

# Monitorización de un servidor dedicado

## Introducción

Todos los servidores de nuestros clientes, así como el conjunto de la red son supervisados 24 horas al día por los equipos técnicos de OVH.

Los técnicos de OVH intervienen en cuanto se produce una alerta (no respuesta a un ping) con el fin de limitar al máximo el tiempo de indisponibilidad de los servidores y de la red.

Si es necesario, reiniciaremos la máquina y le haremos llegar un diagnóstico del incidente a fin de que pueda tomar las medidas necesarias para evitar toda avería de ese tipo en el futuro.

## Estado de perturbación

En caso de fallo de un servidor (no respuesta a PING) salta una alerta de monitoring para que un técnico se haga cargo del servidor y determine la causa del fallo.

Durante ese tiempo que el técnico está interviniendo el servidor está en "**estado de perturbación**".

Mientras un técnico examina y repara su máquina, no podrá reiniciar el servidor, reinstalarlo, acceder a él... hasta que el técnico termine completamente su intervención y cierre el estado de perturbación.

## Paso a modo Rescue

Si el técnico determina que es un error de administración y/o configuración y por esta causa, el servidor no puede iniciarse, dejará el servidor en modo Rescue pro o en modo Kvm para que usted pueda corregir el fallo.

Para más información consulte el cuadro de intervenciones en la última parte de esta guía.

## Monitorización de servicios

La monitorización de servicios le permite controlar adicionalmente al PING (ICMP) del servidor, diferentes puertos que deben permanecer abiertos y responder en todo momento.

Este sistema no crea una alerta en el datacenter, ya que no se trata de un error de hardware, pero a cambio usted recibe un mensaje de advertencia en su correo electrónico indicando el fallo del puerto indicado (80-http, 21-ftp, 22-ssh, etc.)

## Modos de funcionamiento

En cada datacenter existe una pantalla gigante con el esquema de la red, la saturación de los enlaces y todos los servidores monitorizados por el sistema de monitoring.

## OVH

Estas pantallas están disponibles en nuestra página web en tiempo real – actualizadas cada 10 segundos.

En caso de fallo del servidor, usted recibirá en la cuenta del administrador del servidor, los emails de aviso de monitoring y de nuestros técnicos, con todos los detalles de la operación.

Esta monitorización se realiza 24 horas al día, todos los días de la semana, incluidos domingos y festivos.

Si su servidor no se encuentra monitorizado por el monitoring, éste no se tiene en cuenta en la pantalla y si falla, nuestros técnicos no podrán intervenir.

– Puede ver la pantalla de monitorización en nuestra página web :

- <http://travaux.ovh.net/vms/index.html>

– Puede ver el estado de nuestra red en nuestra página web :

- <http://weathermap.ovh.net/>

– Puede ver el estado de las latencias en nuestra página web :

- <http://smokeping.ovh.net/ovh-server-statistics/show.cgi?target=Spain>

### Precauciones

Por defecto su servidor viene preparado para estar monitorizado y vigilado por nuestros técnicos. Si modifica la configuración inicial, deberá tomar una serie de medidas y de precauciones para que su servidor sea monitorizado.

Los firewalls y los filtros de tráfico pueden bloquear el sistema de monitorización.

Si no cumple con alguna de estas medidas, su servidor se retirará de la lista de monitoring y dejará de estar vigilado.

### **Servidores y Firewall**

Si instala un Firewall deberá permitir que el tráfico y en particular el tráfico ICMP llegue a su servidor desde los servidores de monitorización.

### **ADVERTENCIA** /!\

Deberá permitir el acceso a los ordenadores de monitorización :

- **ping.ovh.net** – 213.186.33.13
- **cache.ovh.net** – 213.186.50.100
- **proxy.ovh.net** – 213.186.50.98
- **proxy.p19.ovh.net** – 213.186.45.4
- **proxy.rbx.ovh.net** – 213.251.184.9
- **proxy.rbx2.ovh.net** – 91.121.150.4
- **proxy.rbx3.ovh.net** – 91.121.180.2
- **proxy.rbx4.ovh.net** – 46.105.96.3
- **a2.ovh.net** – 213.186.33.62 (Monitoring firewalls ASA)
- **puertos 6100 a 6200 en TCP y UDP (Puertos de comunicación RTM)**

Estos servidores están manipulados por personal técnico de OVH y cuentan con la mayor de las garantías en materia de seguridad.

No debe tomarlo como un fallo de seguridad, más bien todo lo contrario.

Para autorizar el acceso al servidor SLA y tener RTM, debe autorizar la IP de su servidor terminada en **.250** y **.251**, por ejemplo, si su IP es de la forma **aaa.bbb.ccc.ddd**, debe autorizar el acceso a la dirección **aaa.bbb.ccc.250** y **aaa.bbb.ccc.251**.

Deberá permitir el acceso a las direcciones de SLA y MRTG:

- **sla-X.ovh.net** – **aaa.bbb.ccc.250**
- **mrtg-X.ovh.net** – **aaa.bbb.ccc.251**

Siendo la dirección **aaa.bbb.ccc.ddd**, la dirección IP de su servidor.

Más información en nuestra guía FireWall

Alertas de monitoring

Este sistema de alertas le permite realizar una monitorización de su máquina 24/7 con alertas por email o SMS

#### **ATENCIÓN** /!\

Para las alertas SMS debe tener una dirección de email asociada a su teléfono móvil.

Debe solicitar este servicio a su operador telefónico (Movistar, Vodafone, Orange, Yoigo, etc...).

Para gestionar estas alertas y dónde recibirlas debe entrar en el Manager sección de **Servidor dedicado**

Haga click en la sección *Estado del servidor*

### **Estado del servidor**

Encontrará la opción *Monitoring* en la rúbrica **Seguimiento**

### **Monitoring**

En ausencia de una lista de direcciones de correo a los que enviar las alertas de monitorización e intervenciones, se enviarán a los correos administrativo y técnico.

Para añadir una dirección de correo a la lista pulse la opción *Creación*.

### **Creación**

Para una monitorización del servidor 24/7 con alertas por email o SMS, simplemente debe introducir su email y elegir las opciones :

- **Tipo de alerta**
- **Frecuencia de aviso**
- **Número de alertas durante la alerta**
- **Avisar una vez la incidencia esté solucionada**

### **Atención**

Para las alertas SMS debe disponer de una dirección de email de su operador telefónico en su teléfono móvil.

Consulte con su proveedor (Amena, Vodafone, Movistar) sobre la disponibilidad de un correo electrónico asociado a su número de teléfono.

La opción *Alerta SMS* permite reducir al máximo las informaciones transmitidas a fin de que sean visibles directamente en el mensaje de notificación de email que recibe por SMS.

No se trata de un envío de SMS directamente a su móvil.

Para modificar una dirección de correo de la lista pulse la opción *Modificar*

**Modificar**

Para eliminar una dirección de correo de la lista pulse la opción *Eliminar*

**Eliminar**

Desactivación de monitoring

Si va a realizar tareas de mantenimiento puede desactivar momentáneamente el monitoring. Su servidor dejará de estar vigilado por nuestros sistemas todo el tiempo que lo desee.

Para desactivar la monitorización temporalmente pulse la opción *Desactivar*

**Desactivar**

Para reactivar la monitorización después de una desactivación temporal pulse la opción *Activar*

**Activar**

Igualmente, si necesita tener un Firewall muy restrictivo o bien no necesita el sistema de monitorización 24 horas, puede dejar el sistema desactivado totalmente en su servidor permanentemente.

No es recomendable tener desactivado el sistema de monitoring; su servidor no se beneficiará de la vigilancia 24 horas así como de la solución de problemas en los componentes de su servidor y de la garantía SLA hardware.

Intervenciones en el servidor

Hay una serie de intervenciones que se realizan automáticamente a raíz de una alerta de Monitoring.

Generalmente los técnicos sólo realizan intervenciones de nivel 1 (incidencias) en los servidores al tratarse de servidores sin administración (no administrados y no manejados); pero en el caso de ciertos servicios y productos puede ser necesario realizar intervenciones de nivel superior.

En general existen 3 tipos de intervenciones :

**Nivel 1 - Incidencia**

- En caso de fallo de un servidor (no respuesta a PING) un técnico se hará cargo del servidor y determinará la causa del fallo. Si se trata de un fallo de hardware o de conectividad de red, el técnico reemplazará la pieza o el cable de red afectado.

**Nivel 2 - Asistencia**

## OVH

- Si se trata de un fallo en la manipulación del sistema o fallo de configuración, el soporte de asistencia le indicará los pasos a seguir para corregir el problema y en su caso, le indicará una guía paso a paso.

### **Nivel 3 - Infogerencia**

- En caso de un fallo de configuración grave o una manipulación indebida que precisa tareas de administración, se trata de un problema de nivel 3 (infogerencia) y no puede ser corregido por nuestros técnicos.

Si tiene cualquier problema no dude en contactar con el soporte que podrá orientarle en la resolución del problema o bien proponerle una infogerencia para un problema de nivel 3.

– Consulte la guía sobre niveles de soporte : NivelesSoporte

Niveles de las intervenciones

### **Nivel 1 : Incidencia**

Los fallos de sobrecarga y fallos de componentes hardware (incidencias de nivel 1) se tratan directamente por los técnicos de OVH presentes en el datacenter, el soporte de incidencia.

En caso de fallo de un servidor en el monitoring (no respuesta a PING), un técnico se hará cargo del servidor y determinará la causa del fallo.

- Si el servidor funciona (respuesta a PING, resto de puertos abiertos) el técnico cerrará la incidencia.
- Si el servidor está en línea pero el fallo de ping se debe a un firewall, se desactivará el monitoring para el servidor.
- Si es un fallo durante el proceso de reinstalación del sistema , reiniciará la instalación de nuevo.
  
- Si determina que existe fallo de hardware (pieza material) , cambiará la pieza afectada.
- Si determina que hay un fallo de software (sobrecarga, sistema colgado) , intentará resetear el servidor.
- Si se trata de un fallo de la red, reparará el cable, switch o router que afecte a la conectividad.
  
- En cualquier otro caso, el fallo de ping se debe a un error de software.

Si el técnico, después de todos los intentos, no consigue reiniciar el servidor y el fallo es de software, (fallo de configuración de red, fallo de sistema operativo, ficheros corruptos), dejará el servidor en modo de rescate y mandará un email de aviso para que el cliente corrija el problema. La incidencia pasa a ser de nivel 2.

En total, su servidor no estará nunca inaccesible más del tiempo máximo SLA garantizado (1 hora, 2 horas, 4

horas dependiendo del modelo de servidor) por una incidencia de nivel 1/2.

Si por cualquier razón este periodo garantizado se sobrepasara, OVH se compromete a devolverle una parte de la mensualidad del servidor proporcional al tiempo rebasado, según los términos de la garantía SLA.

### **Nivel 2 : Asistencia**

Si el posible fallo del servidor no provoca un fallo de ping y/o no está provocado por un fallo de hardware, se considera un fallo de nivel 2 y debe tratarse por el soporte de nivel 2 o soporte de asistencia.

El soporte de nivel 2 le ayudará a poner su máquina en funcionamiento lo antes posible utilizando las utilidades de recuperación y las guías. También le ayudará a reparar los elementos lógicos que pudieran estar dañados (particiones, ficheros de configuración, ficheros de sistema...)

El soporte de asistencia le indicará las guías a seguir, cómo utilizar los modos de rescate (Rescue-pro, Winrescue, vKVM), el panel de control Manager (Reboot, Netboot) y en su caso, si tiene backups semanales/incrementales, cómo restaurar la información.

Si el fallo no puede ser recuperado dentro de los usos especificados en las guías, la incidencia pasa a ser de nivel 3.

### **Nivel 3 : Infogerencia**

Los fallos de configuración, administración y de sistema por manipulación se engloban en la categoría de nivel 3. Normalmente para corregir estos problemas es necesario tocar la configuración de la máquina de forma intensiva.

Estas intervenciones dependen de la configuración de la máquina, de las operaciones previas realizadas y de los elementos instalados. Se consideran altamente delicadas y no pueden realizarse por los técnicos de OVH, sino por el administrador del servidor (usted).

Para ello cuenta con los modos de rescate que permiten acceder a la configuración del servidor y modificarla si es necesario :

- Modo de rescate Rescue PRO : ModoRescue
- Modo de rescate vKVM : ModoKvm

En último término, cuenta con un modo de recuperación de datos y de reinstalación del sistema, si viera que no hay ningún modo de recuperar el control del servidor (fallo lógico o de sistema muy grave, entrada con hack al sistema, ficheros perdidos o corruptos, etc...)

- Reinstalar el sistema : ReinstalarServidor

Si tiene cualquier problema no dude en contactar con el soporte de nivel 2 que podrá orientarle en la resolución del problema o bien proponerle una infogerencia de nivel 3.

Más allá de la monitorización

Monitorización de un servidor dedicado

## **RealTimeMonitoring**

Para que su servidor Linux sea monitorizado de manera más avanzada y el técnico pueda tener una serie de datos más precisos sin necesidad de solicitarle el acceso al servidor, puede utilizar nuestra utilidad Real Time Monitoring.

Esta utilidad le proporcionará a nuestros técnicos, información sobre su servidor en caso de fallo y facilitará su labor para reducir el tiempo de indisponibilidad al mínimo.

Consulte la guía sobre RTM : RealTimeMonitoring

## **Servicio de infogerencia de OVH**

En el caso de un servicio no administrado, las intervenciones de nivel 3 no pueden ser tratadas por los técnicos de OVH, ya que se trata de problemas de administración.

De todos modos, si necesita ayuda y desea que nuestros administradores intervengan en su servidor en caso de que se produzca un error de nivel 3, puede solicitar una infogerencia.

Más información en la guía : InfoGerencia

Para que un administrador pueda acceder a su máquina, deberá instalar nuestra llave SSH y permitir el acceso al usuario **root** mediante SSH en el puerto 22, tal y como se entrega el SSH por defecto.

Si ha cambiado el puerto de SSH deberá indicar el nuevo puerto. Si ha bloqueado el acceso root al SSH, deberá indicar un usuario de SSH válido junto con su contraseña.

Por regla general, tanto la llave SSH y como acceso root por SSH vienen instalados y habilitados por defecto en las distribuciones de Linux listas para su uso.

Consulte la guía sobre la Llave SSH : InstalarLlaveOVH

Más información

: InstalarLlaveOVH :: ¿Como instalar la clave SSH OVH para que podamos intervenir en su servidor?  
: RealTimeMonitoring :: Todo sobre la monitorizacion RTM de OVH

: NivelesSoporte :: Niveles de soporte en OVH  
: RecuperarDatosBackup :: Como recuperar los datos del backup.  
: RebootDeLaMaquina :: ¿Cómo puedo reinicializar mi servidor?