

Migrating OSSEC manager installed from packages

1. Backup your current configuration

Stop OSSEC:

```
$ /var/ossec/bin/ossec-control stop
```

Check if you have enough space to create a copy of `/var/ossec`:

```
$ du -h /var/ossec | tail -n1
$ df -h /var
```

Backup `/var/ossec`:

```
$ cp -rp /var/ossec /var/ossec_backup
```

2. Remove your current installation

Debian and Ubuntu:

```
$ apt-get remove ossec-hids --purge
```

CentOS and Red Hat:

```
$ yum remove ossec-hids
```

Remove directory:

```
$ rm -rf /var/ossec
```

3. Install Wazuh server

Follow the next guide in order to install Wazuh server:

- [Install Wazuh server with RPM packages](#)
- [Install Wazuh server with Deb packages](#)

4. Restore configuration

Stop OSSEC:

```
$ systemctl stop wazuh-manager
```

Restore mandatory files:

```
$ cp -p /var/ossec_backup/agentless/.passlist /var/ossec/agentless/
$ cp -p /var/ossec_backup/etc/client.keys /var/ossec/etc/
$ cp -p /var/ossec_backup/etc/ossec.conf /var/ossec/etc/ossec.conf.orig
$ cp -p /var/ossec_backup/etc/local_internal_options.conf /var/ossec/etc/local_internal_options.conf
$ cp -p /var/ossec_backup/etc/local_decoder.xml /var/ossec/etc/decoders/local_decoder.xml
$ cp -p /var/ossec_backup/etc/shared/agent.conf /var/ossec/etc/shared/agent.conf
$ cp -p /var/ossec_backup/rules/local_rules.xml /var/ossec/etc/rules/local_rules.xml
$ cp -p /var/ossec_backup/queue/rids/sender_counter /var/ossec/queue/rids/sender_counter
```

Restore optional files

The following files are required in order to preserve alerts log files and syscheck/rootcheck databases:

```
$ cp -rp /var/ossec_backup/logs/archives/* /var/ossec/logs/archives
$ cp -rp /var/ossec_backup/logs/alerts/* /var/ossec/logs/alerts
$ cp -rp /var/ossec_backup/queue/rootcheck/* /var/ossec/queue/rootcheck
$ cp -rp /var/ossec_backup/queue/syscheck/* /var/ossec/queue/syscheck
```

5. Review ossec.conf

The previous configuration file is saved as `/var/ossec/etc/ossec.conf.orig`. You should review the new configuration file `/var/ossec/etc/ossec.conf` with the old one in case that you want to add some setting from the previous configuration.

6. Start Wazuh

```
$ /var/ossec/bin/ossec-control start
```