

Dateiänderungen überwachen mit auditd

Paket:

- CentOS (6): audit
- openSuSE (13.1): audit
- Debian (ab 7): auditd
- Ubuntu (ab 18.04): auditd

Änderungen an Datei `"/etc/passwd"` überwachen

[/etc/audit/rules.d/passwd.rules](#)

```
-w /etc/passwd -p wa
```

```
service auditd restart
```

testen

```
touch /etc/passwd  
tail /var/log/audit/audit.log  
ausearch -i -f /etc/passwd
```

```
useradd -m klaus  
tail /var/log/audit/audit.log  
ausearch -i -f /etc/passwd
```

Auditd für Änderungen sperren

`/etc/audit/audit.rules` :

```
-e 2
```

Änderungen an `/etc/audit/audit.rules` werden jetzt erst nach reboot aktiv.

Todo

```
auditctl  
aureport
```

From:

<https://wiki.lab.linuxhotel.de/> - **Linuxhotel Wiki**

Permanent link:

https://wiki.lab.linuxhotel.de/doku.php/admin_grundlagen:auditd

Last update: **2022/07/29 15:35**

