

# On-Premises

## Securing the server

### Create a complex root password

This will withstand brute force attacks by hackers to obtain the password.

### Install ClamAV

- Use Yast to install ClamAV and it's offline database.
- Update database and run a complete scan.

```
freshclam  
clamscan -r -i /
```

- Delete all infected files, if any.

### Restrict ssh access by key alone

- Copy the file authorized\_keys to /root/.ssh
- Edit the file sshd\_config

```
vi /etc/ssh/sshd_config
```

and add the following lines:

```
PasswordAuthentication no  
ChallengeResponseAuthentication no
```

\*\*If root access is not permitted,

From:  
<http://wiki.dreamapps.com/wiki/> - **DreamApps Wiki**

Permanent link:  
<http://wiki.dreamapps.com/wiki/doku.php?id=deployment:onpremises&rev=1497075725>

Last update: **2017/06/10 06:22**

