N-Partner

N-REPORTER

How to receive Oracle Auditing Log

V 1.1.2

Preface

This document is to introduce how to receive Oracle audit syslog with N-Reporter. It is mainly about how to open Oracle Audit message and send it through syslog to the remote N-Reporter, and let N-Reporter can process Oracle Audit Log correctly.

N-Reporter is a product of N-Partner. It is one of the main Syslog analyzer in the industry. It is able to calculate and analyze received Syslog, and produce all kinds of professional reports.

Oracle Database is a product of Oracle Corporation. It is one of the best database systems nowadays.

Contents

Contact Information

N-Partner Company

TEL: +886-4-23752865

FAX: +886-4-23757458

Technical Support:

Email: support@npartnertech.com

Sales Information:

Email: sales@npartnertech.com

1 Oracle Database Audit to syslog

Oracle 10g and the later versions all support Syslog function. Here are the setting steps:

We use Linux as the environment for example:

(1) First, connect to the database through SQL Plus. The user must have sysdba authorization.

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

(2) Use spfile to set a temporary pfile.

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

(3) Edit /tmp/inittemp.ora:

```
*.audit_sys_operations=TRUE          ( unnecessary field )
*. transaction_auditing=TRUE
*.audit_syslog_level=local0.info

*.audit_trail='OS'
```

Remark 1：If it needs to audit transaction log, please add "*.transaction_auditing=TRUE ".

Remark 2：The Oracle 10g and the later versions, please use "*._transaction_auditing=TRUE" to replace "*.transaction_auditing=TRUE".

(4) Shutdown instance

```
SQL> shutdown immediate
```

Or you can use srvctl command, to stop the running database.

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

(5) Setting database using the temporary pfile.

```
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) Restart the database:

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

srvctl start database -d SID
```

(8) Edit rsyslog.conf, send oracle audit log to N-Reporter through syslog. Here we use rsyslog for example, modify the configuration file /etc/rsyslog.conf. Here are the settings:

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

Remark：It is <tab> between info and @ on the last line command above, not a space.

(9) Restart Rsyslog

```
/etc/init.d/rsyslog restart
```

N-Partner

Purchases and Sales Cooperation: sales@npartnertech.com

Technical Support: support@npartnertech.com