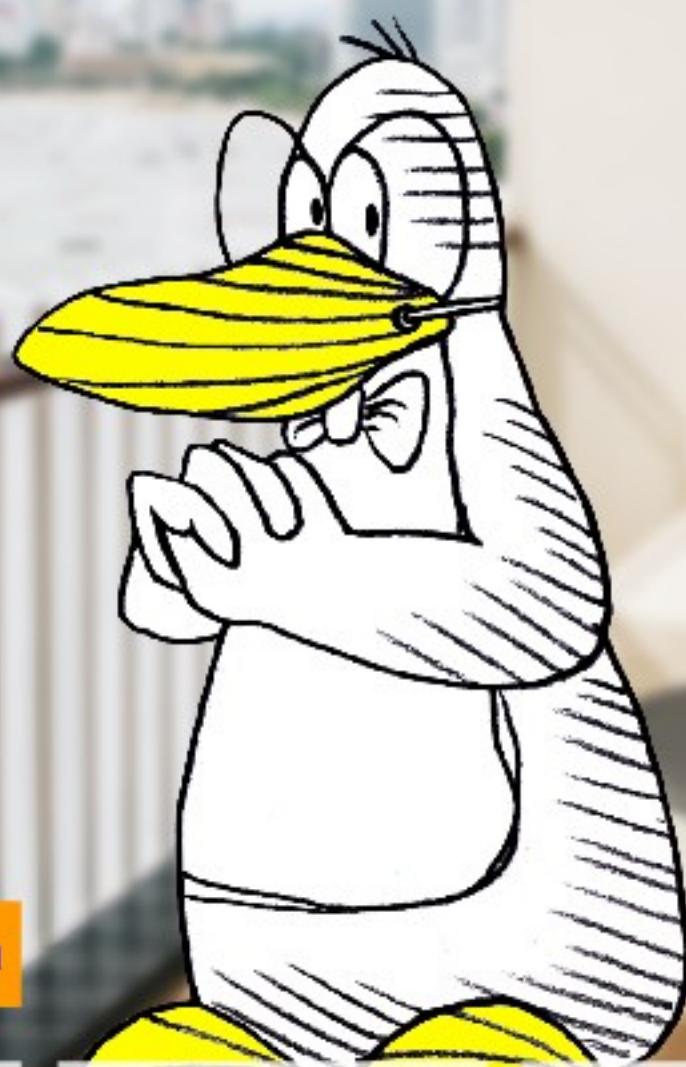


MAGAZINE SOLO LINUX

Nº
14

Tu revista, la revista de tod@s

MARZO 2020



#QuedateEnCasa

Let's Encrypt: Grave alerta de seguridad en sus certificados

Alerta: El navegador Tor ejecuta Javascript en modo seguro

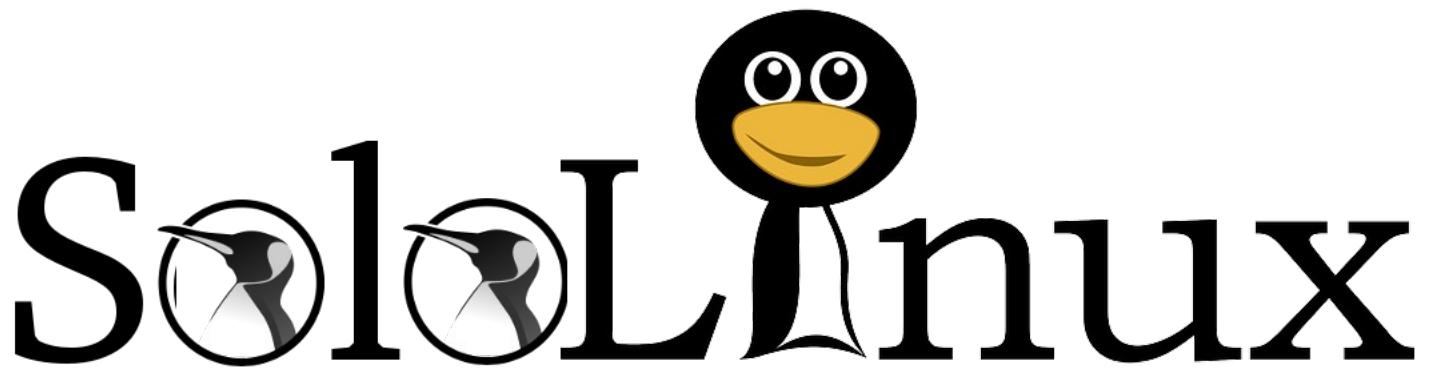
En cuánto tiempo se ejecutan los procesos que más consumen

Cómo limpiar buffers y ram en Linux

Nuevo Wine 5.3 con muchas mejoras y correcciones

Cómo instalar Xtreme Download Manager en Linux

MANUALES, SCRIPTS, SOFTWARE, HARDWARE, DISTROS LINUX, SEGURIDAD, REDES Y MUCHO MAS EN LA WEB...



La revista SOOLINUX esta realizada con Libre Office Impress 6.2.8.



Este obra se publica bajo una
licencia de Creative Commons
Reconocimiento-Compartir-
Igual 4.0 Internacional.

Bienvenido a la Revista SOLOLINUX

Aquí tenemos el numero 14 de la revista SoLoLinux. Gracias a todos los que hacéis posible que esto siga adelante. Desde SOLOLINUX esperamos que os guste este numero.

Igual que en números anteriores nos gustaría animar a todos nuestros lectores para que nos envíen sus **opiniones sobre el Software Libre o sobre GNU/Linux**, pueden enviarlo a adrian@sololinux.es, con ello queremos proponer que cada mes se publicada una o varias de esas opiniones sobre lo mencionado en la nueva sección de la

revista **OPINIÓN DEL LECTOR. Queremos saber la opinión de todos.** Se intentara incluir el máximo de opiniones en cada numero, pero si no sale la tuya este mes no desesperes, al siguiente podría

tener un hueco en la revista. **ANÍMENSE Y ENVÍEN SUS OPINIONES.** Gracias.

Al igual que lo anteriormente mencionado, nos gustaría promover un espacio en la revista sobre los eventos de Software Libre y GNU/Linux en todo el mundo. Los organizadores de estos eventos pueden ponerse en contacto con migo a través de correo electrónico, adrian@sololinux.es

Sin mas **quiero agradecer a todos** los que hacéis posible que esta revista siga adelante.

Personalmente agradezco a Sergio todo su trabajo en la multitud de artículos que realiza a lo largo del mes para que esta revista pueda tener suficiente información mes a mes.

Gracias a TOD@sS

Compartan esta revista en sus redes sociales o web.
Revista digital **SOLOLINUX MAGAZINE**. Tu revista, la revista de todos.



La revista SOLOLINUX
esta realizada con Libre
Office Impress 6.2.8.

Nuestras Webs:

www.sololinux.es
www.solowordpress.es

EDITORIAL

Edición:

- Adrián Almenar
adrian@sololinux.es

Redacción:

- Sergio G. B.
(Administrador y redactor artículos SoloLinux)
info@sololinux.es

- Henry G. R
(Redactor artículos SoloWordPress)
info@solowordpress.es

Agradecimientos:

- Antonio Giuseppe Crobu
(Agradecerte la donación que has realizado)

Publicidad:

Quieres poner publicidad en la revista, ahora puedes hacerlo de forma muy simple, llegando a todo el mundo con esta revista digital de software libre y GNU/Linux en ESPAÑOL

CON SOLOLINUX MULTIPLICARAS TUS CLIENTES

Para mayor información escribe un email a: adrian@sololinux.es

Colabora:

Quieres colaborar en la revista.
Para mayor información escribe un email a: adrian@sololinux.es

La **Revista SOLOLINUX**, se distribuye gratuitamente en forma digital para todo el mundo que quiere disfrutar de ella. Si quieres imprimirla es cosa tuya. Si os cobran por ella, os están timando. :)

Contacto:

Para cualquier consulta sobre las revistas, publicidad o colaboraciones escribir un email a:
adrian@sololinux.es



Este obra se publica bajo una licencia de Creative Commons Reconocimiento-Compartir-Igual 4.0 Internacional.



MANUALES

- 8. Cómo usar el comando echo con ejemplos en Linux
- 17. Cómo convertir un archivo img a un archivo iso en linux
- 18. Uso del comando iostat con ejemplos en linux
- 22. Cómo ejecutar varios comandos en una sola línea
- 24. Transferir archivos de forma segura con el comando scp
- 25. MySQL error en Plesk con linux
- 26. Verificar los servicios que se están ejecutando en linux
- 28. Cómo cambiar la dirección MAC en linux con Macchanger
- 29. Solución al error «E: Could not get lock /var/lib/dpkg/lock»
- 30. Error al establecer la configuración regional a C.UTF-8
- 31. Uso y ejemplos del comando SHUF
- 36. Manual de Htop, la mejor herramienta para monitorizar linux
- 41. Cómo actualizar Manjaro o Arch linux para novatos
- 43. Instalar CyberPanel en Ubuntu 18.04
- 49. Instalar y configurar opcache en php-fpm con Nginx
- 51. Cómo montar un servidor de alto rendimiento con VestaCP
- 53. Cómo optimizar Nginx con PHP-FPM en VestaCP con Centos 7
- 54. Cómo instalar maldet y buscar malware en linux
- 57. Error: Las firmas siguientes no se pudieron verificar GPG
- 59. Instalar y configurar vsFTPD en CentOS y derivados

SEGURIDAD

- 13. Let's Encrypt: Grave alerta de seguridad en sus certificados
- 33. Alerta: El navegador Tor ejecuta Javascript en modo seguro



- 10. Cómo escribir comentarios en bash correctamente.
- 11. Cómo crear bloques multilínea en bash con Heredoc.
- 15. Cuanto tiempo se ejecutan los procesos que más consumen
- 23. Cómo limpiar buffers y ram en linux



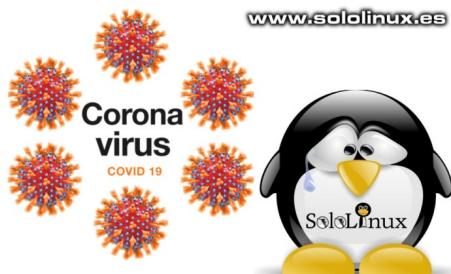
DISTRROS LINUX

- 21. Ubuntu 20.04 LTS listo para que lo pruebes



NOTICIAS

- 45. Cómo afecta el CORONAVIRUS a la tecnología y a linux



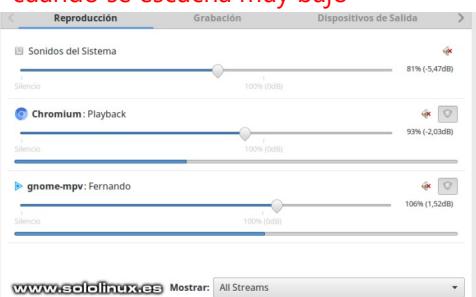
SOFTWARE

- 14. Novedad: nuevo Wine 5.3 con muchas mejoras y correcciones
- 34. Cómo instalar Xtreme Download Manager en linux
- 39. Cómo instalar ONLYOFFICE Community Edition en Ubuntu 18.04
- 42. Cómo instalar Twitter Lite en linux
- 47. Nomacs el visor de imágenes con editor incluido



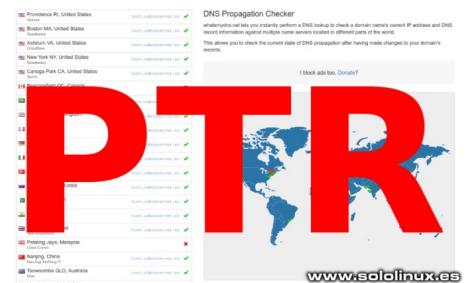
HARDWARE

- 35. Identificar el tipo de raid y si son discos ssd en linux
- 55. No funciona la wifi en Debian después de su instalación
- 61. Cómo subir el volumen en linux cuando se escucha muy bajo



REDES

- 50. Qué es el registro PTR y para qué sirve



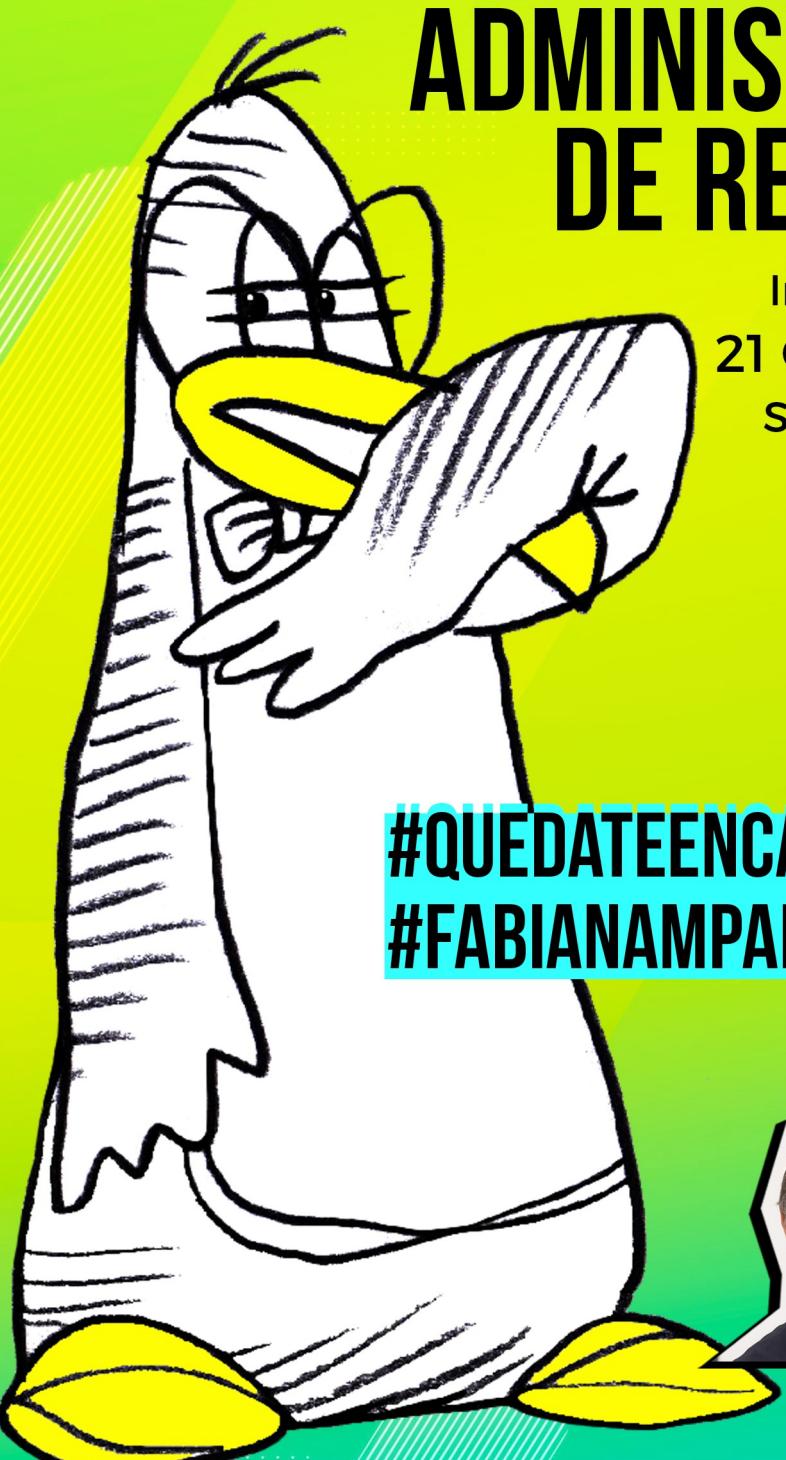
PTR

CURSO 100% ON LINE ADMINISTRADOR DE REDES LINUX

Inicio: 25 de abril del 2020

21 CLASES MAGISTRALES

Sábados 10 a 12 hs. (UTC -3)



#QUEDATEENCASA
#FABIANAMPALIO



PARA ESPAÑA

GRATIS

100% BONIFICADO



TUTOR
FABIÁN AMPALIO

+54 9 11
6969 9993



SEGUINOS EN
Instagram
@fabianampalio

Solowordpress

TU REVISTA SOBRE WORDPRESS

LOS MEJORES PLUGIN DE SEGURIDAD PARA WORDPRESS



WORDPRESS & CSS

GUÍA PARA PRINCIPIANTES DE LA BASE DE DATOS DE WORDPRESS.

CÓMO USAR LA FUNCIÓN
APPLY_SHORTCODES()

+ ADEMÁS

MANUALES
CONSEJOS
TRUCOS

Número 2. Proximamente

Últimas novedades

Trucos

Consejos útiles

Manuales paso a paso

Debates abiertos

Opiniones de expertos

Artículos

¡Si crees que
puedes ayudar contacta
con nosotros!

Solowordpress

Tu revista sobre Wordpress

Solowordpress

Inicio | Contacto

Novedades



WordPress y la Seguridad que no puedes controlar

Recomendado



Cómo hacer un plugin en WordPress

Más vistos



Las Señales de Seguridad

Si el formato digital no te
convence, también tenemos
todo el contenido en una
Página Web

¡Visítanos!

www.solowordpress.es



WordPress y la Seguridad que no puedes controlar



Nueva actualización 5.3.1 La
mayoría de los usuarios de
WordPress nos hemos levantado con la...

Entradas Recientes

WordPress y la Seguridad que no
puede controlar
Nueva actualización 5.3.1
Las Señales de Seguridad
Las señales de seguridad En el
artículo De http a https en
WordPress comentaba que...

VANT

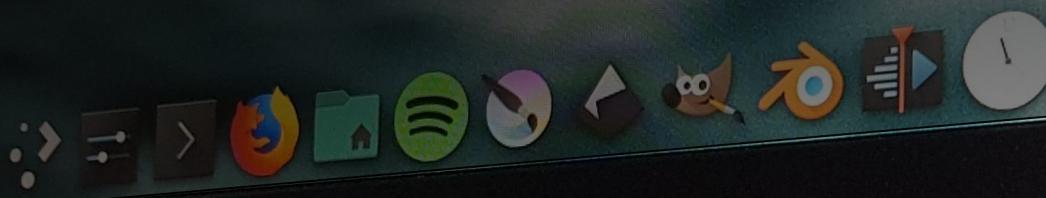
SOMOS LINUXEROS



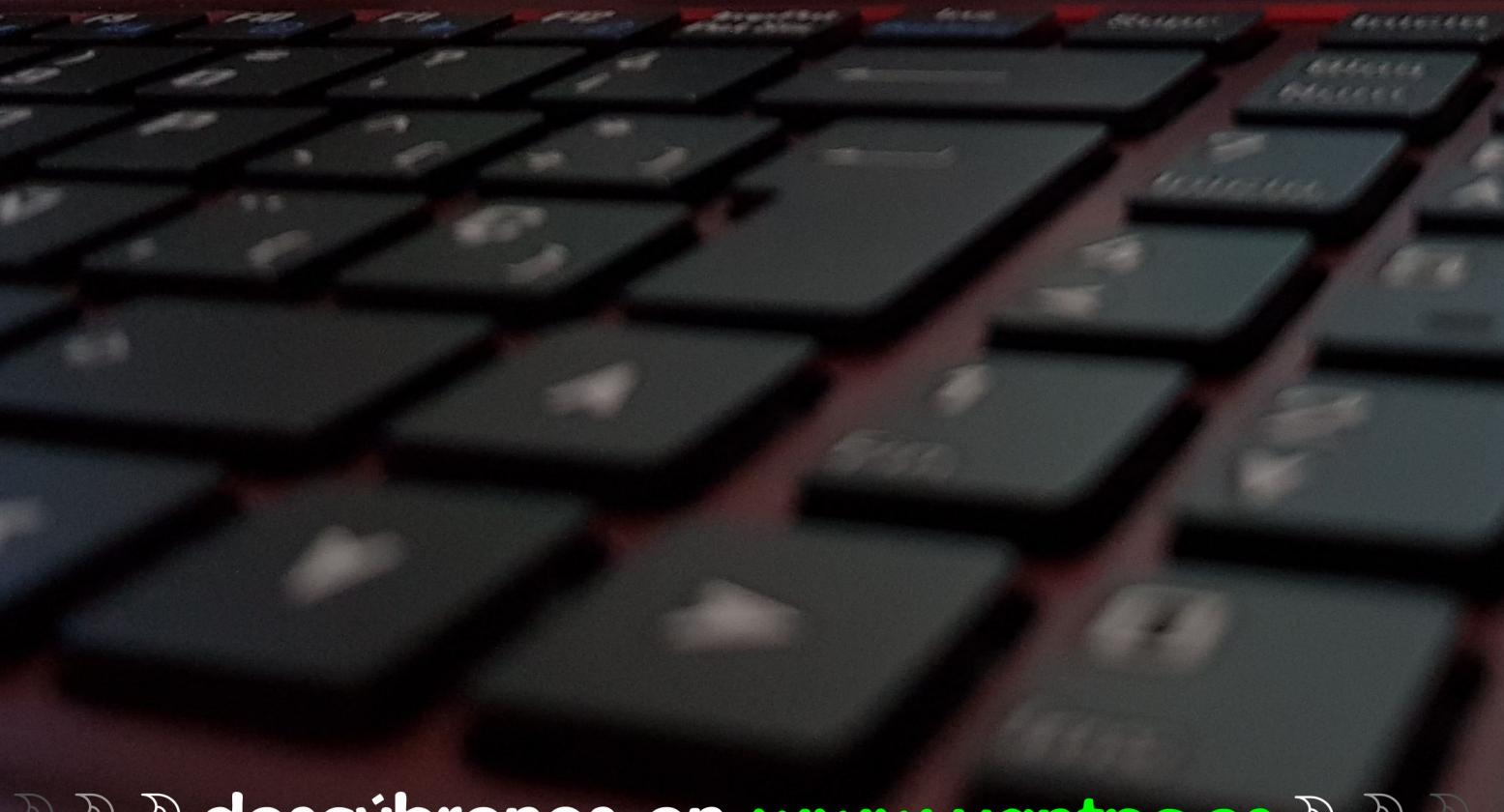
la gama mas completa de ordenadores con GNU/Linux

VEN A LINUX CON TOTAL GARANTÍA

calidad + compatibilidad + soporte + el mejor precio



VANT



descúbrenos en www.vantpc.es

Síguenos para enterarte de todas nuestras noticias, novedades y ofertas



@vantpc



vant.pc



vantpc_es



t.me/vantpc

Cómo usar el comando echo con ejemplos en linux

El **comando echo** es de los más utilizados en shell y **scripts bash**. Este comando tiene como misión imprimir los argumentos definidos con echo en nuestra consola, pueden ser a modo indicativo, informativo o cualquier argumento que necesites visualizar.

La mayoría de intérpretes shell lo tienen incluido, como por ejemplo: **bash**, **Zsh**, **Ksh** o **csh**, por nombrar algunos de los más utilizados en linux. Si quieras puedes verificar que lo tienes instalado con el siguiente comando.

```
type echo
sololinux ~ # type echo
echo es una orden interna del shell
sololinux ~ #
www.sololinux.es
```

Cómo usar el comando echo con ejemplos

Como es habitual en este tipo de comandos, su sintaxis es bastante simple.

```
echo [opciones-secuencias] [ARGUMENTOS]
```

Opciones del comando echo

- **-n**: No imprime la última línea de la consola.
- **-e**: Habilita la interpretación de secuencias de escape.
- **-E**: Deshabilita la interpretación de las secuencias de escape (por defecto).

Secuencias de escape de echo

Ahora vemos las secuencias de escape admitidas por el **comando echo** (recuerda que para imprimir las secuencias de escape debes aplicar la opción «-e»):

- **\`**: Imprime el carácter barra invertida.
- **\a**: Alerta (BEL).
- **\b**: Retroceso.
- **\c**: Suprimir cualquier salida adicional,
- **\e**: Equivale a pulsar la tecla escape.
- **\f**: Muestra los caracteres de un formulario.
- **\n**: Nueva línea.
- **\r**: Retorno de carro (CR).
- **\t**: Impresión en pestaña horizontal.
- **\v**: Impresión en pestaña vertical.

Aunque hoy en día ya no es necesario, es una buena práctica de programación incluir los argumentos entre comillas simples o comillas dobles.

Ejemplos del comando echo

Imprimir un texto de forma estándar

```
echo Hola Sololinux
```

```
sololinux ~ # echo Hola Sololinux
Hola Sololinux
```



Imprimir un texto con caracteres entre comillas dobles

Tienes dos opciones de conseguir el objetivo.

```
echo 'Hola "Sololinux"'
```

```
# o
```

```
echo "Hola \"Sololinux\""
```

```
sololinux ~ # echo "Hola \"Sololinux\""
Hola "Sololinux"
```

```
sololinux ~ # echo 'Hola "Sololinux"'
Hola "Sololinux"
```

Mostrar un texto con una comilla simple

Para una comilla simple (algo normal en otros idiomas), la insertamos entre comillas dobles o utilizamos **ANSI-C** entre comillas simples.

```
echo "I'm a sololinux.es reader"
```

```
# o
```

```
echo $'I\'m a sololinux.es reader'
```

```
sololinux ~ # echo "I'm a sololinux.es reader"
I'm a sololinux.es reader
```

```
sololinux ~ # echo $'I\'m a sololinux.es
reader'
I'm a sololinux.es reader
```



Imprimir un mensaje con caracteres especiales

Recuerda que para usar las secuencias de escape debemos usar la opción «-e». En nuestro ejemplo imprimimos en nueva línea y en formato de pestaña horizontal.

```
echo -e "Mi sitio web favorito es...\\n\\t-
SoloLinux"
```

```
sololinux ~ # echo -e "Mi sitio web favorito
es...\\n\\t- SoloLinux"
Mi sitio web favorito es...
- SoloLinux
```

Buscar e imprimir por coincidencia de patrones

Mediante el uso de comodines (en este caso asterisco), podemos buscar coincidencias de archivos contenidos en un directorio. En nuestro ejemplo buscamos todas las imágenes con extensión jpg.

```
echo Listamos los archivos jpg: *.jpg
```

```
sololinux Carpeta nueva # echo Listamos los
archivos jpg: *.jpg
Listamos los archivos jpg:
IMG_20181014_094747.jpg
IMG_20181014_095910.jpg IMG-
27ba2597b23c226de82492df92e4a146-V.jpg
```

Enviar la salida a un archivo de texto

En vez de imprimir en pantalla el resultado de echo, lo envía a un archivo (si no existe lo crea).

```
echo -e 'Soy un usuario de la comunidad linux\\
nSoloLinux.es' >> /tmp/file.txt
```

En nuestro ejemplo enviamos el texto al archivo «/tmp/file.txt». Puedes ver su contenido con el comando cat.

```
cat /tmp/file.txt
```

Mostrar variables con echo

El comando también nos permite imprimir variables, en nuestro caso identificamos el usuario actual.

```
echo $USER
```

```
sergio@sololinux ~ $ echo $USER
sergio
```

Imprimir salidas de comandos

Con la expresión «\$(comando)», podemos incluir el resultado de un comando en la salida de echo. Nosotros queremos imprimir la fecha actual.

```
echo "Fecha actual: $(date +%D)"
```

```
sololinux ~ # echo "Fecha actual: $(date +%D)"
Fecha actual: 03/02/20
```

Cambiar los colores

Como último ejemplo del comando echo, vemos las secuencias necesarias si queremos modificar los colores de frente, de fondo o incluso las propiedades del texto.

```
echo -e "\033[1;37mBLANCO"
echo -e "\033[0;30mNEGRO"
echo -e "\033[0;34mAZUL"
echo -e "\033[0;32mVERDE"
echo -e "\033[0;36mCYAN"
echo -e "\033[0;31mROJO"
echo -e "\033[0;35mPURPURA"
echo -e "\033[0;33mAMARILLO"
echo -e "\033[1;30mGRIS"
```

```
sololinux ~ # echo -e "\033[1;37mBLANCO"
BLANCO ~ # echo -e "\033[0;30mNEGRO"
sololinux ~ # echo -e "\033[0;34mAZUL"
AZUL ~ # echo -e "\033[0;32mVERDE"
VERDE ~ # echo -e "\033[0;36mCYAN"
CYAN ~ # echo -e "\033[0;31mROJO"
ROJO ~ # echo -e "\033[0;35mPURPURA"
PURPURA ~ # echo -e "\033[0;33mAMARILLO"
AMARILLO ~ # echo -e "\033[1;30mGRIS"
GRIS
```

Como ves con el comando echo podemos insertar textos, espacios, tabuladores, nuevas líneas y mucho más.

Cómo escribir comentarios en bash correctamente

Cuando desarrollamos **scripts Bash**, tenemos que seguir unas reglas de buenas prácticas. El código debe ser limpio y comprensible, organizado por bloques, sangrados y con nombres descriptivos de las variables y funciones.

Otra forma de mejorar el código es con el uso de comentarios. El comentario es una pequeña anotación legible para humanos, donde se explica paso a paso las operaciones a realizar por el **script bash**.

Esta práctica recomendable te ahorrará tiempo y trabajo cuando pasado un tiempo revises de nuevo el código. Por ejemplo, si quieras modificar un script creado hace meses, lo más probable es que no recuerdes por qué escribiste el código de esa manera. Con un comentario lo entenderás enseguida.

Los comentarios también ayudan a otros programadores o **sysadmin**, que quieran modificar o continuar con tu trabajo. Los comentarios deben ser cortos y directos, no son necesarias las explicaciones obvias ni medias tintas.

En este artículo vemos los conceptos básicos de escritura, para que tus scripts bash tengan unos comentarios eficientes.

Cómo escribir comentarios en bash

Lo primero que debes recordar es, que Bash ignora (no ejecuta) todo lo escrito en una línea después de un **hash «#»** (también conocido como almohadilla). Como única excepción a hash, indicamos cuando en la primera línea del script se inserta algo similar a lo siguiente.

```
#!/bin/bash
```

Esto obligará al sistema a usar el intérprete de comandos que nosotros queremos, en el resto del código.

Los comentarios se pueden insertar antes de cada línea o en la misma línea, vemos los dos ejemplos.

```
# Recopilar los valores VAR1 y VAR2
read -r -p "Introduce el primer valor: " VAR1
read -r -p "Ahora el valor a comparar: " VAR2

# o

read -r -p "Introduce el primer valor: " VAR1 # Recopilar valor VAR1
read -r -p "Ahora el valor a comparar: " VAR2 # Recopilar valor VAR2
```

Si observas los ejemplos anteriores te darás cuenta que después de los hash dejamos un espacio. Realmente no es necesario, pero es evidente que aumenta su legibilidad de manera considerable.

Otra utilidad interesante de los comentarios es, que con el hash (#) puedes anular la ejecución de cualquier línea. Es una buena práctica si estás probando scripts, o agregas otras funciones que no siempre son necesarias. Vemos un ejemplo.

```
# Recopilar los valores VAR1 y VAR2 (VAR3 opcional)
read -r -p "Introduce el primer valor: " VAR1
read -r -p "Ahora el valor a comparar: " VAR2
#read -r -p "Compara el resultado con otro valor: " VAR3
```

La inmensa mayoría de lenguajes de programación admiten comentarios multilínea, por su estructura de construcción lectora bash no los admite. Debes insertarlos linea por linea.

```
# Recopilar el valor VAR1
# Recopilar el valor VAR2
read -r -p "Introduce el primer valor: " VAR1
read -r -p "Ahora el valor a comparar: " VAR2
```

Si no te convence el sistema multilínea, puedes usar **HereDoc** que es un tipo de redirección que nos permite pasar múltiples líneas de entrada a un comando. Si **HereDoc** no redirige a ningún comando, lo podemos aprovechar como marcador posicional de comentarios multilínea (hablaremos de **HereDoc** en un próximo artículo).

```
<< 'MULTILINE-COMMENT'
    Las líneas insertadas aquí
    aparecerán en el script
    tal como las ves ahora
MULTILINE-COMMENT
```

Nota final: Escribir comentarios es una buena práctica, ayudan a otros desarrolladores, y a ti mismo a comprender el script. En Bash, todo lo que pongas después de hash (#) y hasta el final de la línea, se considera un comentario.

Canales de Telegram: Canal [SoloLinux](#) – Canal [SoloWordpress](#)

Cómo crear bloques multilínea en bash con Heredoc



Heredoc (Here-document), es una curiosa (y poco conocida) forma de imprimir cadenas de caracteres multilínea, en un formato similar al original.

Si tomamos como ejemplo el **intérprete de comandos bash**, ya vimos en el anterior artículo que [no se permite escribir comentarios multilínea](#). Con Heredoc si podemos, y eso precisamente es lo que vamos a ver en este artículo de hoy además de otros ejemplos de uso.

Crear bloques multilínea en bash con Heredoc

Lo primero que haremos es conocer la sintaxis de Heredoc, a continuación trataremos unos ejemplos de uso y para concluir conocemos Heredoc con ssh.

Sintaxis de Heredoc

La sintaxis básica de Heredoc es como te indico a continuación.

```
[COMMAND] <<[-] 'DELIMITER'
          HERE-DOCUMENT
          DELIMITER
```

La primera línea comienza con un comando opcional (no obligatorio), seguido por el operador de redirección especial <<, y el identificador delimitador.

- Como identificador delimitador puedes usar cualquier cadena, aunque las más comunes son **EOF** y **END**.
- Si no incluyes entre comillas el identificador delimitador, el shell sustituye las variables, comandos y caracteres especiales antes de pasar las líneas de caracteres al comando.
- Si quieras usar una sangría al imprimir las líneas de caracteres, ignorando las tabulaciones originales. Debemos añadir el símbolo menos al operador de redirección, ejemplo: <<- .

En los bloques multilínea se pueden incluir, **cadenas, variables, comandos** o cualquier otro tipo de entrada.

La última línea siempre debe terminar con el identificador delimitador (no se permiten espacios en blanco).

Ejemplos de Heredoc

En el primer ejemplo nos ayudamos del **comando cat**, además imprimimos dos líneas que se completan con variables de entorno.

```
cat << EOF
El directorio actual es: $PWD
Has iniciado sesion como: $(whoami)
EOF
```

```
sergio@sololinux ~ $ cat << EOF
> El directorio actual es: $PWD
> Has iniciado sesion como: $(whoami)
> EOF
El directorio actual es: /home/sergio
Has iniciado sesion como: sergio
```

Si el ejemplo anterior lo quieres utilizar en una instrucción o bucle, tal vez quieras ejecutar el sangrado de la salida. En este caso el operador de redirección es: <<- . Vemos un ejemplo.

```
if true; then
    cat <<- EOF
    El directorio actual es: $PWD
    Has iniciado sesion como: $(whoami)
    EOF
fi
```

Con el operador [>] puedes enviar la salida a un archivo que se creará automáticamente (si existe se sustituye). Con el operador [>>] se agregara la salida al contenido del archivo.

```
# Crea o sobrescribe el archivo
cat << EOF > archivo.txt
El directorio actual es: $PWD
Has iniciado sesion como: $(whoami)
EOF

# Agrega el contenido al actual.
cat << EOF >> archivo.txt
El directorio actual es: $PWD
Has iniciado sesion como: $(whoami)
EOF
```

Ahora incluimos el comando sed para sustituir caracteres.

```
cat <<'EOF' | sed 's/l/e/g'
Soy lector de
SoloLinux
EOF
```

```
sergio@sololinux ~ $ cat <<'EOF' | sed 's/l/e/g'
> Soy lector de
> SoloLinux
> EOF
Soy eector de
SoeoLinux
```

Como último ejemplo vemos cómo incluir comentarios explicativos en nuestros scripts bash.

```
cat << 'MULTILINE-COMMENT'
    Las lineas insertadas aqui
    apareceran en el script
    tal como las ves ahora
MULTILINE-COMMENT
```

```
sergio@sololinux ~ $ cat << 'MULTILINE-COMMENT'
>     Las lineas insertadas aqui
>     apareceran en el script
>     tal como las ves ahora
> MULTILINE-COMMENT
    Las lineas insertadas aqui
    apareceran en el script
    tal como las ves ahora
```

Ejecutar Heredoc con SSH

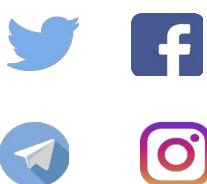
Una de las maneras más fáciles de ejecutar múltiples comandos en un sistema remoto, es a través de **Heredoc**. Mira que simple.

```
ssh -T usuario@remoto << EOF
echo "El directorio actual es: $PWD"
echo "El directorio remoto es: \$PWD"
EOF
```

```
El directorio actual es: /home/sergio
El directorio remoto es: /home/sololinux
```

Como has podido comprobar, **Heredoc** es una gran herramienta desconocida por los usuarios más noveles, pero que a partir de ahora la tendrán en cuenta en sus nuevos proyectos.

Síguenos en las Redes:



Canales de Telegram: Canal [SoloLinux](#) – Canal [SoloWordpress](#)

Let's Encrypt: Grave alerta de seguridad en sus certificados



Aviso importante a todos los que tienen sitios web con el **certificado gratuito Let's Encrypt**. Hace pocas horas recibí una serie de correos, con carácter de urgencia desde el remitente «noreply@letsencrypt.org».

En el mismo se informa a todos los usuarios de sus **certificados gratuitos**, que deben actualizar o renovar los mismos de forma inmediata (el correo no es un fake, es auténtico). Recientemente se ha descubierto un grave error de seguridad identificado como **2020.02.29 CAA Rechecking Bug**, puedes ver el aviso [aquí](#).

Let's Encrypt: Grave alerta de seguridad en sus certificados

El mail original de Let's Encrypt es el siguiente:

We recently discovered a bug in the Let's Encrypt certificate authority code, described here:

<https://community.letsencrypt.org/t/2020-02-29-caa-rechecking-bug/114591>

Unfortunately, this means we need to revoke the certificates that were affected by this bug, which includes one or more of your certificates. To avoid disruption, you'll need to renew and replace your affected certificate(s) by Wednesday, March 4, 2020. We sincerely apologize for the issue.

If you're not able to renew your certificate by March 4, the date we are required to revoke these certificates, visitors to your site will see security warnings until you do renew the certificate. Your ACME client documentation should explain how to renew.

If you are using Certbot, the command to renew is:
certbot renew --force-renewal

If you need help, please visit our community support forum:
<https://community.letsencrypt.org/t/revoking-certain-certificates-on-march-4/114864>

Please search thoroughly for a solution before you post a new question. Let's Encrypt staff will help our community try to answer unresolved questions as quickly as possible.

Your affected certificate(s), listed by serial number and domain names:
xxxxxxxxxxxxxxxxxxxxxxxxxxxx: * .xxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxx: * .xxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxx: * .xxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxx: * .xxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxx: * .xxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxx: * .xxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxx: * .xxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxx: * .xxxxxxxxxxxxxx

If you are receiving this email in error, unsubscribe at:
<http://mandrillapp.com/track/unsub.php?u=XXXXXXXXXXXXXXXXXXXXXXXXXXXX>
Please note that this would also unsubscribe you from other Let's Encrypt service notices, like expiration reminders.

El mail traducido de Let's Encrypt es el siguiente:

Recientemente descubrimos un error en el código de la autoridad de certificación Let's Encrypt, descrito aquí:

<https://community.letsencrypt.org/t/2020-02-29-caa-rechecking-bug/114591>

Desafortunadamente, esto significa que debemos revocar los certificados que se vieron afectados por este error, que incluye uno o más de sus certificados. Para evitar interrupción, deberá renovar y reemplazar sus certificados afectados por Miércoles 4 de marzo de 2020. Nos disculpamos sinceramente por el problema.

Si no puede renovar su certificado antes del 4 de marzo, la fecha en que estamos requerido para revocar estos certificados, los visitantes de su sitio verán seguridad advertencias hasta que renueve el certificado. Su documentación de cliente ACME

Debería explicar cómo renovar.

Si está utilizando Certbot, el comando para renovar es:
certbot renew --force-renewal

Si necesita ayuda, visite nuestro foro de soporte comunitario:
<https://community.letsencrypt.org/t/revoking-certain-certificates-on-march-4/114864>

Busque una solución a fondo antes de publicar una nueva pregunta. Vamos a Cifrar al personal ayudará a nuestra comunidad a tratar de responder preguntas no resueltas lo mas rápido posible.

Sus certificados afectados, enumerados por número de serie y nombres de dominio:

xxxxxxxxxxxxxxxxxxxxxxxxxxxx: * .xxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxx: * .xxxxxxxxxxxxxxxxxxxx

Si recibe este correo electrónico por error, cancele la suscripción en:

<http://mandrillapp.com/track/unsub.php?u=XXXXXXXXXXXXXXXXXXXXXXXXXXXX>

Tenga en cuenta que esto también lo anularía de otra suscripción de Let's Encrypt avisos de servicio, como recordatorios de vencimiento.

En el **comunicado de Let's Encrypt**, se nos dice que actualicemos o renovemos el certificado de los dominios indicados de forma inmediata. Si no lo haces tus clientes, usuarios o visitantes recibirán la temida pantalla **«La conexión no es privada»**.



www.sololinux.es

La conexión no es privada

Es posible que los atacantes estén intentando robar tu información de [REDACTED] (por ejemplo, contraseñas, mensajes o tarjetas de crédito). [Más información](#)

NET::ERR_CERT_COMMON_NAME_INVALID

Ocultar configuración avanzada

Volver para estar a salvo

Este servidor no ha podido probar que su dominio es [REDACTED], su certificado de seguridad procede de [REDACTED]. Este problema puede deberse a una configuración incorrecta o a que un atacante haya interceptado la conexión.

[Acceder a \[REDACTED\] \(sitio no seguro\)](#)

Es un tema urgente, así que no pierdas tiempo y renueva los certificados de todos los dominios inmediatamente.

Novedad: nuevo Wine 5.3 con muchas mejoras y correcciones

Wine, el emulador por excelencia de Windows en Linux, lanza una nueva versión plagada de mejoras y correcciones necesarias.

Las **nuevas características** más destacadas son:

- Manejo de Shell mejorado.
- Excelente soporte para la **normalización Unicode**.
- Se mejora el tiempo de ejecución de **Ucrbase**.
- Varios ajustes relativos al software.



Las **correcciones** más importantes:

- Las vistas gráficas en 2D y 3D de IKEA Home Planner 2010 no se mostraban correctamente. Reparado.
- Lotus Approach (MDI app): al intentar maximizar en algunas ventanas no ampliaban correctamente. Reparado.
- La configuración de «carpetas de Shell» se restablecen a su estado original después de actualizar.
- Varios juegos necesitaban DMO Wrapper Filter. Reparado.
- Mejora del renderizado en juegos como el **Far Cry 2**. Reparado.
- Aplicaciones como ADExplorer de Sysinternals necesitan conexiones ActiveDirectory / ADsOpenObject, y están fallando. Reparado.
- No se permite el desplazamiento en documentos comparados en **winmerge**. Reparado.
- Problema de renderizado 3D en Proteus Direct. Reparado.
- El menú desplegable de ComboBox no funciona si modificas su estilo sin barra de desplazamiento. Reparado.
- Varios juegos requieren IMFSourceReader ReadSample (Danganronpa V3, Resident Evil 2 1-Shot Demo). Reparado.
- Logos Bible Software (.Net 4.7.2 app) se bloquea. Reparado.
- msi: la acción caduca sistemáticamente en Windows 2003. Reparado.
- msi: las pruebas de acción fallan al ejecutarlas dos veces. Reparado.
- Wine no se puede iniciar, aviso de registro: wineboot no pudo iniciar wineboot c00000e5. Reparado.
- Automobilista. Muchos autos y pistas no se muestran en el menú. Reparado.
- Warhammer Online no procesa sin d3dx9_34. Reparado.
- Algunas características de las CPU Intel no son detectadas correctamente. Reparado.
- El área de datos compartidos de usuario debe completar el campo NumberOfPhysicalPages. Reparado.
- winecfg no permite deshabilitar el escritorio de descargas. Reparado.
- Lotus Organizer 97 se bloquea cuando seleccionas una copia de seguridad con el botón 'Examinar'. Reparado.
- Arma Cold War Assault: el cursor se atasca. Reparado.
- Bloqueo de varios instaladores como Hot Wired o Croc installer, no se inicia. Reparado.
- **Win SCP**: Bucle infinito al arrastrar y soltar (error 106). Reparado.
- DISPLAYCONFIG_VIDEO_OUTPUT_TECHNOLOGY (tamaños incorrectos). Reparado.
- AnyDesk se bloquea al iniciar. Reparado.
- QQMusicAgent se bloquea al iniciar por primera vez. Reparado.
- Gothic II Night of the Raven: excepción. Reparado.
- GdipGetNearestColor crash en Subtitle Edit. Reparado.
- iphpapi.NotifyUnicastIpAddressChange () error de llamada. Reparado.

Puedes **descargar Wine 5.3** desde sus enlaces oficiales.

- **Descarga oficial:** <https://dl.winehq.org/wine/source/5.x/wine-5.3.tar.xz>
- **Espejo Wine:** <http://mirrors.ibiblio.org/wine/source/5.x/wine-5.3.tar.xz>

Cuanto tiempo se ejecutan los procesos que más consumen



Hoy vamos a ver dos **scripts bash** muy útiles, pero a la vez un tanto curiosos. En el primero veremos cuanto tiempo llevan activos los **procesos que más consumen memoria ram**, en el segundo los que más consumen **cpu**.

El **script** imprime en pantalla un resultado formateado, de manera que sea legible para un humano. Los datos se obtienen de una secuencia de comandos habituales, estos resultados se guardan en un archivo *.txt en la carpeta temporal, después se leen y se imprimen, así de fácil.

Cuanto tiempo se ejecutan los procesos que más consumen

Script bash procesos en ram

Comenzamos por el script bash que nos dirá el tiempo activos de los procesos que más consumen ram. Lo creamos.

```
nano proc-ram.sh
```

Copia y pega lo siguiente:

```
#!/bin/bash
ps -eo pid,user,ppid,%mem,%cpu,cmd --sort=-%mem |
head | tail -n +2 | awk '{print $1}' > /tmp/pro-
ram.txt
echo
"-----"
echo "User      PID      CMD          Tiempo del
proceso"
echo
"-----"
for userid in `cat /tmp/pro-ram.txt`
do
username=$(ps -u -p $userid | tail -1 | awk '{print
$1}')
pruntime=$(ps -p $userid -o etime | tail -1)
ocmd=$(ps -p $userid | tail -1 | awk '{print $4}')
echo "$username $userid $ocmd $pruntime"
done | column -t
echo
"-----"
```

Guarda el archivo y cierra el editor.

Le concedemos permisos.

```
chmod u+x proc-ram.sh
```

Lo ejecutas:

```
sh proc-ram.sh
```

```
# o
```

```
bash proc-ram.sh
```

```
sololinux # bash proc-ram.sh
```

User	PID	CMD	Tiempo del proceso
sergio	2474	chromium-browse	02:32:29
sergio	3469	chromium-browse	02:20:15
sergio	2550	chromium-browse	02:32:16
sergio	4203	chromium-browse	02:00:45
sergio	2523	chromium-browse	02:32:22
sergio	4551	chromium-browse	01:57:20
sergio	2604	chromium-browse	02:32:15
sergio	2518	chromium-browse	02:32:22
sergio	7503	chromium-browse	02:15

Script bash procesos en cpu

El segundo código nos informa del tiempo que llevan activos los procesos que consumen más **recursos de la cpu**. Creamos el script bash.

```
nano proc-cpu.sh
```

Copiamos y pegamos el script:

```
#!/bin/bash
ps -eo pid,user,ppid,%mem,%cpu,cmd --sort=-%cpu |
head | tail -n +2 | awk '{print $1}' > /tmp/pro-
cpu.txt
echo
"-----"
echo "User      PID      CMD          Tiempo del
proceso"
echo
"-----"
for userid in `cat /tmp/pro-cpu.txt`
do
username=$(ps -u -p $userid | tail -1 | awk '{print
$1}')
pruntime=$(ps -p $userid -o etime | tail -1)
ocmd=$(ps -p $userid | tail -1 | awk '{print $4}')
echo "$username $userid $ocmd $pruntime"
done | column -t
echo
"-----"
```

Guarda el archivo y cierra el editor.

Le concedemos permisos.

```
chmod u+x proc-cpu.sh
```

Lo puedes ejecutar...

```
sh proc-cpu.sh
```

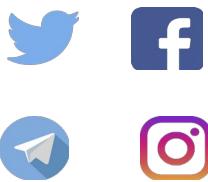
```
# o
```

```
bash proc-cpu.sh
```

Ejemplo de salida...

```
sololinux # bash pro-cpu.sh
-----
User      PID      CMD          Tiempo del proceso
-----
sergio    2474    chromium-browse 02:45:09
sergio    3469    chromium-browse 02:32:55
sergio    2523    chromium-browse 02:45:01
sergio    7503    chromium-browse 14:54
sergio    4203    chromium-browse 02:13:24
root      936     Xorg           03:03:09
sergio    1986    pulseaudio     02:56:06
sergio    7548    chromium-browse 14:42
sergio    7832    chromium-browse 04:30
-----
```

Síguenos en las Redes:



Canales de Telegram: Canal [SoloLinux](#) – Canal [SoloWordpress](#)

Cómo convertir un archivo img a un archivo iso en linux



En Linux, la mayoría de las **distribuciones** se ofrecen en **formato ISO**, pues es muy sencillo trabajar con ellas en nuestros sistemas.

Aun lo dicho, es posible encontrarnos con algún archivo IMG y no poder pasarlo a un CD/DVD, o dispositivo de almacenamiento externo (depende de la herramienta de grabación). En este artículo de hoy, vemos cómo convertir un archivo img a un archivo iso en linux de forma muy simple.

Qué es el formato img – iso

Antes de aprender a convertir entre estos formatos, es interesante dar una pequeña explicación de lo qué es y para que se utiliza cada uno.

Qué es un archivo img

Un archivo IMG puede contener diversos tipos de archivos o aplicaciones, pero normalmente se usa como contenedor de imágenes de CD-DVD-USB. Existen diversas variantes de la **extensión IMG**, la normal que se compone de un archivo, y la específica para **CloneCD** (y derivados) que contiene dos archivos más con información adicional (copia ilegales en Windows), con parámetros para la óptica del dispositivo de grabación.

Qué es un archivo iso

El archivo ISO tiene un formato de imagen de disco CD/DVD basado en el estándar ISO-9660. Normalmente son duplicados exactos de los datos de un disco original.

En una imagen iso se incluyen los datos originales, la información del sistema de archivos, la estructura de los directorios, atributos de los archivos y un archivo con el código de inicio. Son los más comunes para hacer cualquier tipo de copia.

Cómo convertir un archivo img a un archivo iso

Existen muchas herramientas para convertir img a iso, pero es evidente que lo más seguro es desde nuestra **terminal**. Para los usuarios más noveles, también veremos una aplicación con GUI que opera de una forma similar.

Convertir con ccd2iso

Para mi... es sin dudarlo la mejor herramienta en línea de comandos capaz de convertir archivos img a iso es, **ccd2iso**, simple, ligera y fácil de usar. No suele por defecto, así que la instalamos.

Debian, Ubuntu, Linux Mint y derivados:

```
sudo apt update
sudo apt install ccd2iso
```

CentOS, Fedora, y derivados:

OJO!!!, se requiere tener habilitado el **repositorio epel**.

```
# CentOS, Rhel y derivados
yum install ccd2iso

# Fedora y derivados
dnf install ccd2iso
```

Arch Linux, Manjaro y derivados:

```
sudo pacman -S ccd2iso

# en caso de error...
sudo pacman -Rs ccd2iso
```

Una vez tenemos instalada la herramienta en nuestra distribución linux favorita, es tan sencillo como abrir la consola en la carpeta donde tienes el archivo img, y ejecutar lo siguiente.

```
ccd2iso archivo.img archivo.iso
```

Esperas a que termine el proceso y tendrás las dos imágenes, archivo.img y archivo.iso. Fácil eh.

Convertir con Acetoneiso

Si prefieres una aplicación gráfica, no lo dudes. **Acetoneiso** de ser tu elección, a pesar que ya tiene sus años sigue siendo excelente (además tiene más funciones y formatos). Es cierto que algunas distros la quitaron de sus repos oficiales, aun así insisto, vale la pena.

Debian, Ubuntu, Linux Mint y derivados:

```
sudo apt update
sudo apt install acetoneiso
```

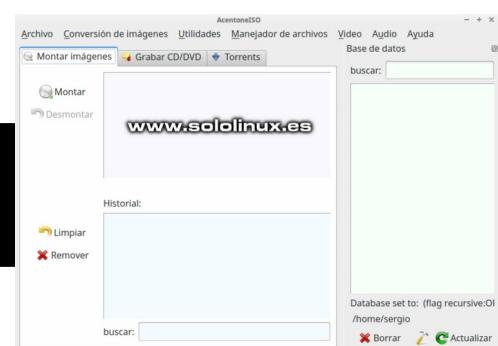
Fedora y derivados:

Debes descargar dependiendo de la versión que tengas instalada. Puedes hacerlo desde [AQUÍ](#).

Arch Linux, Manjaro y derivados:

```
sudo pacman -S acetoneiso

# en caso de error...
sudo pacman -Rs acetoneiso
```

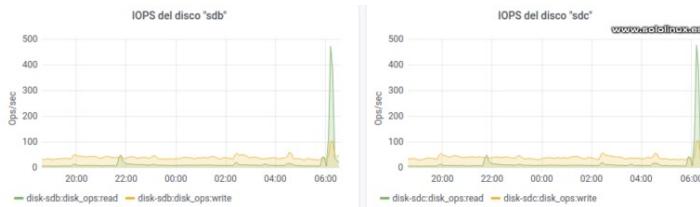


Nota final: Las conversiones con herramientas GUI no siempre son estables, te recomiendo que uses la primera opción propuesta en el artículo.

Uso del comando iostat con ejemplos en linux

El comando **iostat** se usa para monitorear la carga de entrada/salida (**I/O**) del dispositivo del sistema, normalmente el/los discos. La herramienta vigila el tiempo que los dispositivos están activos en relación con sus velocidades promedio de transferencia.

Al invocar **iostat**, se generan informes muy útiles para detectar sobrecargas y poder equilibrar el I/O de los discos del sistema. En este artículo conoceremos las opciones más usadas, así como una detallada explicación del informe.



Uso del comando iostat con ejemplos en linux

Instalar iostat

iostat viene incluido en el paquete **sysstat**. Normalmente no suele venir instalado por defecto, por tanto primero debemos instalarlo.

Debian, Ubuntu, Linux Mint y derivados:

```
sudo apt install sysstat
```

Rhel, CentOS, Fedora y derivados:

```
sudo yum install sysstat
o
sudo dnf install sysstat
```

Arch Linux, Manjaro y derivados:

```
sudo pacman -Sy sysstat
```

Sintaxis y uso básico de iostat

Una vez tengamos instalado el paquete de herramientas **sysstat** ya lo podemos utilizar, pero primero vemos su sintaxis (muchas opciones).

```
iostat [ -c ] [ -d ] [ -h ] [ -N ] [ -k | -m ]
[ -t ] [ -V ] [ -x ] [ -z ] [ [ -T ] -g group_name
] { device [...] | ALL } [ -p [ device [...] |
ALL ] ] [ interval [ count ] ]
```

Para comenzar ejecutamos el comando sin opciones.

```
iostat
```



Obtenemos una salida similar a...

```
Linux 3.10.0-1062.12.1.el7.x86_64 (sololinux.es) 06/03/20 _x86_64_
(8 CPU)

avg-cpu: %user %nice %system %iowait %steal %idle
          1,30    0,05   0,56   0,02   0,00  98,07

Device:      tps   kB_read/s   kB_wrtn/s   kB_read   kB_wrtn
sda        17,56     71,00    229,79  43223900 139898988
```

Explicación del informe de iostat

Si revisamos la salida de ejemplo anterior, observamos que se divide en tres partes.

- Sistema
- CPU
- Dispositivo

La información del sistema es muy básica, pero cumple a la perfección como preámbulo de lo que viene después. Nos dice que tipo de sistema tenemos: Kernel, hostname, fecha, sistema y numero de núcleos de la cpu.

En el segundo apartado la cosa se complica, nos aporta los datos de **consumo de la cpu** que pasamos a explicar en la siguiente tabla.

Nombre	Qué es...
%user	Muestra el porcentaje de uso de la CPU a nivel de usuario normal
%nice	Muestra el porcentaje de uso de la CPU a nivel de usuario con prioridades
%system	Muestra el porcentaje de uso de la CPU del kernel del sistema
%iowait	Muestra el porcentaje de tiempo que las CPU estaban inactivas y el sistema recibió peticiones I/O
%steal	Muestra el porcentaje de tiempo que las CPU permanecían en espera mientras el hipervisor mandaba el servicio a otro procesador
%idle	Muestra el porcentaje de tiempo que las CPU estaban inactivas y el sistema no recibía ninguna petición I/O

Por ultimo tenemos el apartado Device (dispositivo), que también pasamos a ver en una tabla.

Nombre	Qué es...
Device	Nombre del dispositivo como esta en /dev
tps	Número de transferencias por segundo que se emitieron al dispositivo
Blk_read/s (kB_read/s, MB_read/s)	Cantidad de datos leídos del dispositivo indicados en diferentes bloques (kilobytes , megabytes) por segundo
Blk_wrtn/s (kB_wrtn/s, MB_wrtn/s)	Cantidad de datos escritos en el dispositivo indicados en varios bloques (kilobytes, megabytes) por segundo
Blk_read (kB_read, MB_read)	Número total de bloques (kilobytes, megabytes) leídos
Blk_wrtn (kB_wrtn, MB_wrtn)	Número total de bloques (kilobytes, megabytes) escritos
rrqm/s	Número de solicitudes de lectura por segundo en la cola del dispositivo
wrqm/s	Número de solicitudes de escritura por segundo en la cola del dispositivo
r/s	Número de solicitudes de lectura por segundo completadas
w/s	Número de solicitudes de escritura por segundo completadas
rsec/s (rkB/s, rMB/s)	Número de sectores (kilobytes, megabytes) leídos por segundo
wsec/s (wkB/s, wMB/s)	Número de sectores (kilobytes, megabytes) escritos por segundo.
avgqrq-sz	Promedio del tamaño (en sectores) de las solicitudes que se emitieron al dispositivo
avgqu-sz	Promedio del tamaño (en sectores) de la cola de solicitudes que se emitieron al dispositivo
await	Promedio del tiempo (en milisegundos) de las solicitudes I/O emitidas al dispositivo
r_await	Promedio del tiempo (en milisegundos) de las solicitudes de lectura emitidas al dispositivo
w_await	Promedio del tiempo (en milisegundos) de las solicitudes de escritura emitidas al dispositivo
svctm	Promedio del tiempo (en milisegundos) de las solicitudes I/O emitidas al dispositivo (versiones obsoletas de iostat, en desuso)
%util	Promedio del tiempo de uso CPU en el cual se emitieron solicitudes I/O al dispositivo (ancho de banda del dispositivo)

Opciones de iostat

Ahora vemos las opciones de iostat, así como las variables de entorno a tener en cuenta.

Opción	Uso
-c	Uso de la CPU
-d	Uso del dispositivo
-g group_name { device [...] ALL }	Estadísticas de un grupo de dispositivos
-h	Imprimir los informes más fáciles de interpretar por un humano
-k	Estadísticas en kilobytes por segundo
-m	Estadísticas en megabytes por segundo
-N	Muestra los nombres del mapeador de los dispositivos registrados
-p [{ device [...] ALL }]	Muestra las estadísticas de dispositivos por bloque incluyendo las particiones usadas por el sistema
-T	Solo se muestran las estadísticas por grupo de dispositivos
-t	Imprimir la hora en cada informe, no solo la fecha
-V	Versión de sysstat
-x	Estadísticas ampliadas

-x	Estadísticas ampliadas
-z	Omitir la salida del dispositivo que no tiene actividad actualmente

Variables de entorno	
Variables	Casos de uso
S_TIME_FORMAT	Si esta variable existe y su valor es ISO, se omitirá la actual configuración regional y se utilizará el formato ISO 8601 (AAAA - MM - DD)
POSIXLY_CORRECT	Con esta variable las velocidades de transferencia se imprimirán en bloques de 512 K en vez de 1K

Ejemplos de iostat

El uso más común de iostat es con la opción x.

```
iostat -x
```

avg-cpu:	%user	%nice	%system	%iowait	%steal	%idle
	1,30	0,06	0,56	0,02	0,00	98,06
Device:	rrqm/s	wrqm/s	r/s	w/s	rkB/s	wkB/s
avgqrq-sz	avgqu-sz	await	r_await	w_await	svctm	%util
35,40	0,05	9,13	3,41	14,17	70,32	240,96
	0,05	2,79	0,25	3,40	0,08	0,14

Si solo quieres obtener la info de la cpu.

```
iostat -c
```

avg-cpu:	%user	%nice	%system	%iowait	%steal	%idle
	20,69	0,09	5,03	1,60	0,00	72,59

Si por el contrario solo quieres ver las estadísticas del dispositivo.

```
iostat -d
```

Device:	tps	kB_read/s	kB_wrtn/s	kB_read	kB_wrtn
sda	17,58	70,29	240,89	43227940	148144276

Mostrar estadísticas ampliadas del dispositivo.

```
iostat -xd
```

Device:	rrqm/s	wrqm/s	r/s	w/s	rkB/s	wkB/s
avgqrq-sz	avgqu-sz	await	r_await	w_await	svctm	%util
35,39	0,05	9,13	3,41	14,17	70,28	240,88
	0,05	2,79	0,25	3,40	0,08	0,14

Ahora solicitamos el informe de estadísticas tres veces, en un intervalo de dos segundos y en Kilobytes.

```
iostat -k 2 3
```

avg-cpu:	%user	%nice	%system	%iowait	%steal	%idle
	1,30	0,06	0,56	0,02	0,00	98,06
Device:	tps	kB_read/s	kB_wrtn/s	kB_read	kB_wrtn	
sda	17,57	70,21	240,74	43228024	148218228	
avg-cpu:	%user	%nice	%system	%iowait	%steal	%idle
	0,63	0,00	0,13	0,00	0,00	99,25
Device:	tps	kB_read/s	kB_wrtn/s	kB_read	kB_wrtn	
sda	5,00	0,00	44,00	0	88	
avg-cpu:	%user	%nice	%system	%iowait	%steal	%idle
	1,63	0,00	1,00	0,00	0,00	97,37
Device:	tps	kB_read/s	kB_wrtn/s	kB_read	kB_wrtn	
sda	12,50	0,00	272,00	0	544	

Vemos el informe de la CPU dos veces, en un intervalo de dos segundos.

```
iostat -c 2 2
```

	avg-cpu:	%user	%nice	%system	%iowait	%steal	%idle
		1,30	0,06	0,56	0,02	0,00	98,06
		0,13	0,00	0,13	0,00	0,00	99,75

Como ultimo ejemplo mostramos las estadísticas por bloque.

```
iostat -p
```

	avg-cpu:	%user	%nice	%system	%iowait	%steal	%idle
		1,30	0,06	0,56	0,02	0,00	98,06

Device:	tps	kB_read/s	kB_wrtn/s	kB_read	kB_wrtn
sda	17,57	70,19	240,68	43228032	148232928
sda1	0,00	0,04	0,00	21885	104
sda2	17,57	70,11	240,68	43182809	148232824
sda3	0,00	0,03	0,00	21024	0

Conclusión final

Hoy hemos visto una herramienta indispensable para un control total de los dispositivos, ademas tiene la particularidad que no es necesario ser root para poder visualizar las estadísticas. Puedes ver su manual en linea de comandos ejecutando lo siguiente...

```
man iostat
```

Ubuntu 20.04 LTS listo para que lo pruebes

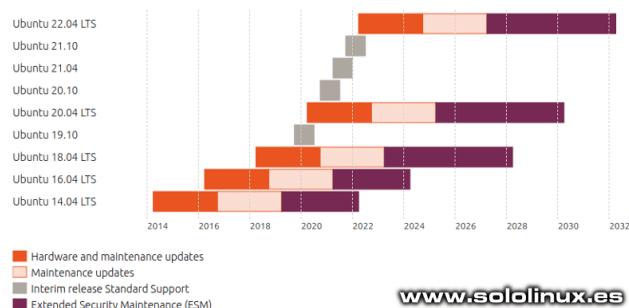
Ubuntu 20.04 LTS, al que han llamado **Focal Fossa** ya está listo para que lo pruebes. Recordemos que Ubuntu 20.04 será la próxima versión con soporte a largo plazo que nos brindara Canonical. Sus fechas son las siguientes.

- **Pruebas** : 9 de enero de 2020
- **UI Freeze** : 19 de marzo de 2020
- **Ubuntu 20.04 Beta**: 2 de abril de 2020
- **Kernel Freeze** : 9 de abril de 2020
- **Release Candidate**: 16 de abril de 2020

Bien, pues a pesar de que faltan pocos días para congelar la versión, y algunos más para su beta; ya puedes descargar Focal Fossa y comenzar a testearla. Recuerda que esta versión aun no es apta para producción, solo para que la pruebes e identifiques posibles errores futuros.

Puedes descargar Ubuntu 20.04 LiveCD en tu escritorio favorito, aquí los enlaces.

- Ubuntu 20.04 LTS Desktop: [64-bit PC \(AMD64\)](#)
- Ubuntu Server 20.04 LTS: [64-bit PC \(AMD64\)](#)
- Kubuntu 20.04 LTS Desktop: [64-bit PC \(AMD64\)](#)
- Lubuntu 20.04 LTS Desktop: [64-bit PC \(AMD64\)](#)
- Xubuntu 20.04 LTS Desktop: [64-bit PC \(AMD64\)](#)
- Ubuntu Budgie 20.04 LTS Desktop: [64-bit PC \(AMD64\)](#)
- Ubuntu Studio 20.04 LTS Desktop: [64-bit PC \(AMD64\)](#)
- Ubuntu Kylin 20.04 LTS Desktop: [64-bit PC \(AMD64\)](#)



Si quieras ir actualizando la iso live cd, para poder comprobar las nuevas actualizaciones te recomiendo que descargas la **herramienta zsync**. Con ella podrás ir actualizando la iso con sus nuevas mejoras, sin tener que descargarla entera de nuevo.

Instalamos zsync.

```
sudo apt install zsync
```

Ahora descargamos la iso de **Ubuntu 20.04** con zsync.

```
zsync http://cdimage.ubuntu.com/daily-live/current/focal-desktop-amd64.iso.zsync
```

Para actualizar la iso debes ejecutar el mismo comando anterior.

```
zsync http://cdimage.ubuntu.com/daily-live/current/focal-desktop-amd64.iso.zsync
```

En nuestro caso la acabamos de descargar y a los pocos minutos intentamos actualizar, la aplicación nos dice que no hay nada que actualizar.

```
zsync http://cdimage.ubuntu.com/daily-live/current/focal-desktop-amd64.iso.zsync
#####
reading seed file focal-desktop-amd64.iso:
*****
*****Read focal-desktop-
amd64.iso. Target 100.0% complete.
verifying download...checksum matches OK
used 2540175360 local, fetched 0
```

Insisto que esta versión es solo a modo de prueba, no la uses en producción.

Cómo ejecutar varios comandos en una sola línea

Todos los **administradores de sistemas Linux** (sysadmin), hacen un uso intensivo de la **Línea de comandos**. Si eres un recién llegado a linux no debes preocuparte, con el tiempo te acostumbras.

El truco radica en ejecutar comandos de ejemplo, y encontrar la forma de que tus tareas habituales sean más eficientes y rápidas. Es evidente, que para lograr nuestro objetivo necesitas de algunos trucos que te facilitaran la interacción con la terminal.

Hoy vemos cómo linux nos permite ejecutar varios comandos en una sola línea. Esta capacidad única, te permite ahorrar mucho trabajo y tiempo.

Cómo ejecutar varios comandos en una sola línea

En este artículo usamos como ejemplo el «**apt**» de **Debian, Ubuntu, Linux Mint y derivados**. En otros sistemas linux es exactamente lo mismo, por ejemplo en «**yum**» de **CentOS**.

Vemos cómo actualizar los repositorios de Ubuntu, y después actualizar el sistema desde una sola línea agregando el símbolo «**&&**» entre comando y comando.

```
sudo apt update && sudo apt full-upgrade -y
```

Los comandos anteriores son comunes, y ampliamente extendidos en la comunidad linux. Pero... tiene un problema que seguro alguna vez has podido observar, si falla la carga de un solo repositorio, el comando siguiente (en este caso **full-upgrade**) ya no se ejecuta.

Para solucionar esto, o simplemente quieres forzar el **comando full-upgrade** debes separar los comandos con punto y coma (;). Vemos un ejemplo.

```
sudo apt-get update; sudo apt-get upgrade -y
```

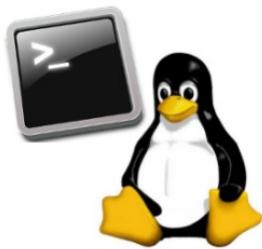
Con el comando anterior, se actualizará el sistema independientemente de si cargaron todos los repositorios o no.

Otro ejemplo más amplio:

```
sudo apt update && sudo apt upgrade -y && sudo apt autoremove -y  
o  
sudo apt update; sudo apt upgrade -y; sudo apt autoremove -y
```

www.sololinux.es

Ejecutar varios comandos en una sola línea



Cómo limpiar buffers y ram en linux

Liberar buffers y ram en linux

www.sololinux.es



Con el paso del tiempo, sobre todo en servidores que siempre están online, notamos que cada vez trabajan más despacio.

Es algo normal, pues con el uso los buffers, ram y swap se van llenando. Si trabajamos en una maquina que va muy sobrada de hardware y con pocos usuarios, no debería haber ningún problema. Si nuestro servidor hace un uso intensivo de sus recursos, la cosa cambia.

Las caches aceleran la vista de un sitio web al usuario, pero es evidente que sobrecargan el servidor. En este articulo veremos unos comandos que te ayudaran a limpiar el sistema, y que podemos convertir en **script bash**.

Cómo limpiar buffers y ram en linux

Todos los comandos propuestos se deben ejecutar con **permisos root**, por ejemplo, si queremos liberar las **pagecache** ejecutamos lo siguiente.

```
echo 1 > /proc/sys/vm/drop_caches
```

Para liberar **inodos** y **dentries**.

```
echo 2 > /proc/sys/vm/drop_caches
```

Para liberar todo lo anterior, **pagecaches**, **inodos** y **dentries**.

```
echo 3 > /proc/sys/vm/drop_caches
```

Un ejemplo de como puedes usar la cadena de comandos al completo:

```
free && sync && echo 3 > /proc/sys/vm/drop_caches &&  
free
```

También es conveniente vaciar la swap, para ello la manera más practica es desactivarla y volverla activar. La swap es una memoria volátil, por tanto desaparece al desactivarla.

```
# Deshabilitar la swap  
swapoff -a  
  
# Habilitar la swap  
swapon -a
```

Crear un script bash limpiador

Ahora creamos un script bash con los comandos anteriores, ademas generamos tiempos de espera entre ellos por si nuestro sistema está un poco sobrecargado.

```
nano limpiar.sh
```

Copia y pega lo siguiente.

```
#limpiar.sh  
#!/bin/bash  
echo "<----->"  
echo "<----->"  
  
echo "Comprobando estado de memoria"  
free  
echo "OK - Comprobacion completada"  
Echo "<----->"  
  
sleep 1s; echo "Limpieza de memoria cache y swap";  
echo "<----->"  
  
sleep 1s; echo "Deshabilitando Swap"  
swapoff -a  
echo "OK - Swap deshabilitado"  
echo "<----->"  
  
sleep 2s; echo "Liberando pagecaches, dentries e  
inodes"  
sync;sysctl -w vm.drop_caches=3;sync  
echo "OK - Server liberado"  
echo "<----->"  
  
sleep 3s; echo "Habilitando la Swap"  
swapon -a  
echo "OK - Swap habilitado"  
echo "<----->"  
  
sleep 2s; free  
echo ".....TODO CORRECTO....."  
echo "<----->"  
echo "<----->"
```

Guarda el archivo y cierra el editor.

Lo puedes ejecutar con el siguiente comando.

```
bash limpiar.sh
```

Como nota final puedes revisar el estado de la memoria, con...

```
cat /proc/meminfo
```

Transferir archivos de forma segura con el comando scp

En sistemas de tipo **Unix** o **Linux**, el comando **scp** se usa para hacer copias seguras. Es similar al **comando cp**, pero con una diferencia importante, **scp** es capaz de transferir archivos y directorios entre hosts a través de **una red encriptada segura**.

Para la transferencia de datos, **scp** hace uso del protocolo **ssh**, por lo tanto al usar la misma autenticación ofrece una alta seguridad. En este artículo, vemos cómo transferir archivos de forma segura con el comando **scp**.



Transferir archivos de forma segura con el comando scp

Antes de comenzar debes verificar que cumples con los siguientes requisitos:

- Recuerda que la herramienta **scp** depende de **ssh**, es imprescindible tener contraseña **ssh** para poder autenticarse en el sistema remoto.
- Asegurate de tener permisos de escritura en el sistema de destino.
- El comando **scp** utiliza dos puntos (:) para distinguir entre local y remoto.
- Si en el destino existe algún archivo con el mismo nombre, será sobreescrito sin avisar al usuario.

Sintaxis del comando scp

Como viene siendo habitual en este tipo de herramientas, es conveniente que entiendas la sintaxis del comando.

```
scp [OPTION] [user@]HOST_LOCAL:]archivo1 [user@]HOST_DESTINO:]archivo2
```

En [OPTION] tienes la posibilidad de insertar diversas opciones, como la configuración **ssh**, cifrado, límite, puerto **ssh** y más.

- 1) [user@]HOST_LOCAL:]archivo1 – Url del archivo local
- 2) [user@]HOST_DESTINO:]archivo2 – Url destino del archivo

Opciones del comando scp

Vemos las opciones más comunes.

INDICADOR	USO
-P	Indica el puerto ssh del host remoto
-p	Las fechas de modificación, modos y tiempos, serán iguales al original
-q	Quitar los posibles mensajes de error y el progreso
-C	Comprime los datos a enviar
-r	Copia los directorios completos de forma recursiva
-S	Permite definir cómo hacemos la conexión encriptada (normalmente SSH)
-v	El modo detallado permite ver los mensajes de progreso. Útil para depurar problemas de conexión, configuración o autenticación

Transferir archivos de local a remoto

Si queremos copiar un archivo local a un sistema remoto, ejecutamos algo similar a:

```
scp /home/sergio/archivo
user@sitio_remoto.com:/home/sololinux/mis_archivos
```

Transferir archivos de remoto a local

Si por el contrario queremos copiar datos de forma segura, del sistema remoto al local...

```
scp
user@sitio_remoto.com:/home/sololinux/mis_archivos/*
/home/sergio/downloads
```

Transferir un directorio de local a remoto

Para copiar directorios completos recuerda que debes usar la opción recursiva, (-r).

```
scp -r /home/sergio/miCarpeta user@url_destino.com:/
home/sololinux/directorio_remoto
```

Transferir archivos entre dos sistemas remotos

Si lo que necesitas es copiar un archivo o directorio entre dos sistemas remotos, ejecuta lo siguiente.

```
scp user1@host_remoto1.com:/dIRECTORIO/archivo1
user2@host_remoto2.com:/dIRECTORIO_DESTINO
```

Como ultimo ejemplo del articulo, vemos como transferir entre dos sistemas remotos enrutando a través de nuestro host local con «-3».

```
scp -3 user1@host_remoto1.com:/dIRECTORIO/archivo1
user2@host_remoto2.com:/dIRECTORIO_DESTINO
```

MySQL error en Plesk con linux

MySQL error en Plesk con linux

plesk
OBSIDIAN

Sin duda alguna, cuando hablamos de **paneles de control web**, **Plesk** es uno de los mejores. Completo, eficiente, seguro y sobre todo muy rápido.

Una combinación excelente es **CentOS 7 + Plesk**. De forma predeterminada CentOS 7 instala **MariaDB 5.5**, lo normal es actualizar a una versión superior antes de **instalar Plesk** para evitar posibles incompatibilidades futuras.

Hace unos días me encontré con el siguiente escenario: Un servidor **CentOS 7** con **Plesk Obsidian**, unos 25 sitios web y 32 bases de datos. La versión de MariaDB era la 5.5 y se requería actualizar a MariaDB 10.3, una tarea común si seguimos [este manual](#).

El proceso de actualización fue correcto, pero la alegría duro poco. Al intentar crear nuevos espacios web para dominios, se detectaron errores de inconsistencia y alguna tabla con mensajes que no debería existir. Plesk no permitía crear más sitios y como error principal lanzaba el siguiente aviso.

```
mysqldump: Couldn't execute 'SHOW FUNCTION STATUS WHERE Db = 'XXXXXXXX_XXX': Column count of mysql.proc is wrong. Expected 21, found 20.
Created with MariaDB 50564, now running 100322.
Please use mysql_upgrade to fix this error (1558)
(<program 'mysqldump' finished with non-zero exit code: %d>, 2)
```

El problema principal radica en el valor **AUTO_INCREMENT** que es menor que el real máximo, por suerte encontré un script que Plesk tenía a disposición de los usuarios. Vemos como ejecutarlo.

Primero hacemos una copia de seguridad.

```
plesk db dump > psa_dump.sql
```

Descargamos el script.

```
curl -LO
https://support.plesk.com/hc/en-us/article_attachments/360009691780/115003292185_auto_increment_fix.php.tar.gz
```

Lo descomprimimos y ejecutamos.

```
tar xf 115003292185_auto_increment_fix.php.tar.gz
```

```
plesk php 115003292185_auto_increment_fix.php -v -y
```

OJO!!!, no siempre se resuelve el problema al ejecutar una vez el script. Debes ejecutarlo de nuevo hasta que se imprima en pantalla lo siguiente...

No inconsistencies were detected.

Ejemplo minimizado de salida...

```
[root@miserver ~]# plesk php
115003292185_auto_increment_fix.php -v -y
Analyzing tables in `psa` database
INFO: Querying INFORMATION_SCHEMA for accounts
INFO: Querying INFORMATION_SCHEMA for admin_aliases
INFO: Querying INFORMATION_SCHEMA for apscategories
.....
INFO: Querying INFORMATION_SCHEMA for
PanelNotificationMessages
INFO: Querying INFORMATION_SCHEMA for module_firewall_rules
INFO: Querying INFORMATION_SCHEMA for
module_firewall_objects
No inconsistencies were detected.
```

Bien... ahora ya puedes crear nuevos espacios web de dominio, pero aunque parezca que todo funciona bien aún tenemos el problema de las tablas. Verificamos que efectivamente tenemos errores en las tablas.

```
plesk repair db -n
```

Los errores aparecen al final de la impresión de salida, para solucionarlos ejecutamos el siguiente comando. Pulsa «y» y enter cuando lo solicite.

```
plesk repair db -verbose
```

La base de datos a sido reparada, suerte.

Verificar los servicios que se están ejecutando en linux

El proceso init es el primer proceso que arranca al encender nuestro sistema. Como ya hemos hablado varias veces en **sololinux**, el **demonio** de **init** es el que maneja el resto de procesos y permanecerá activo hasta que apagues el sistema.

En el articulo de hoy, veremos como identificar los procesos que se están ejecutando en linux con los dos administradores más utilizados, **Systemd** y **SysVinit (SysV)**.

Verificar los servicios que se están ejecutando

Verificar los servicio con Systemd

Al ejecutar el comando básico, se verifican y enumeran todos los servicios en ejecución de un sistema «**systemd**».

```
systemctl
```

Cada columna de salida tiene su título descriptivo.

- **UNIT** : Nombre de la unidad Systemd.
- **LOAD** : Indica si está cargada en memoria actualmente o no.
- **ACTIVE** : Nos dice si está activa o no.
- **SUB** : Si está corriendo el servicio actualmente.
- **DESCRIPTION** : Descripción del servicio.

```
UNIT          LOAD   ACTIVE SUB           DESCRIPTION
proc-sys-fs-binfmt_misc.automount loaded active running  Arbitrary Executable File Fo
sys-devices-pci0000:00-0000:01:0-0:0-0:0-block-sda-sdal.device loaded active plugged  LOGIC
sys-devices-pci0000:00-0000:01:0-0:0-0:0-block-sda-sda2.device loaded active plugged  LOGIC
sys-devices-pci0000:00-0000:01:0-0:0-0:0-block-sda-sda3.device loaded active plugged  LOGIC
sys-devices-pci0000:00-0000:01:0-0:0-0:0-block-sda-sda4.device loaded active plugged  LOGICAL_VD
sys-devices-pci0000:00-0000:01:0-0:0-0:0-0:0-net-eth0.device loaded active plugged  NetXtreme BCM5720 2-port Gig
sys-devices-pci0000:00-0000:01:0-0:0-0:0-0:0-net-eth1.device loaded active plugged  NetXtreme BCM5720 2-port Gig
sys-devices-platform-pnp0:00-tty0.device loaded active plugged  /sys/devices/platform/serial
sys-devices-platform-pnp0:00-tty1.device loaded active plugged  /sys/devices/platform/serial
sys-devices-platform-pnp0:00-tty2.device loaded active plugged  /sys/devices/platform/serial
sys-devices-pnp0:00-01-tty50.device loaded active plugged  /sys/devices/pnp0/00/tty
sys-module-configs.device loaded active plugged  /sys/module/config
sys-subsystem-net-devices-eth0.device loaded active plugged  NetXtreme BCM5720 2-port Gig
sys-subsystem-net-devices-eth1.device loaded active plugged  NetXtreme BCM5720 2-port Gig
└--mount
      loaded active mounted  /boot
www.sololinux.es
```

Para listar las unidades de proceso indicándonos si están activos o no, además de visualmente más humanos ejecuta el siguiente comando:

```
systemctl list-unit-files --type service
```

```
UNIT           FILE                                     STATE
abrt-ccpp.service
abrt-oops.service
abrt-pstoreoops.service
abrt-vmcore.service
abrt-xorg.service
abrtd.service
arp-ethers.service
atd.service
auditd.service
autovt@.service
blk-availability.service
brandbot.service
                                         STATE
                                         enabled
                                         enabled
                                         disabled
                                         enabled
                                         enabled
                                         enabled
                                         disabled
                                         enabled
                                         enabled
                                         enabled
                                         static
www.sololinux.es
```

Si quieres conocer el estado de un servicio en particular (por ejemplo memcached)...

```
systemctl | grep memcached
```

Con más detalle...

```
systemctl status memcached
```

```
● memcached.service - Memcached
   Loaded: loaded (/usr/lib/systemd/system/memcached.service; enabled; vendor preset: disabled)
   Active: active (running) since jue 2020-03-12 04:57:17 CET; 7h ago
     Main PID: 2091 (memcached)
    CGroup: /system.slice/memcached.service
           └─2091 /usr/bin/memcached -p 11211 -m 4000 -c 1024 -l 127.0.0.1
www.sololinux.es
```

Verificar los servicios que se están ejecutando en linux

www.sololinux.es

Ahora listamos solo los procesos que están corriendo en nuestro sistema.

```
systemctl | grep running
```

Para visualizar las unidades de proceso que están en marcha e inician con el sistema...

```
systemctl list-unit-files | grep enabled
```

Ver por grupos el uso de recursos, tareas, CPU, memoria, entrada y salida.

```
systemd-cgtop
```

Path	Tasks	%CPU	Memory	Input/s	Output/s
www.sololinux.es	190	7.8	2.2G	-	-
/	1	-	-	-	-
/system.slice/NetworkManager.service	1	-	-	-	-
/system.slice/abrt-oops.service	1	-	-	-	-
/system.slice/abrtd.service	1	-	-	-	-
/system.slice/atd.service	1	-	-	-	-
/system.slice/audited.service	1	-	-	-	-
/system.slice/chronyd.service	1	-	-	-	-

Como punto final a Systemd puedes usar el comando...

```
pstree
```

Verificar los servicio con SysV (SysVinit)

Para verificar y enumerar todos los servicios en ejecución del administrador de sistema System V (SysV), ejecuta alguno de los siguientes comandos.

```
service --status-all
# o
service --status-all | more
# o
service --status-all | less
```

Si solo quieres ver los que se están ejecutando actualmente.

```
service --status-all | grep running
```

Para listar un servicio en particular (en el ejemplo httpd).

```
service --status-all | grep httpd
```

También su status.

```
service httpd status
```

```
[root@host ~]# service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
   Drop-In: /usr/lib/systemd/system/httpd.service.d
             └─respawn.conf
     Active: active (running) since jue 2020-03-12 06:24:16 CET; 6h ago
       Docs: man:httpd(8)
              man:apachectl(8)
   Main PID: 59443 (httpd)
     Status: "Total requests: 28983; Current requests/sec: 5; Current traffic: 48KB/sec"
    CGroup: /system.slice/httpd.service
            ├─59443 /usr/sbin/httpd -DFOREGROUND
            ├─59444 /usr/sbin/httpd -DFOREGROUND
            ├─59445 /usr/sbin/httpd -DFOREGROUND
            ├─59446 /usr/sbin/httpd -DFOREGROUND
            ├─59447 /usr/sbin/httpd -DFOREGROUND
            ├─59448 /usr/sbin/httpd -DFOREGROUND
            ├─59583 /usr/sbin/httpd -DFOREGROUND
```

www.sololinux.es

Podemos visualizar los servicios que se están ejecutando y que inician con el sistema.

```
chkconfig --list
```

Como último comando de este artículo, tambien puedes ver los procesos que están corriendo, con...

```
initctl list
```

Síguenos en las Redes:



Canales de Telegram: Canal SoloLinux – Canal SoloWordpress

Cómo cambiar la dirección MAC en linux con Macchanger

Los motivos por los que necesitas cambiar la dirección **MAC** pueden ser varios, estás en una red pública por tiempo limitado, alguien a bloqueado tu **MAC**, o simplemente quieres navegar sin exponer ese dato.

Falsificar, o mejor dicho cambiar la dirección MAC es una tarea muy sencilla en linux. Por suerte en nuestro sistema tenemos varias alternativas, pero sin duda alguna, la mejor es la vetusta herramienta Macchanger que no solo se limita a cambiar la MAC, nos ofrece otras posibilidades como falsificar automáticamente cada vez que **reinicies un dispositivo de red**.

Cómo cambiar la dirección MAC en linux con Macchanger

Macchanger no suele venir instalada por defecto en ninguna **distribución linux**, pero si que la podemos encontrar en sus repositorios oficiales. Vemos como **instalar Macchanger**.

Debian, Ubuntu, Linux Mint y derivados:

```
sudo apt install macchanger
```

Rhel, CentOS, Fedora y derivados:

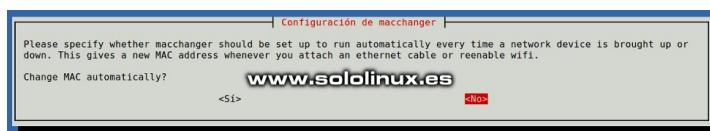
```
sudo yum install macchanger
```

```
sudo dnf install macchanger
```

Arch Linux, Manjaro y derivados:

```
sudo pacman -S macchanger
```

Nos aparece la siguiente pantalla en la cual tenemos que decidir si queremos que cambie automáticamente la MAC cada vez que habilites una nueva conexión a internet. En nuestro caso no lo activamos.



Una vez termine la instalación, vamos a identificar nuestro/s dispositivos de red.

```
ip link show
```

ejemplo de salida (en rojo los dispositivos)...

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: enp1s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOWN mode DEFAULT group default qlen 1000
link/ether 00:13:58:40:86:75 brd ff:ff:ff:ff:ff:ff
3: wlp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DORMANT group default qlen 1000
link/ether 00:18:a8:f1:b8:c8 brd ff:ff:ff:ff:ff:ff
```

Cómo cambiar la dirección mac en linux

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: enp1s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOWN mode DEFAULT group default qlen 1000
link/ether 00:13:58:40:86:75 brd ff:ff:ff:ff:ff:ff
3: wlp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DORMANT group default qlen 1000
link/ether 00:18:a8:f1:b8:c8 brd ff:ff:ff:ff:ff:ff
```

Te recomiendo que guardes todos los datos obtenidos con el anterior comando, en un futuro los puedes necesitar.

Si queremos que la **herramienta macchanger cambie la MAC** por una aleatoria, ejecutamos el siguiente comando (con el nombre del dispositivo).

```
sudo macchanger -r <span style="color: #333333;">wlp2s0</span>
```

Si por el contrario queremos especificar una MAC...

```
#inserta un numero de MAC
```

```
macchanger --mac=XX:XX:XX:XX:XX:XX
```

Independientemente de la opción elegida, tu MAC a cambiado.

Si por cualquier circunstancia quieres revertir los cambios y volver a la MAC original, inserta lo siguiente (con el sobre del dispositivo).

```
macchanger -p <span style="color: #333333;">wlp2s0</span>
```

Recuerda que los cambios no son permanentes, por lo tanto al reiniciar el sistema todo volverá a su estado original.

Solución al error «E: Could not get lock /var/lib/dpkg/lock»

Es una situación común, que al intentar instalar una aplicación en nuestro Ubuntu o derivado, nos aparezca en pantalla el siguiente error (o similar):

E: Could not get lock /var/lib/dpkg/lock

E: No se pudo bloquear /var/lib/dpkg/lock-frontend

```
E: Could not get lock /var/lib/dpkg/lock-frontend - open (11: Resource temporarily unavailable)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontend), is another process using it?
E: No se pudo bloquear /var/lib/dpkg/lock-frontend - open (11: Recurso no disponible temporalmente)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontend), is another process using it?
```

Este problema ocurre porque **apt** o **apt-get** estén siendo utilizados por otro proceso, y esa situación no está permitida.

La solución es bastante simple, lo único que tienes que hacer es localizar el proceso culpable del bloqueo y matarlo. Ejecuta el siguiente comando para identificar el culpable.

```
ps aux | grep -i apt
```

En nuestro caso nos damos cuenta que tenemos dos procesos usando apt, el 7274 y el 7314.

```
sergio    7274  0.0  0.0  4504   832 ?          S    07:43   0:00 /bin/sh /usr/bin/synaptic-pkexec
sergio    7314  0.0  0.0  18256   944 pts/6     S+   07:44   0:00 grep --color=auto -i apt
```

Los matamos.

```
sudo kill -9 7274
```

```
sudo kill -9 7314
```

También tienes la opción de matarlo todo con el siguiente comando.

```
sudo killall apt apt-get
```

Si el problema persiste, tal vez tengas archivos de bloqueo que se generaron en alguna actualización o instalación fallida. Puedes encontrar los procesos que contienen esos archivos con los siguientes comandos.

```
lsof /var/lib/dpkg/lock
```

```
lsof /var/lib/apt/lists/lock
```

```
lsof /var/cache/apt/archives/lock
```

Una vez localizado el proceso del archivo lo matas...

```
sudo kill -9 proceso
```

Y borras el archivo.

```
sudo rm /var/lib/apt/lists/lock
```

Como ultimo apunte del articulo, es interesante borrar los archivos implicados de los directorios cache.

```
sudo rm /var/cache/apt/archives/lock
```

```
sudo rm /var/lib/dpkg/lock
```



Error al establecer la configuración regional a C.UTF-8

¿Alguna vez te has encontrado con algunos de estos mensajes al instalar CentOS 8?.

«Failed to set locale, defaulting to C.UTF-8»

«Error al establecer la configuración regional, por defecto a C.UTF-8»

En este mini tutorial aprenderás a solucionar este problema tan común, pero tan fácil de solucionar.



Error al establecer la configuración regional a C.UTF-8

En plataformas **POSIX** como Linux y otros derivados de **Unix**, los identificadores locales se definen según las normas **ISO/IEC 15897**. Por ejemplo, en el español de España usamos la codificación **UTF-8 – es_ES.UTF-8**.

Pero puede suceder que al instalar alguna herramienta o aplicación, CentOS 8 nos devuelva el error «**Failed to set locale, defaulting to C.UTF-8**». Esto ocurre porque la configuración regional (en este caso España), no está bien establecida.

Para modificar la configuración y establecer el nuevo idioma, podemos utilizar el comando **localectl**.

```
localectl set-locale LANG=es_ES.UTF-8
```

Una vez concluido el proceso, intenta instalar de nuevo el paquete que generaba el error. Si aún así, el error persiste, quiere decir que no tenemos instalado ese paquete de lenguaje en particular. Lo instalamos.

```
yum install glibc-langpack-es
# o
dnf install glibc-langpack-es
```

Como alternativa, también puedes instalar todos los idiomas con el siguiente comando.

```
yum install langpacks-en glibc-all-langpacks -y
# o
dnf install langpacks-en glibc-all-langpacks -y
```

Una vez termines... reinicia el sistema para que cargue completamente la nueva configuración.

```
reboot
```

Uso y ejemplos del comando SHUF



El **comando shuf**, es una curiosa herramienta que genera salidas permutadas aleatoriamente (las mezcla) desde líneas de entrada definidas por nosotros.

Por ejemplo, si le apuntamos un archivo con una lista de números o palabras, baraja las cadenas e imprime el resultado de una forma estándar que puede ser capturado por herramientas comunes. Puedes crear tu juego de **bingo casero**, jajaja.

Uso y ejemplos del comando SHUF

La sintaxis del comando shuf es muy simple.

```
shuf [OPTION/S]... [FILES/CARACTERS]
```

Sus opciones son:

Opción corta	Opc. extendida	Descripción
-e	--echo	Interpreta cada argumento como fichero de entrada
-i	--input-range=IN-SU	Cada número de entrada y salida son entradas
-n	--head-count=LÍNEAS	Número de líneas a imprimir independientemente de las reales
-o	--output=FICHERO	El delimitador de líneas es NUL
-z	--zero-terminated	Obtiene bytes aleatorios de un archivo
-r	--repeat	Permitir líneas repetidas
	--version	Versión de la herramienta shuf
	--random-source=FICHERO	Obtiene bytes aleatorios de un archivo
	--help	Ayuda del comando

Como ejemplo hemos creado un archivo con palabras al que hemos llamado «paises.txt». Vemos su contenido y estructura real con el **comando cat**.

```
cat paises.txt
```

```
sergio@sololinux ~$ cat paises.txt
España
México
Colombia
Venezuela
Perú
Chile
Argentina
Cuba
```

Al ejecutar el archivo de texto con el comando shuf, el resultado es aleatorio.

```
shuf paises.txt
```

```
sergio@sololinux ~$ shuf paises.txt
España
Colombia
Chile
Perú
Venezuela
Cuba
México
Argentina
```

Curioso verdad?, pues tenemos más ejemplos.

Sobre nuestro archivo de ejemplo, vamos a indicar a la herramienta que aleatoriamente solo imprima una salida de cuatro países.

```
shuf -n 4 paises.txt
```

```
sergio@sololinux ~$ shuf -n 4 paises.txt
Colombia
Chile
Venezuela
México
```

También podemos permitir que se repitan los resultados aleatorios con «-r».

```
shuf -r -n 4 paises.txt
```

```
sergio@sololinux ~$ shuf -r -n 4 paises.txt
España
Chile
España
Argentina
```

Se permite la impresión repetitiva, incluso de más cadenas de texto que las que tiene el archivo.

```
shuf -r -n 12 paises.txt
```

```
sergio@sololinux ~$ shuf -r -n 12 paises.txt
Argentina
Chile
México
Cuba
Perú
Peru
Colombia
Mexico
Venezuela
España
España
Perú
```

No siempre es necesario capturar los datos de un archivo, los puedes insertar manualmente. Por ejemplo...

```
shuf -e Me interesa todo sobre linux
```

```
sergio@sololinux ~$ shuf -e Me interesa todo sobre linux
todo
sobre
Me
interesa
linux
```

Puedes hacer un sorteo entre diez (los que tu quieras) números. 😊

```
shuf -i 1-10
```

```
sergio@soloLinux ~$ shuf -i 1-10
3
10
2
9
6
5
1
4
8
7
```

Incluso crear tu propio juego de bingo, jaja.

```
shuf -i 1-99
```

```
sergio@soloLinux ~$ shuf -i 1-99
57
1
46
79
52
76
8
41
29
59
98
84
40
.....etc...
```

Como punto final del articulo, verificamos la version instalada de la herramienta.

```
shuf --version
```

```
sergio@soloLinux ~$ shuf --version
shuf (GNU coreutils) 8.25
Copyright © 2016 Free Software Foundation, Inc.
Licencia GPLv3+: GPL de GNU versión 3 o posterior
<http://gnu.org/licenses/gpl.html>.
Esto es software libre: usted es libre de cambiarlo y redistribuirlo.
No hay NINGUNA GARANTÍA, hasta donde permite la ley.

Escrito por Paul Eggert.
```

Síguenos en las Redes:



Canales de Telegram: Canal [SoloLinux](#) – Canal [SoloWordpress](#)

Alerta: El navegador Tor ejecuta Javascript en modo seguro

The Tor Project advierte a sus usuarios de un error grave en su navegador (**Tor browser**), este fallo permite que se ejecute código **JavaScript** en sitios en los que ha sido bloqueado de manera explícita.

Los desarrolladores de Tor están trabajando en una solución; parece que no es fácil y aún no se conoce la fecha del posible parche que solucionara el problema.

Bloquear la ejecución de código JavaScript, es una de las características de seguridad más importantes de **Tor Browser Bundle (TBB)**, que como todos sabemos es un navegador con características mejoradas y únicas sobre aspectos relativos a la privacidad. Recordemos que también es capaz de enmascarar las direcciones IP reales (la ubicación del usuario) para mantener nuestro anonimato.

Debido a estas características, el navegador es muy utilizado por usuarios diversos, para temas tan delicados (en algún país) como la política, o como una forma de evitar bloqueos y censura en lugares opresivos.

Hace pocas horas, el equipo de Tor anunció que habían encontrado un error en las opciones de seguridad de TBB. Si el navegador se configura para usar el nivel de seguridad más alto, llamado **«El más seguro de todos»**, sigue permitiendo la ejecución de código JavaScript, por tanto estamos ante un grave error de seguridad.

- ⚙️ General
- 🏠 Inicio
- 🔍 Buscar
- 🔒 Privacidad & Seguridad
- 🌐 Tor
- 店加盟 Extensiones y temas
- 💡 Tor Browser Asistencia

Seguridad

Nivel de seguridad

Deshabilita ciertas funciones web que se pueden usar para atacar tu seguridad y anonimato.

[Conocer más](#)

Estándar

Están habilitadas todas las características de Tor Browser y sitio web.

Más seguro

Deshabilita características del sitio web que a menudo son peligrosas, lo que causa que algunos sitios pierdan funcionalidad.

JavaScript está deshabilitado en sitios no-HTTPS.

Algunas fuentes y símbolos matemáticos están deshabilitados.

Audio y video (HTML5 media), y WebGL son click-to-play.

→ **El más seguro de todos**

Sólo permite las características de sitio web requeridas para sitios estáticos y servicios básicos.

Estos cambios afectan a imágenes, medios, y scripts.

JavaScript está deshabilitado por defecto en todos los sitios.

Algunas fuentes, iconos, símbolos matemáticos, e imágenes están deshabilitados.

Audio y video (HTML5 media), y WebGL son click-to-play.



Mientras sale el parche que solucionara el problema y, necesitas si o si deshabilitar la ejecución de JavaScript en el navegador de Tor, puedes seguir las siguientes instrucciones de configuración:

- Abrir **about:config**
- Escribe en la barra de búsqueda:
javascript.enabled
- Si la columna «**Value**» está como «**false**», JavaScript está deshabilitado.
- Si la columna «**Value**» pone «**True**», tienes que hacer clic en el botón derecho del ratón y seleccionar «**Toggle**», o hacer doble clic en la fila para que se marque como **false**.

Si necesitas más información visita [Tor Project Blog](#).

Fuente: [Hispasec](#)

Cómo instalar Xtreme Download Manager en linux

Xtreme Download Manager, más conocido como **XDM** o **XDMAN**, es un conocido administrador de descargas disponible para **Linux** y otros sistemas como **Windows** o **macOS**.

Es compatible con los **navegadores web** más utilizados, lo que permite descargar archivos de forma directa desde el propio navegador. Es especialmente útil para administrar descargas, sobre todo si tienes una conexión lenta o inestable.

Las principales **características** de XDM.

- Pausar y reanudar las descargas.
- **Descargar videos de YouTube** y más.
- Aumento considerable de la velocidad.
- Permite programar descargas.
- Limitar la velocidad de las descargas.
- Integración de los navegadores web más conocidos.
- Soporta servidores proxy.

Instalar Xtreme Download Manager en linux

Xtreme Download Manager (XDM), es una de las mejores herramientas de descargas en linux. Si somos sinceros, casi ninguna **distribución linux** la tiene en sus repositorios oficiales, aun así su instalación es bastante simple.

Lo único que tenemos que hacer es, acceder a su [página oficial](#) y descargar la última versión, en este caso... **64 bits**: [xdm-2018-x64.tar.xz](#), o la de **32 bits**: [xdm-2018-x86.tar.xz](#).

Accedemos al directorio donde hemos descargado el archivo, lo descomprimimos. Desde la misma carpeta abres la terminal y ejecuta lo siguiente según la versión descargada.

```
# 64 bits
cd xdm-2018-x64

# o

# 32 bits
cd xdm-2018-x86
```

La instalación de la herramienta es rápida, tan solo copia y pega lo siguiente.

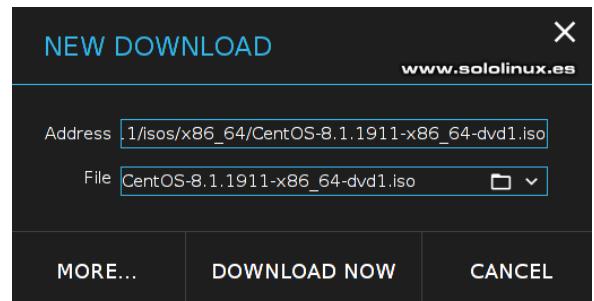
```
sudo ./install.sh
```

```
sololinux xdm-2018-x64 # ./install.sh
Initializing setup...
Extracting files...
Unpacking /opt/xdman/jre/lib/charsets.pack...
Unpacking /opt/xdman/jre/lib/ext/cldrdata.pack...
Unpacking /opt/xdman/jre/lib/ext/nashorn.pack...
Unpacking /opt/xdman/jre/lib/rt.pack...
Finishing installation...
Xtreme Download Manager installed successfully
You can start XDM from start menu, or type xdm in terminal as non
root user
```

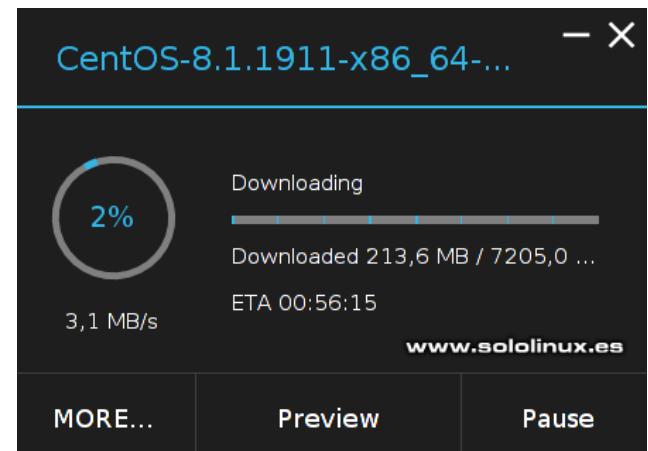
Una vez instalado, busca la herramienta en el menú de aplicaciones de tu entorno de escritorio favorito. La ejecutas.... verás una pantalla super-intuitiva similar a la siguiente imagen.



Puedes revisar sus múltiples opciones (incluso el cambio de idioma), pero si quieres descargar ya, es tan sencillo como insertar los datos de la url, tal como vemos en la siguiente imagen (en nuestro ejemplo la versión extendida de **CentOS 8**).



Seguimiento de la descarga.



Como último apunte, si quieres desinstalar XDM tan solo debes ejecutar el siguiente comando.

```
sudo apt-get remove --purge xdm
```

Como puedes comprobar, su instalación y uso es simple así que ya sabes...

Identificar el tipo de raid y si son discos ssd en linux

Cuando nos hacemos cargo de la administración de un **servidor linux**, es algo común que el propietario no sabe realmente cómo está montado.

Si hablamos de los **sistemas de almacenamiento** (los discos), lo primero que debemos hacer es, asegurarnos del tipo de discos que monta el servidor (mecánicos o SSD), cuantos dispositivos tiene el servidor (discos), y en el caso de que tenga raid... que tipo de raid (0 / 1 / 5 / 10, etc).

En este artículo de hoy vemos como identificar de manera rápida y precisa, todas nuestras dudas al respecto.

Identificar el tipo de raid y si son discos ssd

Para que podáis interpretar los ejemplos de salida de este artículo, os informo de los datos del servidor que vamos a utilizar (de los dispositivos).

- **HDD:** 3 x 256GB (SSD SATA)

Identificar si son discos HDD o SSD

Existen múltiples comandos para identificar si nuestro servidor tiene discos **SSD** o **HDD**, pero sin duda alguna la más sencilla es la que te propongo. Ejecuta lo siguiente.

```
cat /sys/block/sda/queue/rotational
```

El comando anterior detecta si los dispositivos son rotacionales o no. Si es un HDD el disco gira mecánicamente, por tanto la salida será «1». Si nuestro dispositivo es SSD, la respuesta es «0».

Ejemplo de disco/ssd...

```
[root@server ~]# cat /sys/block/sda/queue/rotational  
0
```

Cuantos discos tiene mi servidor

Para saber la cantidad de discos de nuestra máquina, tan solo debes ejecutar lo siguiente:

```
sudo lsblk -fm
```



En nuestro ejemplo nos dice que tenemos tres discos, **sda**, **sdb** y **sdc**.

```
[root@server ~]# sudo lsblk -fm  
NAME FSTYPE LABEL UUID  
MOUNTPOINT NAME SIZE OWNER GROUP MODE  
sda  
  sda    238,5G root disk brw-rw---  
  |sda1 swap          71fb3846-0f78-492b-933b-ec61c85304a3 [SWAP]  
  |  sda1   1G root disk brw-rw---  
  |sda2 linux_ra 1 c29ba9c4-8561-7a88-106a-3b9dfd31d50f  
  |  sda2   231,6G root disk brw-rw---  
  |  |md1 ext4          8059ee78-417b-44d8-8b91-54e6209dcc4a /  
  |  |  lmd1 462,9G root disk brw-rw---  
  |  |sda3 linux_ra 0 85b5b1a9-ee28-4a7f-05c2-5fe377a58498  
  |  |  sda3   1G root disk brw-rw---  
  |  |  |md0 ext4          cab0efee-bc42-46de-8c42-a751366423de /boot  
  |  |  |  lmd0   2G root disk brw-rw---  
sdb  
  sdb    238,5G root disk brw-rw---  
  |sdb1 swap          25a4c1ed-0661-4788-922f-7c9a3a7e6ee7 [SWAP]  
  |  sdb1   1G root disk brw-rw---  
  |sdb2 linux_ra 1 c29ba9c4-8561-7a88-106a-3b9dfd31d50f  
  |  sdb2   231,6G root disk brw-rw---  
  |  |md1 ext4          8059ee78-417b-44d8-8b91-54e6209dcc4a /  
  |  |  lmd1 462,9G root disk brw-rw---  
  |  |sdb3 linux_ra 0 85b5b1a9-ee28-4a7f-05c2-5fe377a58498  
  |  |  sdb3   1G root disk brw-rw---  
  |  |  |md0 ext4          cab0efee-bc42-46de-8c42-a751366423de /boot  
  |  |  |  lmd0   2G root disk brw-rw---  
sdc  
  sdc    238,5G root disk brw-rw---  
  |sdc1 swap          865be5f1-0dfb-4141-9766-dac798d85824 [SWAP]  
  |  sdc1   1G root disk brw-rw---  
  |sdc2 linux_ra 1 c29ba9c4-8561-7a88-106a-3b9dfd31d50f  
  |  sdc2   231,6G root disk brw-rw---  
  |  |md1 ext4          8059ee78-417b-44d8-8b91-54e6209dcc4a /  
  |  |  lmd1 462,9G root disk brw-rw---  
  |  |sdc3 linux_ra 0 85b5b1a9-ee28-4a7f-05c2-5fe377a58498  
  |  |  sdc3   1G root disk brw-rw---  
  |  |  |md0 ext4          cab0efee-bc42-46de-8c42-a751366423de /boot  
  |  |  |  lmd0   2G root disk brw-rw---
```

Que tipo de raid tiene el servidor

En este apartado todo depende de si tienes un hardware específico para el raid, o es raid por software que es el más común. El raid por hardware dado su alto coste se reserva para servidores de alto rendimiento.

Raid por software

Para el raid por software ejecuta el siguiente comando.

```
cat /proc/mdstat
```

```
[root@server ~]# cat /proc/mdstat  
Personalities : [raid6] [raid5] [raid4]  
md0 : active raid5 sda3[0] sdc3[3] sdb3[1]  
      2093056 blocks super 1.2 level 5, 512k chunk, algorithm 2 [3/3] [UUU]  
      bitmap: 0/1 pages [0KB], 65536KB chunk  
  
md1 : active raid5 sda2[0] sdc2[3] sdb2[1]  
      485398528 blocks super 1.2 level 5, 512k chunk, algorithm 2 [3/3] [UUU]  
      bitmap: 1/2 pages [4KB], 65536KB chunk
```

Raid por hardware

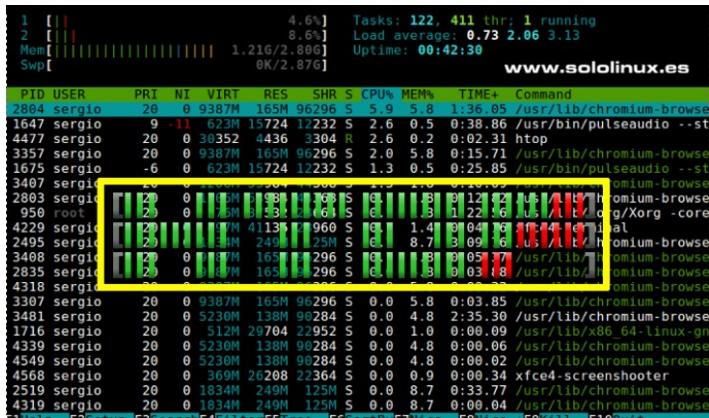
La controladora de raid por hardware más usada es la MegaRAID, puedes verificar que la tienes instalada con el comando...

```
megaclis-as-status
```

Para conocer el tipo de raid...

```
megacli -LDInfo -Lall -aALL
```

Manual de Htop, la mejor herramienta para monitorizar linux



La herramienta **htop** es la mejor alternativa al comando **top**, además nos ofrece muchas características y nuevas opciones si lo comparamos con top.

El concepto básico de **htop**, es el de un visor de procesos interactivo para sistemas basados en Unix. Opera en modo texto y requiere la biblioteca ncurses. Diseñado como una opción a top, las métricas de CPU y memoria se visualizan mediante barras gráficas fácilmente comprensibles.

A diferencia de top, htop nos permite desplazarnos vertical y horizontalmente por la pantalla para ver todos los procesos que se ejecutan en el sistema. Además, podemos vigilar el rendimiento identificando los diferentes **colores de htop**. También podemos hacer cualquier tarea con los procesos activos.

Principales características de htop:

- Permite desplazarnos vertical y horizontalmente para ver todos los procesos y líneas.
- Si lo comparamos con el comando top, htop imprime los datos mucho más rápido.
- Permite eliminar procesos sin ingresar la ID.
- Permite modificar las propiedades de un proceso sin insertar su ID.
- Puedes matar múltiples procesos a la vez.
- Su salida coloreada hace que identifiquemos posibles problemas de forma rápida.

Manual de Htop

Instalar htop

Aunque para muchos **sysadmin** es una herramienta imprescindible, normalmente no viene instalada por defecto en (casi) ninguna **distribución linux**, pero si en sus repositorios oficiales. Vemos con instalarla.

Debian, Ubuntu, Linux Mint y derivados:

```
sudo apt install htop
```

CentOS, RHEL, Fedora y derivados:

```
# CentOS, RHEL
sudo yum install htop
```

```
# Fedora
sudo dnf install htop
```

Arch linux, Manjaro y derivados:

```
sudo pacman -S htop
```

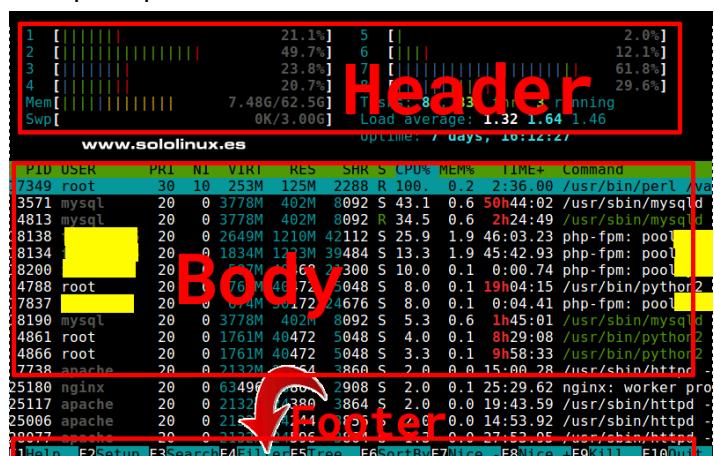
Open Suse, Suse y derivados:

```
sudo zypper install htop
```

Comprender htop

La pantalla principal de Htop se divide en tres partes: Header, Body y Footer (encabezado, cuerpo y pie de página).

- Header:** Muestra el uso de la CPU, la memoria, la swap, los promedios de carga y el tiempo que el sistema lleva encendido.
- Body:** Aquí podemos ver la lista de los procesos que se están ejecutando actualmente en el sistema.
- Footer:** Nos encontramos con el menú principal de la herramienta.



Colores del encabezado

Dividimos los colores del encabezado en tres secciones:

CPU:

- Azul:** Porcentaje de uso de los procesos de baja prioridad.
- Verde:** Porcentaje de uso de los procesos que necesitan los usuarios.
- Rojo:** Porcentaje utilizado por los procesos del sistema.
- Cian:** Porcentaje consumido por caches y otros.

Memoria:

Verde: Porcentaje de la RAM utilizada.

Azul: Búfer.

Amarillo o Naranja: Tamaño de la caché.

Swap:

- Rojo:** Porcentaje de la swap ocupada.

Menú del body

En la parte superior del body nos encontramos con el menú indicativo, explicamos su significado en la siguiente tabla.

Indicación	Que representa
PID	ID del proceso.
USER	Usuario del proceso.
PRI	Prioridad del proceso en el kernel linux.
NI	El "nice" de un proceso tiene una escala desde 19 (baja prioridad) a -20 (alta prioridad). Un valor alto nos indica que el proceso permite que otros tengan más prioridad.
VIRT	Tamaño virtual del proceso.
RES	Nos indica la memoria física que consume un proceso.
SHR	Nos indica la memoria que se puede compartir o comparte con otros procesos.
S	Estado de los procesos: -S: "sleeping" durmiendo (inactivo) -R: "running" activo -D: ininterrumpible -Z: "zombie" -T: trazado o suspendido -W: paginación
CPU%	Porcentaje de tiempo de uso del proceso en la CPU.
MEM%	Porcentaje de memoria utilizada por el proceso.
TIME+	Tiempo del proceso.
Command	Ruta o URL

Organizar la salida de htop

De forma predeterminada y como la gran mayoría de herramientas, Htop ordena la salida a través del valor de uso de la CPU. Si quieres organizar la salida desde otro valor, pulsa la tecla **«F6»**, selecciona la fuente primaria del menú que aparece a la izquierda y pulsa **Enter**.

```
1 [   www.sololinux.es      0.0%] 5 [ ]
2 [   ]                         0.0%]
3 [   ]                         0.1%]
4 [   ]                         0.0%]
Mem[|||||] 1.46G/31.16G Tasks: 95, 243 thr: 1 running
Swap[          0K/3.000] Load average: 0.01 0.07 0.12
Uptime: 00:34:09

sort by PID USER PRI NI VIRT RES SHR S CPU% MEM% TIME+ Command
PID 29174 root 20 0 1896M 2716 1428M 0.0 0.0 0.0 0.00:52 httpd
USER 24632 root 20 0 120M 2648 1500 R 0.7 0.0 0:00:46 httpd
PRIORITY 1 root 19 -1 186M 4184 2588 S 0.7 0.0 0:03:98 /usr/lib/systemd
NICE 4272 root 20 0 1896M 24788 5088 S 0.7 0.1 0:01:55 httpd
VICE 22861 mysql 20 0 2300M 1808 14116 S 0.7 0.6 0:00:06 /usr/sbin/mysqld
SIZE 16647 psadm 20 0 360M 33484 17208 S 0.0 0.1 0:00:02 /usr/bin/sw-engine
RESIDENT 22858 mysql 20 0 2300M 1809 14116 S 0.0 0.6 0:16:38 /usr/sbin/mysqld
SHARE 4195 root 20 0 1896M 24736 5088 S 0.0 0.1 0:00:51 /usr/bin/python2
STATE 4254 root 20 0 1896M 24736 5088 S 0.0 0.1 0:00:62 /usr/bin/python2
PERCENT_CPU 1902 root 20 0 21668 1252 988 S 0.0 0.0 0:00:28 /usr/sbin/irqbalance
PERCENT_MEM 2909 apache 20 0 2134M 1868 3812 S 0.0 0.1 0:03:35 /usr/sbin/httpd
TIME 3661 grafana 20 0 1184M 39626 1984 S 0.0 0.0 0:03:03 /usr/bin/grafana
Command 13754 psadm 20 0 495M 39088 15700 S 0.0 0.1 0:02:62 sw-engine-fpm: po
```

En nuestro ejemplo ordenamos la salida por el tiempo de uso (Time).

PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command
4064	root	20	0	1896M	24736	5088	S	0.0	0.1	0:28.20	/usr/bin/python2
4467	drweb	20	0	446M	439M	2604	S	0.0	1.4	0:24.55	/opt/drweb/drweb
22850	mysql	20	0	2300M	195M	14116	S	0.0	0.6	0:19.75	/usr/sbin/mysqld
12192	apache	20	0	2134M	19764	3824	S	0.7	0.1	0:07.93	/usr/sbin/httpd
8230	www.sololinux.es	20	0	6116	2824	5	S	0.7	0.0	0:05.08	nginx: worker pro

Listar la salida en árbol

A veces, puede ser difícil identificar la raíz real del proceso. Para solucionar este problema pulsa la tecla **«F5»** para cambiar a vista de árbol, así verás la relación padre / hijo de los procesos.

PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command
1	root	20	0	186M	4184	2588	S	0.0	0.0	0:03.24	/usr/lib/systemd/systemd
23421	mysql	20	0	2300M	209M	14298	S	0.7	0.0	0:11.16	/usr/sbin/mysql
23420	mysql	20	0	2300M	209M	14298	S	0.7	0.0	0:12.18	/usr/sbin/mysql
23419	mysql	20	0	2300M	209M	14298	S	0.7	0.0	0:10.50	/usr/sbin/mysql
22957	mysql	20	0	2300M	209M	14298	S	0.7	0.0	0:09.67	/usr/sbin/mysql
22956	mysql	20	0	2300M	209M	14298	S	0.7	0.0	0:10.23	/usr/sbin/mysql
22955	mysql	20	0	2300M	209M	14298	S	0.7	0.0	0:09.66	/usr/sbin/mysql
22879	mysql	20	0	2300M	209M	14298	S	0.7	0.0	0:09.60	/usr/sbin/mysql
22878	mysql	20	0	2300M	209M	14298	S	0.7	0.0	0:09.60	/usr/sbin/mysql
22877	www.sololinux.es	20	0	209M	209M	14298	S	0.0	0.7	0:00.00	/usr/sbin/mysql
22876	mysql	20	0	2300M	209M	14298	S	0.0	0.7	0:00.00	/usr/sbin/mysql

Cómo matar un proceso

Matar un proceso en htop es una tarea muy sencilla; selecciona el proceso, pulsa la tecla **«F9»** y en el menú que aparece a la izquierda marca la señal que quieras enviar al proceso indicado.

Send signal:	PID	USER	PRI	NI	VIRT
0 Cancel	12192	apache	20	0	2134M
1 SIGHUP	19886	root	20	0	120M
2 SIGINT	4064	root	20	0	1896M
3 SIGQUIT	12219	apache	20	0	2134M
4 SIGILL	2975	apache	20	0	2134M
5 SIGTRAP	4310	root	20	0	1896M
6 SIGABRT	4296	root	20	0	1896M
6 SIGIOT	29021	root	20	0	167M
7 SIGBUS	22850	mysql	20	0	2300M
8 SIGFPE	www.sololinux.es		0	0	1256M
9 SIGKILL	13753	psadm	20	0	495M
10 SIGUSR1	3886	grafana	20	0	758M
11 SIGSEGV	4253	root	20	0	1896M
12 SIGUSR2	4298	root	20	0	1896M
13 SIGPIPE	22861	mysql	20	0	2300M
14 SIGALRM	22873	mysql	20	0	2300M
15 SIGTERM	1	root	19	-1	186M
16 SIGSTKFLT	2939	apache	20	0	2134M
17 SIGCHLD	16647	psadm	20	0	360M
18 SIGCONT	2909	apache	20	0	2134M

Cómo buscar un proceso

Si quieres localizar un proceso activo a través de la herramienta htop, pulsa la tecla **«F3»**. Ahora escribe el nombre del proceso y automáticamente se marcará en la salida. En nuestro ejemplo buscamos **«htop»**.

PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command
4064	root	20	0	1896M	24788	5088	S	0.7	0.1	0:56.10	/usr/bin/python2
24632	root	20	0	120M	2648	1500	R	0.7	0.0	0:00.46	htop
1	root	19	-1	186M	4184	2588	S	0.7	0.0	0:03.98	/usr/lib/systemd
4272	root	20	0	1896M	24788	5088	S	0.7	0.1	0:01.55	htop
22861	mysql	20	0	2300M	209M	14260	S	0.7	0.7	0:00:00	/usr/sbin/mysql

Personalizar el encabezado de htop

Htop es totalmente personalizable, al pulsar la tecla «F2» aparece un menú desde el cual puedes modificar el header de la aplicación según tus necesidades.



Nota final: Para abrir la ayuda oficial del monitor pulsa «F1».

Cómo instalar ONLYOFFICE Community Edition en Ubuntu 18.04

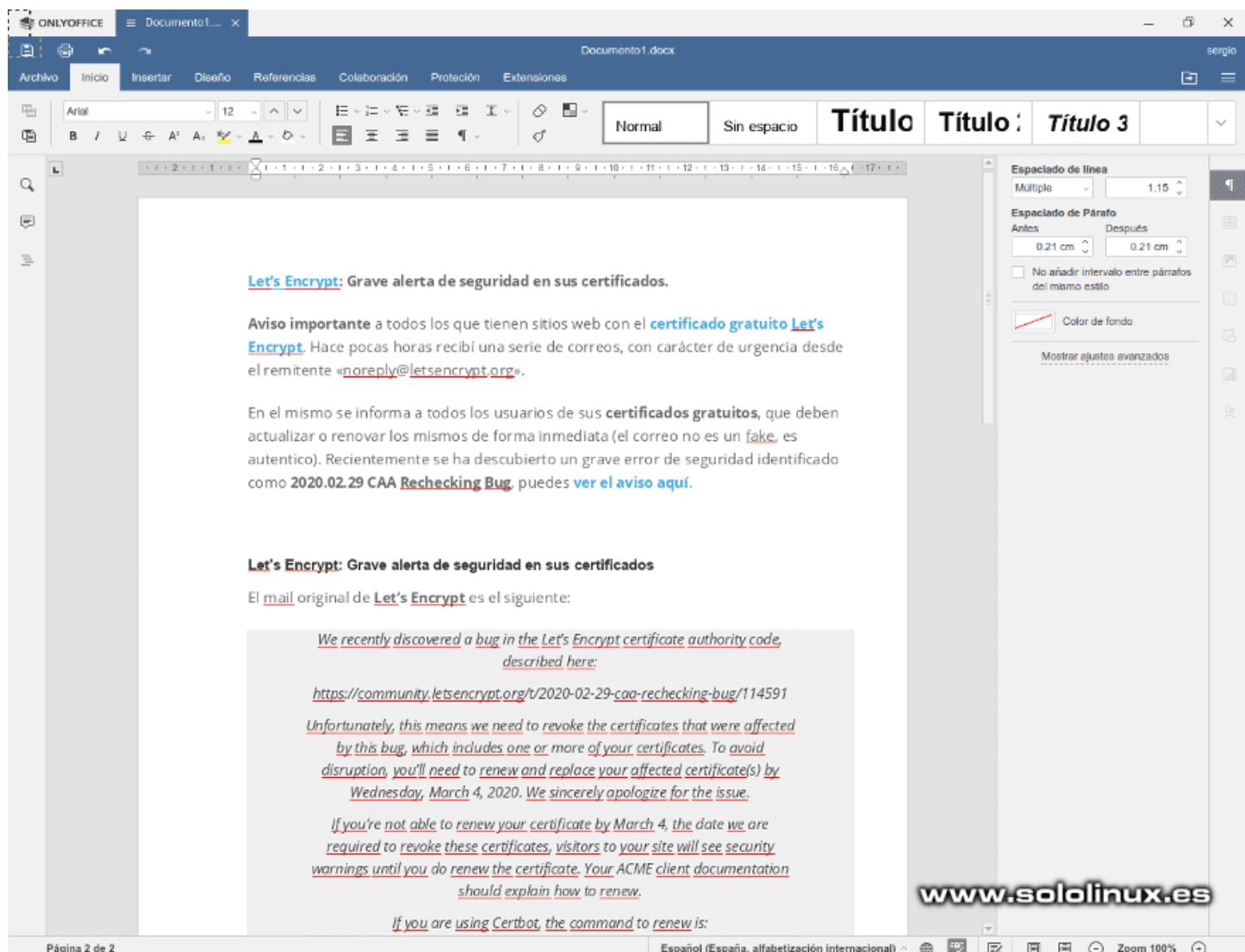
De vez en cuando todos los usuarios tenemos que crear, redactar, colaborar o compartir documentos de texto, hojas de cálculo y presentaciones. Para ello tenemos las **suites ofimáticas**.

En Linux tenemos una gran variedad de aplicaciones de este tipo (a veces preinstalados) y dependiendo de nuestros gustos y necesidades podemos elegir entre una u otra solución. Como indica el título de este artículo, hoy vemos una suite un tanto desconocida pero no por ello deja de ser excelente. Hablamos de **ONLYOFFICE**.

ONLYOFFICE es una suite ofimática online de código abierto que incluye un procesador de texto, un editor de hojas de cálculo y otro de presentaciones. Puedes modificar y utilizar libremente el código fuente de **ONLYOFFICE**, lo puedes encontrar en [GitHub](#).

Escrito en JavaScript, utiliza Canvas de HTML5 para ofrecer un 100% de compatibilidad a la hora de visualizar, convertir, imprimir o guardar documentos en los formatos más populares: DOC, DOCX, ODT, TXT, PDF, HTML.

En el artículo de hoy vemos como instalar ONLYOFFICE en **Ubuntu 18.04 LTS y superiores**.



Instalar ONLYOFFICE Community Edition en Ubuntu

Echando un vistazo a ONLYOFFICE, resulta obvio que se incluyen todas las características que podríamos necesitar para crear o editar nuestros documentos.

Procesador de textos:

- Ajustes extendidos de párrafos y fuentes, márgenes entre líneas y párrafos. Insertar columnas y saltos de página.
- Imágenes, gráficos personalizables, autoformas, tablas y Text Art y todo según tus necesidades.
- Historial de versiones, además destacamos que permite restaurar versiones anteriores con un clic.
- Plugins para insertar vídeos de YouTube, símbolos especiales, traducciones, etc.

Editor de hojas de cálculo:

- Cálculos precisos con más de 400 funciones y fórmulas incluidas de forma predeterminada.
- Plantillas de tablas, rangos por nombre, ordenar y filtrar datos.
- Permite agregar gráficos coloreados con información incluida, así como fórmulas, formas, imágenes, Text Art y vídeos de YouTube.
- Crear, editar y guardar macros nos permite automatizar las tareas comunes.

Editor de presentaciones:

- Crea esquemas claros y bosquejos con autoformas.
- Permite añadir gráficos, tablas y fórmulas para visualizar datos y estadísticas.
- Plugins para insertar vídeos y elementos clip art, traducir textos, añadir símbolos, editar imágenes, etc.

Sorprendentemente ONLYOFFICE es mucho más que una suite ofimática. También es una plataforma colaborativa capaz de, gestionar documentos y proyectos de manera centralizada, analizar y canalizar las relaciones con los clientes (CRM), administrar correos, eventos y más. Consta de seis módulos que permiten hacer lo siguiente:

Gestión de documentos:

- Crear, gestionar y almacenar documentos de texto, hojas de cálculo y presentaciones incluyendo los archivos guardados en otros servicios de almacenamiento en la nube (por ejemplo, Google Drive, Dropbox, ownCloud, Nextcloud, etc...).
- Colaborar en documentos online y compartirlos con otros usuarios o grupos (permite agregar permisos).
- Monitorear los cambios con revisiones y marcas de tiempo de las diferentes versiones.
- Almacenar y reproducir archivos de vídeo y audio, así como imágenes de los formatos más populares con su reproductor multimedia integrado.

Proyectos:

- Hitos, tareas y subtareas para determinar las prioridades de los proyectos.
- Crear diagramas de Gantt para visualizar y analizar el progreso.
- Administrar derechos de acceso a cada proyecto.
- Generar informes.

CRM:

- Bases de datos de clientes.
- Gestión de procesos negociaciones y potenciales acuerdos.
- Facturas.
- Integración de Twilio.

Correo:

- Agregar servidor de correo y buzones de correo corporativos.
- Recibir, guardar y gestionar la correspondencia.
- Creador de plantillas.

Calendario:

- Horarios y calendarios compartidos con otros usuarios o grupos.
- Planificar y gestionar eventos.
- Importar eventos de fuentes como iCal de Google, Apple iCal o Yahoo!.

Comunidad:

- Últimas noticias, pedidos, anuncios, etc.
- Encuestas.
- Blog corporativo y foros.
- Interactuar con otros usuarios (en tiempo real) con su sistema de mensajería instantánea integrada.

Instalar un servidor ONLYOFFICE

Para instalar un servidor ONLYOFFICE necesitas los siguientes requisitos:

- CPU: doble núcleo de 2 GHz o superior.
- RAM: 6 GB.
- HDD: 40 GB.

Una vez verificados los requisitos la instalación es tan simple como ejecutar lo siguiente...

```
wget
http://download.onlyoffice.com/install/opensource-
install.sh
```

Al terminar el proceso de preparación del servidor, lanzamos el siguiente comando.

```
bash opensource-install.sh
```

Bien... ya lo tenemos todo listo. Ahora escribimos la ip del servidor en nuestro navegador web preferido (en local localhost o 127.0.0.1), para acceder a esta completa suite ofimática.

Autor: Sergey Zarubin

Cómo actualizar Manjaro o Arch linux para novatos



Si existe una **distribución linux** fácil de usar para los recién llegados, esa es **Manjaro**; Actualmente y sin dudarlo, el derivado de **Arch Linux** más utilizado por usuarios sin grandes conocimientos.

Este artículo está indicado para los que tiene menos conocimientos de **Manjaro** o **Arch**. Te puede parecer una tontería el cómo aprender a actualizar **Manjaro**, pero te aseguro que para otros menos avanzados no lo es, además existen varias opciones. Las vemos

Cómo actualizar Manjaro o Arch linux

Es evidente que los comandos que te propongo no solo son validos para Arch y Manjaro, también para todos sus **derivados**, que son muchos.

El primer comando que vamos a utilizar, compara la base de datos del paquete local con el repositorio de software de la distribución original. Si no existen nuevas versiones de paquetes disponibles, te dirá que escribas YES para actualizar los paquetes pendientes.

```
sudo pacman -Syy
```

Ahora bien, si quieres forzar al administrador de paquetes a descargar una nueva base de datos, debes ejecutar lo siguiente:

```
sudo pacman -Syyu
```

Si eres comodón y prefieres que la GUI trabaje por ti, tan solo tienes que esperar a que aparezca un aviso en la pantalla de Arch o alguno de sus derivados; Y pulsar en aceptar cuando te indique que tienes actualizaciones pendientes.

		Select All	Updates	
State	Name	Version	Repository	Size
U	About Xfce (libxfce4ui)	4.14.1-2 (4.12.1-2)	extra	271.1 kB
U	Atom (atom)	1.45.0-1 (1.27.0-1)	community	37.8 MB
U	Bluetooth (blueberry)	1.3.5-1 (1.2.20-1)	community	1.2 MB
U	Cantarell (cantarell-fonts)	1.0.201-1 (1.0.101-1)	extra	330.0 kB
U	Catfish (catfish)	1.4.13-2 (1.4.5-1)	community	272.9 kB
U	Character Map (gucharmap)	13.0.0-1 (10.0.4-3+gfi)	extra	2.5 MB
U	Chromium (chromium)	80.0.3987.14 (66.0.3359.14)	extra	58.0 MB
U	Clipman (xfce4-clipman-plugin)	1.4.4-1 (1.4.2-2)	extra	149.2 kB
U	Cool Retro Term (cool-retro-term)	1.1.1-1 (1.0.1-1)	community	1.3 MB
U	Dconf Editor (dconf-editor)	3.36.0-1		

Nota final: El comando «**sudo pacman -Syyu**» es para primeras instalaciones, o casos de extrema necesidad. No te recomiendo abusar de él, consume demasiados recursos y ancho de banda.

Independientemente de como actualices tu sistema Arch, recuerda que debes reiniciar la maquina al terminar el proceso.

Cómo instalar Twitter Lite en linux



Twitter es la red social más utilizada después de **Facebook**. Millones de personas de todo el mundo lo emplean para interactuar con otros usuarios y mantenerse informado de las últimas noticias, eventos, tendencias, música, política o recibir nuevos manuales (por ejemplo de **soloLinux.es**).

Como la aplicación nativa de **Twitter** podía resultar algo pesada en ciertos dispositivos (o redes lentas), lanzaron una versión ligera, conocida como **Twitter Lite** que comparada con la aplicación estándar, es bastante más rápida además de usar menos ancho de banda.

La versión lite ofrece las mismas características principales de Twitter, como línea de tiempo, tweets, notificaciones, búsquedas, mensajes directos, perfiles y más. Destacamos que funciona sin problemas en redes de internet lentas.

Principales características de Twitter Lite:

- Carga muy rápido.
- Mismas características base que la versión estándar.
- Minimiza en gran medida el uso de datos.
- Ocupa menos espacio.
- Opera sin cortes en conexiones de red lentas.
- Admite notificaciones push.
- Soporte off-line.

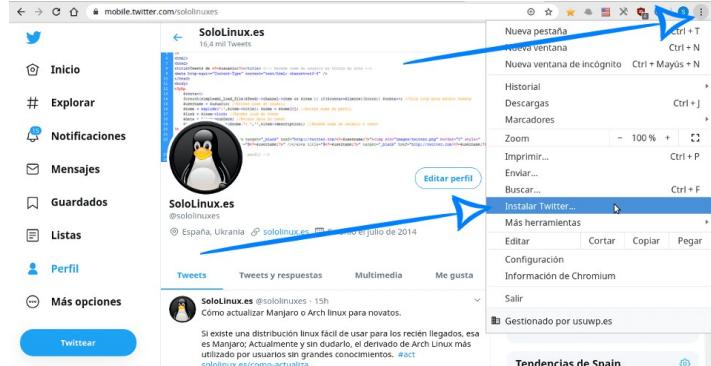
Instalar Twitter Lite en linux

Twitter lite permite su instalación en cualquier distribución linux de una forma sorprendentemente simple (requiere Chrome, Chromium y derivados). Vemos como instalar Twitter Lite en linux.

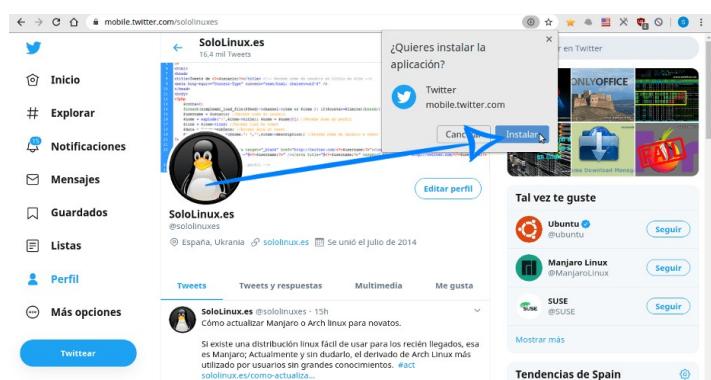
Desde la siguiente dirección url, accedes a tu cuenta de Twitter.

<https://mobile.twitter.com/>

Sigue los pasos indicados en la imagen siguiente, menu / instalar Twitter.

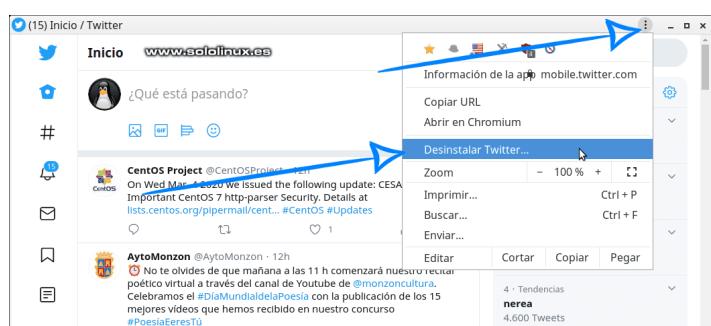


Como puede ver en la imagen de ejemplo, se abre una ventana de notificación. Pulsa en instalar.



Bien, ya lo tienes instalado en tu linux, así de simple. Puedes abrir Twitter lite desde el menú de aplicaciones.

La herramienta ocupa un espacio mínimo, pero si por cualquier motivo la quieras desinstalar abres el menú y haces click en desinstalar Twitter.



Como has podido comprobar, la instalación de Twitter Lite en linux es un proceso muy sencillo.

Instalar CyberPanel en Ubuntu 18.04

CyberPanel es un **panel de control web** de código abierto, del que hemos hablado largamente en **sololinux** que utiliza **OpenLiteSpeed** como servidor web.

Desarrollado como herramienta de última generación, está especialmente diseñado para ser extremadamente rápido, seguro y estable. Es gratuito y no tiene ninguna limitación en cuanto a dominios y subdominios. Si en un principio se creó para CentOS, hoy en día también admite servidores Ubuntu.

De **CyberPanel** podemos destacar las siguientes características.

- Soporte integrado para mod_security.
- Firewall básico y **firewall CSF**.
- SSL con un clic.
- Permite límites en el correo electrónico.
- Soporta htaccess.
- Instalador automático.
- Rainloop Webmail, LSCache, Git y más.

Su instalación y uso es sencillo e intuitivo. Vemos como instalar este fabuloso **panel de control** en Ubuntu 18.04.



Instalar CyberPanel en Ubuntu 18.04

Como es habitual cuando trabajamos en Ubuntu, Debian y derivados, primero actualizamos el sistema.

```
sudo apt update  
sudo apt full-upgrade
```

Normalmente al instalar Ubuntu server, se incluye de forma predeterminada un servidor lamp básico. Debemos eliminarlo para evitar conflictos posteriores.

```
systemctl stop apache2  
systemctl stop mysql  
systemctl stop postfix  
systemctl stop dovecot  
sudo apt purge apache2* libapache2* mysql-client* mysql-common* mysql-server* postfix* dovecot*  
sudo apt autoremove  
sudo apt clean  
rm -rf /var/lib/mysql
```

Ahora descargamos la última **versión de CyberPanel** y le damos los permisos necesarios.

```
cd /opt  
wget -O installer.sh https://cyberpanel.net/install.sh  
chmod 755 installer.sh
```

Comenzamos la instalacion...

```
sh installer.sh  
# 0  
bash installer.sh
```

El script verificará que se cumplen los requisitos necesarios.

Checking root privileges...
You are running on root...
Checking OS...

Detecting Ubuntu 18.x...
Pre-flight check completed...
Process check completed...

Selecciona la opción que más te convenga, si es una nueva instalación completa selecciona la 1 y pulsas enter.

```
CyberPanel Installer v2.0
```

1. Install CyberPanel.
2. Install Addons.
3. Exit.

```
Please enter the number[1-3]: 1
```

Después de verificar el tamaño de la ram y el espacio del disco, nos pregunta la versión a instalar. Debes elegir la Open, la Enterprise tiene un coste.

1. Install CyberPanel with OpenLiteSpeed.
2. Install Cyberpanel with LiteSpeed Enterprise.
3. Exit.

```
Please enter the number[1-3]: 1
```

Ahora debes seleccionar los paquetes añadidos que te interese instalar por defecto.

```
Install minimal service for CyberPanel? This will
skip PowerDNS, Postfix and Pure-FTPd.
Minimal installation [y/N]: N

Do you wish to install Postfix?
Postfix installation [Y/n]: Y

Do you wish to install PowerDNS?
PowerDNS installation [Y/n]: Y

Do you wish to install Pure-FTPd?
Pure-FTPd installation [Y/n]: Y

Please choose to use default admin password
1234567, randomly generate one (recommended) or
specify the admin password?
Choose [d]efault, [r]andom or [s]et password: [d/r/
s] d

Admin password will be set as 1234567

Replace JS/CSS files to JS Delivr?
This may improve panel loading speed in Asia
Pacific region...
Please select [y/N]: y

Install Memcached extension for PHP?
Please select [y/N]: y

Install LiteSpeed Memcached?
Please select [y/N]: y

Install Redis extension for PHP?
Please select [y/N]: y

Install Redis?
Please select [y/N]: y
```

La instalación comienza, así que tómate algo y descansa que dependiendo del sistema puede tardar más o menos.

Al concluir la instalación aparece en la pantalla los datos de acceso.

```
Visit: https://ip-del-servidor:8090
Panel username: admin
Panel password: 1234567
```

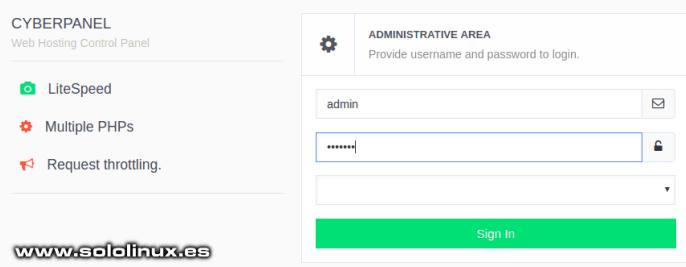
```
Please change your default admin password
If you need to reset your panel password, please
run:
adminPass YOUR_NEW_PASSWORD
```

```
If you change mysql password, please modify file in
/etc/cyberpanel/mysqlPassword with new password as
well
```

Para acceder al panel de control web CyberPanel, escribe en la url de tu navegador preferido...

<https://ip-del-servidor:8090>

El usuario es **admin** y la password **1234567** (no olvides cambiarla en cuanto accedas).



Una vez dentro del panel ya puedes comenzar a configurar tu primer dominio. Te dejo un par de artículos que te pueden interesar sobre cómo **configurar CyberPanel**.

- [Manual 1](#)
- [Manual 2](#)

Canales de Telegram:
[Canal SoloLinux](#)
[Canal SoloWordpress](#)

Cómo afecta el coronavirus a la tecnología y a linux



No voy a engañar a nadie, hace días que tenía este artículo en mente pero me resistía a escribirlo, tal vez mi subconsciente creía que todo era un sueño. Lamentablemente... después de días y días, no lo es.

Nuestros mayores están en peligro, un serio peligro que no podemos obviar pues ellos fueron los que nos hicieron como somos; ellos trabajaron de sol a sol para legar a sus hijos y nietos un país mejor. Gracias a todos, esperando una pronta solución al **covid-19**.

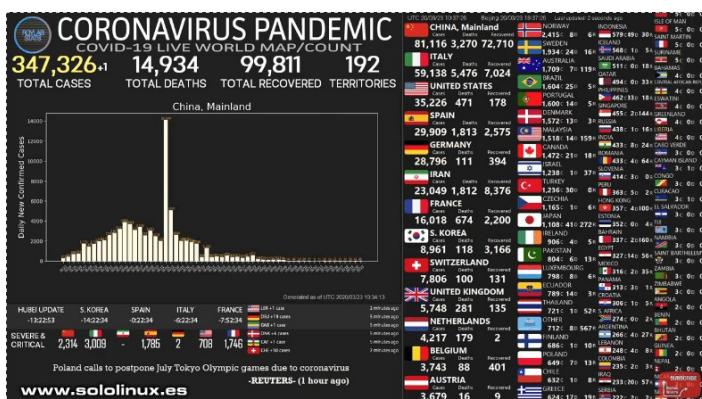
Vale... no nos pongamos tristes, pero ya que estamos inmersos en esta pandemia vamos a analizar sus efectos sobre la tecnología y sobre todo en nuestro sistema operativo favorito, linux.

Cómo afecta el coronavirus a la tecnología y a linux

Detectado por primera vez en la ciudad de **Wuhan** (diciembre de 2019), está causando estragos en la vida cotidiana de todos los países del mundo. Como no podía ser menos afecta de manera significativa a las industrias tecnológicas, también lo aprovechan los **ciberdelincuentes**.

Puedes ver el avance en tiempo real en la siguiente dirección:

<https://www.youtube.com/watch?v=qgylp3Td1Bw>



importa un pimiento el sufrimiento de otros y su único fin es lucrarse. No hablamos de hackers, pues un hacker sabe a quien ataca, sabe lo que hace y sabe el porque. Son **lamers** que lo único que saben hacer es copiar el trabajo de otros con el único fin de enriquecerse.

Tal como está la cosa ahora mismo, es evidente que las búsquedas en internet sobre el COVID-19 son considerables, muchas veces por usuarios inexpertos en seguridad. Los ciberdelincuentes (lamers) hacen uso de lo que se conoce como ingeniería social para que hagan clic en enlaces maliciosos.

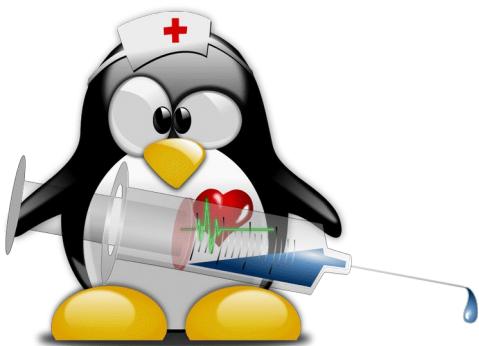
Estos usuarios de forma inconsciente ejecutan el **malware** del atacante, dicho y hecho, se abrió la puerta a la infección por ransomware. El **ransomware** toma el control de tu sistema y ejecuta un bloqueo total hasta que el incauto usuario pague una suma de dinero más o menos considerable.

Dos formas de ataque

Hay dos posibles métodos de ataque, ambos son sobre **phishing**. El primero instala el malware **AZORult**, para después meter el ransomware.

La segunda se basa en el **troyano Emotet**. En este, las víctimas reciben correos electrónicos que dicen contener información importante sobre el coronavirus, jaja, mentira, al hacer clic en el enlace se activa **Emotet**.

Seguramente aun no has recibido ningún ataque de AZORult, ni de Emotet. Debes estar alerta, tarde o temprano llegará.



El coronavirus y linux

Es evidente que el coronavirus no afecta a nuestro sistema operativo (sería un absurdo), pero si es cierto que el efecto de la desaceleración en la fabricación de los componentes necesarios para que Linux se ejecute, puede suponer un verdadero quebradero de cabeza y no solo en servidores, también en otras maquinas incluyendo las domesticas. Vemos algunos ejemplos.

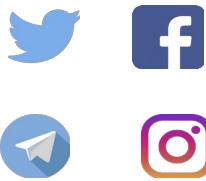
- **Purism** : Los smartphones Librem 5 con linux PureOS son los más afectados por el covid-19, el retraso en sus entregas serán considerables.
- **Dell** : Si, lees bien, el gigante de las computadoras Dell, a comunicado que posiblemente la principal fuente de suministros será interrumpida. Esto afectará de forma masiva a toda su producción, incluyendo sus máquinas con Ubuntu.
- **System76** : De los desarrolladores del sistema operativo Pop_OS!, no hace mucho tiempo llegaron sus propias máquinas. Lamentablemente los avisos de cese de fabricación (temporal) son constantes.
- **Pine64** : Que decir del fabricante de los famosos portátiles (de bajo coste) Pinebook Pro, el más asequible del mundo, que además admite la instalación de cualquier distribución linux. Al igual que los anteriores, también anuncia retrasos considerables en su producción.
- Grandes empresas relacionadas con el desarrollo de linux, están paralizando proyectos ante la situación extrema que viven sus programadores.

Conclusión final

Hoy más que nunca, debemos sumarnos todos para que esta pandemia acabe lo antes posible. Nuestro sistema linux nos ayudará a seguir trabajando; tal vez sea el momento de aprender aún más. Tampoco es el momento de reprochar nada a nadie, todos sabemos donde empezó todo y quien se va a llenar los bolsillos con ello.

Suerte a todos y seguir solo las instrucciones que provienen de fuentes oficiales.

Síguenos en las Redes:



Canales de Telegram: Canal [SoloLinux](#) – Canal [SoloWordpress](#)

Nomacs el visor de imágenes con editor incluido



www.sololinux.es

Todas las **distribuciones Linux** tienen su propio visor de imágenes predeterminado, dada su velocidad y eficacia únicamente la gran mayoría utilizan **Ristretto Image Viewer** (de **XFCE**).

Ristretto es un excelente visor, pero lo dicho... un visor. Existe una aplicación similar, muy rápida y segura que tal vez no conoces. Hablamos de **Nomacs** y en este artículo vemos sus principales características y como instalarlo en nuestro linux.

Nomacs el visor de imágenes con editor incluido

A pesar de ser muy ligero, nomacs no se limita a ser un simple visor de imágenes. Cuenta con unas particularidades únicas en este tipo de herramientas, ademas de un editor básico que seguro te puede sacar de algún apuro. Vemos sus principales características.

Características del visor de imágenes

- Admite los formatos de imagen más usados, incluido RAW.
- Vista previa en miniatura instantánea.
- Vista previa en cuadrícula con zoom de miniaturas.
- Muestra la información exif.
- Visualización sin marco.
- Permite modificar la transparencia de las ventanas.
- Información general sobre las imágenes: histograma, info del archivo, etc.
- Filtros de búsqueda y clasificación.
- Anti-aliasing mejorado.
- Permite ocultar el menú y la barra de herramientas.
- Diapositivas:
- Información de la imagen.
- Reproducir / pausar con un intervalo de tiempo a definir.
- Color de fondo adaptable.

Características del editor de imágenes

- Recortar imágenes.
- Modificar el tamaño de las imágenes.
- Varias funciones de color.
- Permite ajustar el color: brillo, contraste, saturación, etc.
- Permite exportar TIFF.
- Rotar las imágenes.
- Arrastrar y soltar.
- Guarda automáticamente capturas de pantalla.
- Borrar y renombrar imágenes.
- Crear imagen en mosaico.

Características de sincronización

- Sincronizar múltiples instancias.
 - Zoom sincronizado.
 - Vista panorámica sincronizada.
 - Adelante / atrás sincronizado.
 - Superposición de imágenes sincronizadas
 - Organizar instancias sincronizadas
- Sincronizar múltiples instancias en una red.
 - Zoom sincronizado.
 - Vista panorámica sincronizada.
 - Permite enviar imágenes a través de tu red.

Instalar nomacs en linux

Después de ver sus fantásticas características, vamos a instalar nomacs en nuestro linux favorito.

Instalar nomacs en Ubuntu, Linux Mint y derivados:

```
sudo add-apt-repository ppa:nomacs/stable  
sudo apt update  
sudo apt install nomacs
```

Instalar nomacs en Debian y derivados:

```
sudo apt install nomacs
```

Instalar nomacs en Fedora y derivados:

```
sudo dnf install nomacs
```

Instalar nomacs en Arch Linux, Manjaro y derivados:

```
pacman -S nomacs
```

Instalar nomacs en Suse, Open Suse y derivados:

En Open Suse puedes descargar la herramienta (según tu versión), desde su [página oficial](#).

Instalar nomacs con snap:

Si tienes problemas para instalar nomacs o simplemente prefieres usar paquetes snap, también es posible.

```
sudo snap install nomacs --edge
```

Ejecutar nomacs en linux

Una vez tengas instalada la herramienta, puedes lanzarla desde su ícono en el menú de aplicaciones o desde la propia terminal.

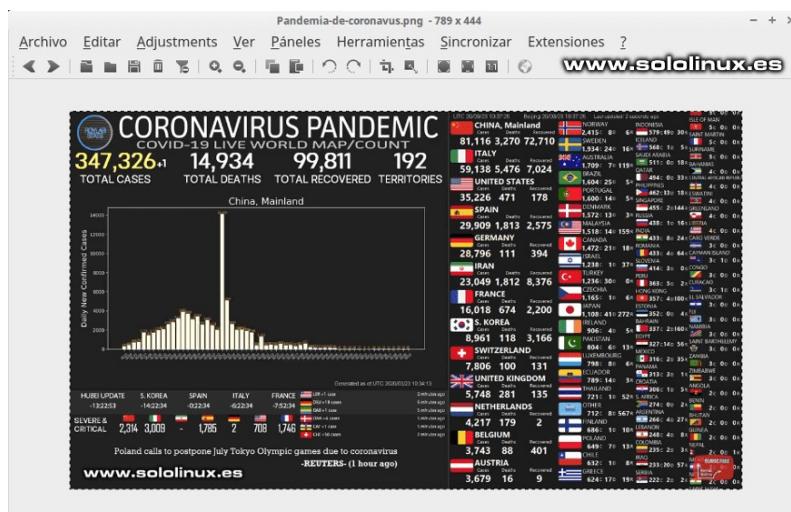
nomacs

Al iniciar por primera vez nos pregunta qué lenguaje queremos que sea el predeterminado. Selecciona el tuyo y reinicia el visor nomacs.



www.sololinux.es

Ya tenemos el visor con editor nomacs en nuestro idioma preferido.



Navega y prueba las opciones del menú, te sorprenderá lo potente que es nomacs.

Instalar y configurar opcache en php-fpm con Nginx



Cuando tienes un servidor **Nginx con php-fpm** y aun quieres mejorar un poco más su rendimiento, la primera acción que debes tomar es instalar y configurar opcache.

Un lector de **soloLinux.es** tenia dudas sobre como instalar y configurar opcache en Nginx, así que en este articulo vemos como realizar la operacion de manera rápida y sencilla. Nosotros operamos sobre un sistema CentOS 7 con el **panel de control VestaCP** instalado, en otras **distros linux** es similar.

Instalar opcache en php-fpm con Nginx

Para instalar **opcache** en **VestaCP** ejecutamos lo siguiente.

```
yum install php-opcache
```

Una vez tengamos opcache instalado, reiniciamos php-fpm.

```
systemctl restart php-fpm
```

Ahora Nginx.

```
systemctl restart nginx
```

Normalmente opcache se activa y habilita de forma automática, lo podemos verificar con el siguiente comando.

```
php -i | grep opcache.enable
```

Si todo salio bien, verás algo similar a...

```
[root@... ~]# php -i | grep opcache.enable
opcache.enable => On => On
opcache.enable_cli => On => On      www.soloLinux.es
```

Configurar opcache en php-fpm con Nginx

Opcache ya tiene su propia configuración predeterminada, pero es posible que la quieras modificar. Debes asegurarte de la versión php que tienes instalada y editar el archivo que corresponda, en nuestro ejemplo **php-fpm 7.3**.

```
nano /etc/php/7.3/fpm/php.ini
```

Busca la sección [opcache] y modifacas los valores según tus necesidades, no te olvides que para habilitar las indicaciones debes quitar el punto y coma «;» que aparece al principio de cada linea.

```
[opcache]
opcache.enable=1
opcache.memory_consumption=256
opcache.max_accelerated_files=9500
opcache.max_wasted_percentage=20
```

Una vez hayas terminado, guardas el archivo y cierras el editor.

Solo nos falta reiniciar los servicios.

```
sudo service nginx restart && sudo service php7.3-fpm restart
```

Ya tienes opcache corriendo en tu servidor Nginx.

Síguenos en las Redes:



Canales de Telegram:

Canal [SoloLinux](#)

Canal [SoloWordpress](#)

Qué es el registro PTR y para qué sirve

El **registro PTR (PTR records)**, es todo lo contrario a los **registros A** de los **nameservers (servidor de nombres)**.

La principal diferencia es que mientras un registro de tipo A, apunta un dominio a una **dirección IP**; el **registro PTR** resuelve la dirección IP a un servidor. Parecen similares verdad, pero lo cierto es que son dos registros independientes.

Los **registros PTR** se usan para encontrar las **DNS inversas** (Reverse DNS). Con la dirección IP podemos verificar a qué dominio o servidor se asocia. Debes tener presente que cada registro PTR necesita de un registro de tipo A.

Como saber si tenemos registro PTR

Desde la consola de nuestro sistema linux, es tarea sencilla verificar nuestro PTR. Existen muchas opciones pero sin duda... dos destacan sobre el resto.

Con «host» obtenemos exclusivamente los apuntes, pero ya es suficiente para verificar que nuestro PTR es válido.

```
host [ip]
```

```
sololinux ~ # host 163.138.161.87
87.161.138.163.in-addr.arpa domain name pointer host.miserver.com.
```

Personalmente prefiero usar el comando dig, nos aporta mucha más información.

```
dig -x [ip]
```

```
sololinux ~ # dig -x 163.172.107.87
```

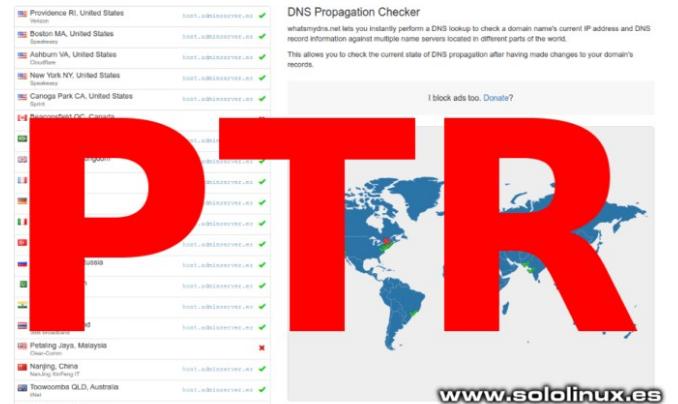
```
; <>> DiG 9.10.3-P4-Ubuntu <>> -x 163.138.161.87
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26580
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;87.161.138.163.in-addr.arpa. IN PTR

;; ANSWER SECTION:
87.161.138.163.in-addr.arpa. 82976 IN PTR host.miserver.com.

;; Query time: 7 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Wed Mar 25 20:46:23 EET 2020
;; MSG SIZE rcvd: 89
```

Este mini tutorial seguro que aclarara tus dudas.



Cómo montar un servidor de alto rendimiento con VestaCP

Hoy en día la velocidad de un sitio web es fundamental, de hecho cada día tiene más relevancia de cara al SEO. Por ello, vamos a crear dos artículos correlativos donde explicaremos como montar tu propio **servidor o VPS** de alto rendimiento.

- Cómo montar un servidor de alto rendimiento con VestaCP en CentOS 7
- Cómo optimizar Nginx con PHP-FPM en VestaCP con Centos 7.

Alguna vez me han preguntado porqué monto mis servidores con **CentOS 7**... bueno, tambien utilizo Debian, pero la verdad es que CentOS me parece mucho más versátil y abierto a cambios si lo comparamos con **Debian**, también por costumbre.

No es necesario puntualizar que estas instrucciones son válidas para cualquier servidor o VPS, aunque si necesitas un servidor dedicado totalmente administrado desde 15€, ponte en [contacto con nosotros](#) y te informaremos.

Montar un servidor de alto rendimiento con VestaCP

Instalar VestaCP

Partimos de la base que ya tienes VestaCP instalado con Nginx y php-fpm, si no es así... desde su [página oficial](#) puedes generar los comandos de instalación. Una buena selección es la que te indico en la siguiente imagen. No instales **softaculos**, es muy pesado y no es totalmente gratis (está capado, muy capado)



www.sololinux.es

Hostname	Email	Password
miserver.com	demo@miserver.es	123456789

```
# Connect to your server as root via SSH
ssh root@your.server

# Download installation script
curl -O http://vestacp.com/pub/vst-install.sh

# Run it
bash vst-install.sh --nginx yes --phpfpm yes --apache no --named yes --remi yes --vsftpd yes --proftpd no --iptables
yes --fail2ban yes --quota no --exim yes --dovecot yes --spamassassin yes --clamav no --softaculous no --mysql yes
--postgresql no --hostname miserver.com --email demo@miserver.es --password 123456789
```

Una vez instalado, lo primero que debemos hacer es actualizar e instalar el [repositorio epel](#).

```
yum update
yum install epel-release
yum update
```

Dependiendo de la versión que tengas de CentOS 7, se habrá instalado php 5.4, o php 5.6, esto es inadmisible. Si o si, debes instalar php 7.1 o superior. Mi recomendación a dia de hoy es php 7.2, ya que es la máxima que es 100% compatible con todos los plugins y temas de WordPress modernos.

Actualizar PHP en VestaCP

Para actualizar la versión de php debes habilitar el repositorio remi con la versión php que más te interese.

PHP 7.1

```
yum-config-manager --enable remi-php71
```

PHP 7.2

```
yum-config-manager --enable remi-php72
```

PHP 7.3

```
yum-config-manager --enable remi-php73
```

PHP 7.4

```
yum-config-manager --enable remi-php74
```

Actualizamos el sistema y reiniciamos php-fpm.

```
yum update
```

```
systemctl restart php-fpm
```

Instalar Opcache en VestaCP

La instalación de Opcache en VestaCP con Centos 7, es muy simple. Sigue los pasos indicados.

```
yum install php-opcache
```

```
systemctl restart php-fpm
```

```
systemctl restart nginx
```

Fácil verdad?. Si quieres modificar las opciones de opcache revisa el [articulo anterior](#).

Actualizar MariaDB en VestaCP

De manera predeterminada, **CentOS 7** viene con **MariaDB 5.5**. Es altamente recomendable actualizar como mínimo a MariaDB 10.3.

Primero hacemos una copia de seguridad por si acaso.

```
cp -a /var/lib/mysql/ /var/lib/mysql.bak
```

También necesitamos hacer un dump en temporales (inserta tu password root).

```
mysqldump -u root -Passdelroot --all-databases >
/tmp/all-database.sql
```

Creamos el repositorio de MariaDB 10.3.

```
sudo nano /etc/yum.repos.d/MariaDB10.repo
```

Copia y pega lo siguiente:

```
# MariaDB 10.3 CentOS repository list -  
sololinux.es  
#[mariadb]  
name = MariaDB  
baseurl = http://yum.mariadb.org/10.3/centos7-amd64  
gpgkey=https://yum.mariadb.org/RPM-GPG-KEY-MariaDB  
gpgcheck=1
```

Guarda el archivo y cierra el editor nano.

OJO!!!, antes de actualizar es conveniente borrar la versión anterior.

```
sudo yum remove mariadb-server mariadb mariadb-libs
```

Limpiamos la cache de los repositorios de CentOS 7.

```
sudo yum clean all
```

Instalamos la nueva versión de MariaDB.

```
sudo yum -y install MariaDB-server MariaDB-client
```

Una vez termine la actualización, iniciamos y habilitamos MariaDB 10.3.

```
sudo systemctl start mariadb  
sudo systemctl enable mariadb  
# o  
sudo systemctl enable mariadb.service
```

Importamos los datos anteriores (en caso de que los tuviéramos).

```
mysql_upgrade
```

Para concluir esta sección, actualizamos el sistema y verificamos la versión instalada de MariaDB.

```
sudo yum update  
mysql -V
```

```
[root@miserver ~]# mysql -V  
mysql Ver 15.1 Distrib 10.3.22-MariaDB, for Linux  
(x86_64) using readline 5.1
```

Instalar Redis en VestaCP

Redis es sistema de almacenamiento de datos estructurados en memoria, muy útil como memoria caché. Instalamos **Redis** ya que su rendimiento es superior a otras alternativas.

```
sudo yum install redis
```

Iniciamos Redis y lo habilitamos para que arranque con el sistema.

```
sudo systemctl start redis
```

```
sudo systemctl enable redis.service  
# o  
sudo systemctl enable redis
```

Habilitar Redis en WordPress con VestaCP

Si utilizas WordPress para crear tus sitios, es interesante agregar Redis como su sistema de almacenamiento en caché.

Lo instalamos:

```
sudo yum install php-devel
```

Ahora agregamos la extensión PHPRedis.

```
pecl install redis
```

Pulsa enter cuando aparezcan mensajes similares a...

```
enable igbinary serializer support? [no]
```

Para concluir es necesario agregar la extension a nuestro php.ini.

```
sudo nano /etc/php.ini
```

Al final del archivo agrega la siguiente linea.

```
extension=redis.so
```

Un plugin de cache que funciona muy bien con Redis es «[W3 Total Cache](#)». En su configuración elije 'Redis' como caché de página y caché de base de datos, después marca la casilla de verificación 'habilitar' en cada opción antes de hacer clic en el botón 'Guardar todas las configuraciones'. Esta configuración se debe hacer antes de reiniciar php-fpm y Nginx.

Como punto final al articulo reiniciamos php-fpm y nginx.

```
sudo systemctl restart php-fpm  
sudo systemctl restart nginx
```

Cómo optimizar Nginx con PHP-FPM en VestaCP con Centos 7

Si en el articulo anterior vimos cómo montar un servidor de alto rendimiento con **VestaCP** en **CentOS 7**, hoy terminamos la serie aprendiendo a optimizar Nginx con PHP-FPM en **VestaCP** con **Centos 7**.

- Cómo montar un servidor de alto rendimiento con VestaCP en CentOS 7.
- Cómo optimizar Nginx con PHP-FPM en Vesta CP con Centos 7.

Nginx + PHP-FPM son dos de las mejores opciones para un servidor de alto rendimiento, aportan gran velocidad y seguridad a los sitios web que tengamos alojados. **Nginx** ofrece el contenido estático y **PHP-FPM** trabaja como servidor de aplicaciones mejorando el primer byte de forma que los sitios web carguen muy rápido.

A pesar de que las configuraciones predeterminadas son aceptables, siempre las podemos mejorar, sobre todos si tenemos mucho tráfico o demasiados sitios web. En este articulo vemos como **optimizar Nginx** con PHP-FPM en nuestro servidor o VPS de alto rendimiento.



Optimizar Nginx

Abrimos el archivo de configuración.

```
nano /etc/nginx/nginx.conf
```

Busca la siguiente línea (el valor puede ser diferente).

```
#worker_rlimit_nofile    65535;
```

La descomentamos (borras la almohadilla).

```
worker_rlimit_nofile    65535;
```

Ahora busca la linea que te indico...

```
worker_connections 1024;
```

La modificamos.

```
worker_connections 5000;
```

Guarda el archivo y cierra el editor, nos falta reiniciar el servicio.

```
service nginx restart
```

Optimizar

php-fpm

De manera predeterminada **php-fpm** crea un archivo de configuración para cada sitio, debes acceder al directorio principal...

```
cd /etc/php-fpm.d
```

Y editar cada dominio por separado, en nuestro ejemplo **sololinux.es**

```
nano sololinux.es.conf
```

Nos encontramos con los siguientes datos.

```
pm.max_children = 4  
pm.max_requests = 4000
```

Los modificas por...

```
pm.max_children = 10  
pm.max_requests = 6000
```

Guarda el archivo y cierra el editor, es necesario reiniciar el servicio.

```
service php-fpm restart
```

La configuración propuesta, debe ser capaz de manejar alrededor de 2500 usuarios a la vez sin mucho esfuerzo.

Cómo instalar maldet y buscar malware en linux

maldet

anti malware



www.sololinux.es

Maldet (LMD) es una de las mejores herramientas que podemos encontrar en linux, para escanear un **sistema linux** en busca de malware. Normalmente archivos de sitios web infectados con código malicioso.

Los malwares son temidos por los servidores, envían correos electrónicos spam desde tu ip, aumenta la carga del servidor, son capaces de lanzar **ataques ddos**, en fin... un auténtico desastre.

Linux Malware Detect (LMD) es capaz de escanear el malware para Linux, detectarlo y enviar un mail a la cuenta que definas con el reporte. Si lo instalas junto a ClamAV también intentará desinfectar o poner en cuarentena el archivo; si escaneas un servidor web no es recomendable (puede borrar algo necesario).

En este artículo nos centraremos en cómo instalar Maldet y, buscar malware en cualquier distribución linux.

Instalar Linux Malware Detect en linux

La instalación de maldet es sencilla, tan solo sigue la secuencia de comandos que te indico.

```
cd /usr/local/src
```

```
rm -Rf maldetect-*
```

```
wget http://www.rfxn.com/downloads/maldetect-current.tar.gz
```

```
tar xfz maldetect-current.tar.gz
```

```
cd maldetect-*
```

```
./install.sh
```

Para actualizar las listas de firmas, ejecuta...

```
maldet -u
```

También puedes actualizar la herramienta maldet.

```
maldet -d
```

Escanear linux con Maldet

Para escanear de forma normal (recomendado) usaremos la opción «-a»

```
maldet -a [ruta]
```

```
maldet -a /home/*/public_html
```

```
maldet -a /home
```

Otro ejemplo interesante es analizar todos los dominios / suscripciones en Plesk (en Cpanel debes modificar los datos).

```
maldet -a /var/www/vhosts
```

Si quieras un escaneo en modo profundo (puede tardar muchas horas), modificamos las opciones por...

```
maldet -b --scan-all [ruta]
```

```
maldet -b --scan-all /home/*/public_html
```

Ver los registros de análisis

Se generan varios informes, los listamos todos.

```
maldet --report list
```

```
[root@host5 ~]# maldet --report list
Linux Malware Detect v2.4.4
(C) 2019 Ryan McDonald <ryan0r@rfxn.com>
This program may be freely redistributed under the terms of the GNU GPL v2

Mar 28 2020 03:45:49 | SCANID: 200328-0343.24468 | RUNTIME: 228s | F
ILES: 165 | HITS: 0 | CLEANED: 0
Mar 27 2020 12:04:46 | SCANID: 200327-1204.27624 | RUNTIME: 5351s | F
ILES: 24236 | HITS: 0 | CLEANED: 0
Mar 27 2020 11:59:38 | SCANID: 200327-1159.24477 | RUNTIME: 0s | F
ILES: 2 | HITS: 0 | CLEANED: 0
```

Si observas la imagen de ejemplo, verás la opción «**SCANID**». Anota las referencias posteriores a scanid y abres el informe con el siguiente comando.

```
maldet -q [informe]
```

```
maldet --report 200327-1204.27624
```

Poner en cuarentena los archivos infectados

Con la opción «q», podemos poner en cuarentena todos los archivos infectados de un informe.

```
maldet -q [informe]
```

```
maldet -q 200327-1204.27624
```

Alertas por correo electrónico

De forma automática maldet realiza análisis cada cierto tiempo, si quieras recibir las alertas por mail es posible. Accedemos al archivo de configuración.

```
cd /usr/local/maldetect/
```

```
nano conf.maldet
```

Busca la opción «**mail_alert**» e insertas «1».

```
email_alert="1"
```

Unas líneas más abajo introduces el correo donde quieras recibir las alertas (en **email_addr**).

```
email_addr="mail@tudominio.com"
```

Desinstalar Maldet

Hace unos años, para **desinstalar maldet** se debía borrar todo de forma manual. Por suerte, en las últimas versiones se introdujo un **script bash** que hace el trabajo por ti.

```
sh
/usr/local/maldetect/uninstall.sh
```

Solicita confirmación.

```
[root@host5 maldetect]# sh uninstall.sh
```

This will completely remove Linux
Malware Detect from your server
including all quarantine data!

Would you like to proceed? [y/n] y

La desinstalación de **Linux Malware Detect** a concluido.

```
Removed symlink
/etc/systemd/system/multi-
user.target.wants/maldet.service.
Linux Malware Detect has been
uninstalled.
```

No funciona la wifi en Debian después de su instalación

www.sololinux.es



Uno de los errores más comunes al instalar por primera vez la **distribución linux Debian**, es que no funciona la wifi.

Este problema se genera sobre todo en las tarjetas **Wifi Intel Wireless**, el motivo es evidente, Debian de manera predeterminada no instala drivers ni firmwares privativos. Los modelos afectados son los siguientes:

MODELO	FIRMWARE
Intel Wireless 8260 Bluetooth configuration, version 20.10.0.8	intel/ibt-11-5.ddc
Intel Wireless 8260 Bluetooth firmware, version 20.100.0.3	intel/ibt-11-5.sfi
Intel Wireless 8265 Bluetooth configuration, version 20.30.0.1	intel/ibt-12-16.ddc
Intel Wireless 8265 Bluetooth firmware, version 20.100.0.3	intel/ibt-12-16.sfi
Intel Wireless 9460/9650 (var 0 rev 1) Bluetooth configuration, version 20.10	intel/ibt-17-0-1.ddc
Intel Wireless 9460/9650 (var 0 rev 1) Bluetooth firmware, version 20.30.0.1	intel/ibt-17-0-1.sfi
Intel Wireless 9460/9650 (var 16 rev 1) Bluetooth configuration, version 20.60.0.2	intel/ibt-17-16-1.ddc
Intel Wireless 9460/9650 (var 16 rev 1) Bluetooth firmware, version 20.100.0.3	intel/ibt-17-16-1.sfi
Intel Wireless 9160/9260 (var 0 rev 1) Bluetooth configuration, version 20.10	intel/ibt-18-0-1.ddc
Intel Wireless 9160/9260 (var 0 rev 1) Bluetooth firmware, version 20.30.0.1	intel/ibt-18-0-1.sfi
Intel Wireless 9160/9260 (var 16 rev 1) Bluetooth configuration, version 20.60.0.2	intel/ibt-18-16-1.ddc
Intel Wireless 9160/9260 (var 16 rev 1) Bluetooth firmware, version 20.100.0.3	intel/ibt-18-16-1.sfi
Intel Wireless 3160 (B6) Bluetooth firmware patch, version 19.30	intel/ibt-hw-37.7.10-fw-1.0.1.2d.d.bseq
Intel Wireless 3160 (B4) Bluetooth firmware patch, version 19.01	intel/ibt-hw-37.7.10-fw-1.0.2.3.d.bseq
Intel Wireless 7260 (B5) Bluetooth firmware patch, version 20.60.0.2	intel/ibt-hw-37.7.10-fw-1.80.1.2d.d.bseq
Intel Wireless 7260 (B3) Bluetooth firmware patch, version 20.60.0.2	intel/ibt-hw-37.7.10-fw-1.80.2.3.d.bseq
Intel Wireless 7260 Bluetooth firmware generic patch	intel/ibt-hw-37.7.bseq
Intel Wireless 7265 (C0) Bluetooth firmware patch, version 19.30	intel/ibt-hw-37.8.10-fw-1.10.2.27.d.bseq
Intel Wireless 7265 (D0) Bluetooth firmware patch, version 20.60.0.2	intel/ibt-hw-37.8.10-fw-1.10.3.11.e.bseq
Intel Wireless 7265 (D1) Bluetooth firmware patch, version 20.70.0.4	intel/ibt-hw-37.8.10-fw-22.50.19.14.f.bseq

Intel Wireless 7265 Bluetooth firmware generic patch	intel/ibt-hw-37.8.bseq
Intel Wireless 100 firmware, version 39.31.5.1	iwlwifi-100-5.ucode
Intel Wireless 105 firmware, version 18.168.6.1	iwlwifi-105-6.ucode
Intel Wireless 135 firmware, version 18.168.6.1	iwlwifi-135-6.ucode
Intel Wireless 1000 firmware, version 39.31.5.1	iwlwifi-1000-5.ucode
Intel Wireless 2200 firmware, version 18.168.6.1	iwlwifi-2000-6.ucode
Intel Wireless 2230 firmware, version 18.168.6.1	iwlwifi-2030-6.ucode
Intel Wireless 3160 firmware, version 25.228.9.0	iwlwifi-3160-9.ucode
Intel Wireless 3160 firmware, version 17.bfb58538.0	iwlwifi-3160-17.ucode
Intel Wireless 3168 firmware, version 22.391740.0	iwlwifi-3168-22.ucode
Intel Wireless 3168 firmware, version 29.3e3b4de5.0	iwlwifi-3168-29.ucode
Intel Wireless 3945 firmware, version 15.32.2.9	iwlwifi-3945-2.ucode
Intel Wireless 4965 firmware, version 228.61.2.24	iwlwifi-4965-2.ucode
Intel Wireless 5100, 5300 and 5350 firmware, version 8.83.5.1	iwlwifi-5000-5.ucode
Intel Wireless 5150 firmware, version 8.24.2.2	iwlwifi-5150-2.ucode
Intel Wireless 6000 firmware, version 9.221.4.1	iwlwifi-6000-4.ucode
Intel Wireless 6005/6205 firmware, version 17.168.5.3	iwlwifi-6000g2a-5.ucode
Intel Wireless 6005/6205 firmware, version 18.168.6.1	iwlwifi-6000g2a-6.ucode
Intel Wireless 6030 firmware, version 18.168.6.1	iwlwifi-6000g2b-6.ucode
Intel Wireless 6250 firmware, version 41.28.5.1	iwlwifi-6050-5.ucode
Intel Wireless 7260 firmware, version 25.228.9.0	iwlwifi-7260-9.ucode
Intel Wireless 7260 firmware, version 17.bfb58538.0	iwlwifi-7260-17.ucode
Intel Wireless 7265 firmware, version 25.228.9.0	iwlwifi-7265-9.ucode
Intel Wireless 7265 firmware, version 17.bfb58538.0	iwlwifi-7265-17.ucode
Intel Wireless 7265D firmware, version 22.391740.0	iwlwifi-7265D-22.ucode
Intel Wireless 7265D firmware, version 29.3e3b4de5.0	iwlwifi-7265D-29.ucode
Intel Wireless 8000C firmware, version 22.391740.0	iwlwifi-8000C-22.ucode
Intel Wireless 8000C firmware, version 36.9f0a2d68.0	iwlwifi-8000C-36.ucode
Intel Wireless 8265 firmware, version 22.391740.0	iwlwifi-8265-22.ucode
Intel Wireless 8265 firmware, version 36.9f0a2d68.0	iwlwifi-8265-36.ucode
Intel Wireless 9000 firmware, version 34.ba501b11.0	iwlwifi-9000-pu-b0-jf-b0-34.ucode
Intel Wireless 9000 firmware, version 38.755cfdd8.0	iwlwifi-9000-pu-b0-jf-b0-38.ucode
Intel Wireless 9000 firmware, version 41.fc1a7aea.0	iwlwifi-9000-pu-b0-jf-b0-41.ucode
Intel Wireless 9260 firmware, version 34.ba501b11.0	iwlwifi-9260-th-b0-jf-b0-34.ucode
Intel Wireless 9260 firmware, version 38.755cfdd8.0	iwlwifi-9260-th-b0-jf-b0-38.ucode
Intel Wireless 9260 firmware, version 41.fc1a7aea.0	iwlwifi-9260-th-b0-jf-b0-41.ucode

Solución: No funciona la wifi en Debian

Por suerte la solución es bastante simple, tan solo debes descargar el paquete deb que corresponda a tu versión, e instalarlo de forma manual desde la siguiente url oficial.

Package firmware-iwlwifi

Otra propuesta es conectar tu sistema a la red con un cable RJ45 y, seguir las instrucciones que te planteo.

Abres «Configuración > Repositórios», o buscas en el menú de aplicaciones «Software y actualizaciones». Marcas las opciones de paquetes no libres (non-free).



Una vez habilitados los nuevos repositorios debes actualizar el sistema.

```
sudo apt update
```

Instalas los nuevos controladores iwlwifi.

```
sudo apt install firmware-iwlwifi
```

Una vez termine la instalación, solo necesitas reiniciar Debian.

```
reboot
```

Listo!!!, ahora ya debería funcionar tu tarjeta de red wifi.

Error: Las firmas siguientes no se pudieron verificar GPG

```

Err:4 http://archive.canonical.com/ubuntu xenial InRelease
  Las firmas siguientes no se pudieron verificar porque su clave pública no está disponible: NO_PUBKEY 40976EAF437D05B5 NO_PU
BKEY 3B4FE6ACC0B21F32
Des:1 http://ppa.launchpad.net/klaus-vormweg/bluefish/ubuntu xenial InRelease [17,5 kB]
Ign:8 http://ftp.mgts.jp/pub/linuxmint/packages/sylvia Release.gpg
Ign:10 http://dl.google.com/linux/chrome/deb/stable/Release.gpg
Des:15 http://ppa.launchpad.net/mkuspo/ppa/ubuntu xenial InRelease [18,0 kB]
Err:16 http://mirror.datacenter.by/ubuntu xenial InRelease
  Las firmas siguientes no se pudieron verificar porque su clave pública no está disponible: NO_PUBKEY 6A9653F936FD5529
Err:3 http://mirror.datacenter.by/ubuntu xenial InRelease
  Las firmas siguientes no se pudieron verificar porque su clave pública no está disponible: NO_PUBKEY 40976EAF437D05B5 NO_PU
BKEY 3B4FE6ACC0B21F32
Des:17 http://ppa.launchpad.net/nomacs/stable/ubuntu xenial InRelease [17,5 kB]
Err:11 http://mirror.datacenter.by/ubuntu xenial-updates InRelease
  Las firmas siguientes no se pudieron verificar porque su clave pública no está disponible: NO_PUBKEY 40976EAF437D05B5 NO_PU
BKEY 3B4FE6ACC0B21F32
Des:12 http://ppa.launchpad.net/purplecactus/stable/ubuntu xenial InRelease [17,5 kB]
Err:13 http://ppa.launchpad.net/quitters/guitters/ubuntu xenial InRelease [17,5 kB]
Des:14 http://ppa.launchpad.net/klaus-vormweg/bluefish/ubuntu xenial InRelease
  Las firmas siguientes no se pudieron verificar porque su clave pública no está disponible: NO_PUBKEY 8938CE95036FE61D
Err:15 http://ppa.launchpad.net/tista/adapte/ubuntu xenial InRelease
  Las firmas siguientes no se pudieron verificar porque su clave pública no está disponible: NO_PUBKEY 3729827454BBC8AC
Des:19 http://ppa.launchpad.net/tista/adapte/ubuntu xenial InRelease [17,5 kB]
Err:16 http://ppa.launchpad.net/deadsnakes/ppa/ubuntu xenial InRelease
  Las firmas siguientes no se pudieron verificar porque su clave pública no está disponible: NO_PUBKEY D99B1D2629935E8D
Err:17 http://ppa.launchpad.net/purple-developer/stable/ubuntu xenial InRelease
  Las firmas siguientes no se pudieron verificar porque su clave pública no está disponible: NO_PUBKEY 957B591768AFBC6
Des:20 http://ppa.launchpad.net/atareao/telegram/ubuntu xenial InRelease
  Las firmas siguientes no se pudieron verificar porque su clave pública no está disponible: NO_PUBKEY 957B591768AFBC6
Err:18 http://ppa.launchpad.net/atareao/telegram/ubuntu xenial InRelease
  Las firmas siguientes no se pudieron verificar porque su clave pública no está disponible: NO_PUBKEY 957B591768AFBC6
Des:19 http://ppa.launchpad.net/tista/adapte/ubuntu xenial InRelease

```

Error: Las firmas siguientes no se pudieron verificar porque su clave pública no está disponible: NO_PUBKEY 40976EAF437D05B5 NO_PUBKEY 3B4FE6ACC0B21F32.

Es un error bastante común en Ubuntu, Debian, Linux Mint y todos sus derivados, que al actualizar el sistema salte el famoso mensaje de que no encuentra las claves públicas de repositorios.

También puede aparecer el mismo error pero con un formato diferente:

W: Error de GPG: http://ppa.launchpad.net precise Release: Las firmas siguientes no se pudieron verificar porque su llave pública no está disponible: NO_PUBKEY 40976EAF437D05B5 NO_PUBKEY 3B4FE6ACC0B21F32

*Las firmas siguientes no se pudieron verificar porque su clave pública no está disponible: NO_PUBKEY 40976EAF437D05B5 NO_PUBKEY 3B4FE6ACC0B21F32
Obj:11 http://ppa.launchpad.net/deadsnakes/ppa/ubuntu xenial InRelease*

Err:4 http://security.ubuntu.com/ubuntu xenial-security InRelease

*Las firmas siguientes no se pudieron verificar porque su clave pública no está disponible: NO_PUBKEY 40976EAF437D05B5 NO_PUBKEY 3B4FE6ACC0B21F32
Obj:12 http://ppa.launchpad.net/klaus-vormweg/bluefish/ubuntu xenial InRelease*

Err:5 http://ppa.launchpad.net/atareao/telegram/ubuntu xenial InRelease

*Las firmas siguientes no se pudieron verificar porque su clave pública no está disponible: NO_PUBKEY 6A9653F936FD5529
Obj:13 http://ppa.launchpad.net/mkuspo/ppa/ubuntu xenial InRelease*

*Err:6 http://archive.canonical.com/ubuntu xenial InRelease
Las firmas siguientes no se pudieron verificar porque su clave pública no está disponible: NO_PUBKEY 40976EAF437D05B5 NO_PUBKEY 3B4FE6ACC0B21F32*

Obj:14 http://ppa.launchpad.net/homacs/stable/ubuntu xenial InRelease

Err:7 http://mirror.datacenter.by/ubuntu xenial-updates InRelease

Error: Las firmas siguientes no se pudieron verificar

Este error se produce (normalmente) por cuatro motivos totalmente diferentes:

- El servidor remoto tiene problemas de conectividad.
- Tu archivo de claves está corrupto.
- La key a caducado y no es posible actualizarla.
- Consciente o inconscientemente has borrado el archivo de claves.

Por ejemplo... si obtienes errores continuos o simplemente por mantener limpio el archivo, es conveniente **borrar el archivo de keys**. Lo puedes hacer de manera sencilla con el siguiente comando.

```
sudo rm /etc/apt/trusted.gpg
```

En este momento si ejecutas «**sudo apt update**», todos los repositorios te darán error. Podríamos solucionarlo agregando las keys manualmente con...

```
sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys [key]
```

El proceso descrito anteriormente es un tanto engorroso, sobre todo si son muchas. Yo te propongo otra solución, instalar la herramienta «**Y PPA Manager**» para que haga todo el trabajo por ti.

Instalar Y PPA Manager

La instalación es tan simple como seguir las siguientes indicaciones...

```
sudo add-apt-repository ppa:webupd8team/y-ppa-manager
```

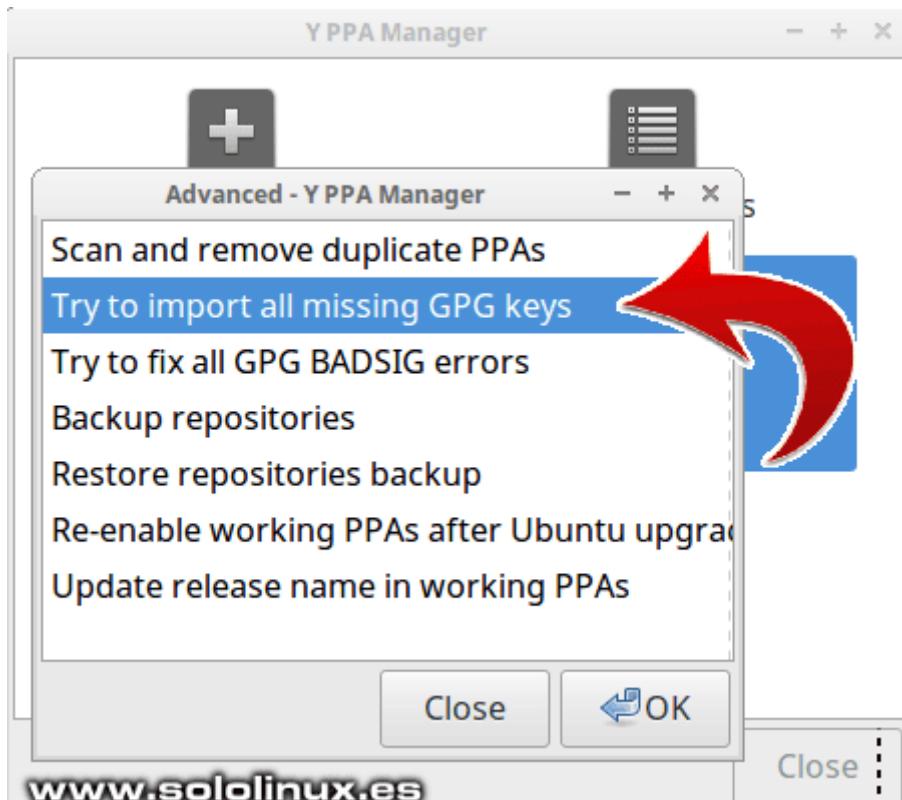
```
sudo apt-get update
```

```
sudo apt-get install y-ppa-manager
```

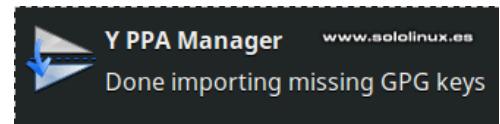
Busca la herramienta **Y PPA Manager** en tu menú de aplicaciones y la ejecutas. Te solicitará la contraseña del usuario con permisos. Pulsa en **Advanced**.



Ahora selecciona «Try to import all missing GPG keys» (importar las claves GPG) y, haz clic en OK.



Dependiendo de la conexión puede tardar más o menos. Si la importación es correcta verás una notificación de aviso similar a la siguiente imagen de ejemplo.

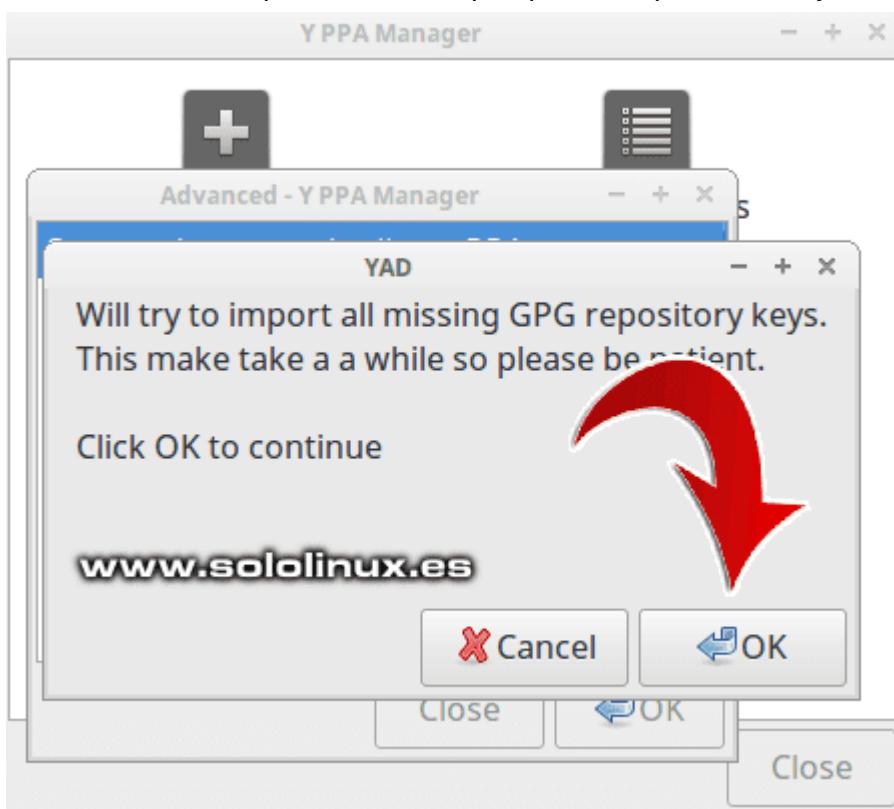


Bueno... ya tenemos nuestras keys recien importadas y renovadas. Ahora ya puedes actualizar el sistema, no tendras ningun problema.

```
sudo apt update
```

```
Sudo apt full-upgrade
```

Pulsa de nuevo OK para confirmar que quieres importar las keys.



Instalar y configurar vsFTPD en CentOS y derivados



El servidor **ftp**, **vsftpd**, es el preferido por la mayoría de **administradores de sistemas**. Sin duda alguna y pese a ser un veterano, es uno de los más potentes y completos que tenemos a nuestra disposición en cualquier **distribución Linux**.

VsFTPD ofrece una configuración sencilla pero muy completa y, eso es algo a tener en cuenta si lo comparamos con el resto de **servidores ftp**. En el artículo de hoy vemos como instalar y configurar (de forma básica), un **servidor vsFTPD** de forma que lo puedas tener en marcha en pocos minutos.

Instalar y configurar vsFTPD en CentOS

Instalar vsFTPD en CentOS, Fedora y derivados

Este **servidor ftp** está incluido en los repositorios oficiales, por lo tanto su instalación es tan simple como ejecutar el siguiente comando.

```
sudo yum install vsftpd
```

Una vez termine la instalación iniciamos vsFTPD.

```
sudo systemctl start vsftpd
```

Habilitamos su inicio al arrancar el sistema.

```
sudo systemctl enable vsftpd
```

Verificamos que se esta ejecutando de forma correcta.

```
sudo systemctl status vsftpd
```

```
[root@AMS-190854 ~]# sudo systemctl status vsftpd
● vsftpd.service - Vsftpd ftp daemon
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; vendor preset: disabled)
   Active: active (running) since mar 2020-03-31 08:15:52 CEST; 13s ago
     Main PID: 22210 (vsftpd)
        Group: /system.slice/vsftpd.service
           └─22210 /usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf

mar 31 08:15:52 AMS-190854 systemd[1]: Starting Vsftpd ftp daemon...
mar 31 08:15:52 AMS-190854 systemd[1]: Started Vsftpd ftp daemon.      www.sololinux.es
```

Configurar vsFTPD

Abrimos el archivo de configuración.

```
sudo nano /etc/vsftpd/vsftpd.conf
```

Como podrás comprobar existen muchas opciones que puedes configurar según tus necesidades, nosotros indicamos las básicas para un correcto funcionamiento del servidor. Debes asegurarte que ninguna de las siguientes líneas están comentadas.

```
# Habilitar o deshabilitar que un usuario anónimo acceda al servidor.
anonymous_enable=NO

# Permitir que los usuarios locales del sistema puedan acceder.
local_enable=YES

# Habilitar la escritura en vsFTPD.
write_enable=YES

# Habilitar lista de usuarios con acceso.
userlist_enable=YES

# Ruta de la lista de usuarios.
userlist_file=/etc/vsftpd/user_list

# No bloquear a los usuarios de la lista.
userlist_deny=NO

# Forzar archivos
force_dot_files=YES
```

Guarda el archivo y cierra el editor. Reiniciamos el servicio.

```
sudo systemctl restart vsftpd
```

Asegurar la transferencia ftp con SSL / TLS

Este paso es opcional, pero si quieres asegurar la transferencia de datos FTP con SSL / TLS, puedes seguir los pasos indicados a continuación.

Abrimos otra vez el archivo de configuración.

```
sudo nano /etc/vsftpd/vsftpd.conf
```

Al final del archivo agrega estas líneas...

```
ssl_enable=YES
rsa_cert_file=/etc/vsftpd/vsftpd.pem
rsa_private_key_file=/etc/vsftpd/vsftpd.pem
```

Guarda el archivo y cierra el editor.

Podemos generar un certificado autofirmado con este comando.

```
sudo openssl req -x509 -nodes -days 3650 -newkey
rsa:2048 -keyout /etc/vsftpd/vsftpd.pem -out
/etc/vsftpd/vsftpd.pem
```

Reinicia el servicio.

```
sudo systemctl restart vsftpd
```

Agregar FTP a FirewallD y SELinux

Si nuestro servidor CentOS tiene habilitado FirewallD, entonces es necesario abrir el puerto FTP 21.

```
sudo firewall-cmd --permanent --add-port=21/tcp  
# o  
sudo firewall-cmd --permanent --add-service=ftp
```

Recargamos la herramienta firewall.

```
sudo firewall-cmd --reload
```

En el caso que utilicemos SELinux...

```
sudo setsebool -P ftp_home_dir on
```

Agregar usuarios a vsFTPD

Creamos los usuarios de la manera habitual (en nuestro ejemplo, el usuario **sololinux**).

```
sudo adduser sololinux
```

Creamos la contraseña.

```
sudo passwd sololinux
```

ejemplo...

```
[root@myserv ~]# sudo passwd sololinux  
Cambiando la contraseña del usuario sololinux.  
Nueva contraseña: *****  
Vuelva a escribir la nueva contraseña: *****  
passwd: todos los símbolos de autenticación se actualizaron con éxito.
```

Como punto final del artículo, agregamos el usuario a la lista de permitidos.

```
sudo echo "sololinux" | sudo tee -a /etc/vsftpd/user_list
```

Nota: También puedes agregar usuarios directamente en el archivo.

```
nano /etc/vsftpd/user_list
```

Cómo subir el volumen en linux cuando se escucha muy bajo

Pulseaudio es el servidor de audio por excelencia en **derivados de Unix**, por ejemplo linux. Cuenta con unas características increíbles, citamos algunas:

- *Cada aplicación tiene su propio control de volumen.*
- *Arquitectura ampliable con soporte para módulos.*
- *Funciona con prácticamente la totalidad de reproductores.*
- *Soporta muchas fuentes de audio.*
- *Soporta la medición de la latencia.*
- *Hace uso del principio Zero Copy de memoria para mejorar el rendimiento del sistema.*
- *Si estás en una red local con otras sistema que también usan PulseAudio, se permite reproducir el sonido de tu sistema en los altavoces de otra máquina de la red.*
- *Puedes cambiar el dispositivo de salida en plena reproducción del audio.*
- *Tiene interfaz CLI en línea de comandos.*
- *Visor de conversión y muestreo.*
- *Es posible combinar varias tarjetas de sonido como si fueran una sola.*
- *Se permite sincronizar múltiples canales de reproducción.*

A pesar de la particularidad de Pulseaudio, si el volumen del sistema suena muy bajo aunque lo subamos al 100%, es evidente que no es culpa de la aplicación pulse.

Cuando se instala pulseaudio se realizan una serie de pruebas automáticas, en las cuales se analiza la tarjeta de audio, tipo de altavoces y sistema. Basándose en reglas de volumen y calidad, el servidor de audio establece el tope máximo de volumen (100%).

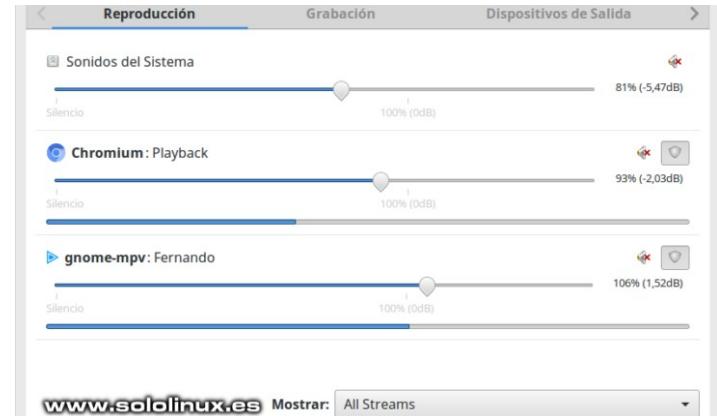
Pero claro... puede darse el caso que algún video o audio ha sido grabado a un volumen muy bajo (normalmente por una tasa de bits baja) y su reproducción normal no es buena, se escucha muy bajo.

Subir el volumen en linux cuando se escucha muy bajo

No te preocupes, pulseaudio nos permite forzar el sistema para que aumente el volumen del sistema. Lo único que tenemos que hacer es instalar las utilidades de pulseaudio (si no las tenemos instaladas).

Debian, Ubuntu, Linux Mint y derivados:

```
sudo apt install pulseaudio-utils
```



www.sololinux.es Mostrar: All Streams

CentOS, Fedora y derivados:

```
# CentOS  
sudo yum install pulseaudio-utils  
  
# Fedora  
sudo dnf install pulseaudio-utils
```

Arch Linux, Manjaro y derivados:

```
pacman -S pulseaudio
```

Una vez instalado podemos subir el volumen a un valor más acorde (en nuestro ejemplo a 150%), con el siguiente comando:

```
pactl set-sink-volume 0 150%
```

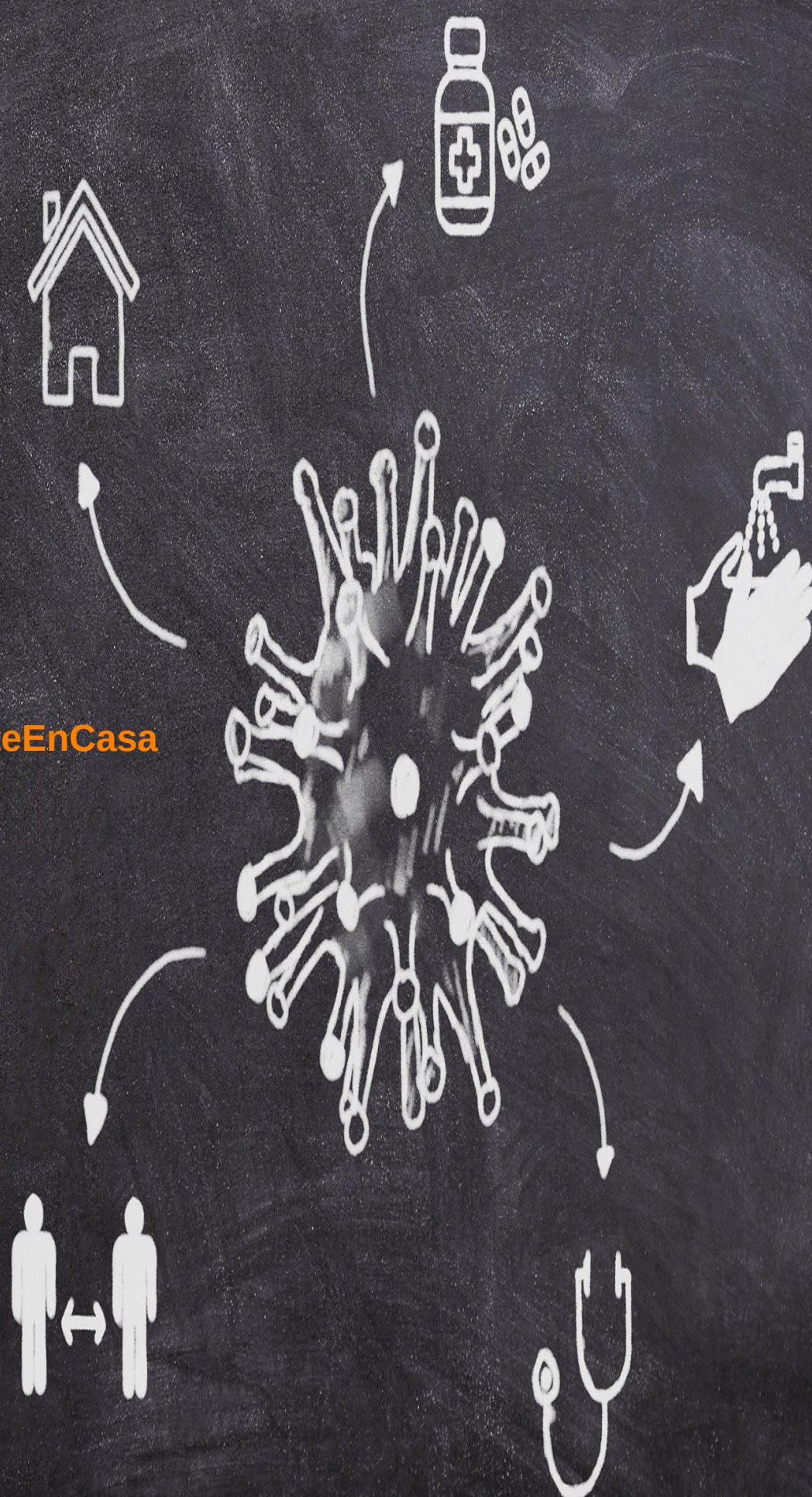
El volumen aumentó de forma considerable verdad?. No te recomiendo que excedas de 175 o 180, es el umbral donde si se pierde mucha calidad.

Si observas el comando con el que hemos subido el volumen, verás que antes del 150% insertamos un «0». El cero es por defecto el hardware de audio de los sistemas que solo tienen una tarjeta de audio, si tienes más de una ejecuta el siguiente comando para averiguar el número correspondiente a la que te interese.

```
pacmd list-sinks | grep -e 'name:' -e 'index'
```

```
sergio@sololinux ~ $ pacmd list-sinks | grep -e 'name:' -e 'index'  
* index: 0 ----->  
      name: <alsa_output.pci-0000_00_1b.0.analog-stereo>
```

Con este artículo finalizamos el triste mes de marzo del 2020. Suerte a todos y quedáros en casa, no vayáis a pillar el bicho (covid-19).



#QuedateEnCasa

