

Modo Rescue pro

Introducción

Existen tres modos de rescate OVH : el modo vkvm, el modo win-rescue y el modo rescue pro.

El Modo Rescue pro está pensado para acceder a sus discos duros. Le permite acceder a ellos y también verificar el hardware de su servidor.

La ventaja es que no necesita programar una intervención, abrir un ticket o llamar para realizarlo, ya que con el Manager puede realizar sus tests en todo momento, cuando le convenga y cause las menos molestias a la utilización de su servidor.

Software & Administración

- lanzar un **fsck / e2fsck**
- consultar y analizar los **logs**
- **corregir** los problemas de software
- **reconstruir / verificar** le RAID
- **salv guarda** de datos

Hardware

- **memtest**: para controlar la memoria (RAM)
- **cpuburn**: para verificar el procesador (CPU)
- **fsck** : para chequear el sistema de ficheros
- **state** para chequear el disco
- **explorer** : para consultar/modificar ficheros

En esta guía explicamos el uso del modo Rescue PRO de las dos formas

- A través de la interfaz (Check de hardware)
- A través de SSH (Conexión a su servidor)

¡ATENCIÓN!

Los códigos de acceso al modo de rescate rescue-pro serán enviados por email al contacto administrador. Esta dirección de email no debe encontrarse en el servidor que va a poner en modo de rescate.

Si no le es posible cambiar esa dirección, una copia del mensaje estará disponible en su espacio de cliente (en la sección Administración -> Mis parámetros -> Histórico de emails) y podrá consultarla a través del Manager v3.

Inicio en modo Rescue Pro

Hay diferentes formas de que su servidor arranque en modo Rescue pro :

- Solicitándolo usted mismo desde el Manager v3
- A través de una intervención del departamento técnico
- A través del sistema de monitoring

- En el primer caso es usted quien decide cuándo se inicia el servidor directamente a través del Manager v3.
- En el segundo caso, se trata de una intervención programada mediante un ticket de incidencia a través del Manager v3, posiblemente debido a un fallo del sistema de red
- En el tercer caso, se trata de una alerta de monitoring (fallo de ping) cuya causa no es un fallo de hardware. El técnico ha dejado su servidor en modo Rescue pro para que usted corrija el error.

Arranque en modo rescue

A través del Manager

Para iniciar su servidor en modo de Rescate, puede dirigirse a su espacio **Manager** en la sección de **Servidor dedicado**.

Haga click en la sección *Servicios*

Servicios

Encontrará la opción *Seleccionar Netboot* en la rúbrica **Netboot**

Seleccionar Netboot

Aparecerá el menu que permite elegir la forma de arrancar la máquina.

En el servicio de Netboot puede escoger el '*modo rescue pro*' y reinicie el servidor.

ATENCIÓN !/:

Una vez seleccionado el Netboot que desea arrancar en su Manager, puede iniciar su máquina en *soft* a través de ssh:

```
#!/sbin/reboot
```

O a través del panel de control (Webmin, Plesk, etc...)

Reinicie en modo HARD **SÓLO si no tiene otra alternativa**

Una vez reiniciado su servidor, recibirá en su correo de administrador la contraseña que le permitirá acceder a su servidor en modo 'rescue'.

Consulte la guía NetBoot si necesita más información.

Por una intervención

Puede ocurrir igualmente, que uno de nuestros técnicos haya intervenido en su servidor.

Si no se ha podido establecer la causa de fallo del servidor, principalmente por ser un fallo de su configuración personal, el técnico le dejará en modo 'rescue' para que usted pueda intervenir más fácilmente sobre él y corregir los problemas antes de volver a ponerlo en línea.

Es posible que nuestros técnicos hayan encontrado su máquina arrancada y hayan seleccionado el modo rescue de manera automática para que usted intervenga en él.

Después de solucionar el fallo, no se olvide, antes de reiniciar, de volver a seleccionar un modo de arranque habitual.

Check de Hardware

Una vez que su servidor pasa en modo Rescue, recibirá un email que contiene un enlace y una contraseña para conectarse al test de hardware.

Una vez introducida aparecerá la interfaz de chequeo de hardware :

Si uno de los test falla o muestra errores, basta con dirigirse al Manager, sección de Soporte y hacer clic en la parte : Declarar un incidente.

Ponga simplemente el resultado del test incorrecto, por ejemplo :

El servidor se ha colgado durante el cpu burn.

Intervendremos de inmediato para reemplazar su hardware.

ATENCIÓN !/: : No es posible utilizar el interfaz **WEB** y el **SSH** al mismo tiempo. No se deben lanzar de checks de disco en la interfaz web y montar en SSH las particiones. Esto puede causar pérdida de datos.

Lista de checks

- **Hard Drives:** le permite ver los discos instalados
- **Processors:** hace un check de la CPU. En este check, es posible que no tenga el resultado del check, sino que el servidor se cuelga o se reinicia. Es signo de que hay un problema, debe comunicárnoslo de inmediato.
- **Partitions State:** verifica el disco
- **Partitions File System:** verifica el sistema de ficheros A menudo una inconsistencia del sistema de ficheros se confunde con un disco duro defectuoso. En este caso, basta con reinstalar el sistema operativo para que todo vuelva a funcionar. Sobre todo, en el caso que el servidor ponga ficheros en el directorio lost+found
- **Partitions Explore:** que permite explorar los ficheros. No vamos a poder editarlos a través de esta utilidad, pero podremos guardar una copia, por ejemplo.
Importante : podemos leer los logs de la máquina sin ir forzosamente en SSH
- **Memory:** verifica la memoria RAM Tenga en cuenta que un memtest lleva mucho tiempo y consume mucha CPU. Si el test se cuelga o la máquina se reinicia, es posible que la CPU esté defectuosa. Si el fallo es de la RAM, debería poder llegar al final del test y obtener un informe que contiene los errores encontrados.

Todos los problemas no pueden detectarse por esta interfaz. Como por ejemplo, los reboots irregulares, etc.

No dude en realizar el test y consultar al soporte técnico para que pueda ayudarle a analizar el servidor.

ATENCIÓN !/!:

Si realiza un test de RAM, posiblemente encuentre un error hacia el 64 % del test de la RAM:

your server hasn't reacted for a least 20 seconds. it is probably down you can try to refresh the page if the

server crashed while doing a cpu test. it is possible that the cpu is faulty.

Puede hacer clic en **OK**. A menudo es porque la prueba que se ejecuta hacia el 64% es muy larga.

Conexión a su máquina

Conéctese en SSH a su máquina una vez haya arrancado en modo de rescate y haya recibido los códigos:

```
user:~$ ssh root@nsXXXXXX.ovh.net
The authenticity of host '213.186.xx.yy (213.186.xx.yy)' can't be
established.
RSA key fingerprint is 02:11:f2:db:ad:42:86:de:f3:10:9a:fa:41:2d:09:77.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '213.186.xx.yy' (RSA) to the list of known
hosts.
Password:

rescue:~#
```

Montar los discos duros

Ahora está conectado pero sus ficheros no están accesibles. Hace falta 'montar' el sistema de ficheros :

Normalmente dependiendo del sistema (IDE, SATA, SCSI, RAID) el disco principal se llamará :

- /dev/nfs para RPS
- /dev/sd para SCSI, SATA, Raid Hard
- /dev/hd para los discos IDE
- /dev/md para los RAID Soft
- /dev/rd/c0d0p para los raid Mylex

Puede igualmente utilizar los denominadores devfs.

¿Cómo saber el tipo de disco?

Si no sabe qué disco tiene, ni cuál es su tabla de partición, puede utilizar los comandos **fdisk** o **sfdisk** para averiguarlo. He aquí un ejemplo del comando y lo que devuelve:

```
rescue:~# fdisk -l
```

Disk /dev/hda 40.0 GB, 40020664320 bytes
 255 heads, 63 sectors/track, 4865 cylinders
 Units = cylinders of 16065 * 512 = 8225280 bytes

```
Device Boot Start End Blocks Id System
/dev/hda1 * 1 1305 10482381 83 Linux
/dev/hda2 1306 4800 28073587+ 83 Linux
```

```
/dev/hda3 4801 4865 522112+ 82 Linux swap / Solaris
```

Disk /dev/sda 8254 MB, 8254390272 bytes
 16 heads, 32 sectors/track, 31488 cylinders
 Units = cylinders of 512 * 512 = 262144 bytes

```
Device Boot Start End Blocks Id System
/dev/sda1 1 31488 8060912 c W95 FAT32 (LBA)
```

Aquí el servidor está equipado de dos discos:
 Primero, el disco /dev/hda con el asterisco (*) que indica que es arrancable.
 Luego, el disco USB.

Para montar su sistema de archivos basta con hacer:

```
rescue:~# mount /dev/hda1 /mnt/
```

¿Cómo saber las particiones de disco?

Normalmente la partición de datos de Linux está en la segunda partición del disco (en ese caso /dev/hda2).

La partición de datos generalmente se monta en **/home** para la mayoría de distribuciones Linux.

Montamos la partición de datos después de montar el sistema la partición de sistema con el comando :

Nota : La partición /home no tiene que ser forzosamente la partición de datos, también puede que sus datos estén en /var, por ejemplo en las distribuciones Linux–Plesk?.

Para estar seguro de su tabla de particiones de su sistema Linux, después de montar la partición principal, deberá ejecutar el comando :

```
# cat /mnt/etc/fstab
```

Este fichero contiene las particiones del servidor que se cargan al arrancar. He aquí un ejemplo :

```
rescue:# cat /mnt/etc/fstab
```

```
1.
/dev/hda1 / ext3 errors=remount-ro 0 1
/dev/hda2 /var ext3 defaults,usrquota,grpquota 1 2
/dev/hda3 swap swap defaults 0 0
/dev/devpts /dev/pts devpts gid=5,mode=620 0 0
/dev/shm /dev/shm tmpfs defaults 0 0
/dev/proc /proc proc defaults 0 0
/dev/sys /sys sysfs defaults 0 0
```

En este ejemplo se puede ver que la partición de datos /dev/hda2 se debe montar en **/var** y no en /home; posiblemente se trate de un sistema Linux-Plesk?.

En este caso, debe montar la partición con el comando :

```
rescue:~# mount /dev/hda2 /mnt/var
```

En caso de que aparezca /home en la lista, montamos normalmente la partición, es decir en /home con el comando :

```
rescue:~# mount /dev/hda2 /mnt/home
```

Ejemplos de montaje

A continuación damos unos ejemplos para montar los discos duros de varios servidores.

Habitualmente la primera partición, /dev/XXX1 es su partición raíz [/] y la segunda partición /dev/XXXX2 corresponde a sus cuentas de usuario [**/home**].

1. Montaje de discos en RPS

Para los RPS que están en modo NFS, basta con introducir el comando :

```
rescue:~# mount -a
```

Los discos de la SAN (iSCSI/NFS) se montarán a continuación.

2. Montaje de discos en IDE

Para un disco IDE normal :

```
rescue:~# mount /dev/hda1 /mnt/  
rescue:~# mount /dev/hda2 /mnt/home/
```

3. Montaje de discos en RAID

Para un disco RAID :

```
rescue:~# mount /dev/md1 /mnt/  
rescue:~# mount /dev/md2 /mnt/home/
```

4. Montaje de discos en SAS/SATA

Para un disco SAS o SATA :

```
rescue:~# mount /dev/sda1 /mnt/  
rescue:~# mount /dev/sda2 /mnt/home/
```

5. Montaje de discos en LVM

Para un disco con volúmenes lógicos LVM :

```
rescue:~# vgscan  
Reading all physical volumes. This may take a while...  
Found volume group "VolGroup" using metadata type lvm2  
  
rescue:~# vgchange -a y VolGroup  
[make VolGroup available]  
  
rescue:~# lvdisplay  
--- Logical volume ---  
LV Name      /dev/VolGroup/LogVol01  
VG Name      VolGroup  
  
rescue:~# mount /dev/VolGroup/LogVol01 /mnt/
```

Chroot

Una vez montados los discos, podemos editar los ficheros utilizando el camino `/mnt/var/...` por ejemplo el fichero `/mnt/etc/lilo.conf`.

En algunas ocasiones sin embargo es necesario hace falta estar en root sobre el sistema que se encuentra instalado en el disco y no es posible con el root del rescue.

Para estas operaciones hace falta utilizar el comando **chroot**:

```
rescue:~# chroot /mnt/  
rescue:/#
```

Vemos que después de hacer un chroot, el retorno del comando coloca la / del servidor en el disco duro. Ahora se pueden ejecutar comandos directamente en el sistema del disco.

Ejemplos de uso del modo SSH

Cambiar la contraseña root Linux

Si ha perdido la contraseña root, es posible cambiarla a través del modo rescue :

```
# chroot /mnt/  
#  
# passwd
```

Corrección de datos de disco

Podemos igualmente modificar ficheros de configuración del disco duro.

Tomamos el ejemplo de `/etc/fstab` suponiendo que, en nuestro caso, haya sido el culpable de la indisponibilidad del servidor.

```
# chroot /mnt/  
#  
# cd /etc  
# ls
```

Esto nos sitúa en el directorio `/etc` del disco duro. Con el comando `ls` podremos ver los ficheros del directorio y ver si `fstab` está disponible.

En caso afirmativo, procedemos a editarlo con el editor de textos nano :

```
# nano fstab
```

Basta con corregir los datos del fichero y salvarlos con `<Ctrl> + x` y aceptar con `"Y" o "S" + <ENTER>`.

Ejemplo de backup de datos por FTP

Si lo desea puede realizar un backup de los datos antes de hacer cualquier modificación o reinstalación del sistema.

- Si utiliza un servidor Linux siga la guía [Release2Rescue](#)
- Si utiliza un servidor Windows siga la guía [WindowsRescue](#)

Instalar la SSH key de OVH

Es posible instalar la SSH key de OVH en el servidor principal desde el modo Rescue. Para ello ejecute los comandos siguientes:

```
# chroot /mnt/  
#  
# wget ftp://ftp.ovh.net/made-in-ovh/cle-ssh-public/installer_la_cle.sh  
-O keyInstaler.sh  
# sh keyInstaler.sh
```

Test de la conexión Vrack a través de SSH

Nota: Esta verificación es posible hacerla únicamente en modo SSH contra un Vrack definido en el Manager desde un servidor con tarjeta de red Gigabit Ethernet.

Para verificar la conexión con el Vrack, basta con configurar la tarjeta Gigabit Ethernet con el número del VRACK a través del comando *vconfig* y hacer ping a la pasarela 172.31.255.254.

```
# vconfig add eth0 XXXX  
  
# ifconfig eth0.XXXX 172.16.0.1 netmask 255.240.0.0  
  
# ping 172.31.255.254  
PING 172.31.255.254 (172.31.255.254) 56(84) bytes of data.  
64 bytes from 172.31.255.254: icmp_seq=1 ttl=61 time=0.386 ms  
64 bytes from 172.31.255.254: icmp_seq=2 ttl=61 time=0.367 ms  
64 bytes from 172.31.255.254: icmp_seq=3 ttl=61 time=0.351 ms
```

3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.351/0.368/0.386/0.014 ms

Sustituyendo el valor **XXXX** por el número de VRACK que tenga asignado.

Otros ejemplos

Hay más ejemplos con más posibilidades de rescate en proceso de redacción.
En breve le daremos una pequeña lista con las manipulaciones más solicitadas.

Salir del modo Rescue

Después de realizar las modificaciones y correcciones, debe volver al Manager v3 para seleccionar en **Netboot** el modo de arranque habitual.

Nota: Los RPS no aceptan el modo de Netboot en **disco duro HD**, debe seleccionar el modo **linux 2.6** que tuviera el servidor previamente

Consulte la guía NetBoot

Una vez que haya seleccionado el modo y haya validado la opción, realice un reinicio SOFT de la máquina:

```
rescue:~# /sbin/reboot
Broadcast message from root (pts/0) (Tue Apr 12 15:56:17 2005):
The system is going down for reboot NOW!
```

Conclusión

Si se respetan las reglas básicas de administración, como se explican en la guía AdministracionBasica, podrá recuperar en todo momento su servidor y reducir al mínimo el tiempo de indisponibilidad.

Más información

- : NetBoot:: ¿Cómo seleccionar un kernel mediante Netboot?
- : RebootDeLaMaquina :: ¿Cómo puedo reinicializar mi servidor?
- : AdministracionBasica :: Administración de un servidor dedicado.
- : ServidorHackee :: Cuando el servidor sufre el ataque de un hacker.
- : ServidorSemiHackeado :: Una máquina atacada con un daño "reparable".
- : ModoWinRescue :: Rescate en modo Rescue Win-PE
- : ModoKvm :: Rescate en modo KVM