba 特權用戶審計

```
SQL> show parameter audit_sys_operations
```

(8) 修改審計記錄到作業系統

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

(9) 啟用 sysdba 特權用戶審計

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

(10) 修改審計記錄 facility: local0 info 訊息

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

(11) 停止 Oracle 資料庫服務

```
SQL> shutdown immediate
```

(12) 啟動 Oracle 資料庫服務

```
SQL> startup
```

(13) 顯示審計參數

```
SQL> show parameter audit
```

(14) 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.*
```

```
@192.168.8.184
```

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
```

(6) 顯示審計等級

```
SQL> show parameter audit_syslog_level
```

(7) 顯示 sysdba 特權用戶審計

```
SQL> show parameter audit_sys_operations
```

(8) 修改審計記錄到作業系統

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

(9) 啟用 sysdba 特權用戶審計

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

(10) 修改審計記錄 facility: local0 info 訊息

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

(11) 停止 Oracle 資料庫服務

```
SQL> shutdown immediate
```

(12) 啟動 Oracle 資料庫服務

```
SQL> startup
```

(13) 顯示審計參數

```
SQL> show parameter audit
```

(14) 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.*
```

```
@192.168.8.184
```

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/adump
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>
```

(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/adump
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.* @192.168.8.184
```

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
```

(6) 顯示審計等級

```
SQL> show parameter audit_syslog_level
```

(7) 顯示 sysdba 特權用戶審計

```
SQL> show parameter audit_sys_operations
```

(8) 修改審計記錄到作業系統

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

(9) 啟用 sysdba 特權用戶審計

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

(10) 修改審計記錄 facility: local0 info 訊息

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

(11) 停止 Oracle 資料庫服務

```
SQL> shutdown immediate
```

(12) 啟動 Oracle 資料庫服務

```
SQL> startup
```

(13) 顯示審計參數

```
SQL> show parameter audit
```

(14) 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.* @192.168.8.184
```

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
```

(6) 顯示審計等級

```
SQL> show parameter audit_syslog_level
```

(7) 顯示 sysdba 特權用戶審計

```
SQL> show parameter audit_sys_operations
```

(8) 修改審計記錄到作業系統

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

(9) 啟用 sysdba 特權用戶審計

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

(10) 修改審計記錄 facility: local0 info 訊息

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

(11) 停止 Oracle 資料庫服務

```
SQL> shutdown immediate
```

(12) 啟動 Oracle 資料庫服務

```
SQL> startup
```


(13) 顯示審計參數

```
SQL> show parameter audit
```

(14) 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.* @192.168.8.184
```

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;
```

(6) 顯示審計等級

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

(7) 顯示 sysdba 特權用戶審計

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

(8) 修改審計記錄到作業系統

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

(9) 啟用 sysdba 特權用戶審計

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

(10) 修改審計記錄 facility: local0 info 訊息

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

(11) 停止 Oracle 資料庫服務

```
SQL> shutdown immediate;
```

(12) 啟動 Oracle 資料庫服務

```
SQL> startup;
```

(13) 顯示審計參數

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

(14) 離開 Oracle 資料庫

```
SQL> exit;
```

4.2 設定 Syslogd

(1) 編輯 syslog 設定檔

```
# vi /etc/syslog.conf
```

(2) 將 Oracle log 轉發到 N-Reporter

```
# Send Oracle log to N-Reporter
```

```
local0.* @192.168.8.184
```

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

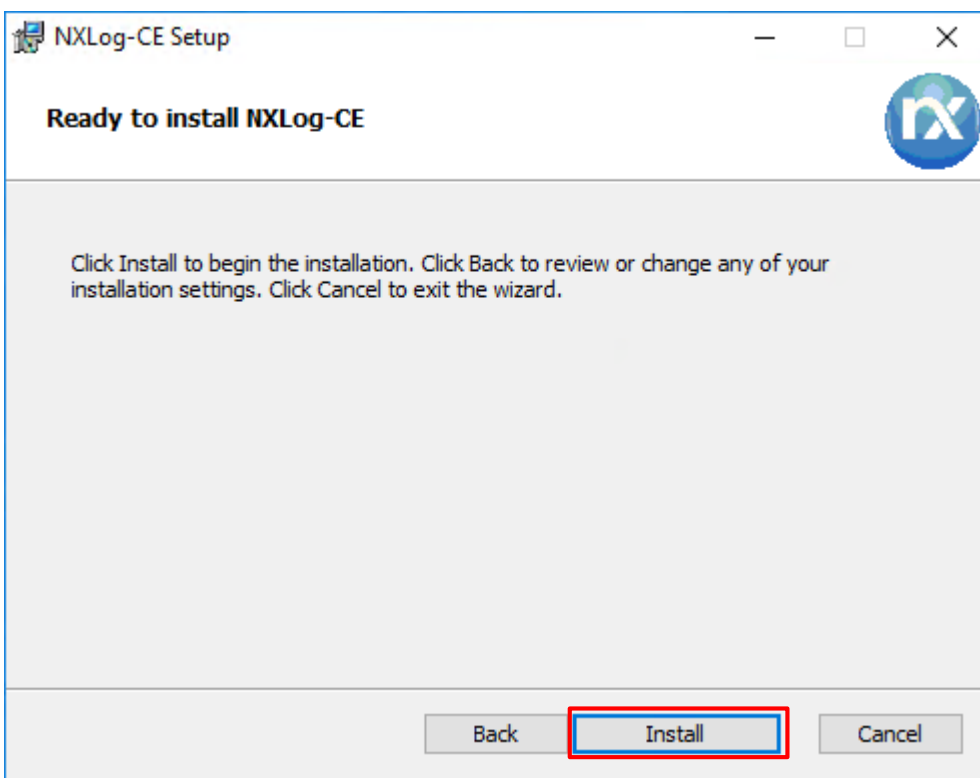
前往網址 <https://nxlog.co/products/nxlog-community-edition/download>

下載網址最新版 nxlog-ce-x.x.xxxx.msi · 範例: nxlog-ce-2.10.2150.msi



(2) 安裝 NXLog

點擊 [nxlog-ce-2.10.2150.msi] -> 按 [Install] 到 [Finish]



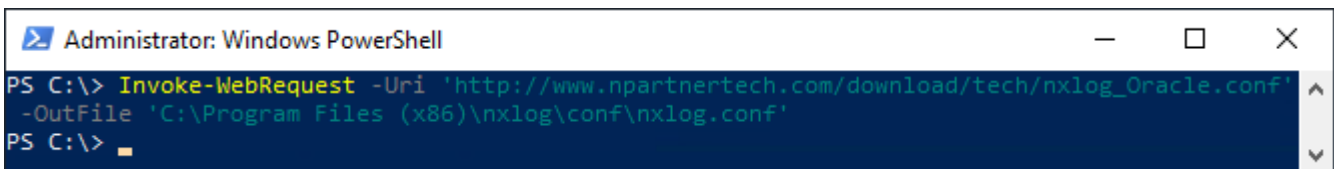
5.1.2 NXLog 設定檔下載

(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 (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 192.168.8.184
define ROOT   C:\Program Files (x86)\nxlog

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

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 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 和 Oracle 執行個體名稱

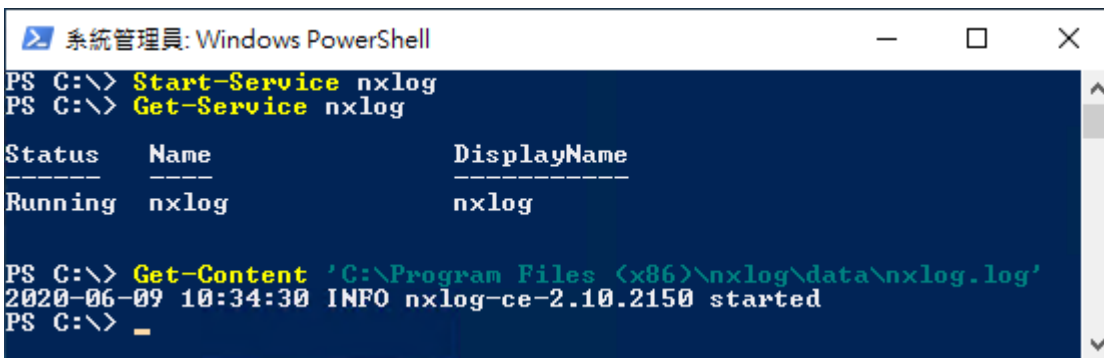
5.1.4 NXLog 啟動服務

(1) 開啟 [Windows PowerShell]



(2) 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 (x86)\nxlog\data\nxlog.log'
```

A screenshot of a Windows PowerShell console window titled "系統管理員: Windows PowerShell". The window has a dark blue background and white text. The commands and their outputs are as follows:

```
PS C:\> Start-Service nxlog
PS C:\> Get-Service nxlog

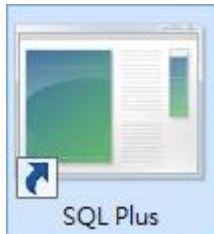
Status      Name          DisplayName
-----
Running     nxlog         nxlog

PS C:\> Get-Content 'C:\Program Files (x86)\nxlog\data\nxlog.log'
2020-06-09 10:34:30 INFO nxlog-ce-2.10.2150 started
PS C:\> _
```

5.2 Oracle Database

5.2.1 Oracle 12c Audit 設定

(1) 開啟 [SQL Plus]



(2) 輸入 user-name: 和 password:

A screenshot of a Windows terminal window titled 'SQL Plus'. The window has a blue title bar with standard Windows window controls (minimize, maximize, close). The terminal text is as follows:

```
SQL*Plus: Release 12.2.0.1.0 Production on Wed Jul 7 14:27:03 2021
Copyright (c) 1982, 2016, Oracle. All rights reserved.

Enter user-name: sys as sysdba
Enter password:

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

(3) 顯示審計參數

SQL> show parameter audit;

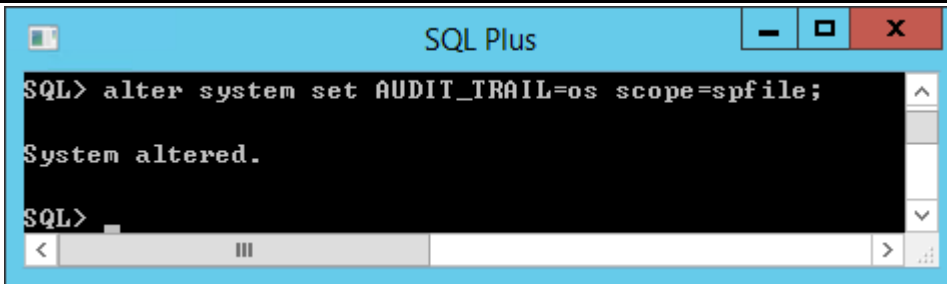
A screenshot of a Windows terminal window titled 'SQL Plus' showing the output of the 'show parameter audit;' command. The window has a blue title bar with standard Windows window controls. The terminal text is as follows:

```
SQL> show parameter audit;

NAME                                TYPE                VALUE
-----                                -
audit_file_dest                      string              C:\ORACLE\APP\ADMINISTRATOR\AD
MIN\ORCL\ADUMP
audit_sys_operations                  boolean             TRUE
audit_trail                           string              DB
unified_audit_sga_queue_size         integer             1048576
SQL>
```

(4) 修改審計記錄到作業系統

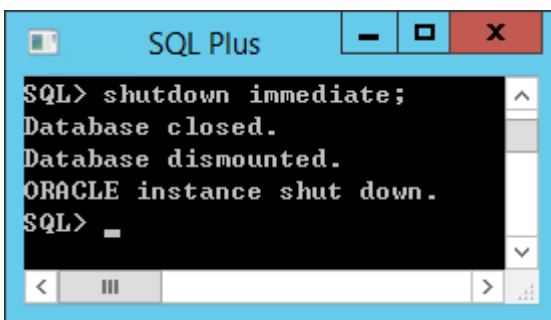
```
SQL> alter system set AUDIT_TRAIL=os scope=spfile;
```



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

(5) 停止 Oracle 資料庫服務

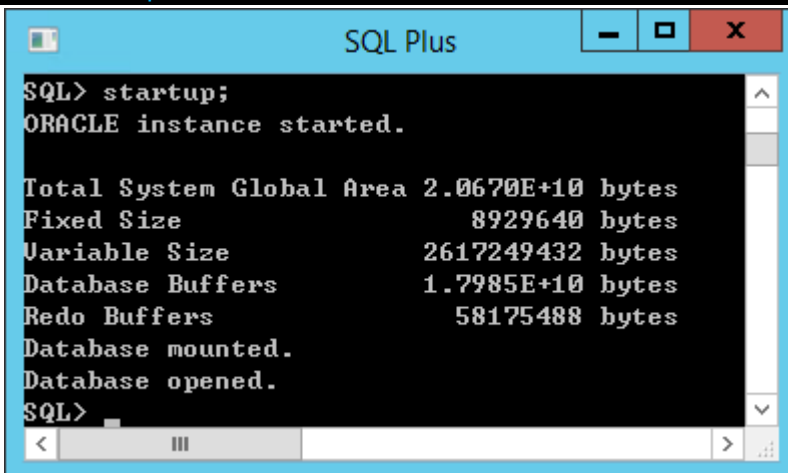
```
SQL> shutdown immediate;
```



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

(6) 啟動 Oracle 資料庫服務

```
SQL> startup;
```

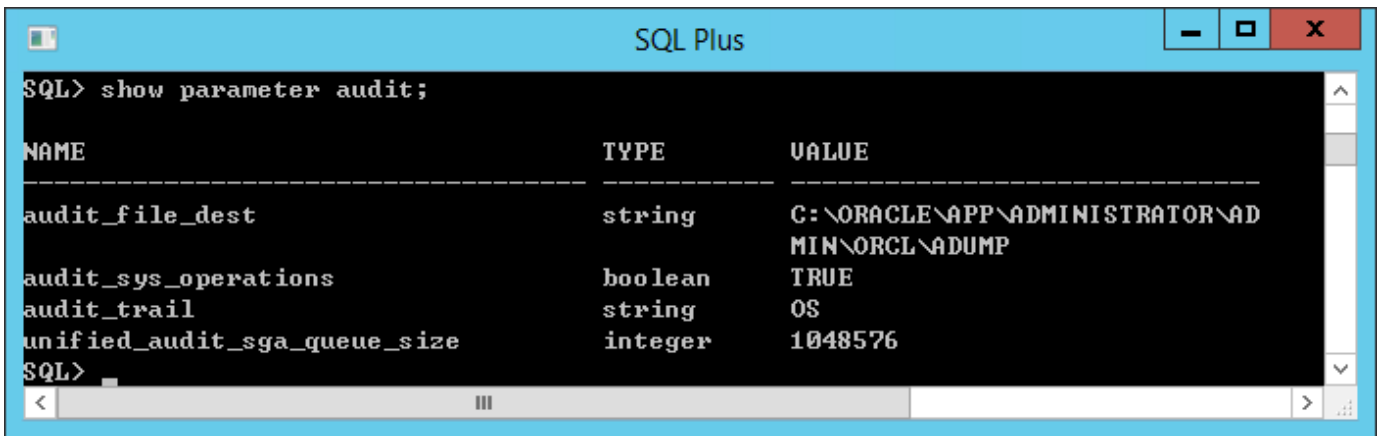


```
SQL> startup;
ORACLE instance started.

Total System Global Area 2.0670E+10 bytes
Fixed Size                  8929640 bytes
Variable Size               2617249432 bytes
Database Buffers           1.7985E+10 bytes
Redo Buffers                 58175488 bytes
Database mounted.
Database opened.
SQL>
```

(7) 顯示審計參數

SQL> show parameter audit;



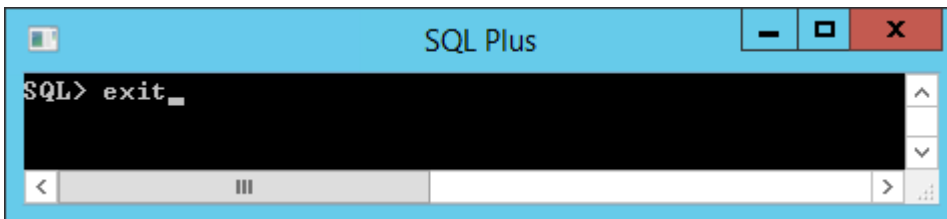
```
SQL> show parameter audit;
```

NAME	TYPE	VALUE
audit_file_dest	string	C:\ORACLE\APP\ADMINISTRATOR\ADMIN\ORCL\ADUMP
audit_sys_operations	boolean	TRUE
audit_trail	string	OS
unified_audit_sga_queue_size	integer	1048576

```
SQL>
```

(8) 離開 [SQL Plus]

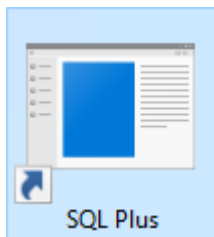
SQL> exit;



```
SQL> exit_
```

5.2.2 Oracle 19c Audit 設定

(1) 開啟 [SQL Plus]



(2) 輸入 `user-name:` 和 `password:`

```
SQL Plus
SQL*Plus: Release 19.0.0.0.0 - Production on Wed Jul 7 13:35:06 2021
Version 19.3.0.0.0

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

Enter user-name: sys as sysdba
Enter password:

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

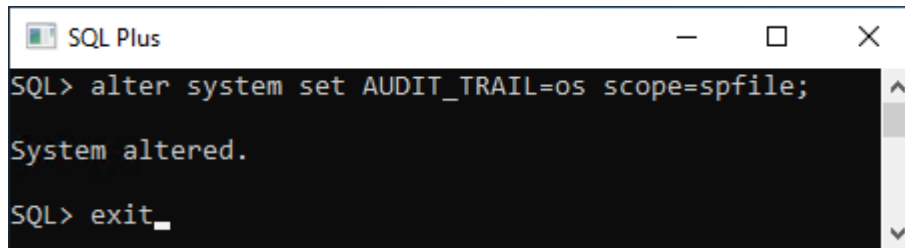
```
SQL> show parameter audit;
```

```
SQL Plus
SQL> show parameter audit;

NAME                                TYPE                                VALUE
-----                                -
audit_file_dest                      string                             C:\USERS\ADMINISTRATOR\DESKTOP
\ADMIN\ORCL\ADUMP
audit_sys_operations                  boolean                             TRUE
audit_trail                           string                             DB
unified_audit_sga_queue_size         integer                             1048576
unified_audit_systemlog               boolean                             FALSE
SQL> _
```

(4) 修改審計記錄到作業系統

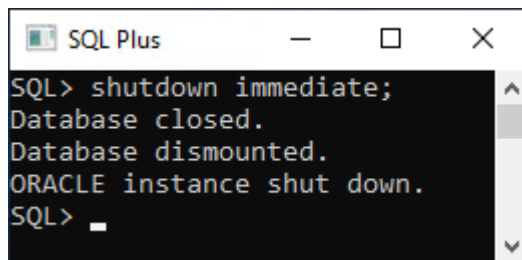
```
SQL> alter system set AUDIT_TRAIL=os scope=spfile;
```



```
SQL Plus
SQL> alter system set AUDIT_TRAIL=os scope=spfile;
System altered.
SQL> exit_
```

(5) 停止 Oracle 資料庫服務

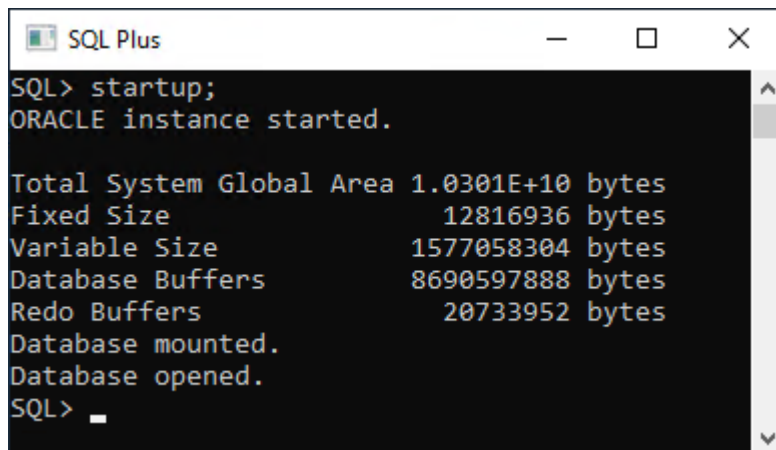
```
SQL> shutdown immediate;
```



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

(6) 啟動 Oracle 資料庫服務

```
SQL> startup;
```

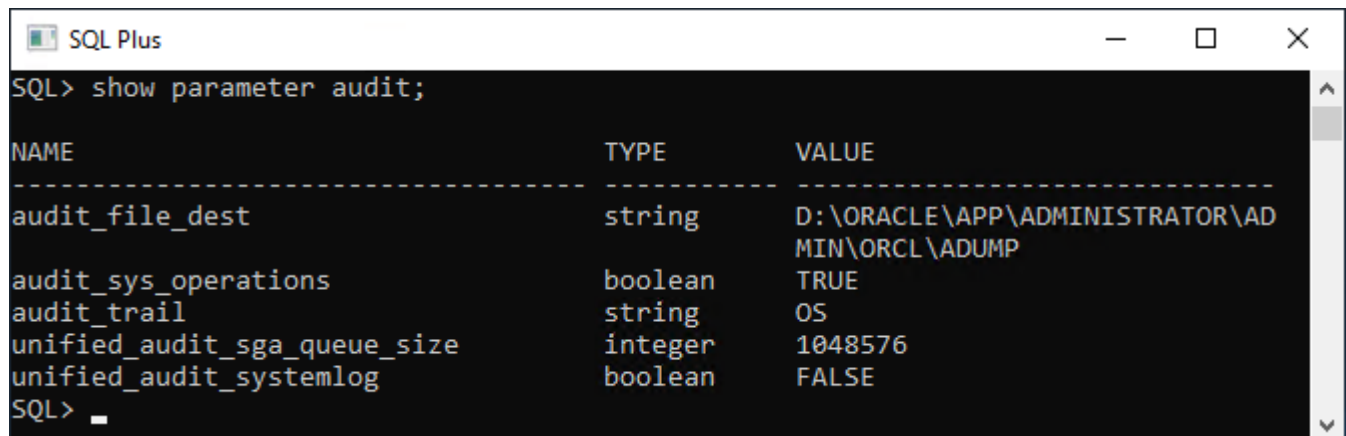


```
SQL Plus
SQL> startup;
ORACLE instance started.

Total System Global Area 1.0301E+10 bytes
Fixed Size                 12816936 bytes
Variable Size              1577058304 bytes
Database Buffers           8690597888 bytes
Redo Buffers                20733952 bytes
Database mounted.
Database opened.
SQL>
```

(7) 顯示審計參數

SQL> show parameter audit;



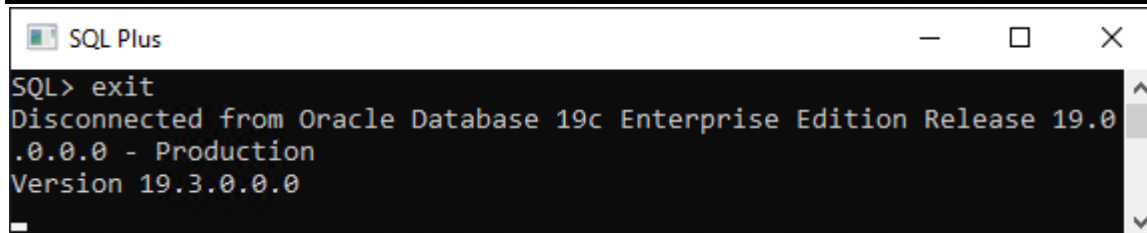
The screenshot shows a terminal window titled "SQL Plus" with the following output for the command "show parameter audit;":

NAME	TYPE	VALUE
audit_file_dest	string	D:\ORACLE\APP\ADMINISTRATOR\AD MIN\ORCL\ADUMP
audit_sys_operations	boolean	TRUE
audit_trail	string	OS
unified_audit_sga_queue_size	integer	1048576
unified_audit_systemlog	boolean	FALSE

The prompt "SQL>" is visible at the bottom of the terminal.

(8) 離開 [SQL Plus]

SQL> exit;



The screenshot shows a terminal window titled "SQL Plus" with the following output for the command "exit;":

```
SQL> exit
Disconnected from Oracle Database 19c Enterprise Edition Release 19.0
.0.0.0 - Production
Version 19.3.0.0.0
```

The prompt "SQL>" is visible at the bottom of the terminal.

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/spfile.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/audit_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-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.* @192.168.8.184
```

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/spfile.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/adump
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.*
```

```
@ 192.168.8.184
```

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

選擇 [設備管理] -> [設備樹狀圖] -> 按下 [新增]

The screenshot displays the N-Reporter web application interface. On the left is a dark blue sidebar menu with the following items: 'Admin (Global) v', '事件', '報表', '智慧分析', '設備管理' (highlighted with a red box), '設備樹狀圖' (highlighted with a red box), '介面列表', '告警樣版', '設備異常告警', '系統管理', and '使用者手冊'. The main content area shows the breadcrumb 'Home / 設備管理 / 設備樹狀圖' and the title '設備樹狀圖'. Below the title is a search bar with a search icon, a refresh icon, a green '+ Add' button (highlighted with a red box), a green 'U' button, and a yellow speaker icon. The main content area shows a tree structure with a root node 'Global (2)' and a child node '未知設備 (1)'.

7.1 Linux / AIX

(2) 設定 Oracle Database 設備的資料格式

輸入名稱和 IP -> 勾選設備種類: [Syslog] -> 選擇資料格式: [Oracle] 和 Facility: [(16) local use 0 (local0)] -> 選擇設備 Icon: [icon-host] -> 點選接收狀態: [啟用] -> 按下 [確定]

新增設備

設備基本設定

名稱
Oracle-192.168.1.188

IP
192.168.1.188

設備種類
 Syslog Flow SNMP

Syslog 相關設定

資料格式
Oracle

Facility
(16) local use 0 (local0)

編碼方式
UTF-8

設備進階設定

ICMP 告警樣版
----- N/A -----

設備 Icon
icon-host

Login Account
[Empty field]

Login Password
[Empty field]

接收狀態
 啟用 停用

暫無資料告警
 啟用 Syslog/Flow 暫無資料告警

確定 取消

7.2 Windows

(2) 設定 Oracle Database 設備的資料格式

輸入名稱和 IP -> 勾選設備種類: [Syslog] -> 選擇資料格式: [Windows] -> 選擇設備 Icon: [icon-host] -> 點選接收狀態: [啟用] -> 按下 [確定]

新增設備

設備基本設定

名稱
Oracle-192.168.1.188

IP
192.168.1.188

設備種類
 Syslog Flow SNMP

Syslog 相關設定

資料格式
Windows

Facility

編碼方式
UTF-8

設備進階設定

ICMP 告警樣板
----- N/A -----

設備 Icon
icon-host

Login Account

Login Password

接收狀態
 啟用 停用

暫無資料告警
 啟用 Syslog/Flow 暫無資料告警

資料保留天數

確定 取消

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@npartnertech.com
技術詢問 / support@npartnertech.com