

VMware

- [Desbloquear root en ESXi](#)
- [Cómo activar SNMP en VCSA](#)
- [Purple Screen Of Death](#)
- [SNMP en VMWare ESXi](#)
- [VMware cambiar ubicación de los Snapshots](#)
- [VMware Saber IP iDRAC DELL](#)
- [VMWare comandos de consola útiles](#)

Desbloquear root en ESXi

Si la cuenta root se bloquea debido a demasiados intentos fallidos de inicio de sesión, pierde el cliente web vsphere y el acceso ssh al host, la única forma de desbloquearlo es hacerlo a través de la consola DCUI-> ESX Shell, el siguiente comando restablecerá la cuenta root.

```
esxihost01# pam_tally2 --user root --reset
```

En un host ESXi independiente sin que vCenter lo administre, solo puede establecer reglas de firewall mediante esxcli a través de SSH o ESX Shell. Los siguientes comandos permiten que solo la red a.b.c.d / e acceda al cliente web de vSphere y SSH.

```
esxcli network firewall ruleset set --allowed-all false --ruleset-id=vSphereClient
esxcli network firewall ruleset set --allowed-all false --ruleset-id=sshServer
esxcli network firewall ruleset allowedip add --ip-address=a.b.c.d/e --ruleset-id=vSphereClient
esxcli network firewall ruleset allowedip add --ip-address=a.b.c.d/e --ruleset-id=sshServer
```

Cómo activar SNMP en VCSA

El primer paso es activar SNMP si no está activado, para ello nos logaremos por SSH en nuestro vCenter Appliance VCSA

```
etaboada@MacBookProEdu ~ % ssh root@X. X. X. X

VMware vCenter Server Appliance 6.5.0

Type: vCenter Server with an embedded Platform Services Controller

root@X. X. X. X's password:
Last login: Fri Oct 16 05:27:48 2020 from Y. Y. Y. Y
Connected to service

* List APIs: "help api list"
* List Plugins: "help pi list"
* Enable BASH access: "shell.set --enabled True"
* Launch BASH: "shell"

Command>
```

Copy

Teclearemos snmp.get

```
Command> snmp.get
Config:
  Enable: True
  Users:
  Notraps:
  Privacy: none
  Loglevel: warning
  V3targets:
  Pid: 29643
```

```
Syslocation: Yécora 4, 28022 Madrid, Spain
Targets:
Remoteusers:
Authentication: none
Communities: At3incoSNMPMng
Engineid: 80001adc808ad6440eb8497b5f00000000
Port: 161
Syscontact: sistemas@ateinco.es
Command>
```

Copy

Vemos que está activado. En el caso de que el campo Enable estuviera en false, deberemos de configurar el SNMP

En el siguiente comando vamos a configurar SNMP de manera básica usando la comunidad public, a su vez vamos a decirle que quiero que nos lance todas las traps al Host de PRTG, y posteriormente que solamente envíe las notificaciones de warning y error.

```
Command> snmp.set --communities public
Command> snmp.set --targets 192.168. X. X@162/public
Command> snmp.set --loglevel warning
Command> snmp.enable
```

Purple Screen Of Death

VMware: ESXi pantalla rosa, reinicio automático

A veces VMware provoca una pantalla rosa o púrpura cuando existe algún fallo. El problema es que VMware se queda ahí y no se reinicia, con lo que perdemos totalmente el control de la máquina

En ocasiones nos puede interesar configurar el host ESXi para que se reinicie si se produce una pantalla rosa

Para configurar el reinicio automático del host ESXi en caso de kernel panic (pantalla rosa) desde CLI:

Haremos login via ssh al host ESXi, y una vez dentro teclearemos

```
esxcfg-advcfg -s 15 /Misc/BlueScreenTimeout
```

El valor 15 indica el número de segundos de espera antes del reinicio. Podemos provocar un Kernel Panic para comprobar el funcionamiento, para ello teclearemos:

```
vsish -e set /reliability/crashMe/Panic 1
```

OJO MUY IMPORTANTE. Esto provocará un Kernel Panic, no hagas esto si la máquina está en producción y tiene VM arrancadas.

SNMP en VMWare ESXi

Configurar SNMP en VMWare ESXi

Comprobar si el SNMP está activo en VMWare ESXi

Para configurar los nodos ESXi, debemos comprobar que el SNMP está activo, para ello vamos a la configuración de servicios, y comprobamos si el servicio SNMP está arrancado, en caso de que no esté arrancado, trataremos de iniciar el servicio. Si nos arroja un error, lo más normal es que esto venga dado por un problema en los retornos de carro del fichero de configuración de SNMP en el nodo de ESXi que en muchos casos viene mal en las ISO de instalación. Este problema que está reportado por VMware se soluciona de la siguiente forma:

Hacemos login por ssh al nodo ESXi. En caso de que no podamos accederé s necesario habilitar el ssh. Para ello haz clic con el botón derecho en Host desde el inventario de VMware Host Client.

Selecciona Servicios en el menú desplegable y, a continuación, Secure Shell (SSH). Si SSH está deshabilitado, haz clic en Habilitar para habilitarlo.

En el caso de usar el cliente convencional de VMWare, en configuración, perfil de seguridad.

En algunos sistemas VMWare ESXi, aparece un warning cuando se habilita, si se desea que el SSH esté habilitado y quitar el warning, vamos a Configuración en el host ESXi, vamos a Opciones Avanzadas y buscamos en UserVars , hay una opción que se llama UserVars.SuppressShellWarning. Cambiamos el valor de 0 a 1, pulsamos Ok y ya lo tenemos

Ahora que tenemos todo, y habilitado el SSH, procedemos a hacer login

```
etaboda@MacBookProEdu ~ % ssh root@mad01vmw009. xxxxx.net
Password:

The time and date of this login have been sent to the system logs.
VMware offers supported, powerful system administration tools. Please
see www.vmware.com/go/sysadmintools for details.

The ESXi Shell can be disabled by an administrative user. See the
vSphere Security documentation for more information.

[root@mad01vmw009: ~]
```

Vamos a la carpeta de configuración de vmware

```
[root@mad01vmw009: ~] cd /etc/vmware
```

Realizamos una copia del fichero de configuración de SNMP

```
[root@mad01vmw009: ~] cp snmp.xml snmp.xml.OLD
```

A continuación, editamos el fichero snmp.xml

```
[root@mad01vmw009: ~] vi snmp.xml
```

Borramos el contenido del fichero. Ahora con el fichero vacío, debemos de copiar el siguiente contenido.

```
<?xml version='1.0' encoding='ISO-8859-1' ?>
<config>
<snmpSettings>
<enable>true</enable>
<port>161</port>
<syscontact>correo@midominio.com</syscontact>
<syslocation>Calle, CP, Ciudad, Pais</syslocation>
<EnvEventSource>indications</EnvEventSource>
<communities>MICOMUNIDAD</communities>
<loglevel>info</loglevel>
<authProtocol></authProtocol>
<privProtocol></privProtocol>
</snmpSettings>
</config>
```

En este caso, pondremos como Syscontact la dirección de correo o el nombre del administrador del sistemas. Como ubicación la dirección donde está el servidor o algún valor que nos sea útil. Si ponemos la dirección como calle, código postal, ciudad, país. El SNMP nos ubicará el servidor en el mapa.

En la cadena de comunidades en lugar de MICOMUNIDAD; pondremos el nombre de nuestra comunidad SNMP.

Guardamos el fichero y comprobaremos que el servicio SNMP se inicia y lo configuraremos si es así, para que se inicie con el host

VMware cambiar ubicación de los Snapshots

En infraestructuras virtuales VMware ESXi, en ocasiones, nos podemos encontrar con la necesidad de **cambiar la ubicación de los snapshots de una máquina virtual**.

Como ya sabemos, el software de copias de seguridad a nivel de hipervisor utiliza snapshots durante el proceso de la copia de seguridad.

Dicho de otra forma, al iniciar una copia de seguridad de una VM, se realiza un snapshot de la misma y al finalizar se borra.

El problema viene cuando disponemos de poco espacio en el datastore y la VM, durante el proceso de backup, se realizan cambios sobre la misma, por ejemplo, aplicación de parches etc... pueden provocar que el snapshot crezca y por tanto peligre el espacio libre en el datastore.

El hecho es que de forma predeterminada, los ficheros asociados al snapshot, se guardan en la misma ubicación que el resto de ficheros de la máquina virtual.

Por tanto, de forma predeterminada, los ficheros de la VM y los ficheros asociados al snapshot se guardan en el mismo datastore.

Veamos cómo cambiar ubicación por defecto de los snapshots de una VM:

Para ello, seguiremos los siguientes pasos:

1) Buscamos una ruta donde ubicar los snapshots.

Si conectamos vía SSH, veremos los datastores que tiene montados el host ESXi, ejecutando:

```
ls -lF /vmfs/volumes
```

Por ejemplo, podemos crear una carpeta dedicada a los snapshots en el DATASTORE1, para la VM1:

```
mkdir /vmfs/volumes/DATASTORE1/VM1/snapshots
```

Entendemos que la VM1, actualmente reside en otro datastore.

2) Paramos la VM.

3) Editamos el fichero VMX de la VM y añadimos:

```
workingDir="/vmfs/volumes/DATASTORE1/VM1/snapshots"
```

y a partir de ESXi 5, añadimos también:

```
snapshot.redoNotWithParent = "true"
```

4) Debemos desregistrar y registrar la VM en el inventario.

Si queremos realizar el proceso vía SSH, bastará con ejecutar:

A) Listamos las VMs para obtener el vmid de la VM que queremos desregistrar:

```
vim-cmd vmsvc/getallvms
```

B) Desregistramos la VM, indicando el vmid:

```
vim-cmd vmsvc/unregister vmid
```

C) Registramos la VM, indicando la ruta al fichero VMX:

```
vim-cmd solo/registervm /ruta-al-fichero-vmx
```

5) Iniciamos la VM.

VMware Saber IP iDRAC DELL

En ocasiones, nos podemos encontrar en un entorno VMware ESXi con que no sabemos la dirección IP de la tarjeta iDRAC de un servidor DELL.

Las tarjetas iDRAC (Integrated Dell Remote Access Controller) permiten al administrador monitorizar y administrar de forma remota un servidor DELL.

Con la iDRAC, incluso podemos actualizar el firmware del servidor o acceder a la consola del servidor.

Existen varias formas de saber la dirección IP de nuestra iDRAC.

En el caso de que:

- No podemos reiniciar el host VMware ESXi.
- No podemos instalar las herramientas de DELL.
- No podemos acceder al Virtual Center.

Disponemos de esta alternativa:

Entrar vía SSH en el host ESXi y ejecutar:

```
enum_instances OMC_IPMIIPProtocolEndpoint root/cimv2 | grep IPv4Address
```

Ejecutando esta acción, conseguimos obtener la dirección IPv4 de nuestra iDRAC.

No confundir este comando, con el comando `esxcli` para obtener las direcciones IPv4 de las NICs del host VMware ESXi:

```
[root@ESX-CPD-C:~] esxcli network ip interface ipv4 get
Name IPv4 Address IPv4 Netmask IPv4 Broadcast Address Type DHCP DNS
-----
vmk0 10.126.1.40 255.255.255.0 10.126.1.255 STATIC false
vmk1 192.168.1.40 255.255.255.0 192.168.1.255 STATIC false
[root@ESX-CPD-C:~]
[root@ESX-CPD-C:~]
[root@ESX-CPD-C:~] enum_instances OMC_IPMIIPProtocolEndpoint root/cimv2 | grep IPv4Address
IPv4Address = 10.126.1.140
[root@ESX-CPD-C:~]
[root@ESX-CPD-C:~]
```

- 1) Lista de direcciones IP de los interfaces de red de VMware ESXi.
- 2) Dirección IP de la iDRAC DELL.

VMWare comandos de consola útiles

En el caso de no disponer de acceso a la consola web de VMWare, a veces necesitamos realizar ciertas acciones y sin este acceso no se pueden realizar.

La solución consiste en usar los comandos de consola de VMWare ESXI para realizarlos.

Habilita la sesión SSH con acceso root:

Desde el vSphere Client

En VMware vSphere Client, navega hasta Hosts y clústeres y selecciona el host ESXi, luego haz clic en Servicio >> Configurar >> SSH.

Haz clic en Iniciar para iniciar el servidor SSH.

En la consola de ESXi (DCUI)

Accedemos a la consola de ESXi (DCUI) y en opciones de solución de problemas (Troubleshooting Options) entramos y hacemos click en habilitar SSH.

Login en la consola SSH

Hacemos login como root en la consola ssh y ya podremos ejecutar los comandos necesarios para trabajar.

Listado de las máquinas VMWare

Escribe el siguiente comando para obtener una lista de todos los hosts virtuales registrados, identificados por su VMID, nombre para mostrar y ruta al archivo de configuración .vmx:

```
vim-cmd vmsvc/getallvms
```

Obtendremos una salida como la que mostramos

```
[root@vmw253: ~] vim-cmd vmsvc/getallvms
```

Vmid	Name	File	Guest
OS	Version	Annotation	
175	VMFW01	[SSD253_01] VMFW01/VMFW01. vmx	
freebsd64Guest	vmx- 11		
191	Management	[SSD253_01] Management/Management. vmx	
otherLinux64Guest	vmx- 11		
2	VMTS001	[SSD253_01] VMTS001/VMTS001. vmx	
winNetEnterpriseGuest	vmx- 07	Terminal Server1	
238	VMWS015	[SSD253_02] VMWS015_NEW/VMWS015_NEW. vmx	
winNetEnterpriseGuest	vmx- 07		
239	VMWS016	[SSD253_02] VMWS016_NEW/VMWS016_NEW. vmx	
winNetEnterpriseGuest	vmx- 07		
240	VMWS010	[SSD253_02] VMWS010_NEW/VMWS010_NEW. vmx	
winNetEnterpriseGuest	vmx- 07		
241	VMWS014	[SSD253_02] VMWS014_NEW/VMWS014_NEW. vmx	
winNetEnterpriseGuest	vmx- 07		
245	VMWS013	[SSD253_02] VMWS013_NEW/VMWS013_NEW. vmx	
winNetEnterpriseGuest	vmx- 07		
247	vcenter62022	[SSD253_01] vcenter62022/vcenter62022. vmx	
sles11_64Guest	vmx- 08	VMware vCenter Server Appliance	
254	VMDESA3	[SSD253_01] VMDESA3/VMDESA3. vmx	
winNetEnterpriseGuest	vmx- 07	desarrollo1	
255	VMDESA4	[SSD253_01] VMDESA4/VMDESA4. vmx	
winNetEnterpriseGuest	vmx- 07	desarrollo2	
257	VMWS_ORIGINAL	[SSD253_01] VMWS_ORIGINAL/VMWS_ORIGINAL. vmx	
winNetEnterpriseGuest	vmx- 07		
259	VMTS001_BACKUP	[SSD253_02] VMTS001_BACKUP/VMTS001_BACKUP. vmx	
winNetEnterpriseGuest	vmx- 07	Terminal Server2	
260	VMBD001_BK	[SSD253_01] VMBD001_BK/VMBD001_BK. vmx	
winNetEnterpriseGuest	vmx- 07		
261	TW2019_EN_BLANCO	[SSD253_01] TW2019_EN_BLANCO/TW2019_EN_BLANCO. vmx	
windows9Server64Guest	vmx- 11		
262	TW10_EN_BLANCO	[SSD253_01] TW10_EN_BLANCO/TW10_EN_BLANCO. vmx	
windows9_64Guest	vmx- 11		
263	TW10_CD-CT	[SSD253_01] TW10/TW10. vmx	
windows9_64Guest	vmx- 11	desarrollo3	
264	TW2019	[SSD253_01] TW2019/TW2019. vmx	
windows9Server64Guest	vmx- 11		
265	VMWS017	[SSD253_02] VMWS017/VMWS017. vmx	

```

winNetEnterpriseGuest    vmx-07
266    VMWS018            [SSD253_01] VMWS018/VMWS018.vmx
winNetEnterpriseGuest    vmx-07
267    VMWS019            [SSD253_02] VMWS019/VMWS019.vmx
winNetEnterpriseGuest    vmx-07
268    VMWS011            [SSD253_02] VMWS011/VMWS011.vmx
winNetEnterpriseGuest    vmx-07
269    VMWS012            [SSD253_01] VMWS012/VMWS012.vmx
winNetEnterpriseGuest    vmx-07
270    VMWS020            [SSD253_02] VMWS020/VMWS020.vmx
winNetEnterpriseGuest    vmx-07
271    VMWS021            [SSD253_01] VMWS021/VMWS021.vmx
winNetEnterpriseGuest    vmx-07
273    TW10_XA81          [SSD253_02] TW10_XA81/TW10_XA81.vmx
windows9_64Guest         vmx-11    desarrollo4
46     VMWS244_VCliente    [SSD253_01] VMWS245/VMWS245.vmx
windows9Server64Guest    vmx-11    VClient
48     VMWS001            [SSD253_01] VMWS001/VMWS001.vmx
winNetEnterpriseGuest    vmx-07
5      VMDB001            [SSD253_01] VMDB001/VMDB001.vmx
winNetEnterpriseGuest    vmx-07
9      VMDESA2            [SSD253_01] VMDESA02/VMDESA02.vmx
winNetEnterpriseGuest    vmx-07    Desarrollo 12
91     VMDESA1            [SSD253_01] VMDESA11/VMDESA11.vmx
winNetEnterpriseGuest    vmx-07    desarrollo 11
[root@vmw253: ~]

```

Lista de máquinas virtuales en ejecución en ESXi

Puedes ver todas las máquinas virtuales en ejecución en el host

```
esxcli vm process list
```

EL resultado sería como el siguiente

```

[root@vmw253: ~] esxcli vm process list
VMDB001
    World ID: 35733

```

```
Process ID: 0
VMX Cartel ID: 35732
UUID: 42 2e 4d 7d 3f ec ac 8c-f8 99 23 d5 fd fb 01 05
Display Name: VMDB001
Config File: /vmfs/volumes/5e3c400a-49fe189e-39f0-1866da5503b8/VMDB001/VMDB001.vmx
```

VMWS244_VCliente

```
World ID: 35756
Process ID: 0
VMX Cartel ID: 35755
UUID: 42 2e 69 54 de 34 7e d0-f7 d8 db 7a 44 99 ea 32
Display Name: VMWS244_VCliente
Config File: /vmfs/volumes/5e3c400a-49fe189e-39f0-1866da5503b8/VMWS245/VMWS245.vmx
```

VMTS001

```
World ID: 35779
Process ID: 0
VMX Cartel ID: 35778
UUID: 42 2e cd 34 5a c5 49 79-2f ba f1 94 dc b1 e3 f7
Display Name: VMTS001
Config File: /vmfs/volumes/5e3c400a-49fe189e-39f0-1866da5503b8/VMTS001/VMTS001.vmx
```

.....

Parar máquinas desde consola

Apagar la máquina virtual desde el comando ESXi ESXCLI

Este comando apaga la máquina si no hay otra forma de hacerlo, matando el proceso de la máquina virtual. Más abajo encontrarás formas mas "civilizadas" de hacerlo.

El comando esxcli se puede utilizar de forma local o remota para apagar una máquina virtual que se ejecuta en ESXi 5.x o posterior.

Apagar una máquina virtual de la lista ejecutando este comando:

```
esxcli vm process kill --type= [soft,hard,force] --world-id= WorldNumber
```

En el caso anterior sería por ejemplo para apagar de forma ordenada la máquina VMDB001 (aparece con el World ID: 35733)

```
esxcli vm process kill --type= soft --world-id= WorldNumber = 35733
```

Encender máquinas desde consola

Ejecutamos la lista de máquinas

```
vim-cmd vmsvc/getallvms
```

O bien

```
vim-cmd vmsvc/getallvms | grep VMDB001
```

Veremos el ID de la máquina en la primera columna

```
266 VMWS018 [SSD253_01] VMWS018/VMWS018.vmx winNetEnterpriseGuest vmx-07
267 VMWS019 [SSD253_02] VMWS019/VMWS019.vmx winNetEnterpriseGuest vmx-07
268 VMWS011 [SSD253_02] VMWS011/VMWS011.vmx winNetEnterpriseGuest vmx-07
269 VMWS012 [SSD253_01] VMWS012/VMWS012.vmx winNetEnterpriseGuest vmx-07
270 VMWS020 [SSD253_02] VMWS020/VMWS020.vmx winNetEnterpriseGuest vmx-07
271 VMWS021 [SSD253_01] VMWS021/VMWS021.vmx winNetEnterpriseGuest vmx-07
273 TW10_XA81 [SSD253_02] TW10_XA81/TW10_XA81.vmx windows9_64Guest vmx-11
46 VMWS244_VCliente [SSD253_01] VMWS245/VMWS245.vmx windows9Server64Guest vmx-11
48 VMWS001 [SSD253_01] VMWS001/VMWS001.vmx winNetEnterpriseGuest vmx-07
5 VMDB001 [SSD253_01] VMDB001/VMDB001.vmx winNetEnterpriseGuest vmx-07
9 VMDESA2 [SSD253_01] VMDESA02/VMDESA02.vmx winNetEnterpriseGuest vmx-07
91 VMDESA1 [SSD253_01] VMDESA11/VMDESA11.vmx winNetEnterpriseGuest vmx-07
[root@vmw253:~]
```

Comprobamos el estado

```
vim-cmd vmsvc/power.getstate [ID DE LA MAQUINA]
```

En este caso

```
[root@vmw253: ~] vim-cmd vmsvc/power.getstate 5
Retrieved runtime info
Powered on
[root@vmw253: ~]
```

Ahora si queremos encender esa máquina (en el caso de que esté apagada) ejecutaremos

```
vim-cmd vmsvc/power.on
```

En nuestro ejemplo

```
vim-cmd vmsvc/power.on 5
```

Apagar máquinas desde consola

Para apagarla ejecutaremos


```
vim-cmd vmSvc/power.off
```

En nuestro ejemplo

```
vim-cmd vmSvc/power.off 5
```