

Proxmox

Cosas sobre Proxmox

- [Git pull, error: server certificate verification failed. CAfile: none CRLfile: none](#)
- [\[PRIV\] Instalar Proxmox desde 0](#)
- [LVM Práctico para Proxmox y OVH](#)
- [Red OVH vrack para Proxmox 7](#)
- [Como arreglar el error Sender address rejected: need fully-qualified address \(in reply to RCPT TO command\)](#)
- [Proxmox, Hetzner, y bloques de Ips adicionales en modo Routed](#)
- [Desactivar los mensajes de log en la consola \(Proxmox\)](#)

Git pull, error: server certificate verification failed. CAfile: none CRLfile: none

Introducción

El problema me apareció en un proxmox desactualizado, cuando quise hacer un pull de mis utilidades.

```
“ git pull fatal: unable to access 'https://*****.castris.com/root/utilidades.git/':  
server certificate verification failed. CAfile: none CRLfile: none
```

Tras verificar que el problema no estaba del lado de mi gitlab, sospeche de la desactualización de Proxmox. Como nunca actualizo un Proxmox, ya la solución de actualizar sólo los ca-certificates y paquetes relacionados, no funcionó opte por una tip rápido.

```
“ No actualizo los proxmox, porque desde la versión 3, que ya son años, he tenido  
4 incidentes de actualización, con sus correspondientes problemas derivados.  
Así que prefiero hacer un un turn-over en mi proveedor, coger una máquina  
nueva cada dos o tres años, y dejarme de tonterías. Atención, a mis máquinas  
proxmox no se acceden sino es desde mis ips, otra imposición que me puse  
dado que he visto muchos proxmox hackeados vía web. Así que al estar capado,  
no tengo miedo a no "actualizar"
```

Modificación de Git para no verificar ssl

```
root@pro12:~/utilidades# git config --global http.sslverify false  
root@pro12:~/utilidades# git pull  
remote: Enumerating objects: 23, done.  
remote: Counting objects: 100% (23/23), done.
```

```
remote: Compressing objects: 100% (14/14), done.
remote: Total 18 (delta 9), reused 12 (delta 4), pack-reused 0
Unpacking objects: 100% (18/18), done.
From https://gitlab.castris.com/root/utilidades
   10bda88..c93d331  master    -> origin/master
Updating 10bda88..c93d331
Fast-forward
 .gitignore          |    2 +
 actualiza.sh        |    2 +-
 basura.sh           |    4 +
 compress-dovecot.sh |   164 ++++++++
 csf/proxmox.csf.conf |  2678
+++++
+++++
 fixpermissions.sh   |   164 ++++++++
 6 files changed, 3013 insertions(+), 1 deletion(-)
 create mode 100644 compress-dovecot.sh
 create mode 100644 csf/proxmox.csf.conf
 create mode 100644 fixpermissions.sh
```

Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

[PRIV] Instalar Proxmox desde 0

OVH

Seguridad

```
mkdir /root/soft;cd /root/soft/; wget https://download.configserver.com/csf.tgz; tar xvfz
csf.tgz; cd csf; sh install.sh; cd ..; rm -Rf csf/ csf.tgz; \
echo '.cpanel.net
.googlebot.com
.crawl.yahoo.net
.search.msn.com
.paypal.com
.paypal.es' > /etc/csf/csf.rignore;\
wget -O /etc/csf/csf.conf https://gitlab.castris.com/root/utilidades/-
/raw/main/csf/proxmox.csf.conf; \
wget -O /etc/csf/csf.blocklists https://gitlab.castris.com/root/utilidades/-
/raw/main/csf/csf.blocklists; \
wget -O /etc/csf/csf.allow https://gitlab.castris.com/root/utilidades/-/raw/main/csf/csf.allow;
\
wget -O /etc/csf/csf.dyndns https://gitlab.castris.com/root/utilidades/-
/raw/main/csf/csf.dyndns
```

Discos

[Discos proxmox](#)

Utilidades

```
cd ~ && git clone https://gitlab.castris.com/root/utilidades.git
```

Red

[Red OVH vrack para Proxmox 7](#)

zabbix

Discos remotos

LVM Práctico para Proxmox y OVH

Introducción

Es un tip que uso para **mis necesidades**. Entre otras, no uso **ZSF** por la carga que supone para el sistema, y porque suplo sus bondades por decisión propia con otros mecanismo de salvaguarda.

“ Cada modelo de máquina de OVH y cada instalación deja diferencias sutiles que pueden hacer que uno tenga que modificar los datos de particiones, discos, interfaces de red.

LVM

En una instalación sin uso de RAID por software del instalador tenemos en la versión del instalador de OVH que instala 7.2-14 de Proxmox un **volumen** llamado **vg** en el disco primario

```
pvs
PV          VG Fmt Attr PSize PFree
/dev/nvme0n1p5 vg lvm2 a-- 1.72t  0
lvscan
ACTIVE                '/dev/vg/data' [1.72 TiB] inherit
```

Sobre el cual ha creado un **volume** llamado **vg** y un **volumen lógico** llamado **data** con el tamaño máximo

“ Mal por todo, porque asigna todo el espacio y no permite hacer snapshots.

Este modelo no me sirve pues yo nunca uso virtualización por **OpenVZ** así que hay que eliminar y reconstruir

Copia de la partición


```
=                crc=1          finobt=1, sparse=1, rmapbt=0
=                reflink=1       bigtime=0
data             =                bsize=4096   blocks=5242880, imaxpct=25
=                sunit=32        swidth=32 blks
naming           =version 2      bsize=4096   ascii-ci=0, ftype=1
log              =internal log   bsize=4096   blocks=2560, version=2
=                sectsz=4096     sunit=1 blks, lazy-count=1
realtime         =none           extsz=4096   blocks=0, rtextents=0
Discarding blocks...Done.
```

Obtención del UUID

```
blkid
...
/dev/mapper/vg-data: UUID="c0ede30d-f8a6-4897-a392-39c9dfc542a6" BLOCK_SIZE="4096" TYPE="xfs"
```

Edición de fstab

```
UUID=c0ede30d-f8a6-4897-a392-39c9dfc542a6 /var/lib/vz/xfs defaults 0 0
```

Restauración de ficheros del directorio

```
rsync -avv --progress /old_vz/ /var/lib/vz/
systemctl restart pve-cluster pvedaemon pveproxy pvestatsd
```

Creación de volúmenes LVM

En mi caso, y en este en particular, no deseo ampliar el volumen, sino que prefiero tener 3 volúmenes independientes, por el tipo de máquina que uso y el uso que se va a dar, ya que la velocidad y cargas en el proceso, me son más interesante con 3 volúmenes, que con uno, a la par que la posibilidad de una rotura de LVM es mayor y un riesgo que llevo años sin querer sufrirlo (que alguna vez lo he sufrido) y en los últimos 8 años, no he tenido ningún percance con varias máquinas con este aprovechamiento.

Reconocimiento de discos

```
disk -l
Disk /dev/nvme1n1: 1.75 TiB, 1920383410176 bytes, 3750748848 sectors
Disk model: SAMSUNG MZQL21T9HCJR-00A07
```

```
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 131072 bytes / 131072 bytes
```

```
Disk /dev/nvme2n1: 1.75 TiB, 1920383410176 bytes, 3750748848 sectors
```

```
Disk model: SAMSUNG MZQL21T9HCJR-00A07
```

```
Units: sectors of 1 * 512 = 512 bytes
```

```
Sector size (logical/physical): 512 bytes / 4096 bytes
```

```
I/O size (minimum/optimal): 131072 bytes / 131072 bytes
```

```
Disk /dev/nvme0n1: 1.75 TiB, 1920383410176 bytes, 3750748848 sectors
```

```
Disk model: SAMSUNG MZQL21T9HCJR-00A07
```

```
Units: sectors of 1 * 512 = 512 bytes
```

```
Sector size (logical/physical): 512 bytes / 4096 bytes
```

```
I/O size (minimum/optimal): 131072 bytes / 131072 bytes
```

```
Disklabel type: gpt
```

```
Disk identifier: 991EADF9-826A-4A35-B37C-5A1C3D255A5D
```

Device	Start	End	Sectors	Size	Type
/dev/nvme0n1p1	2048	1048575	1046528	511M	EFI System
/dev/nvme0n1p2	1048576	3145727	2097152	1G	Linux filesystem
/dev/nvme0n1p3	3145728	45088767	41943040	20G	Linux filesystem
/dev/nvme0n1p4	45088768	47185919	2097152	1G	Linux filesystem
/dev/nvme0n1p5	47185920	3750739967	3703554048	1.7T	Linux LVM
/dev/nvme0n1p6	3750744752	3750748814	4063	2M	Linux filesystem

```
Partition 6 does not start on physical sector boundary. // No importante
```

```
Disk /dev/mapper/vg-data: 20 GiB, 21474836480 bytes, 41943040 sectors
```

```
Units: sectors of 1 * 512 = 512 bytes
```

```
Sector size (logical/physical): 512 bytes / 4096 bytes
```

```
I/O size (minimum/optimal): 131072 bytes / 131072 bytes
```

Tenemos pues los discos `nvme1n1` y `nvme2n1` disponibles

Creación de los grupos de volúmenes

Como uso una dinámica de nombres para así hacer más fácil las migraciones entre máquinas Proxmox, haré lo mismo.

“ Es importante crear los volúmenes de almacenamiento en **particiones** y no sobre el disco completo.

Partición

Usare mi [Parted mejor que fdisk](#)

Creamos las etiquetas

```
parted -s /dev/nvme1n1 mklabel gpt
parted -s /dev/nvme2n1 mklabel gpt
```

Creamos las particiones

```
parted -s /dev/nvme1n1 mkpart primary 0% 100%
parted -s /dev/nvme2n1 mkpart primary 0% 100%
```

Creación de los volúmenes

```
vgcreate lvm /dev/nvme1n1p1
Physical volume "/dev/nvme1n1p1" successfully created.
Volume group "lvm" successfully created

vgcreate lvm2 /dev/nvme2n1p1
Physical volume "/dev/nvme2n1p1" successfully created.
Volume group "lvm2" successfully created

pvscan
PV /dev/nvme1n1p1  VG lvm          lvm2 [<1.75 TiB / <1.75 TiB free]
PV /dev/nvme2n1p1  VG lvm2         lvm2 [<1.75 TiB / <1.75 TiB free]
PV /dev/nvme0n1p5  VG vg           lvm2 [1.72 TiB / <1.71 TiB free]
Total: 3 [<5.22 TiB] / in use: 3 [<5.22 TiB] / in no VG: 0 [0  ]
```

Final

A partir de aquí, ya tenemos nuestra estructura deseada en LVM para Proxmox.

Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

Red OVH vrack para Proxmox 7

Introducción

El artículo es para un escenario de uso del **vrack** de **OVH** en un escenario específico. El alcance es dejar un tip, que uso muy a menudo, y en el que pongo énfasis en poder utilizar asegurándome de que si algo falla, puedo volver atrás con facilidad.

Configurar la red para OVH Rack con Proxmox 7

Copiar configuracion original

```
rsync -avv /etc/network/interfaces /root/interfaces.bak
```

Editar la configuración

Editamos la interface que puede ser diferente en cada caso pues con el tiempo cambian, y con los modelos de OVH cambian su forma de conexión a OVH

Es importante entender que hay dos interfaces de red y que esas son las que debemos configurar para usar vrack.

El modelo que uso, es particular, para mis necesidades. Hay muchas formas de configurar la red con vrack dependiendo de que estemos desplegando en nuestra máquina Proxmox y la red que queremos.

```
auto lo
iface lo inet loopback

iface eno1 inet manual

#auto vmbr0
#iface vmbr0 inet static
# address IP.IP.IP.2/24
```

```
# gateway IP.IP.IP.254
# bridge-ports eno1
# bridge-stp off
# bridge-fd 0
# hwaddress XX:XX:XX:XX:XX:XX

# nuevo modelo OVH DHCP
auto vmbr0
iface vmbr0 inet dhcp
    address IP.IP.IP.IP/24
    gateway IP.IP.IP.254
    bridge-ports eno1
    bridge-stp off
    bridge-fd 0

# for routing
auto vmbr1
iface vmbr1 inet manual
    bridge_ports dummy0
    bridge_stp off
    bridge_fd 0

# Bridge vrack 1.5
auto vmbr2
iface vmbr2 inet manual
    bridge_ports eno2
    bridge_stp off
    bridge_fd 0
```

“ Un consejo por si hay que reiniciar y usar el IPMI para arreglarlo si la cosa no ha funcionado. Cambiar la contraseña por una sin signos ya que el IPMI no es precisamente amigable con los teclados nacionales.

Reinicio

Hacemos un shutdown de la máquina, y ya tendríamos nuestra red con vrack instalada.

Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

Como arreglar el error Sender address rejected: need fully-qualified address (in reply to RCPT TO command)

Introducción

Algunas veces tenemos hosts (máquinas) de servicio, como Proxmox, en las que las peculiaridades y operativas, nos dejan con ciertos problemas de envío de correo, como los enviados por root (alertas, etc) que son enviados con el nombre corto de `host` en lugar del FQDN. Están configurados con **Postfix**, y el servidor remoto, no permite este tipo de envío de correos (normal) por lo que debemos hacer un mapping en el servidor que está enviando los correos con el hostname corto.

```
Jan 29 00:00:19 smtp postfix/smtpd[389410]: NOQUEUE: reject: RCPT from pro18.XXX.XXX[Z.Z.Z.Z]:  
504 5.5.2 <root@pro18>: Sender address rejected: need fully-qualified address;  
from=<root@pro18> to=<sistemas@mydomain.com> proto=ESMTP helo=<pro18.XXX.XXX>
```

Solución

Crear el fichero `/etc/postfix/canonical`

```
@local @pro18.mydomain.tld  
@pro18 @pro18.mydomain.tld
```

Añadir la referencia a este fichero de hash

```
canonical_maps = hash:/etc/postfix/canonical
```

Activar el fichero de hash

```
postmap /etc/postfix/canonical  
service postfix restart
```

Documentación

[Postfix :: Canonical address mapping](#)

Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

Proxmox, Hetzner, y bloques de Ips adicionales en modo Routed

Introducción

Tra una experiencia desastrosa con el proveedor **Scaleway** y su sistema **Elastic Metal** decidí que lo mejor era marcharme. Dado que lo único que me queda allí, era una máquina de Proxmox con failover de máquinas en #OVH, revise los requerimientos de tráfico (Hetzner te da solo 20 TB de tráfico de salida) y me sobraba, ya que la mayoría casi 24TB es tráfico de entrada.

Aunque ya había estado allí hace muchos años, nunca lo hice con Proxmox. Os dejo aquí mi experiencia, ya que sus manuales son un poco cuadrículados y ausente para ciertas cosas, y su soporte es nulo, más allá de enviarte a sus manuales.

“ Casi todos los soportes de grandes proveedores de Hosting y Colo, son parecidos. En cierta manera les entiendo, pero si dan 0 soporte sus manuales tienen que ser impecables.

Proxmox Modo Routed en lugar de bridge

El porqué es claro. Hetzner solo te permite 7 ips por servidor o pasas por caja para coger un bloque, y sus bloques no funcionan en modo bridge.

“ El modo bridge es como el OVH para IP Failover. Tienes que asignar un MAC vía ticket, robot, api.. El método routed no.

El [Manual Hetzner](#) es necesario leerlo, o puedes llevarte una sorpresa.

En mi caso, la instalación estaba clara: Sin raid (por software es una patata, y además, el alcance de este servidor no requiere de raid), modelo de Routed forzado por el sistema de Hetzner para bloques de IPS adicionales.

Bien lo primero que observe y que produjo un choque, fue que las imágenes de las acciones en el frontend de Proxmox para crear y modificar la red, no concuerdan con lo que luego graba en el fichero `/etc/network/interfaces`

Además hay algunos puntos sutiles respecto a la notación de algunas IP.

IPV4/CIDR

El ejemplo te puede llevar a error porque te pone un CIDR `/26` tanto en el texto como el gráfico, si mayor explicación.

Resulta que Hetzner no te entrega toda la información en su Robot, y por tanto te aconsejo que calcules tu red.

Por si te olvidaste cómo hacerlo mejor te dejo esta [calculadora de redes](#) aunque es posible que sea mejor que Hetzner te lo diga en un ticket.

Fichero `/etc/network/interfaces`

En vez del frontend pasamos a modo shell

Notas sobre algunos elementos usados

- CIDR [Classless Inter-Domain Routing](#)
- `enp41s0` es la interfaz de red que puede ser distinta según modelo.

```
source /etc/network/interfaces.d/*

auto lo
iface lo inet loopback

iface lo inet6 loopback

auto enp41s0
iface enp41s0 inet static
  address IP_SERVIDOR/CIDR
  gateway GATEWAY_IP_SERVIDOR
  up route add -net IP_BLOQUE_IPS netmask 255.255.NETMASK_BLOQUE gw IP_SERVIDOR/ dev enp41s0
  #Routed mode

iface enp41s0 inet6 static
  address SUBNET_IPV6::2/64 # Atención al 2
  gateway fe80::1 # Revisar al gateway que te da Hetzner para el bloque IPv6

auto vmbro
```

```
iface vmbr0 inet static
  address IP_SERVIDOR/32
  bridge-ports none
  bridge-stp off
  bridge-fd 0

iface vmbr0 inet6 static
  address SUBNET_IPV6::2/64
```

/etc/network/interfaces.d/vm-routes

```
iface vmbr0 inet static
  #up ip route add IP_BLOQUE_IPS/28 dev vmbr0 # no me funciona
  up ip route add IP_BLOQUE_IPS.193/32 dev vmbr0
  up ip route add BLOQUE_IPS.194/32 dev vmbr0
  up ip route add BLOQUE_IPS.195/32 dev vmbr0
  up ip route add BLOQUE_IPS.196/32 dev vmbr0
  up ip route add BLOQUE_IPS.197/32 dev vmbr0
  up ip route add BLOQUE_IPS.198/32 dev vmbr0
  up ip route add BLOQUE_IPS.199/32 dev vmbr0
  up ip route add BLOQUE_IPS.200/32 dev vmbr0
  up ip route add BLOQUE_IPS.201/32 dev vmbr0
  up ip route add BLOQUE_IPS.202/32 dev vmbr0
  up ip route add BLOQUE_IPS.203/32 dev vmbr0
  up ip route add BLOQUE_IPS.204/32 dev vmbr0
  up ip route add BLOQUE_IPS.205/32 dev vmbr0
  up ip route add BLOQUE_IPS.206/32 dev vmbr0
iface vmbr0 inet6 static
  up ip -6 route add SUBNET_IPV6::/64 dev vmbr0
```

Configserver Firewall

A mi no me gusta nada el firewall que usa Proxmox, así que sigo usando Configserver CSF, pero esto requiere ciertos añadidos

Necesitamos pasarle a CSF la interfaz que hace de Bridge o enrutador.

Para ello añadimos el fichero `/etc/csf/csfpre.sh` con los siguientes datos.

```
#!/bin/sh
iptables -A INPUT -i vmbr0 -j ACCEPT
iptables -A OUTPUT -o vmbr0 -j ACCEPT
iptables -A FORWARD -j ACCEPT -p all -s 0/0 -i vmbr0
iptables -A FORWARD -j ACCEPT -p all -s 0/0 -o vmbr0
```

Y reiniciamos CSF con `csf -ra`

Ahora el tráfico funcionará hacia los hosts.

VPS KVM

Centos 7

De momento solo he migrado dos máquinas con Centos 7, más adelante pondré los datos de máquinas con modelo Ubuntu y Debian.

```
cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=none
IPADDR=BLOQUE_IPS.XXX
NETMASK=255.255.255.255
SCOPE="peer IP_SERVIDOR_PROXMOX"
IPV6INIT=no
GATEWAY=peer IP_SERVIDOR_PROXMOX
```

Nota importante

Tras dos problemas con sod VPS, he encontrado que esta configuración sólo funciona usando NetworkManager. (fecha: 26/02/2023). Espero el lunes o martes tener una respuesta distinta, ya que el NetworkManager no debe estar activo con el peso de cPanel.

El problema reside en que no levanta la tabla de rutas de forma correcta, por lo que no hay enrutamiento correcto hacia internet

Importante revisar por si venimos de algún proveedor con otro sistema, que no tengan algún fichero de rutas especificado de su despliegue.

Lecturas por si acaso

Por ejemplo si usas un Centos 6 que teneia el sistema udev antiguo, y cargaba las tarejtas de red con su mac

- [Change Network Interface Name: eth0,eth1,eth2+](#)

Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

Desactivar los mensajes de log en la consola (Proxmox)

Introducción

Una de las cosas que hago al comenzar con una nueva máquina de Proxmox, es desactivar la redirección de los mensajes de kernel log hacia la consola virtual. Es una pesadilla si te olvidas de hacerlo, pues el próximo día que necesites acceder a tu servidor Proxmox, vía KVM a distancia (no la con sola de Proxmox si no la de OVH por ejemplo, la de Hetzner) sufrirás la continua emisión de logs a la consola virtual, lo cual hace muchas veces imposible el trabajo en la consola.

Solución para desactivar los mensajes del log en la consola virtual

/etc/sysctl.conf

Bien como Proxmox se ejecuta sobre una Debian, edita el fichero `/etc/sysctl.conf` y dejalo como esta aquí debajo:

```
# Uncomment the following to stop low-level messages on console
kernel.printk = 3 3 3 3
```

No necesitas hacer un restart si no quieres.

Puedes activar la configuración como siempre que modificas ese fichero con:

```
sudo sysctl -p
```

Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).