[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. También existe una opción de automatizar los backups.

Monitorización del vCenter

Para ello se puede ir a la pestaña de performance dentro del propio vCenter, lo que nos muestra el consumo de CPU, RAM, red… y nos proporciona las opciones “tasks” y “Events” donde se muestra que tareas se han ejectuado y cuanto y en “Events” Muestra todos los eventos que han ido ocurriendo y se han almacenado en los logs. Todo esto puede ser enviado por correo o por SNMP Traps a un colector para verlo en un servidor de monitorización.

Hay varios niveles de log:

- None: Desactiva el log
- Error: Solo muestra errores
- Warning: Solo muestra errores y alertas
- Info: Por defecto, muetra información de errores e información de warning
- Verbose (No recomendado)
- Trivia (No recomendado)

Los niveles de log se pueden cambiar desde la pestaña de configure→General→Logging Settings. Toda esta información se guarda en el vCenter y en los Hosts ESXi. Si falla el vCenter o alguno de los host ESXi se pierden dichos hosts. Para evitar la pérdida de estos datos se suele usar un SIEM, esto se puede configurar desde las sección de backups en la pestaña de syslog. En los ESXi no se pueden

mandar estos datos a un SIEM desde la inerfaz gráfica, hay que ir a los parámetros avanzados.

También se monitoriza la saluz de una base de datos, obserbandose tanto el rendimiento como el espacio. Esto nos permite configurar alarmas para que nos avisen en caso de problemas como la falta de espacio. Al 95% de la ocupación del disco duro los servicios del vCenter se paran. Cuando se arranca el vCenter hay una opción en services para configurar los daemons, donde podemos ver que procesos están arrancados o no y su estado de salud.

Switch Virtual

Normalmente se define un grupo de puertos como una vLan. También existen los VM Kernel Ports que se usan para tráfico especial:

- Almacenaminento IP
- VSAn
- Fault Tolerance
- VMotion
- Administración Host ESXi

En la actualidad la mayor parte de las organizaciones usan VLANs para aislar el tráfico. Generalmente se genera una máquina virtual portgroup asociada a una Vlan. Los switches standar son sencillos y tienen pocas funcionalidades, mientras que los switches distrbuidos tienen muchas más funcionalidades y a nivel de seguridad son mejores, el problema es que necesitan la licencia Enterpirse Plus de VMWARE (Super Caro).

Políticas de red y seguridad

Estas políticas pueden ser configuradas a nivel de portgroup o a nivel de virtual switch.

- Modo promiscuo: Una máquina puede ver el tráfico que pasa a través de ella
- Mac Address Change: Permite tanto enviar como recibir tráfico con la mac alterada. Se permite a una máquina virtual recibir tráfico de una mac diferente a la de su tarjeta de red física
- Forged Transmits Se quiere que una máquina virtual mande tráfico con una mac distinta a la de su tarjeta de red física