Zabezpečení Proxmox VE

Cluster

Minimalisticky quorum server (lze nainstalovat do kontejneru, pokud je na hostiteli povoleno FUSE)

```
apt install pve-cluster
pvecm add node1
pvecm status
```

Jeste lehci setup by nejspis sel udelat ciste pomoci baliku corosync-qnetd. To jsem zatim nezkousel.

Reverzní proxy před pveproxy

Návod volně založen na

- http://the-bleeding-edge.info/blog/?p=24
- https://www.jamescoyle.net/how-to/1522-proxy-the-proxmox-web-gui-with-nginx-over-https-with-load-balancing

/etc/default/pveproxy

```
ALLOW_FROM="127.0.0.1"
DENY_FROM="all"
POLICY="allow"
```

```
/etc/init.d/pveproxy restart

apt install nginx-light
```

/etc/nginx/sites-available/proxmox

```
server {
    listen 80;
    server_name _;
    return 302 https://$host$request_uri;
}

server {
    listen 443 ssl; #choose your port or just use 443
    server_name _; #place your domain or ip here if needed

    #root /usr/share/nginx/www;

    ssl_certificate /etc/letsencrypt/live/pve1.spoje.net/fullchain.pem;
```

```
    ssl_certificate_key
/etc/letsencrypt/live/pve1.spoje.net/privkey.pem;

    #Internal letsencrypt:
    #ssl_certificate /etc/pve/local/pveproxy-ssl.pem;
    #ssl_certificate_key /etc/pve/local/pveproxy-ssl.key;

    proxy_redirect off;

    auth_basic "SPOJE.NET VPS";
    auth_basic_user_file /etc/nginx/.htpasswd;

    #proxy_ssl_verify off; #default

    location ~ ^.+websocket$ {
        proxy_pass https://127.0.0.1:8006;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection "upgrade";
    }

    location / {
        proxy_pass https://127.0.0.1:8006;
    }
}
```

```
username=virtual; echo "${username}:`openssl passwd -apr1`" >>
/etc/nginx/.htpasswd
```

```
/etc/init.d/nginx restart
```

Spolecna nastaveni LXC

Todo: zamyslet se jestli to nepatri do /etc/lxc/default.conf

/usr/share/lxc/config/common.conf.d/99-spoje.conf

```
#Pripojime tmpfs
lxc.mount.entry = tmpfs tmp tmpfs
defaults,nosuid,noexec,nodev,size=256M

#Omezime pocet procesu/threadu
lxc.cgroup.pids.max = 600

#Povolime tun/tap (openvpn)
lxc.cgroup.devices.allow = c 10:200 rwm
lxc.hook.autodev = sh -c "modprobe tun; cd ${LXC_ROOTFS_MOUNT}/dev;
mkdir net; mknod net/tun c 10 200; chmod 0666 net/tun"
```

```
#Povolime FUSE (pozor, ma problemy s lxc-freeze, takze zadny snapshoty, zalohy, migrace, replikace, atd...)
lxc.hook.autodev: sh -c "mknod -m 0666 ${LXC_ROOTFS_MOUNT}/dev/fuse c 10 229"
```

Po editaci tohodle souboru je vhodny zkontrolovat syntaxi treba prikazem `pct list`. Pokud je neco spatne, tak proxmox vypisuje chybovy hlasky a vsechny virtualy prestanou bejt pouzitelny a bezici se zacnou tvarit jako vypnuty!

Zakazat dmesg

pridat na konec souboru:

/usr/share/lxc/config/common.seccomp

```
syslog errno 1
```

Pozor, soubor se prepisuje po upgradu, TODO: doresit lepsi umisteni

From:
https://wiki.spoje.net/ - **SPOJE.NET**

Permanent link:
https://wiki.spoje.net/doku.php/howto/vps/proxmox-ve/security

Last update: **2018/05/29 16:38**