

# Real Time Monitoring (RTM)

## Introducción

Para monitorizar un alto número de servidores de manera precisa, OVH ha desarrollado su propia utilidad de monitorización denominada RTM.

RTM trata varios datos técnicos de su servidor (rendimiento, utilización, fallos de seguridad, actualizaciones), los procesa, los almacena y los proporciona en diferentes formas.

Como RTM es un cliente muy ligero, no falsifica con su funcionamiento las estadísticas que proporciona, al contrario de otros sistemas (SNMP, MRTG,...) que consumen muchos recursos de CPU y aumentan la carga de la máquina con su propio funcionamiento.

## Modos de funcionamiento

El funcionamiento de RTM es extremadamente simple y muy seguro:

- En cada servidor dedicado, se ejecuta un cliente RTM cada 60 segundos
- El cliente envía en UDP varios datos sobre el funcionamiento de la máquina
- Los datos se recuperan en nuestro servidor central RTM.

Estos datos sobre el funcionamiento del servidor se proporcionan a los técnicos de OVH en caso de una intervención de nivel 1 o de nivel 2, lo que les permite localizar los fallos de manera más precisa.

Además de proporcionar esta información en las intervenciones, los datos de RTM se utilizan en varias utilidades de alerta y se presentan en varios sitios :

- \* Servidor SOAP / WSDL
- \* Manager - sección RTM
- \* Alertas de email sobre el mal funcionamiento de la máquina / fallos hardware
- \* Alertas de email acerca de puertas traseras instaladas por hackers
- \* Utilidades internas OVH, que permiten al soporte de asistencias ayudarle en una consulta

## 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.

## **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.

Estos servidores son :

- **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)**

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.

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.

Más información en nuestra guía FireWall

¿ Mi servidor está monitorizado por RTM ?

Para saber si su servidor está monitorizado con RTM debe entrar en el Manager y seleccione el servidor que desea comprobar.

Haga click en la sección *Estado del servidor*

### **Estado del servidor**

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

### **Real Time Monitoring**

Allí encontrará todos los datos que almacena el servidor RTM y que, en caso de fallo, serán facilitados a nuestros técnicos presentes 24 horas en el datacenter para solucionar cualquier fallo.

### Instalación en Linux

La instalación descrita a continuación para el servicio RTM es únicamente compatible con los sistemas Linux.

Si su distribución de Linux es una distribución de base (Debian, Fedora, etc), puede instalar la utilidad de manera muy sencilla en dos pasos.

### **Procedimiento**

1 - Conéctese a su servidor en SSH con el superusuario **root**.

2 - Ejecute dos sencillas órdenes :

```
# wget ftp://ftp.ovh.net/made-in-ovh/rtm/install_rtm.sh -O install_rtm.sh
# sh install_rtm.sh
```

**Nota:** RTM depende de 2 programas / paquetes externos.

- **hddtemp** permite saber la temperatura de un disco duro IDE
- **dmidecode** permite tener información sobre la placa base, la memoria utilizada...

Instalar RTM bajo Windows

Debe previamente instalar Activeperl siguiendo el enlace :  
<http://www.activestate.com/activeperl/>

A continuación descargue la última versión de RTM en el enlace :  
<ftp://ftp.ovh.net/made-in-ovh/rtm/windows/>

Proceda a la instalación como administrador. Para ello haga clic con el botón derecho en el fichero de instalación y seleccione la opción "Ejecutar como administrador"

### Algunos ejemplos de los informes RTM

- Ejemplo 1

```
Backdoor/Hacks detection  
status: 6
```

```
port: 8146  
procname 8146  
pid 31157  
uid vpopmail  
status 5  
cmdline ./8146  
exe /dev/shm/8146
```

```
port: 1144  
procname 8146  
pid 31157  
uid vpopmail  
status 5  
cmdline ./8146  
exe /dev/shm/8146
```

Detección de 2 backdoors en un servidor, debido a un fallo de seguridad en AwStats

- Ejemplo 2

**Placa base / CPU**  
Manufacture:

## OVH

Model: P4M266A-8235?  
CPU: Intel(R) Pentium(R) 4 CPU 3.06GHz  
Speed: 3073 MHz

### **memoria RAM**

Pos 1: 512 MB  
Pos 2: 512 MB  
Pos 3:  
Pos 4:

### **discos duros**

Model: Maxtor 6E040L0  
Size: 41 GB  
Smart: 446  
Status: ERROR

Un disco duro que muestra debilidad, probablemente fallará en varios días/horas

### **Intervenciones en el servidor**

Aunque el servidor está monitorizado las 24 horas y los técnicos corrigen en tiempo real la mayoría de problemas, existen varios niveles de intervención dentro del monitoring :

#### **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**

- 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.

El monitor RTM ayudará a los técnicos de nivel 1 y nivel 2 en los casos dudosos, a saber varios datos del servidor y así determinar las posibles causas del fallo (disco duro lleno, error de disco, sobrecarga del servidor...)

## OVH

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
- Consulte la guía sobre la monitorización : ServidorMonitoring

### Más información

- : InstalarLlaveOVH :: ¿Como instalar la llave SSH OVH para que podamos intervenir en su servidor?
- : ReleasePatchSeguridad :: ¿Como aplicar los patches y las actualizaciones de seguridad?
- : ReactivarLosServicios :: ¿Como reactivar propiamente los servicios?
  
- : ServidorMonitoring :: Como ser advertido cuando se produce una alerta sobre el servidor
- : RecuperarDatosBackup :: Como recuperar los datos del backup.
- : RebootDeLaMaquina :: ¿Cómo puedo reinicializar mi servidor?