Audit Files & Folders

Per monitorare un'azione fatta su un file o folder, si puo utilizzare il servizio audit.

Per installare questo servizio eseguire su Ubuntu/Debian:

```
apt-get install auditd audispd-plugins
```

In genere CentOs ha gia audit installato (audit and audit-libs).

Creare una rule per la cartella da monitorare:

```
auditctl -w /tmp/testing -k nomerule -p w
```

Per eliminare la rule:

```
auditctl -W /tmp/testing -k nomerule -p w
```

NB: La W è maiuscola.

Per avere una lista delle rules:

```
auditctl -l
```

Per iniziare,fermare,riavviare il servizi:

```
service auditd start/stop/restart
```

I log del audit si trovano in:

```
/var/log/audit/audit.log
```

Si possono vedere il log della rule creata con il seguente commando:

```
ausearch -k nomerule
```