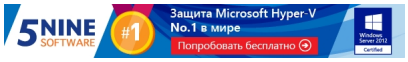
Автор:
12.11.14 13:01 -

12/11/2014

Реклама:



Пост:

Многие пользователи в целях безопасности хотят отключить использование USB-портов на хостах VMware ESXi - а то кто-нибудь зайдет в серверную комнату и утащит данные на диске.

К сожалению, на текущих версиях платформы VMware vSphere сделать этого нельзя. Можно, конечно, отключить USB Arbitrator service следующей командой (как написано в от тут
):

/etc/init.d/usbarbitrator stop

Но это лишь отключит проброс USB-устройств в виртуальные машины, при этом само устройство (например, /dev/usb0101) отключено не будет. Поэтому, тут остается два решения:

- Отключить USB-устройства в BIOS - но это поддерживают не все производители железа.
- Мониторить использование локальных USB-устройств и слать алерты менеджеру по ИБ.

Второй вариант можно реализовать с помощью продукта VMware vRealize Log Insight , который позволяет мониторить логи хостов ESXi и слать по ним алерты при их появлении и повторении. Вот, например, в выводе этого лога мы видим, что кто-то подключал USB-девайс к хосту:

Автор:
12.11.14 13:01 -

2014-10-24 15:33:39.470	2014-06-10T05:11:20.426Z localhost.localdomain vmkernel: cpu1:33298)<6>usb 1-1: usbfs: registered usb0102 source event_type hostname appname
2014-10-24 15:33:39.470	2014-06-10T05:11:20.425Z localhost.localdomain vmkernel: cpu1:33298)<6>usb 1-1: device is not available for passthrough source event_type hostname appname
2014-10-24 15:33:39.458	2014-06-10T05:11:20.418Z localhost.localdomain vmkernel: cpu1:33298)<6>usb 1-1: Interface Subclass: 0x06, Protocol: 0x50 source event_type hostname appname
2014-10-24 15:33:39.458	2014-06-10T05:11:20.418Z localhost.localdomain vmkernel: cpu1:33298)<6>usb 1-1: Vendor: 0x090c, Product: 0x1000, Revision: 0 source event_type hostname appname
2014-10-24 15:33:39.450	2014-06-10T05:11:20.364Z localhost.localdomain vmkernel: cpu1:33298)<6>usb 1-1: SerialNumber: 111203050611 31TJS3OD source event_type hostname appname
2014-10-24 15:33:39.450	2014-06-10T05:11:20.364Z localhost.localdomain vmkernel: cpu1:33298)<6>usb 1-1: Manufacturer: SMI Corporation source event_type hostname appname
2014-10-24 15:33:39.450	2014-06-10T05:11:20.364Z localhost.localdomain vmkernel: cpu1:33298)<6>usb 1-1: Product: USB DISK source event_type hostname appname
2014-10-24 15:33:39.450	2014-06-10T05:11:20.364Z localhost.localdomain vmkernel: cpu1:33298)<6>usb 1-1: New USB device strings: Mfr=1, Product=2, SerialNumber=3 source event_type hostname appname
2014-10-24 15:33:39.448	2014-06-10T05:11:20.364Z localhost.localdomain vmkernel: cpu1:33298)<6>usb 1-1: New USB device found, idVendor=090c, idProdu source event_type hostname appname
2014-10-24 15:33:39.085	2014-06-10T05:11:20.045Z localhost.localdomain vmkernel: cpu1:33298)<6>usb 1-1: new high speed USB device number 2 using ehc source event_type hostname appname

[illegible] Вот такой вот [illegible] Вот [illegible] Вот [illegible] что [illegible] [illegible] [illegible]