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
```

Revisión #6
Creado 16 octubre 2023 21:03:18 por Greivin
Actualizado 27 octubre 2023 16:32:54 por Greivin