

Misceláneo

Capítulo destinado a diferentes acciones, técnicas, procedimientos en respuesta a casos de incidentes no categorizados e incluye incidentes por errores de configuración en software que tienen el objetivo de recuperar el servicio e información.

- [Recrear datastore eliminado VMware vSphere](#)
- [Exportar e importar posts de wordpress a una nueva instalación](#)
- [Recuperar acceso root mediante cambio de contraseña](#)

Recrear datastore eliminado VMware vSphere

- Identificar el “Device Name”

```
esxcli storage vmfs extent list
```

En este ejemplo el resultado del comando anterior es “mpx.vmhba0:C0:T0:L0” (Device Name) , reemplazar con el valor correspondiente a su instalación

- Identificar el bloque de inicio

```
offset="128 2048"; for dev in `esxcfg-scsidevs -l | grep "Console Device:" | \
awk {'print $3'}`; do disk=$dev; echo $disk; partedUtil getptbl $disk; \
{ for i in `echo $offset`; do echo "Checking offset found at $i:"; \
hexdump -n4 -s $((0x100000+(512*$i))) $disk; \
hexdump -n4 -s $((0x1300000+(512*$i))) $disk; \
hexdump -C -n 128 -s $((0x130001d + (512*$i))) $disk; done; } | \
grep -B 1 -A 5 d00d; echo "———"; done
```

En este ejemplo el inicio del bloque es 2048:

Checking_offset_found_at_2048:

- Obtener los sectores usables. Usar el “device name” correspondiente a su instalación

```
partedUtil getUsableSectors /vmfs/devices/disks/mpx.vmhba0:C0:T0:L0
```

En este ejemplo el valor de los sectores usables es 83886046

- Recrear partición usando los “sectores usables” y el “device name” correspondiente a su instalación

```
partedUtil mklabel /vmfs/devices/disks/mpx.vmhba0:C0:T0:L0 gpt
```

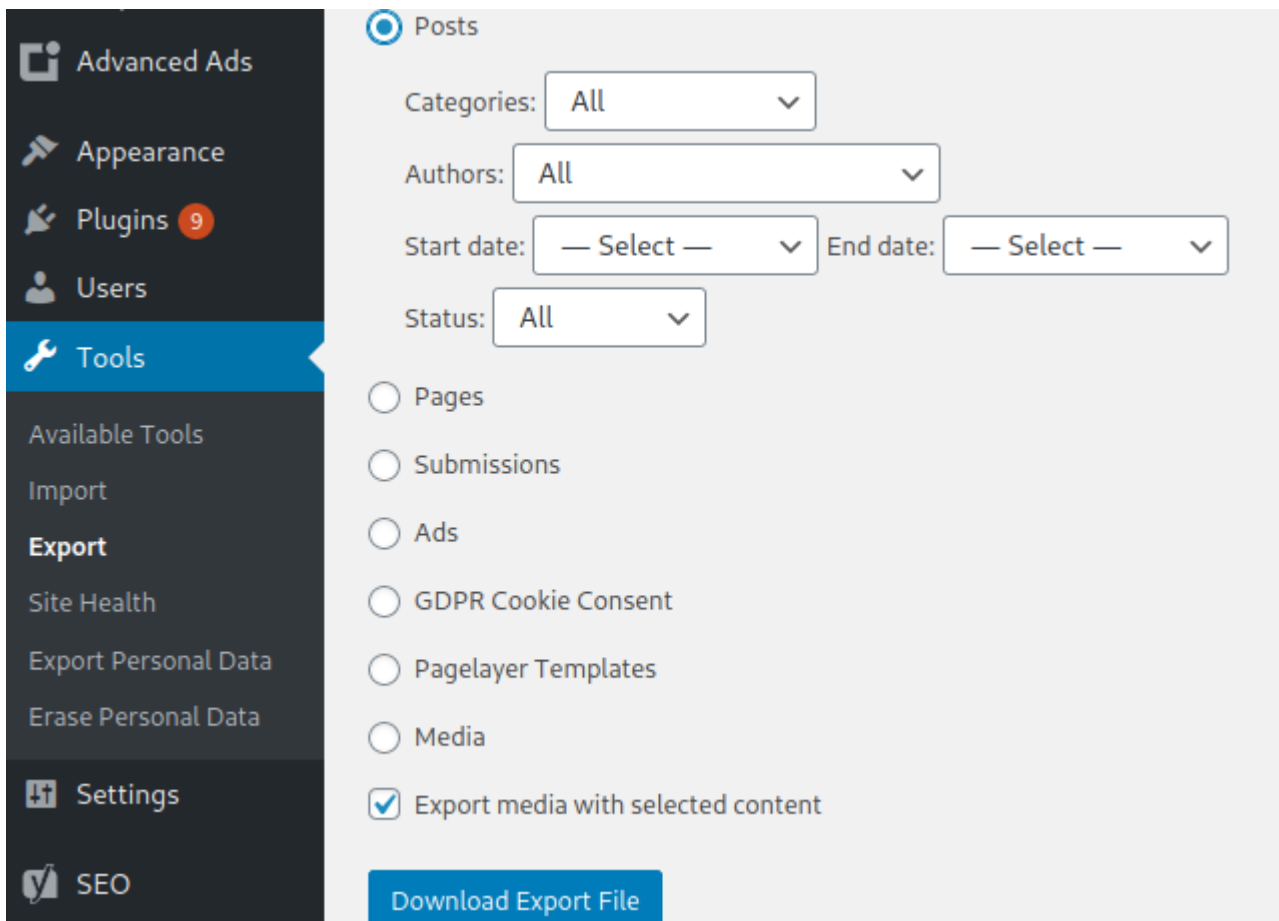
```
partedUtil setptbl "/vmfs/devices/disks/mpx.vmhba0: C0: T0: L0" gpt "1 2048 83886046
```

```
AA31E02A400F11DB9590000C2911D1B8 0"
```

Exportar e importar posts de wordpress a una nueva instalación

Exportar los posts

- Instalar y activar este plugin en la instalación de wordpress de donde se exportara los posts <https://wordpress.org/plugins/export-media-with-selected-content/>
- Exportar los posts (Seleccionar la opción de exportar con contenido multimedia)



The screenshot shows the WordPress dashboard's 'Tools' menu. The 'Tools' menu item is highlighted in blue. Below it, the 'Export' option is selected, and the 'Download Export File' button is visible at the bottom.

Tools

- Advanced Ads
- Appearance
- Plugins 9
- Users
- Tools**
- Available Tools
- Import
- Export**
- Site Health
- Export Personal Data
- Erase Personal Data
- Settings
- SEO

Posts

Categories: All

Authors: All

Start date: — Select — End date: — Select —

Status: All

☐ Pages

☐ Submissions

☐ Ads

☐ GDPR Cookie Consent

☐ Pagelayer Templates

☐ Media

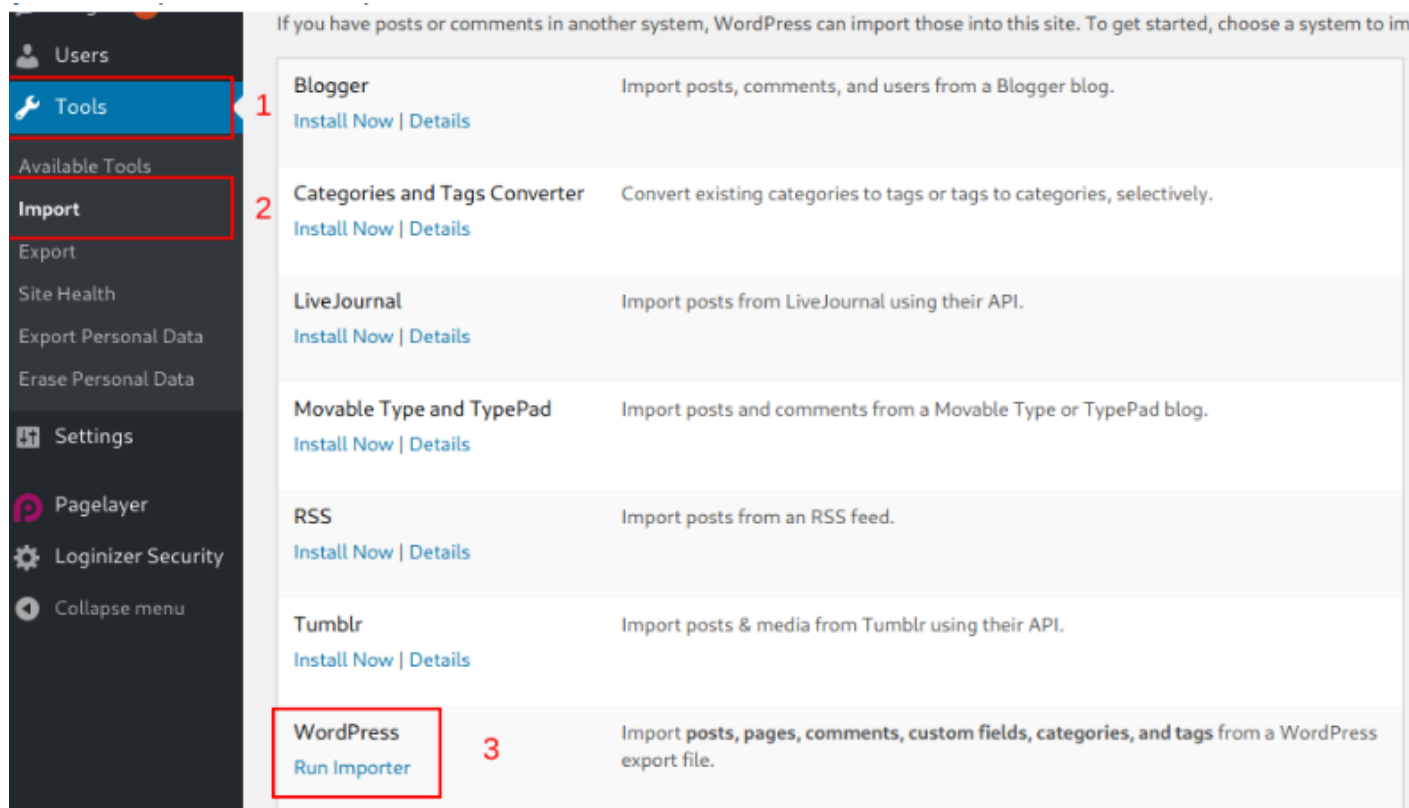
☒ Export media with selected content

[Download Export File](#)

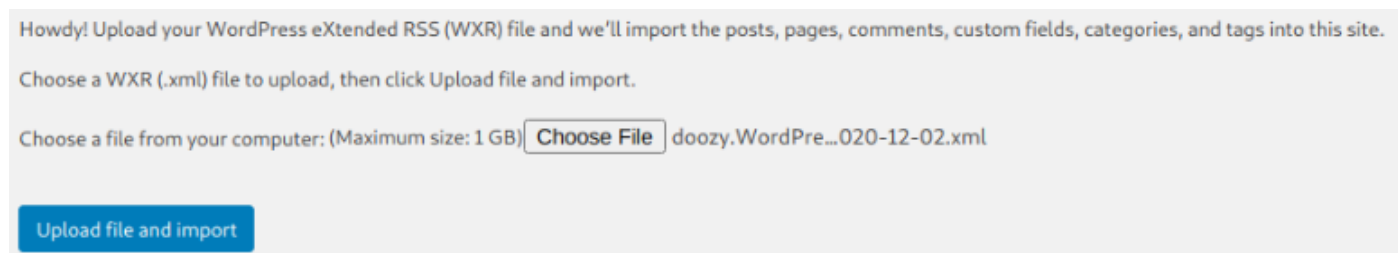
- Se descargara un archivo xml con los posts. Si se genera muchos errores 50x debido a la sobrecarga del servidor se recomienda exportar el contenido por meses para que el servidor no tenga que procesar tantos archivos en una sola petición

Importar los posts

- Ejecutar el importador de WordPress



- Cargar el archivo generado anteriormente



- Asignar con que autor se importara el contenido (Seleccionar la opción de descargar e importar adjuntos)

Assign Authors

To make it simpler for you to edit and save the imported content, you may want to reassign the au

If a new user is created by WordPress, a new password will be randomly generated and the new u

1. Import author: **d00zyAdmin (d00zyAdmin)**

or create new user with login name:

or assign posts to an existing user:

admin-news (admin-news) ▼

Import Attachments

☒ Download and import file attachments

Submit

-
- Importará automáticamente las categorías

Recuperar acceso root mediante cambio de contraseña

Reiniciando el sistema

- Reiniciar el sistema y presione cualquier tecla para detener el proceso de inicio. Presione “e” para editar los parámetros de la línea de comandos del kernel.
- Adicionar el parámetro “init=/bin/bash” e iniciar el sistema (F10)
- Para montar el sistema de archivos raíz en “modo lectura-escritura”.
- Cambiar el password con el comando passwd
- Reiniciar el sistema y ingresar con el nuevo password

Sin reiniciar el sistema

La unica opcion para este escenario es la ejecución remota de código (RCE) mediante la explotación de alguna vulnerabilidad para cambiar password del usuario root. Las vulnerabilidades identificadas para Debian 9 son:

- CVE-2019-11815 Dificil de explotar y existe una gran probabilidad de causar una denegacion de servicio. No existe exploit público
- CVE-2020-15862 No existe exploit público

Fuente: <https://security-tracker.debian.org/tracker/CVE-2019-11815>