# 

**Tripwire** có khả năng ghi lại những thuộc tính của tập tin hệ thống quan trọng và định kỳ sau đó so sánh trạng thái hiện hành của những tập tin này với những gì đã lưu trữ và báo cáo cho người quản trị khi có bất kỳ thay đổi đáng ngờ nào.

Using Tripwire is to capture information on any file or directory that could cause administrative problems or worse, system downtime, if compromised. This is a big task on even the simplest network .

===============================================================================

Report Summary:

===============================================================================

Host name: prod-db-srv

Host IP address: 192.168.1.10

Host ID: None

Policy file used: /opt/tripwire/etc/tw.pol

Configuration file used: /opt/tripwire/etc/tw.cfg

Database file used: /opt/tripwire/lib/tripwire/prod-db-srv.twd

Command line used: ./tripwire --check --interactive

Remove the "x" from the adjacent box to prevent updating the database

with the new values for this object.

Added:

[x] "/u01/app/oracle/diag/rdbms/proddb/proddb/trace/proddb\_m000\_11376.trc"

[x] "/u01/app/oracle/diag/rdbms/proddb/proddb/trace/proddb\_m000\_11376.trm"

Modified:

[x] "/u01/app/oracle/diag/rdbms/proddb/proddb/metadata/INC\_METER\_CONFIG.ams"

[x] "/u01/app/oracle/diag/rdbms/proddb/proddb/metadata/INC\_METER\_INFO.ams"

Added object name: /u01/app/oracle/diag/rdbms/proddb/proddb/trace/proddb\_m000\_11376.trc

Property: Expected Observed

------------- ----------- -----------

\* Object Type --- Regular File

\* Device Number --- 2049

\* Inode Number --- 12026017

\* Mode --- -rw-r-----

\* Num Links --- 1

\* UID --- oracle (1082)

\* GID --- oinstall (1083)

\* Size --- 837

\* Modify Time --- Sat 06 Dec 2008 10:01:51 AM PST

\* Blocks --- 8

\* CRC32 --- AYxMeo

\* MD5 --- AXSkOul8R/np0fQP4q3QLv

Modified object name: /u01/app/oracle/diag/tnslsnr/proddb/listener/trace/listener.log

Property: Expected Observed

------------- ----------- -----------

Object Type Regular File Regular File

Device Number 2049 2049

Inode Number 2295281 2295281

Mode -rw-r----- -rw-r-----

Num Links 1 1

UID oracle (1082) oracle (1082)

GID oinstall (1083) oinstall (1083)

\* Size 5851880 5858608

\* Modify Time Sat 06 Dec 2008 09:58:53 AM PST

Sat 06 Dec 2008 11:39:56 AM PST

\* Blocks 11456 11472

\* CRC32 ANdM8R CK+bWM

\* MD5 DCW84lCuD2YJOhQd/EuVsn CV8BMvZNJB9KQBXAf5yRDY

Please enter your local passphrase:

Incorrect local passphrase.

Please enter your local passphrase:

Wrote database file: /opt/tripwire/lib/tripwire/prod-db-srv.twd

All the tripwire report files with \*.twr extension are stored under /opt/tripwire/lib/tripwire/report directory. tripwire report file \*.twr is not a text file, which you can view directly. In order to view the report, use twprint and convert the \*.twr file to a readable text format as shown below.

# **./twprint --print-report --twrfile \**

**/opt/tripwire/lib/tripwire/report/prod-db-srv-20081204-114336.twr > \**

**/tmp/readable-output.txt**