ESXi

- Agrega vTPM sin vCenter
- Synology ABB - VMware - CBT is not enabled on VM
- ESXi en Deskmeet PSOD

Agrega vTPM sin vCenter

La fuente de este articulo es esta: https://williamlam.com/2023/10/support-for-virtual-trusted-platform-module-vtpm-on-esxi-without-vcenter-server.html

En mi caso no pude quedarme con la duda, y decidi probarlo rapidamente.

La idea de este articulo, es simplificar al maximo el paso a paso, pensando en alguien que nunca ha trabajado con VMware. Todo el credito de este trabajo es para William Lam.

Antes que nada, sera importante instalar algunas dependencias. Ya que en estas instrucciones se usan cmdlets que estan incluidos en el modulo **`VMware.VimAutomation.Core`**

1. Instalar VMware PowerCLI
   - Abra PowerShell como administrador y ejecute:

   ```
   Install-Module -Name VMware.PowerCLI -Scope CurrentUser
   ```

2. Descargue el archivo de funciones vTPMStandaloneESXiFunctions.ps1 y ejectutelo usando el siguiente comando.

   ```
   . ./vTPMStandaloneESXiFunctions.ps1
   ```

3. Ahora, puede conectarse a un host ESXi. Reemplace <servidor> con la dirección de su servidor y proporcione las credenciales según sea necesario.

   ```
   Connect-VIServer -Server 192.168.10.15 -User root
   ```

4. Prepare el host para el cifrado.

   ```
   Prepare-VMHostForEncryption
   ```

   Prepare-VMHostForEncryption.png
5. Ahora temenos que general la llave de encriptacion, esto se hace una sola vez, note que se creara un archivo CSV, es muy importante mas adelante.

   ```
   New-InitialVMHostKey -Operation CREATE -KeyName "host-key-1"
   ```

   esxi key.png

6. Ahora podemos generar las llaves de encriptacion para el vTPM de una virtual. Use algo descriptivo como el hostname.

   ```
   New-VMTPMKey -Operation CREATE -KeyName "NombreDescriptivo"
   ```

   image.png

7. Agregue la vTPM a la virtual y encríptela usando la llave creada particularmente para ella. (antes de correr el comando, asegurese que la virtual en cuestion esta apagada)

   ```
   Reconfigure-VMWithvTPM -KeyName "NombreDescriptivo" -VMName "NombreVM"
   ```

   image.png

8. Con eso es suficiente para ver el vTPM reflejado en la virtual.
   image.png

Comandos adicionales.

`Get-VMHostTPMKeys` consigues una lista de las llaves que estan en el ESXi.

`Remove-VMTPMKey -KeyName "NombreDescriptivoDeLlave"` remueve la llave de encriptacion.

`Disconnect-VIServer -Confirm:$false` Si desea desconectarse del servidor al final de su sesión.

Importante.

Por defecto, ESXi NO guarda ninguna clave de cifrado después de reinicios. Si no vuelves a añadir las claves de cifrado asignadas, no podrás iniciar las VMs.

Como solución alternativa, se pueden respaldar automáticamente las claves utilizando funciones de PowerCLI, guardándolas en un archivo CSV llamado "tpm-keys.csv"

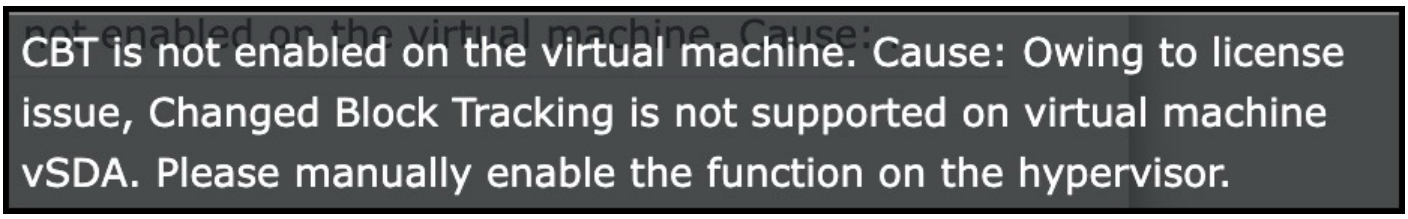
Si tienes un chip TPM 2.0 compatible, puedes activar una función en ESXi que mantiene las claves de cifrado en el chip, incluso después de los reinicios. Instrucciones aqui. `se que esto no es para todos, pero en mi caso aunque TPM estaba activado, tuve que asegurareme de no estuviera en "auto" y forzarla a 2.0. (Advanced | Trusted Computing)`

Si no tienes este chip, es critico tener un respaldo de las claves que por defecto se guardan en “tpm-keys.csv”
Aquí hay un ejemplo de como usar la operación IMPORT para un host en particular.

```
Prepare-VMHostForEncryption
New-InitialVMHostKey -Operation IMPORT -KeyName "host-key-1" -CSVTPMKeyFile tpm-keys.csv
New-VMTPMKey -Operation IMPORT -KeyName "NombreDeLaLlave" -CSVTPMKeyFile tpm-keys.csv
```

```
Get-VMHostTPMKeys
```

Synology ABB - VMware - CBT is not enabled on VM



El mensaje indica que el seguimiento de bloques cambiados (CBT) no está habilitado en la máquina virtual debido a un problema de licencia. La máquina virtual llamada "vSDA" no soporta CBT por este problema. Se te aconseja habilitar manualmente la función de CBT en el hipervisor.

Para resolver este problema, deberás revisar las configuraciones del hipervisor para asegurarte de que la licencia permita el uso de CBT. Si la licencia no es suficiente, puede que necesites actualizarla. Una vez resuelto el problema de licencia, puedes habilitar CBT para la máquina virtual, ya sea a través de la interfaz de administración del hipervisor o utilizando comandos o herramientas específicas proporcionadas por la plataforma del hipervisor (como ESXi, por ejemplo).

1. **Acceda a la Interfaz Web de ESXi**

2. **Apague la Máquina Virtual**

3. **Edite la Configuración de la Máquina Virtual**:

• Una vez que la máquina virtual esté apagada, haga clic en la pestaña **Editar** (Edit) o en **Ajustes de la VM** (VM Options) dentro de la vista de la máquina virtual.

• Seleccione **Opciones VM** (VM Options) en el menú de la izquierda.

• Desplácese hacia abajo hasta encontrar **Opciones avanzadas** (Advanced Options) y haga clic en **Editar parámetros de configuración** (Edit Configuration Parameters).

4. **Agregue Parámetros de CBT**:

• En la ventana de **Parámetros de Configuración**, haga clic en **Agregar fila** (Add Row).

• Añada los siguientes parámetros y valores:

• ctkEnabled = TRUE

• scsi0:0.ctkEnabled = TRUE

• Si la máquina tiene más de un disco, agregue una línea similar para cada uno, reemplazando scsi0:0 con el identificador correspondiente del disco (por ejemplo, scsi0:1).

5. **Guarde los Cambios**:

• Una vez que haya ingresado todos los parámetros, haga clic en **Aceptar** (OK) para guardar los cambios.

6. **Encienda la Máquina Virtual**:

• Después de guardar los cambios, encienda la máquina virtual desde la interfaz web.

7. **Verifique la Configuración**:

• Para asegurarse de que CBT está habilitado, puede revisar si se han creado archivos .ctk en el datastore de la máquina virtual. Esto se puede hacer navegando al datastore correspondiente y buscando los archivos .ctk en el directorio de la VM.

ESXi en Deskmeet PSOD

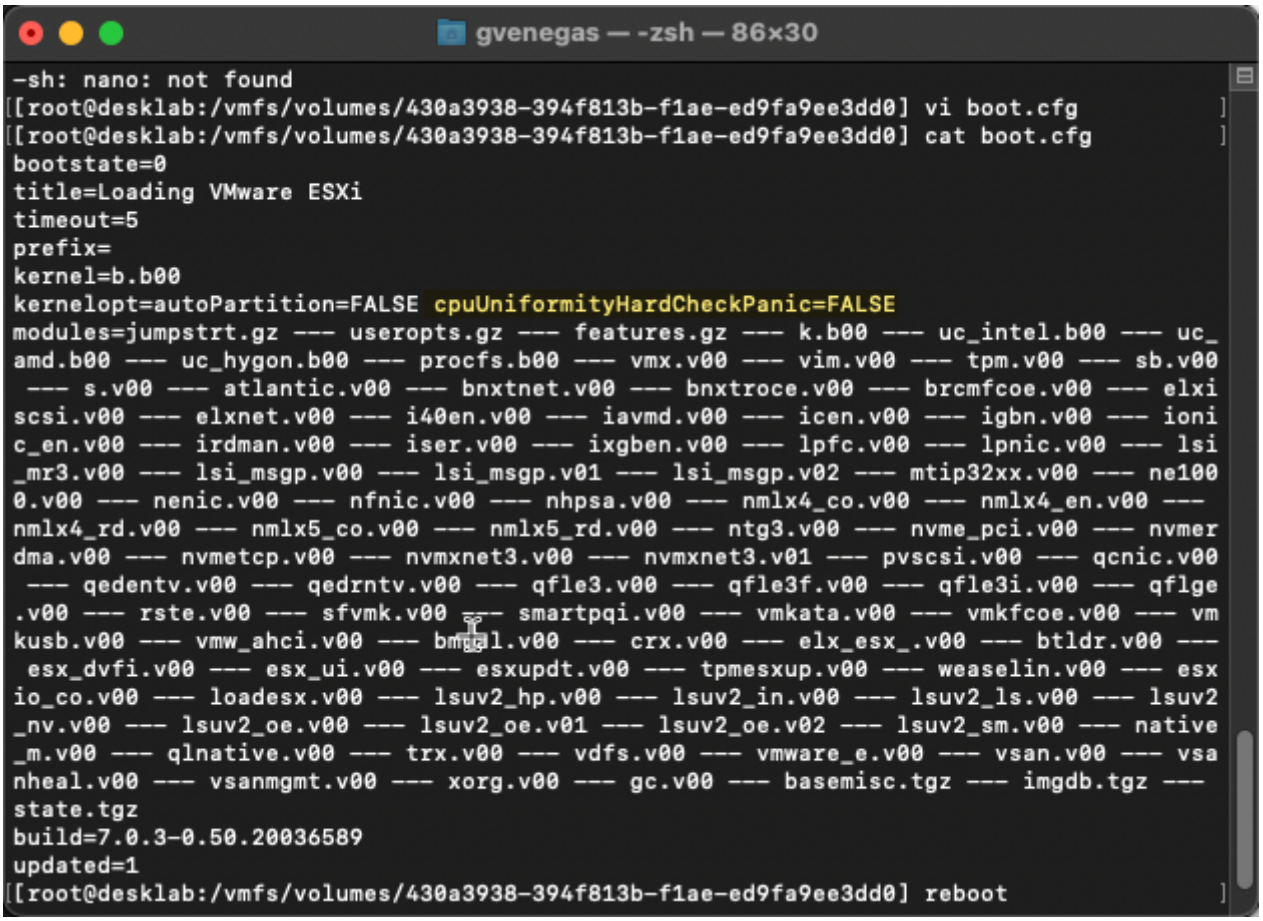
Si al instalar ESXi obtiene un PSOD (Purple Screen of Death), es importante saber que esto puede deberse a una incompatibilidad con el CPU.

Para resolverlo, se debe deshabilitar la verificación del CPU.

El procedimiento implica modificar el archivo boot.cfg para agregar el parámetro `cpuUniformityHardCheckPanic=FALSE`. Este cambio debe realizarse en las rutas `/bootbank/boot.cfg` y `/altbootbank/boot.cfg` de su medio de arranque (que puede ser un disco SATA local, USB u otro medio).

Para hacer este ajuste, agregue el parámetro en la sección “kernelopt” del archivo mencionado. Como referencia, puede usar un editor como VI a través de SSH, que fue el método que utilicé en mi caso.

Este ajuste desactiva la verificación que provoca el error de incompatibilidad de CPU, lo que debería permitirle completar la instalación sin problemas.


gvenegas — -zsh — 86×30
-sh: nano: not found
[[root@desklab:/vmfs/volumes/430a3938-394f813b-f1ae-ed9fa9ee3dd0] vi boot.cfg]
[[root@desklab:/vmfs/volumes/430a3938-394f813b-f1ae-ed9fa9ee3dd0] cat boot.cfg]
bootstate=0
title=Loading VMware ESXi
timeout=5
prefix=
kernel=b.b00
kernelopt=autoPartition=FALSE cpuUniformityHardCheckPanic=FALSE
modules=jumpstrt.gz --- useropts.gz --- features.gz --- k.b00 --- uc_intel.b00 --- uc_
amd.b00 --- uc_hygon.b00 --- procfs.b00 --- vmx.v00 --- vim.v00 --- tpm.v00 --- sb.v00
--- s.v00 --- atlantic.v00 --- bnxtnet.v00 --- bnxtroce.v00 --- brcmfcoe.v00 --- elxi
scsi.v00 --- elxnet.v00 --- i40en.v00 --- iavmd.v00 --- icen.v00 --- igbn.v00 --- ioni
c_en.v00 --- irdman.v00 --- iser.v00 --- ixgben.v00 --- lpfc.v00 --- lpnic.v00 --- lsi
_mr3.v00 --- lsi_msgp.v00 --- lsi_msgp.v01 --- lsi_msgp.v02 --- mtip32xx.v00 --- ne100
0.v00 --- nenic.v00 --- nfnic.v00 --- nhpsa.v00 --- nmlx4_co.v00 --- nmlx4_en.v00 ---
nmlx4_rd.v00 --- nmlx5_co.v00 --- nmlx5_rd.v00 --- ntg3.v00 --- nvme_pci.v00 --- nvmer
dma.v00 --- nvmetcp.v00 --- nvmxnet3.v00 --- nvmxnet3.v01 --- pvscsi.v00 --- qcnic.v00
--- qedentv.v00 --- qedrntv.v00 --- qfle3.v00 --- qfle3f.v00 --- qfle3i.v00 --- qflge
.v00 --- rste.v00 --- sfvmk.v00 --- smartpqi.v00 --- vmkata.v00 --- vmkfcoe.v00 --- vm
kusb.v00 --- vmw_ahci.v00 --- bmcal.v00 --- crx.v00 --- elx_esx_.v00 --- btldr.v00 ---
esx_dvfi.v00 --- esx_ui.v00 --- esxupdt.v00 --- tpmesxup.v00 --- weaselin.v00 --- esx
io_co.v00 --- loadesx.v00 --- lsuv2_hp.v00 --- lsuv2_in.v00 --- lsuv2_ls.v00 --- lsuv2
_nv.v00 --- lsuv2_oe.v00 --- lsuv2_oe.v01 --- lsuv2_oe.v02 --- lsuv2_sm.v00 --- native
_m.v00 --- qlnative.v00 --- trx.v00 --- vdfs.v00 --- vmware_e.v00 --- vsan.v00 --- vsa
nheal.v00 --- vsanmgmt.v00 --- xorg.v00 --- gc.v00 --- basemisc.tgz --- imgdb.tgz ---
state.tgz
build=7.0.3-0.50.20036589
updated=1
[[root@desklab:/vmfs/volumes/430a3938-394f813b-f1ae-ed9fa9ee3dd0] reboot]