Universidad Nacional Autónoma de México
Secretaría de Desarrollo Institucional
Dirección General de Cómputo y de Tecnologías de la Información y Comunicación.

Septiembre 2021

Implementación de aplicaciones de monitoreo en entornos virtuales PROXMOX

Versión 1.0

Índice

1. Introducción

El presente manual pretende servir de guía para la implementación de un sistema de monitoreo en la UNAM de forma estándar que permita a otros tener un punto de partida en la implementación de herramientas de monitoreo que se utilizan con apoyo de servidores virtuales sobre un Hipervisor que puede ser propietario (ESXi VMWARE) pero que se recomienda sea open source basado en KVM (como lo es PROXMOX) debido a las limitaciones y costos que puede representar el software licenciado para virtualización.

La implementación de una herramienta virtualizada confiable para el monitoreo depende del control que se tenga tanto el hardware, sistema virtualizado como la herramienta que realiza la tarea por lo que en este documento se darán recomendaciones para que los sistemas que se implementes sean estables, confiables en su operación y cuenten con los aspectos mínimos necesarios para que sean funcionales dentro de una infraestructura que desee ser monitoreada.

2. Objetivo

Ofrecer una guía práctica a forma de manual de las consideraciones necesarias para que los encargados de implementar herramientas para la administración y monitoreo de redes de datos puedan implementarlas sobre una plataforma virtualizada y que esta sea operacional y confiable.

3. Alcance

Realizar recomendaciones sobre aspectos de Hardware a considerar en la implementación de herramientas.

Explicar la importancia de los aspectos de software a considerar en el Hipervisor para la instalación de herramientas.

Identificación de diferencias entre implementaciones en servidor dedicado y virtualizados.

Recomendaciones sobre el respaldo y recuperación de los sistemas que operan en entornos virtuales como PROXMOX

4. Preparación del entorno virtual

La implementación de un Hipervisor requiere de la planeación sobre el interés de implementar un sistema que gestione virtualmente a otros para agilizar su administración, para ello es importante considerar que la flexibilidad aparente de montar un hipervisor sobre un sistema operativo solo agrega complejidad a la propia administración del hardware por lo que la recomendación para entornos operativos es que el Hipervisor siempre sea el sistema anfitrión, a continuación se muestran los 2 tipos existentes:

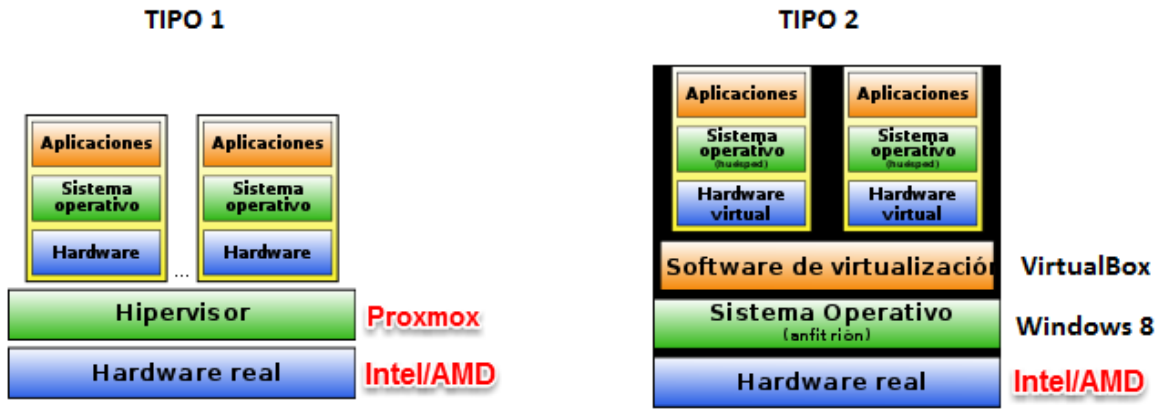

Imagen recuperada de:
https://administradoresit.files.wordpress.com/2015/02/06690f8486e060922679d7b48d3de334.png

5. Aspectos de Hardware a considerar en la implementación de herramientas

Las recomendaciones siempre van a estar orientadas a no tener que intervenir constantemente el hardware ya que estas acciones provocan los tiempos más largos de interrupción de los servicios.

En su lugar hay que realizar una implementación considerando los siguientes aspectos:

- Alojamiento físico: Con fuentes redundantes de ser posible, temperatura regulada, almacenamiento en RAID y de ser posible externo al Hipervisor.

- Conexión de red: en caso de tener un solo site, equipo, Cluster es importante que esos encuentren vías de acceso redundantes a la red local e internet para ser resilientes ante las fallas. En cambio si se cuenta con más de un local y diferentes acceso a Internet se puede optar por esquemas redundantes o Activo pasivo que permitan mantener el mayor tiempo posible la disponibilidad de los servicios.

Un aspecto muy importante en los servidores Hipervisores es el rendimiento de los recursos, entre mejor se aprovechen exista la posibilidad de manejar más máquinas virtuales por lo que se recomienda:

- Implementar procesadores de alta velocidad de procesamiento
- Discos duros de alta velocidad de lectura y escritura
- Conexiones de red de 10 Gbps de ser posible y redundantes

Estas recomendaciones ayudan a que los recursos utilizados por los procesos de los equipos virtualizados realicen tareas más eficientes apoyando a respuestas más rápidas de aplicaciones y liberación de recursos para otros sistemas con quien compartan recursos en el entorno hipervisor.

Las recomendaciones de la organización PROXMOX se resumen en contar con las características de virtualización:

- Intel EMT64 or AMD64 con Intel VT/AMD-V CPU. **“Es importante activar el soporte para virtualización previo al arranqué”.**
- Memoria, minima 2 GB para el SO Proxmox VE. **“Es muy poco, hay que considerar siempre tener el consumo por debajo del 80% para tener sistemas operando adecuadamente”.**
- SSD disks. **”Estrictamente necesario porque conviven varios sistemas, como alternativa almacenamiento distribuido de sistemas”.**
- OS storage: Hardware RAID, **“Dependiendo del nivel de respaldo deseado”.**
- Conexiones redundantes a Gigabit NICs, **“De ser possible más de 2 encasos especales considerar 10Gbps que está soportado”.**
- Para PCI(e) considerar active el CPU con VT-d/AMD-d CPU habilitado**. “Mejora el rendimiento”.**

6. Aspectos de software a considerar en el Hipervisor para la instalación

Para la implementación del hipervisor se considera importante para el monitoreo local tener implementadas las herramientas del sistema anfitrión, en la siguiente tabla se indican con su funcionalidad:

Se recomienda una serie de herramientas recomendadas en el Hipervisor:

1) fdisk (dispositivos HDD y SDD) 2) lshw (listar dispositivos físicos identificados por el sistema) 3) du (identificar lista el almacenamiento) 4) netstat (conexiones activas) 5) ethtool (interfacz de red físicas) 6) iftop (monitoreo local de red) 7) top (consumo de procesos) 8) htop (monitoreo de procesos) 9) curl (pruebas de conexión web) 10) wget (Pruebas de conexión web)	11) dig (traducción de dominios) 12) route (configuración de rutas) 13) iptables (firewall de sistema) 14) tcptraceroute (traza de ruta) 15) tcpflow 16) ssh (acceso remoto) 17) ftrace (traza de ruta) 18) iotop (top de procesos lectura/escritura) 19) iptraf 20) tiptop	21) ltrace (traza de rutaz) 22) sysdiag (diagnóstico del sistema) 23) dmesg (mensajes del sistema) 24) ss 25) snmp utils (monitoreo)

Previo a la implementación de aplicaciones sobre el hipervisor es importante que se tome en cuenta el soporte para virtualización:

En caso de la tecnología Intel:

INTEL: grep – -color vmx /proc/cpuinfo

Y en caso de la tecnología AMD:

AMD: grep – -color svm /proc/cpuinfo

7. Diferencias entre implementaciones en servidor dedicado y virtualizado

A continuación se enumeran las diferencias más importantes a considerar en la implementación de servidores dedicados con la de servidores virtualizados y su recomendación de implementación:

- Ventajas de virtualizar
  - La implementación de un nuevo sistema se realiza sin contacto con el hardware
  - Agregar interfaces de red o de almacenamiento es automático

- Se puede asignar recursos de memoria RAM de forma semi automática
- Mover un sistema requiere de poco tiempo
- Una vez virtualizado se vuelve portable el sistema incluso entre hipervisores
- Se puede tener comunicación local entre los sistemas que conviven en el mismo hipervisor limitado únicamente por la capacidad del procesador central

- Desventajas de virtualizar
  - Si el hipervisor falla fallan todos los sistemas que dependen de el
  - Se comparte el enlace de comunicación físico
  - El monitoreo de los recursos asignados a las máquinas virtuales depende de las herramientas instaladas en el hipervisor para este propósito
  - Una ventana de mantenimiento afecta a todos los sistemas virtualizados

8. Respaldo y recuperación

- Existen varios tipos de respaldo para los equipos virtualizados, estos tienen diferentes características:

- Respaldo por medio de Snapshot
  - Almacenado en el mismo dispositivo

- Respaldo por medio de copia completa de la virtual
  - Empleando formato OVF/OVA/QCOW2
  - Puede ser comprimida

- Replicación con apoyo de servidor alterno y almacenamiento distribuido
  Requiere servidor adicional físico

Para el caso del Hiérvisor Proxmox se sugiere emplear alguno de los métodos ofrecidos:

Cada ovalo indica los límites de acceso de la organización a los servicios de monitoreo implementados.

9. Mantenimiento

Se recomienda tener una línea base de operación de los equipos con umbrales de operación para identificar la necesidad de realizar tanto mantenimientos preventivos como prevenir fallas críticas ante el mal funcionamiento del Hipervisor y los componentes que require para su funcionamiento:

Fecha Implementación	% de utilización	Tiempo de vida de hardware estimado	Mantenimiento preventivo realizado
Servidor	Realizdo/pendiente	Fecha planificada	Fecha planificada
Memoria RAM	Realizdo/pendiente	Fecha planificada	Fecha planificada
Almacenamiento	Realizdo/pendiente	Fecha planificada	Fecha planificada

Permitiendo contar con un control y tomar decisiones sobre las soluciones de monitoreo.

10. Anexo de documentos y enlaces de apoyo

Los siguientes enlaces se adjuntan como apoyo para implementación de cada una de las recomendaciones que en el presente manual se enumeran:

Como se elabora un sistema de políticas, with paper KPMG:
https://assets.kpmg/content/dam/kpmg/es/pdf/2016/12/Cuadernos_Legales_N5.pdf

Políticas de Seguridad en cómputo para la facultad de Ingeniería:
http://www.ingenieria.unam.mx/~unica/pdf/seguridad_computo.pdf

Descripción rápida de comandos en Linux, Facultad de Ingeniería República de Uruguay:
https://www.fing.edu.uy/inco/cursos/sistoper/recursosLaboratorio/tutorial0.pdf

Estándar completo sobre la distribución jerarquica de los archivos en Linux
http://www.pathname.com/fhs/

RFC IETF, well kown ports (puertos conocidos)
https://tools.ietf.org/html/rfc1340

Documentación oficial sobre la administración de la aplicación OpenVPN:
https://openvpn.net/images/pdf/OpenVPN_Access_Server_Sysadmin_Guide_Rev.pdf

Manual de administración por la Linux Fundation:
http://linux-training.be/linuxfun.pdf

CONTROL DE ELABORACIÓN

	Elaboró	Revisó	Autorizó
Nombre	**Esteban Roberto Ramírez Fernández**		
Función	**Técnico Académico del Centro de Operación y Monitoreo de RedUNAM (NOC REdUNAM)**		
Firma			
CLAVE DE DOCUMENTO: NOC_DGTIC__Manual_Proxmox_v1.0		**EMISION: 19 de diciembre 2022**	**REVISIÓN:**

CONTROL DE CAMBIOS

Revisión	Fecha	Motivo del Cambio
NOC_DGTIC__INCIDENTES_v1.0	02 de diciembre 2021	**Se toma como recomendación lo contenido en el documento DT_PROCGESTINCIDENTES_v1.3 elaborado en 2017.**
	02 de diciembre 2021	**Se da formato al documento**
	02 de diciembre 2021	**Se agrega el contenido de los Anexos A - E**