[CD] Arquitectura VMWare

VMWare usa un Hypervisor llamado ESXi que es de pago. Esxi destaca por lo siguiente:

- Tiene un Firewall que destaca por limitar tanto salidas como entradas mientras que otras otras otras soluciones solo bloquean las entradas.
- Memory Hardening: Usa posiciones de memoria aleatorias para evitar ataques dirigidos.
- Integridad de Módulos de Kernel: Los modulos de kernel debe ser firmados y cifrados por fuentes de confianza.
- TPM 2.0
- UEFI Secure Boot
- Core Dumps Cifrados
- Arranque rápido para parcheos y actualizaciones

Virtual Center Server Appliance (vCenter)

Máquina virtual Linux basada en Photon OS de VMWare. Tiene una base de datos postgreSQL, también soportando Oracle SQL. Normalmente en la arquitectura de vCenter hay mínimo 2 máquinas con ESXi, conteniendo una de ellas el vCenter. Las comunicaciones se hacen seguras a través del puerto 443. Un host ESXi puede ser gestionado directamente (No se debe hacer) o puede ser gestionado desde un vCenter (Lo recomendable). La única razón por la que uno se debe conectar directamente a un Host ESXi es para arrancar el vCenter en caso de fallo.

Para conectar al vCenter se usa el vSphereClient o a través de PowerCLI. Si uno se conecta directamente a un Host ESXi se puede usar el EXCLI, PowerCLI y a través del host client (No recomendable).

Permisos

Existen los siguientes conceptos:

- Rol: Conjunto de privilegios
- Privilegio: Una acción que se puede realizar
- Usuario o Grupo: Quien recibe el rol
- Permiso: Da a un usuario o grupo un rol para el objeto seleccionado.

vCenter HA (High Avaliability)

Puede tener muchas definiciones:

- Funcionalidad de un cluster de VMWare (Alta Disponibilidad): VMWare lo entiende como volver a arrancar una máquina cada vez que cae, por lo que se podría decir que no es una alta disponibilidad real. Si cae una máquina en un host o cae el host entero, la arranca en otro host. Este tipo de alta disponibilidad solo protege contra la caida de hardware de un nodo. Si una máquina falla a nivel de software está vCenter HA.

- vCenter HA: Consiste en tener 3 vCenter, un testigo (Witness), uno principal (Activo) y uno de respaldo (Pasivo) que comparten un disco duro en red, de forma que cuando falle el principal, el de respaldo toma su lugar y continúa dando servicio. Para saber si el otro nodo sigue activo se van mandando señales heartbeat para comprobar si el otro equipo funciona o no. El testigo está conectado a los dos nodos y al disco compartido, de forma que este puede evitar un split brain (Una máquina piensa por error que otra ha caido e intenta tomar su lugar, pudiendose corromper el disco duro al estar las dos usando el disco a la vez.)

Un vCenter HA se monta para estructuras extremadamente críticas, no es muy común tenerlo montado.

Backup y restauración de vCenter

El lider del mercado para realizar copias de seguridad es Veeam Backup. VMWare no tiene herramienta oficial de backup (Existió una en el pasado pero se descontinuó). Para proteger el vCenter VMWare recomienda usar una herramienta de backup. Para ello se le dice a veeam cuando se quiere hacer una máquina y donde almacenar la copia, en ese momento se crea un snapshot y se copia la máquina donde se ha indicado. De esta forma si falla una máquina se puede restaurar desde Veeam.

Para vCenter desde el puerto 5580 se puede acceder a una sección que entre otras opciones, permite realizar backup. Esta función genera un fichero .zip con toda la configuración del vCenter en un momento determinado. Para restaurar la copia se usa el mismo programa que se usó para desplegar el vcenter seleccionando la opción restore. Esto no suele ser muy utilizado.

From:
https://knoppia.net/ - **Knoppia**

Permanent link:
https://knoppia.net/doku.php?id=master_cs:centros_datos:vmw&rev=1742236981

Last update: **2025/03/17 18:43**