

Seguridad en servidores Dedicados

Introducción

En sus servidores dedicados OVH añade una serie de elementos de fabricación propia (creados y verificados por los administradores de OVH) para mejorar la seguridad.

Enumeramos y explicaremos a continuación todos estos elementos :

- Kernel made-in-ovh (con GRsecurity)
- OVH SSH Key
- Real Time Monitoring (RTM)

Nota : Estos elementos vienen en las distribuciones Linux listas para su uso. Si utiliza una distribución Windows o bien una distribución base, puede que le falte alguno de ellos o la totalidad

Kernel made-in-ovh (con GRsecurity)

Constantemente, surgen nuevas actualizaciones para los kernel de Linux, algunas de ellas corrigen fallos importantes de seguridad.

Los administradores de OVH vigilan y prueban cada nueva actualización del kernel. Las actualizaciones críticas que corrigen fallos de seguridad o que mejoran el rendimiento significativamente, se aplican de inmediato (en menos de 6 horas desde su aparición).

Cada vez que surge una nueva versión, los administradores compilan el nuevo kernel en diferentes versiones para los diferentes modelos de servidor. A continuación pasan una batería de pruebas para confirmar su estabilidad y su rendimiento. Si pasan la prueba, el kernel se añade automáticamente al Netboot (seleccionable desde el Manager) y se deja la nueva versión en el repositorio de FTP made-in-ovh.

Los servidores que hayan contratado el servicio de seguridad total, se actualizan a la nueva versión de forma automática (los propios administradores realizan la instalación del nuevo kernel) y el resto puede utilizar el Netboot para usar el nuevo kernel de forma inmediata.

Consulte la guía para más información en NetBoot

Si por el contrario desea instalar el kernel en su disco duro, o bien recompilarlo con sus propios parámetros puede recoger los fuentes en kernel.org y los ficheros de configuración en el FTP de OVH para instalar su propio kernel en su servidor.

OVH

Consulte la guía para más información en [InstalarKernelOVH](#)

OVH SSH Key

Por defecto los servidores llevan una SSH Key que permite al equipo de administradores acceder a su servidor en caso de problemas.

La SSH Key está instalada y activa por defecto, aunque si lo desea puede desactivarla o eliminarla en el fichero de keys SSH :

```
/root/.ssh/known_hosts
```

Si desea que los técnicos de OVH puedan intervenir durante 24 horas en su servidor para solucionar problemas, la SSH key deberá estar activa y el SSHd deberá estar en el puerto 22 con acceso a la cuenta de root. Es decir tal y como se entrega el servidor por defecto.

De lo contrario, si alguna de las condiciones no se cumple, los administradores no entrarán en su máquina y no podrá beneficiarse de intervenciones de infogerencia.

Consulte la guía para más información en [InstalarLlaveOVH](#)

Si lo desea, puede configurar una regla de Firewall/IPtables con la IP de origen para añadir mayor seguridad al puerto 22, manteniendo el acceso a los administradores.

Consulte la guía para más información en [FireWall](#)

Real Time Monitoring (RTM)

Los técnicos del datacenter le aseguran intervenciones básicas (nivel 1 y 2) en su servidor durante las 24 horas del día.

Esto es particularmente útil si su servidor se cuelga o deja de dar ping por una sobrecarga o ataque.

El sistema de monitorización controla la respuesta al PING de su servidor. Si por cualquier razón, va a bloquear el acceso al puerto de PING en su servidor, puede desactivar previamente la monitorización para que los técnicos de OVH no intervengan – se imaginarán que su máquina está bloqueada.

Consulte la guía para más información en [ServidorMonitoring](#)

Gracias al sistema de monitorización en tiempo real (RTM) los técnicos pueden controlar todos los servidores del datacenter desde una pantalla de manera fácil en tiempo real, así como ciertos parámetros de su funcionamiento – los valores de carga, ocupación de disco, rendimiento de memoria, etc..

Estos valores se utilizan para localizar un fallo más eficientemente, en caso de una falta de respuesta a PING, como hemos indicado anteriormente.

El sistema RTM viene por defecto configurado en las distribuciones de Linux. Si lo desea puede instalarlo en el resto de distribuciones de base, siguiendo las instrucciones indicadas en la guía de RTM. Igualmente, si lo desea puede eliminar el programa RTM si estima que ese servicio no va a ser útil.

Consulte nuestra guía RealTimeMonitoring.

Más información

: RealTimeMonitoring ::
: ServidorMonitoring ::

: FireWall ::
: NetBoot ::

: InstalarKernelOVH ::
: InstalarLlaveOVH ::