N-Partner

N-REPORTER

如何接收 Oracle Auditing Log

V 1.1.2 (简体)

前言

这份文件主要描述如何使用 N-Reporter 接收 Oracle audit syslog 。文件着重于如何开启 Oracle Audit 讯息，同时将讯息透过 syslog 送到远程的 N-Reporter，使得 N-Reporter 能正确的处理 Oracle Audit Log。

N-Reporter 为 N-Partner 所有。为目前业界主要的 Syslog 分析仪。能够统计分析接收的 Syslog，产生各式各样的专业报表。

Oracle Database 为美商甲骨文公司所有。是现今效能最优秀的数据库系统之一。

文件章节如下：

连络信息

N-Partner 公司连络方式：

TEL: +886-4-23752865

FAX: +886-4-23757458

有关技术问题请洽：

Email: support@npartnertech.com

有关业务相关问题请洽：

Email: sales@npartnertech.com

1 Oracle Database Audit to syslog

Oracle 9i 和之后推出的版本，支持 Syslog 的功能。设定的方法如下：

以下范例以操作系统为 Linux 为范例：

(1)首先请透过 SQL Plus 联机到数据库，用户必须具备 sysdba 权限

```
SQL> connect / as sysdba
```

(2)利用 spfile 建立暂时的 pfile

```
SQL> create pfile='/tmp/inittemp.ora' from spfile;
File created.
```

(3)编辑 /tmp/inittemp.ora:

```
*.audit_sys_operations=TRUE        （非要字段）
*. transaction_auditing=TRUE
*.audit_syslog_level=local0.info

*.audit_trail='OS'
```

注：若是需要稽核 transaction log，请新增"*.transaction_auditing=TRUE"配置。

注：Oracle 10g 版包含与之后版本请以"*._transaction_auditing=TRUE"代替"*.transaction_auditing=TRUE"。

(4) Shutdown instance

```
SQL> shutdown immediate
```

或者你可以选择使用 srvctl command ，停止运行中的数据库

```
srvctl stop database -d SID
```

(5)使用暂时 pfile，重启数据库

```
SQL> startup mount pfile=/tmp/inittemp.ora
. . .
Database Mounted.
SQL> show parameter audit

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
audit_file_dest                      string      /var/log/oracle
audit_sys_operations                 boolean     TRUE
```

```
audit_syslog_level                string      LOCAL0.INFO
audit_trail                       string      OS
```

(6) Create a new shared spfile from the existing pfile:

```
SQL> create spfile=' location of existing spfile.ora with filename'
from pfile='/tmp/inittemp.ora';
```

(7) 重新启动数据库:

```
SQL> shutdown immediate
. . .
Database Shutdown.


srvctl start database -d SID
```

(8) 编辑 syslog.conf ，将 oracle audit log 透过 syslog 送至 N-Reporter。此范例使用 syslog 模块为例子，syslog.conf 位于/etc/syslog.conf。设定如下：

```
#local0.info /var/log/oracle/oracle_audit.log
#
#Send oracle auditing to remote n-reporter system
local0.info       @192.168.2.1
```

注：syslog.conf 设定格式为"$facility.$severity<tab>@$N-Reporter_IP"，新增的行中 info 和@之间必须是<tab>，不是空白。

(9) Restart syslogd

```
/etc/init.d/syslog restart
```

N-Partner

採購與銷售合作：sales@npartnertech.com

技術諮詢：support@npartnertech.com