Universidad de Buenos Aires

Facultades de Ciencias Económicas,
Cs. Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática
Trabajo Final de Especialización

Tema

Seguridad en Ambientes Virtuales

Título

MEJORES PRÁCTICAS DE SEGURIDAD EN AMBIENTES VIRTUALES

Autor: Ing. Carlos Hipólito Tapia Ayala

Tutor del Trabajo Final:
Dr. Pedro Hecht

Año de presentación
2019

Cohorte del cursante
2017

Declaración Jurada de origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales de Maestría vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

Carlos Hipólito Tapia Ayala

Nro. Documento 0925045254

DNI (Argentina): 95730994

Resumen

El presente trabajo final de especialización, contemplará la base sobre la cual se fundamentará el trabajo final de titulación en la maestría en seguridad informática, en el cual se realizará un análisis sobre el amplio espectro de la seguridad en los ambientes virtuales y sus vulnerabilidades.

La construcción e implementación de un laboratorio de prueba virtual para la realización de pruebas a nivel de seguridad, será fundamental para demostrar que la necesidad de contar con las debidas herramientas y configuraciones a nivel de hardware y software es fundamental e importante a la hora de estructurar un proyecto de infraestructura virtual en las organizaciones; para alcanzar este cometido u objetivo será necesario el análisis de Hipervisores, Centralización de Hypervisores, Switches Virtuales, Almacenamiento de red local Virtual, Migración de Máquinas Virtuales, Balanceo de Carga y alta disponibilidad en los servicios virtualizados; todo eso acompañado de un documento donde se especifique la aplicación de mejores prácticas al momento de implementar ambientes virtuales, dichas mejores prácticas se aplicarán en los componentes que intervienen en un ambiente virtual.

Se utilizará el componente VPSHERE versión 6.0 perteneciente al producto VMWARE para la implementación del ambiente virtual de prueba ya que es considerado como uno de los mejores en el mundo el cual cumple principalmente con los estándares y normas de seguridad internacionales, catalogado así por el Cuadrante Mágico de Garnet en el apartado de “Virtualización de Infraestructura de Servidores” [1] y además de tener experiencia en la administración e implementación de dicho producto desde hace muchos.

Palabras Claves

Virtualización, Ambientes virtuales, entorno tecnológico, hypervisores, máquinas virtuales, vulnerabilidades, almacenamiento de red local, Autenticación única, migración, balanceo de carga y alta disponibilidad

Tabla de Contenido

Tabla de Figuras

INTRODUCCIÓN

En la actualidad la instrumentación de la virtualización de ambientes o entornos tecnológicos, ha sido fundamental para la reducción de costos en las organizaciones, pero cuando hablamos de seguridad a nivel de estos entornos virtuales, entramos en un campo que aún no ha sido explorado a profundidad y es en este sentido que el presente proyecto de Seguridad en Ambientes Virtuales pretende dilucidar cuales son las mejores prácticas de la virtualización desde su implementación hasta su monitoreo, haciendo énfasis en la seguridad de estos ambientes.

En retrospectiva y analizando que la mayoría de compañías y entidades de gobierno poseen actualmente infraestructura en ambientes virtuales, para lo cual dichos ambientes tienen las mismas necesidades de seguridad que los físicos, para eso es importante que las áreas de Tecnología de la Información TI y Seguridad de la Información SI trabajen de manera conjunta para disminuir el riesgo de ataques informáticos y así lograr que la información de la organización no se vea comprometida.

Debido al incremento de ataques informáticos que se han venido presentando a nivel mundial en los últimos años, siendo el de Ransomware el más conocido en mayo de 2017, se desprende la necesidad de contar con un documento que proporcione los criterios de implementación de ambientes virtuales seguros, con base en las mejores prácticas a nivel de seguridad.

El primer capítulo de este documento describirá sobre la Virtualización, su historia, su definición, sus funciones y sus ventajas y desventajas desde el punto de vista de la organización y los principales vendors para construcciones de ambientes virtuales.

El segundo capítulo de este documento, describirá sobre del por qué la elección de VMWARE, una breve descripción de los productos de VMWARE y lo más importante detallar sobre VPSHERE, software utilizado para la virtualización de ambientes virtuales en las organizaciones.

El tercer capítulo de este documento describirá sobre los componentes existentes en el software de VPSHERE y agregando dos más como el Balanceo de Carga y Alta disponibilidad necesarias para la implementación de un ambiente virtual, dichos dos últimos componentes no pertenecen a VSPHERE.

Y por último, el capítulo 4, describirá sobre la instalación, configuración y aplicación de mejores prácticas en la implementación del ambiente virtual.

CAPITULO 1: VIRTUALIZACIÓN

Marco Teórico

La Compañía “International Business Machine” IBM, en los años 60 fue la creadora y diseñadora de una herramienta de Virtualización capaz de virtualizar tanto plataformas (o sistemas) y aplicaciones. IBM fue el que introdujo el nombre de “Máquina Virtual” VM por primera vez en el mundo de la Tecnología el cual tiene su origen que se detalla a continuación:

El primer sistema operativo en soportar virtualización completa para VMs fue el Conversational Monitor System (CMS). El CMS soportaba virtualización parcial o completa. A comienzos de los años 1970, IBM introdujo la familia VM de sistemas, que ejecutaba múltiples sistemas operativos de usuario individual, sobre su VM Control Program—un hipervisor temprano tipo-1.

Uno de los primeros usos de la virtualización de aplicación ocurrió en los años 1960, para el Basic Combined Programming Language (BCPL). El BCPL era un lenguaje imperativo desarrollado por Martin Richards en la Universidad de Cambridge y fue un precursor del lenguaje B que luego evolucionó hasta el lenguaje C que usamos hoy. [1]

Definición de Virtualización

La virtualización es una tecnología que permite crear uno o muchos entornos virtuales o simulados de manera dedicada desde Datacenters, Clúster de servidores y máquinas virtuales. La Virtualización también, puede aplicar tanto a servidores individuales, aplicaciones, almacenamiento y redes. Quiere decir, que gracias a la virtualización se utiliza a través del software para simular la existencia de hardware individual con un aprovechamiento al máximo de los recursos de hardware dispuestos. [2]

Ventajas y Desventajas de la Virtualización

Entre las ventajas que brinda este servicio, podemos mencionar las siguientes:

- Permite que las empresas ejecuten más de un sistema virtual, además de múltiples sistemas operativos y aplicaciones, en un único servidor físico.
- Mejora la escalabilidad y las cargas de trabajo, al tiempo que permite usar menos servidores y reducir el consumo de energía,
- Permite un alto ahorro en costos de infraestructura y el mantenimiento.
- Mejora y ayuda las políticas de backup en la organización.

- Permite tener una alta disponibilidad en los servicios.
- Permite una administración centralizada de todas las máquinas virtuales, switches virtuales y SAN virtual.
- Centralización de logs y monitoreo de la infraestructura virtual y física.
- Permite en un bajo costo crear diferentes ambientes, como de Desarrollo, Control Calidad previo el salto a Producción.
- Permite convertir servidores físicos en virtuales.
- Permite la restitución de los servicios ante una interrupción de forma automática, ya que provee la capacidad de organizar el arranque de cada servidor virtual en orden definido según los servicios de IT.
- Provee la posibilidad de implementar y mantener alta redundancia en almacenamiento de Data Store, lo cual incrementa la seguridad en la integridad y disponibilidad de la información.

Sus Desventajas son:

- Necesidad de adquirir o de tener hardware robusto o de alta gama. (Costos de inversión medianos - altos).
- Necesidad de contar hardware suficiente para construir un HA (High Available) a nivel de máquinas virtuales, ya que de no tener hadware adicional que permita proveer redundancia, se corre el riesgo que los servicios core del negocio se queden indisponible cuando el servidor físico que contiene dichos servicios presente incidente crítico.
- De no contar con sistemas de backup almacenamientos tipo DataStore, VTL, DRS, entre otros, que permita configurar respaldos automáticos y/o realizar esquemas de balanceos de almacenamiento de las máquinas virtuales, podría afectar el tiempo de restitución de servicios al momento de necesitar realizar un restore de una Máquina Virtual.
- La implementación de un Ambiente Virtual contando con Alta Disponibilidad (HA), Balanceo de Carga (DRS), Segmentación de Datos, Management y Storage (VLAN), requiere tiempo para su diseño e implementación todo proyecto de infraestructura de TI.
- Por ser un software propietario, en un punto que representa una inversión importante dentro del OpEX que las organizaciones deben de asumir.

- El equipo de especialistas de TI y SI deben de contar con la capacitación necesaria en la administración de estos servicios, a fin de poder atender alguna necesidad o resolución de incidentes.

[3]

OPEX – Gasto Operacional que cubre la organización.

Principales Vendors de Virtualización

Según el Cuadrante de Gartner en el apartado de "Infraestructura Virtualización de Servidores x86", tenemos a los siguientes vendors con su respectivo producto:

Vendors	Producto
VMware	vPshere
Microsoft	Hyper-V
Red Hat	Enterprise Linux with Smart Virtualization Red Hat Virtualization
Citrix	Citrix hypervisor
Nutanix	Acropolis hypervisor (AHV)
SUSE	Suse Linux Enterprise Server
Oracle	VM Server
Virtuozzo	Virtuozzo
Sangfor	Sangfor HCI

Tomado del sitio oficial de Gartner [4].

CAPITULO 2: VMWARE

Por qué VMWARE?

La elección de VMWare fue con base a la experiencia desarrollada desde hace muchos años en la administración e implementación de ambientes virtuales y soluciones de alta disponibilidad, redundancia con este producto.

VMWARE cuenta con una Suite completa que cubren los tres pilas de la seguridad de la información contando con una administración y monitoreo centralizada ayudando así a un mejor control, seguimiento y administración de plataformas virtualizadas en soluciones de TI y SI.

Además VMware cumple con los estándares internacionales de auditoría, seguimiento y control, así como la integración con herramientas específicas de seguridad donde cada uno de los componentes administrados por el

producto, son auditables y con controles de acceso solo por entornos permitidos.

También permiten alta disponibilidad en HA y en DRS para datastore, lo cual incrementa la disponibilidad del servicio y el procesamiento de la información, y en cuanto a la integridad de la información, el producto se integra fácil y ágilmente con soluciones de almacenamientos redundantes y de alta disponibilidad que permiten distintos arreglos RAID, empleando también en alta disponibilidad a través de equipos de comunicaciones especializados con accesos restringidos y exclusivo a los administradores.

Principales productos de VMWARE

Hiperconvergencia: Esta solución permite la escalabilidad de manera vertical y horizontal de los recursos de hardware tanto en procesamientos, almacenamiento y red, permitiendo una administración rápida y efectiva.

VSAN: Esta solución permite crear almacenamiento de datos destinados para los ESXI que contienen las máquinas virtuales.

NSX: Esta plataforma permite virtualizar a través de software las redes para los DataCenter, la cual proporciona seguridad separadas de la infraestructura física adyacente.

VREALIZE: Es una suite que permite la gestión de Clouds ya sean híbridas, públicas o privadas. Es capaz de administrar otras plataformas como de AWS, Openstack y KVM.

VMWare VSPhere

vSphere se puede decir que es el producto estrella de VMWARE, esta suite incluye el software hypervisor ESXI capaz de virtualizar los servidores x86 y crear máquinas virtuales. Además incluye VCENTER que es el encargado de centralizar y administrar dichos hypervisores. Además cuenta con otros servicios de move en caliente máquinas y discos virtuales sin tener inactividad en el servicio entre otras funciones.

[5]

CAPITULO 3: COMPONENTES DE VSPHERE

HYPERVISORES VSPHERE ESXI

Definición de Hypervisores ESXI:

En los ambientes virtuales, el hipervisor es una plataforma compuesta por una capa de software que permite almacenar y crear máquinas virtuales VM en las cuales contienen sistemas operativos.

En las VMs utilizan los recursos propios del servidor físico (Host), de esta manera el hypervisor crea una capa de abstracción entre el hardware del host y el sistema operativo de la VM. [6]

Datastore almacenamiento de los hipervisores de VMware para almacenar Máquinas virtuales

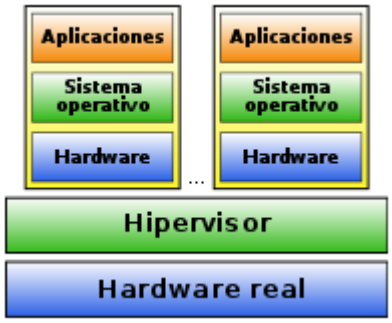


Figura 1. Estructura de un Servidor Virtualizado

El Software encargado de virtualizar servidores físicos es el ESXI, software propietario de vMWare.

ESXI es un software que puede ser utilizado sin necesidad de adquirir una licencia, pero en nuestro caso, se utilizará una licencia en modo prueba, ya que los hypervisores serán administrados por el vCenter que después hablaremos de él.

Para su administración se pueda acceder vía web, desde la versión del hypervisor 6.5 en adelante ya soporta HTML5 dando al sitio más seguridad y estabilidad y compatibilidad a los browser. Cabe mencionar que las versiones anteriores a la 6.5 eran con base al plugin de adobe flash player.

Funciones del Hypervisores ESXI:
Sus funciones son las siguientes:

- Creación de Máquinas Virtuales.
- Movimiento de máquinas virtuales y discos virtuales entre hosts sin afectación del servicio.
- Convertir servicios que se encontraban instalados de manera física a virtual.

[6]

ADMINISTRACIÓN CENTRALIZADA DE HYPERVISORES CON VSPHERE VCENTER

Definición de vCenter:
Es un componente que permite gestionar de una manera centralizada una gran cantidad de host con ESXI y Máquinas Virtuales VM y sirve como único punto de administración central en nuestro entorno virtual. [7]

Funciones del vCenter:

Entre sus principales funcionalidades nos permite aplicar lo siguiente:

- Alta Disponibilidad HA
- Balanceo de carga
- Fault Tolerancia
- vMotion de Máquinas Virtuales
- vMotion Storage (Discos virtuales vmdk)
- Asignación de accesos y permisos de forma granular para la administración de los hosts. Dichos permisos se los puede realizar por grupos o un usuario en específico.
- Permite crear una base LDAP para gestión de usuarios o vincular una base externa basada en LDAP o Kerberos que puede ser un Active Directory de Windows.
- Permite despliegue de parches de manera automática o manual a los hosts. [7]

SWITCH VIRTUALES DISTRIBUIDOS VSPHERE VSWITCH

Definición de vSwith
El virtual swtich es una aplicación que se encuentra dentro de los ESXI que cumple las mismas funciones de un físico y permite la comunicación entre máquinas virtuales, hosts, vSAN o cluster [8]

Funciones del vSwitch Distribuidos:
Entre sus principales funciones son:

- Permite el despliegue y migración de servidores virtuales de una manera fácil y sencilla.
- Permite definir políticas para VLANs, segmentación de redes, Alta disponibilidad.
- Permite creación de subredes para las redes de Storage, Management y vMotion.
- Permite la administración de hasta 500 hosts.

[8]

ALMACENAMIENTO DE RED LOCAL VSPHERE VSAN

Definición de vSAN

El Almacenamiento de red local Virtual llamado vSAN, es una solución que se encuentra dentro de la suite de vSphere, el cual permite la creación de Almacenes de datos compartidos y distribuidos para el almacenamiento de las VMs. [9]

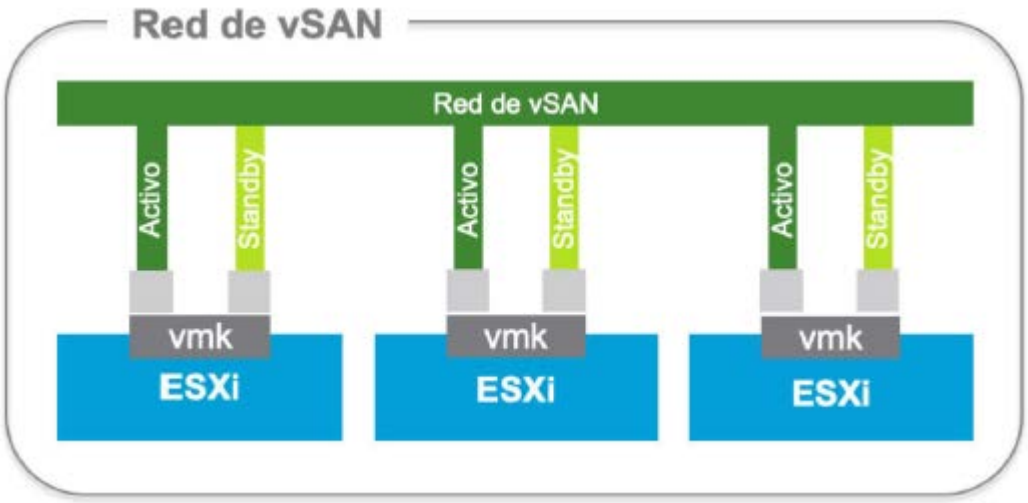


Figura 2. Estructura de una red vSAN

Funciones de VSAN

Entre sus principales funciones son:

- Se requiere mínimo dos hosts que contengan discos SSD o HDD.
- Permite el agrupamiento de discos SSD y HDD creando un Cluster, del cual sale el o los "DataStore" el cuál será accedido para los todos ESXI del Cluster.
- Permite el escalamiento de manera horizontal agregando simplemente otro hosts que contenga discos SSD o HDD.
- Permite un alto nivel de performance.

- Permite la administración desde el vSphere client o desde la web.

[9]

MIGRACIÓN DE MAQUINAS VIRTUALES CON VMOTION

Definición de vMotion

vMotion es otra de las funcionalidades que proporciona vSphere en el cual es el encargado de permitir el movimiento de VMs o VMDK en caliente entre hosts perteneciendo al mismo vCenter o entre vCenter o hosts que no se encuentran dentro de los mismos sin tener interrupción en los servicios. [10]

Ver imagen de los dos casos citados.

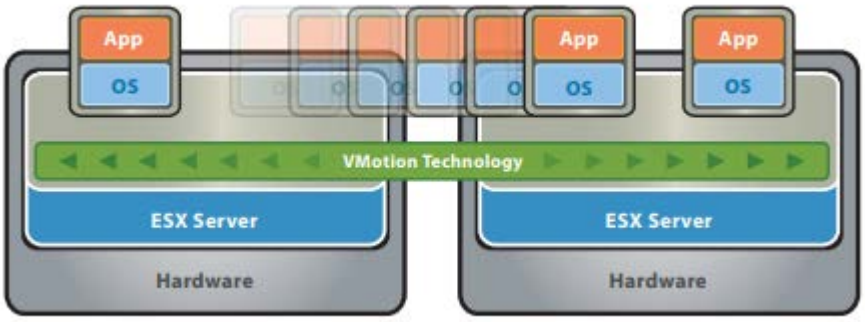


Figura 3. Movimientos de VMs entre Hosts

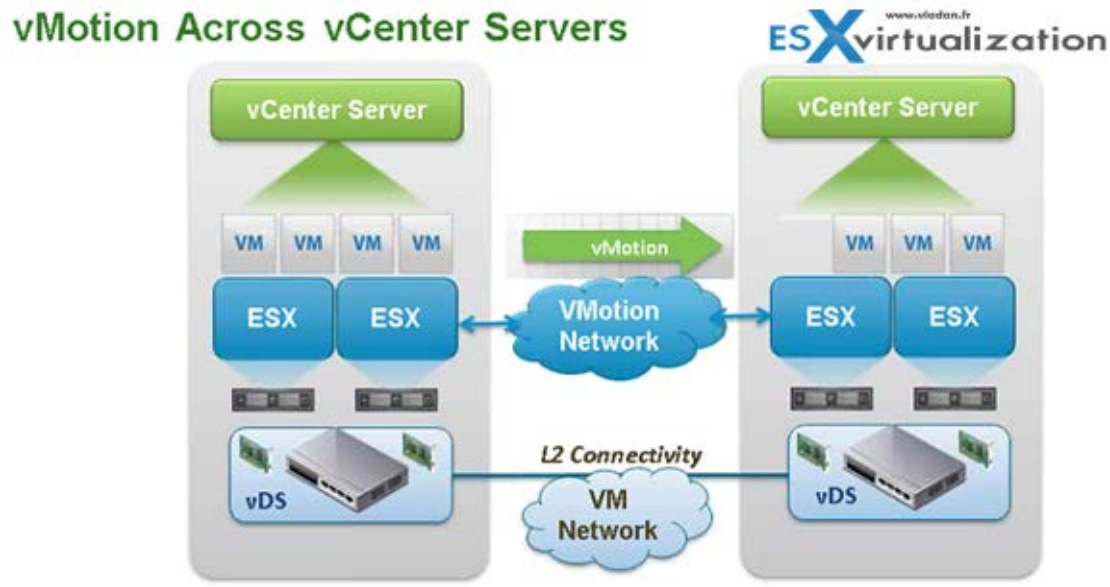


Figura 4. Movimientos de VMs entre vCenter

Funciones de vMotion

- Permite el movimiento de VMs en caliente sin necesidad de apagar y además sin tener tiempo de inactividad.
- Permite el movimiento de los discos virtuales en caliente sin necesidad de apagar y además sin tener tiempo de inactividad.
- Permite a través de vMotion tener opción de operar otras funciones como el Esquema de Distribución de Recursos DRS y la Administración de Distribución de Poder DPM.

[10]

PROGRAMADOR DISTRIBUIDO DE Recursos VSPHERE DRS

Definición de DRS

DRS es otro servicio que incluye vSphere que proporciona un balanceo de cargas con disponibilidad de recursos en un ambiente virtualizado gracias a su resources pool. Ver imagen. [11]

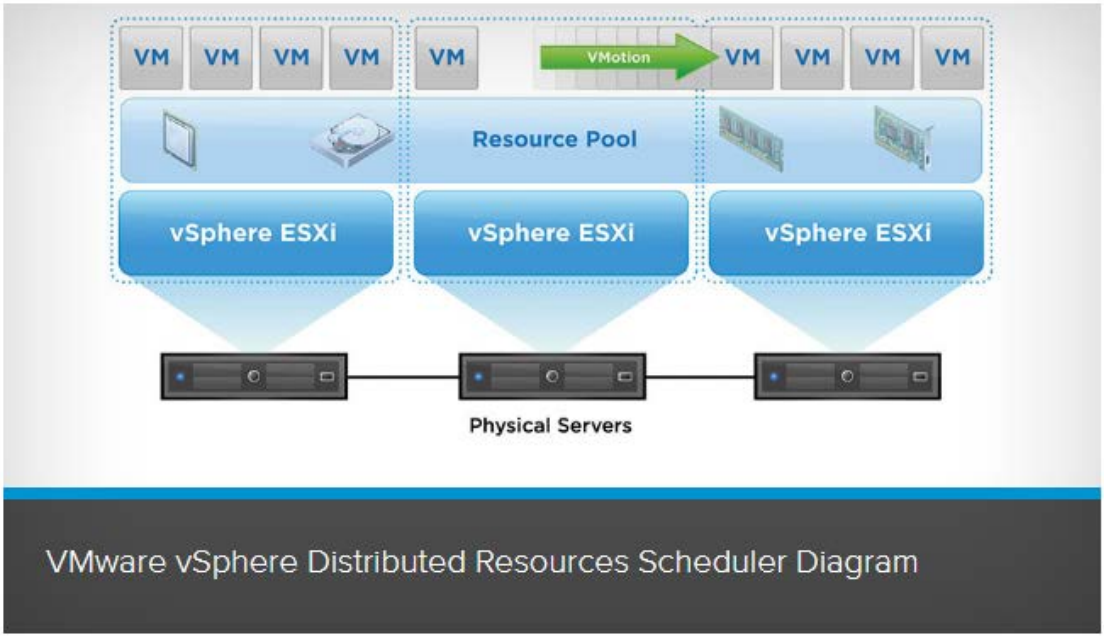


Figura 5. Diagrama DRS

Funciones de DRS

- Permite definir de manera fácil reglas para a la asignación de recursos físicos que serán distribuidos entre las VMs. Dichas reglas se las puedes configurar para control ya sea manual o automático.
- Permite configuraciones dedicas de manera individual de la infraestructura de acuerdo a las unidades core de negocio de la organización.
- Permite un monitoreo del hardware de manera centralizada y su utilización.
- Permite priorización de los recursos de acuerdo a la importancia del servicio que esté operativo.
- Permite el mantenimiento de los hosts que se encuentren libres de inactividad y alta optimización del consumo energético.

[11]

CAPÍTULO 4: MEJORES PRÁCTICAS QUE ASEGURA DISPONIBILIDAD Y REDUNDANCIA PREVIA LA CONSTRUCCIÓN DEL AMBIENTE VIRTUAL

Previo al despliegue, configuración y seguridad del Ambiente Virtual, es necesario tomar en cuenta las mejores prácticas sobre el rendimiento, alta disponibilidad, etc, las cuales se describen a continuación:

Mejores prácticas de Rendimiento, Seguridad y Disponibilidad.
Para las pautas de mejores prácticas de rendimiento, es importante comenzar primero asegurándose de que:

- Todo el hardware que utiliza en el sistema se encuentra en la lista de compatibilidad de hardware para esa versión específica del software VMware.
- Asegúrese de que el hardware de su elección cumpla con los requisitos mínimos de configuración que admite el software VMware.
- También se considera una mejor práctica probar la memoria del sistema durante 72 horas para permitirle verificar cualquier error de hardware.

Al considerar la CPU, es importante obtener una CPU que sea compatible con los requisitos de VMware vMotion que tengan una relación directa con el DRS (Distributed Resource Scheduler).

También debemos considerar la compatibilidad de la CPU con la tolerancia a fallas de VMware asociada.

Por otro lado, en términos de procesadores, los procesadores más recientes tanto de AMD como de Intel incluyen características de hardware específicas que están orientadas a ayudar a la virtualización. Aunque los procesadores de la primera generación introdujeron la virtualización de la CPU, el VT-x de Intel y el AMD-V de AMD, las cosas han cambiado desde entonces. Para un mejor rendimiento, se recomienda utilizar los procesadores de segunda generación que tienen una virtualización adicional de la Unidad de administración de memoria (MMU). Estos incluyen el procesador AMD RVI (indexación rápida de virtualización) y el Intel EPT (tablas de páginas extendidas).

Vale la pena señalar que existe una función de administración de memoria de E/S aún más nueva en los procesadores actuales que permite a las máquinas virtuales tener acceso directo a varios dispositivos de entrada y salida, como controladores de almacenamiento y tarjetas de red. En los procesadores Intel, esta función se conoce como VT-d (Tecnología de virtualización para entrada / salida dirigida). En los procesadores AMD, esta función se llama IOMMU o AMD-Vi (AMD I / O Virtualization).

Por otro lado, es conocido que la configuración de almacenamiento de back-end afecta mucho el rendimiento y la mayoría de las veces; Las instancias con un rendimiento de almacenamiento inferior al esperado generalmente se deben a problemas de configuración.

El rendimiento del almacenamiento depende de una variedad de factores, como la carga de trabajo, el tamaño de la memoria caché, el hardware, el proveedor utilizado, el tamaño de la franja y el nivel de RAID entre una serie de otras actividades. Teniendo en cuenta que muchas cargas de trabajo son muy sensibles a la latencia de las operaciones de E/S, la importancia de tener los dispositivos de almacenamiento configurados correctamente no se puede exagerar.

Es recomendable que, al elegir el hardware para este debemos elegir un hardware de almacenamiento que admita VAAI (API de VMware vStorage para la integración de Array) para descargar algunas de las operaciones al hardware de almacenamiento en lugar de realizarlas en ESXi y mejorar la escalabilidad del almacenamiento.

Mejores prácticas de rendimiento de alta disponibilidad (HA) para garantizar la Seguridad y Disponibilidad:

Este software hace que el uso de la infraestructura sea menos expansivo y más simple para proporcionar niveles más altos de disponibilidad y seguridad y disponibilidad del servicio para aplicaciones muy importantes y críticas, así mismo permite a las organizaciones aumentar de forma muy rentable el nivel básico de disponibilidad provisto para todas las aplicaciones. Una de las

mejores prácticas clave es eliminar los puntos únicos de falla, lo cual se puede lograr creando redundancia en puntos vulnerables para ayudar a eliminar o reducir el tiempo de inactividad causado por fallas de hardware.

Estos deberían estar en estas cuatro capas, a saber:

- Componentes del servidor como adaptadores de bus de host y adaptadores de red.
- Componentes de red, redes de almacenamiento y matrices de almacenamiento.
- Servidores que incluyen fuentes de alimentación de rack, chasis y hojillas y enclousers.

Al implementar o crear un clúster de alta disponibilidad (HA) de vSphere, normalmente se considera la mejor práctica construir el clúster con hardware de servidor idéntico, ya que esto simplifica enormemente la administración y configuración de los servidores que utilizan perfiles de host disponibles y también reduce la fragmentación de recursos y aumenta la capacidad para manejar las fallas del servidor. El uso de hardware radicalmente diferente en un clúster conduce a un clúster desequilibrado que hace que el clúster sea menos productivo.

También es importante tener en cuenta el tamaño general del grupo. Se sabe que los clústeres de menor tamaño requieren un porcentaje relativo mayor de todos los recursos de clúster disponibles que se reservan como capacidad de reserva para poder manejar las fallas de manera adecuada. Siempre tenga en cuenta que un clúster de solo tres nodos requerirá que al menos el 33% de los recursos del clúster se mantengan en reserva para la conmutación por error, mientras que un clúster de diez nodos solo requerirá el 10% de los recursos del clúster reservados para la conmutación por error. Cabe señalar, sin embargo, que la complejidad del clúster aumenta considerablemente.

Cuando se toma en consideración el diseño de la red, es importante tener en cuenta que las dos áreas principales en las que las mejores prácticas se enfocan claramente es aumentar la resistencia y seguridad de las redes del lado del cliente y aumentar la capacidad de recuperación de los canales de comunicación utilizados por la propia HA. Si los Switches en la red física que conectan los servidores admiten PortFast o una configuración equivalente, entonces esto se debe habilitar, con lo cual se permite que el host recupere rápidamente la conectividad después del inicio. También se recomienda que la supervisión del host se desactive en cualquier momento en el mantenimiento de la red capaz de deshabilitar las rutas de los *Heartbeat* entre los hosts en ese grupo en particular, ya que esto puede desencadenar una respuesta de aislamiento.

Heartbeat.- Servicio que proporciona funcionalidad de infraestructura en Cluster o HA.

PortFast.- Es una función que permite a las estaciones de usuarios finales obtener acceso inmediato a la red de capa 2

En entornos donde se utilizan los protocolos IPv4 e IPv6, se considera como Best Practice de Seguidad que para VMware vSphere se configure los Switches distribuidos en todos los hosts para permitir el acceso a ambas redes cuando solo cuando sea necesario. Esto evita la posibilidad de encontrar problemas de partición de red que pueden ser causados por una falla del host o la pérdida de una sola pila de redes IP.

Para aumentar la seguridad y mejorar la disponibilidad general de la red, es recomendable configurar a lo largo de los datos de heartbeat los almacenes de la red de administración redundante desde los hosts de ESXi a otro hardware de conmutación de redes. El uso de equipos de adaptador de red también es recomendable.

CAPÍTULO 5: MEJORES PRÁCTICAS EN LA SEGMENTACIÓN Y ACCESO A LA INFRAESTRUCTURA VIRTUAL – SEGURIDAD A NIVEL DE CAPA 3 y 7

Es muy importante tener el control y saber quién o quienes acceden a la infraestructura virtual de nuestra organización, en nuestro caso en el LAB (Aplicable a los ambientes Productivos), por esta razón tanto vMWARE y mi experiencia en la administración y segurización hacen que se determine las siguientes mejores prácticas:

Definición de VLAN

Como mejor práctica de seguridad se deben crear VLAN para poder separar el tráfico que genera los diferentes componentes de un Ambiente virtual, de esta manera podemos tener un mejor control de acceso a los mismos.

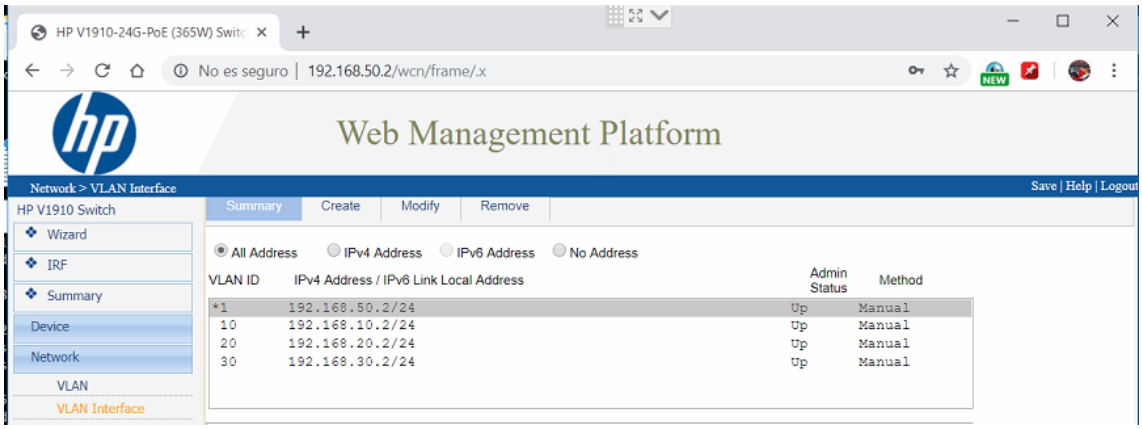


Figura 6. Listado de VLANs

SEGMENTO	VLAN ID	Detalle
192.168.50.0/24	1	Administración - Equipos físicos que incluye Switch, iLOs de los SRVs
192.168.10.0/24	10	Hipervisores - hosts físicos ESXi
192.168.20.0/24	20	Máquinas Virtuales - Incluye vCenter
192.168.30.0/24	30	vMOTION - Destinado a las interfaces de vMotion

Control de Acceso a través del Firewall

Una vez creado las VLAN y creados los vSwitch en los ESXI, se procede a realizar la conexión de las interfaces en el Firewall, de esta manera se puede gestionar el control de acceso y filtramos el tráfico basándose en la IP, Puerto, Protocolo origen destino, además a nivel de capa 7 podemos inspeccionar los paquetes de red y degenar solicitudes como HTTP, POST, GET.

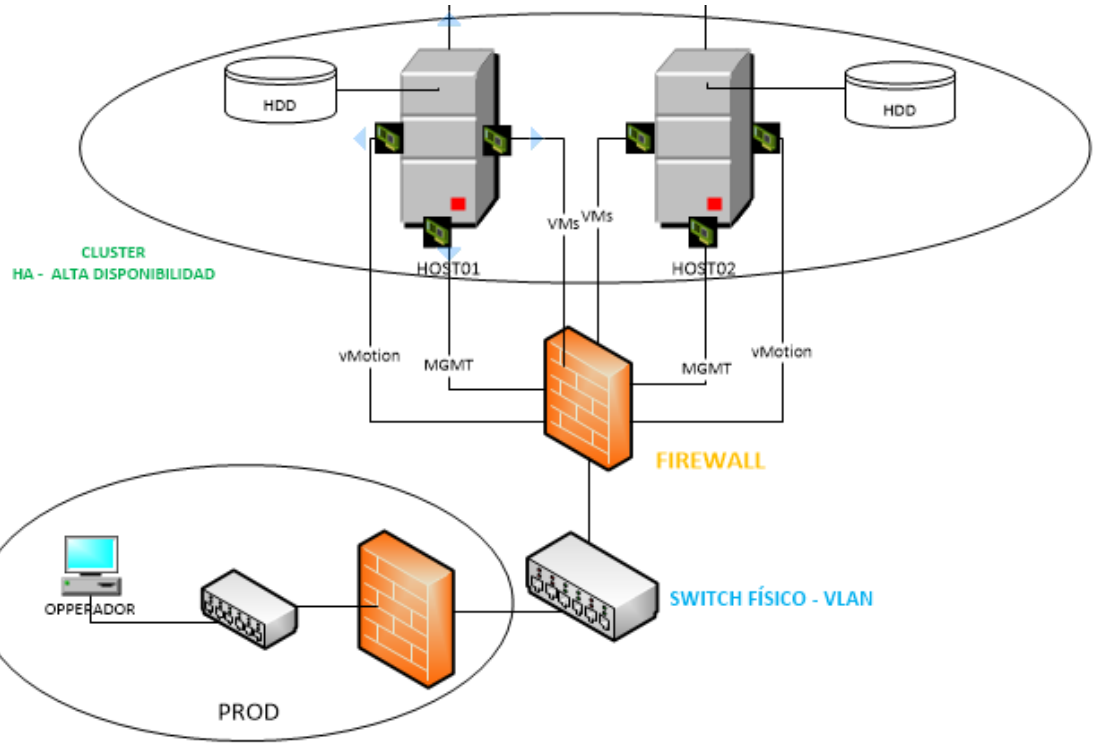


Figura 7. Ubicación de Firewalls

CAPÍTULO 6: CONSTRUCCIÓN DE AMBIENTE VIRTUAL PARA LABORATORIO

Diseño de Laboratorio

A continuación el diseño del laboratorio, en la construcción del mismo, existen todos los componentes excepto el Switch de PROD y el Firewall, esos ya existen en la organización y en el firewall se creó reglas de acceso para que los segmentos creados de los Operadores tengan acceso a la infraestructura de Laboratorio.

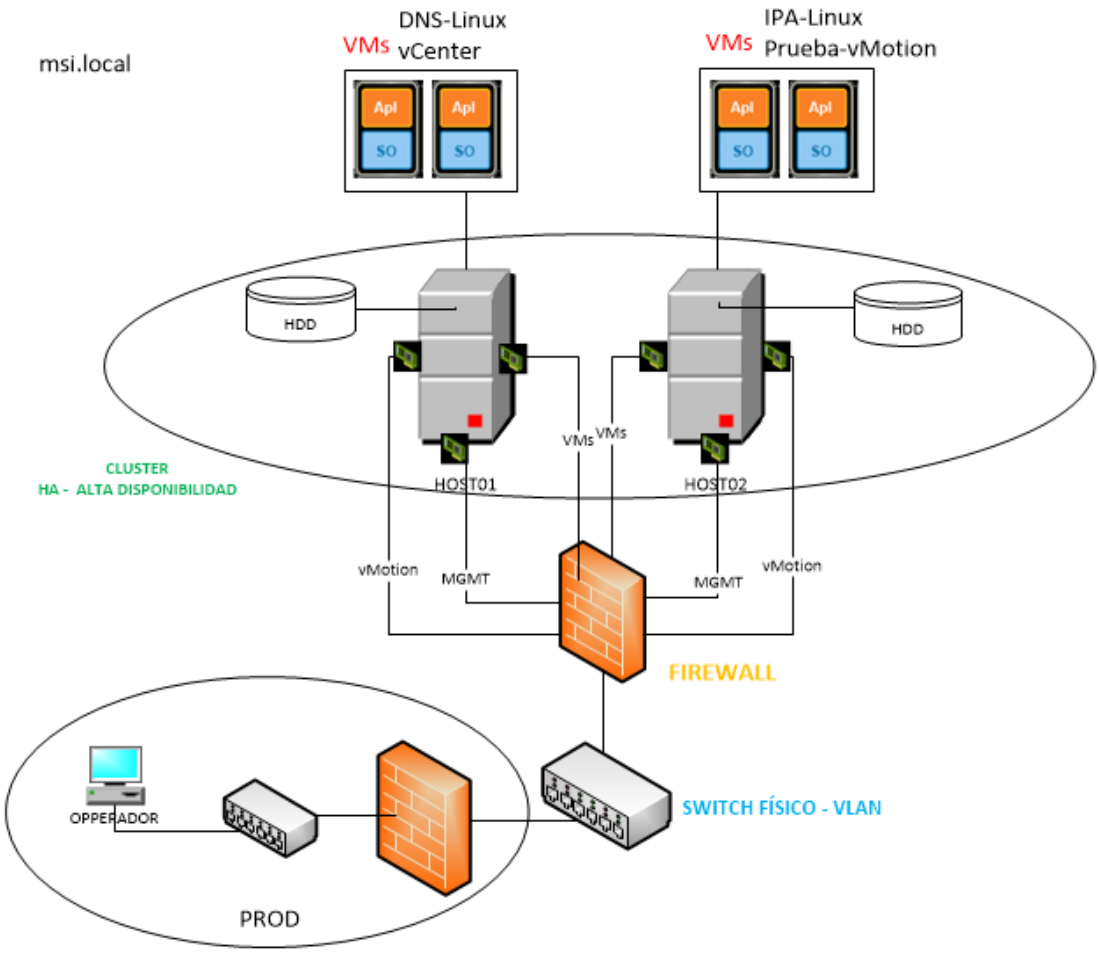


Figura 8. Diseño del Laboratorio

Recomendaciones Obligatorias:
Para la construcción de este laboratorio se recomienda de manera obligatoria construir y configurar los servicios de DNS y un Directorio Activo de usuarios/grupos.

Se construyó un servidor de directorio activo y dominio llamado "**msi.local**" y servidor de DNS necesarios para la instalación de los componentes y la aplicación de mejores prácticas en la construcción del Ambiente Virtual basado en Seguridad.

Servidor de DNS

FQDN: dns01.msi.local - IP: 192.168.20.15

```
[root@dns01 ~]# dig dns01.msi.local

; <<>> DiG 9.9.4-RedHat-9.9.4-73.el7_6 <<>> dns01.msi.local
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46852
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;dns01.msi.local.               IN      A

;; ANSWER SECTION:
dns01.msi.local.        86400   IN      A       192.168.20.15

;; AUTHORITY SECTION:
msi.local.              86400   IN      NS      dns01.msi.local.

;; Query time: 1 msec
;; SERVER: 192.168.20.15#53(192.168.20.15)
;; WHEN: Thu Jul 04 21:14:59 -05 2019
;; MSG SIZE  rcvd: 74
```

Figura 9. DNS Server

Directorio Activo

FQDN: ipa.msi.local - IP: 192.168.20.18

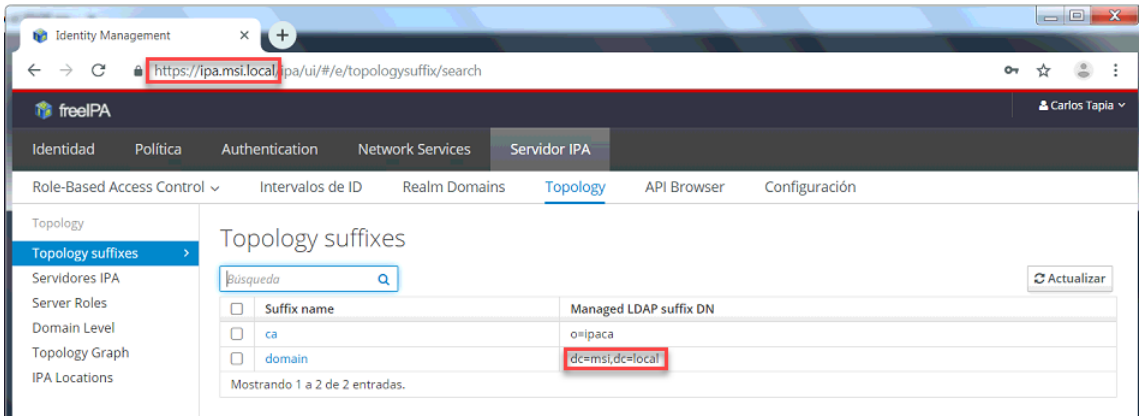


Figura 10. Servidor de Directorio Activo

Compatibilidad en el Hardware

Antes de realizar la adquisición del hardware, se recomienda revisar la compatibilidad con respecto a los hipervisores. Revisar el sitio web del fabricante. [14]

En el caso del hardware utilizado en este laboratorio es: ProLiant ML350e Gen8 y su compatibilidad con respecto al hipervisor es el siguiente:

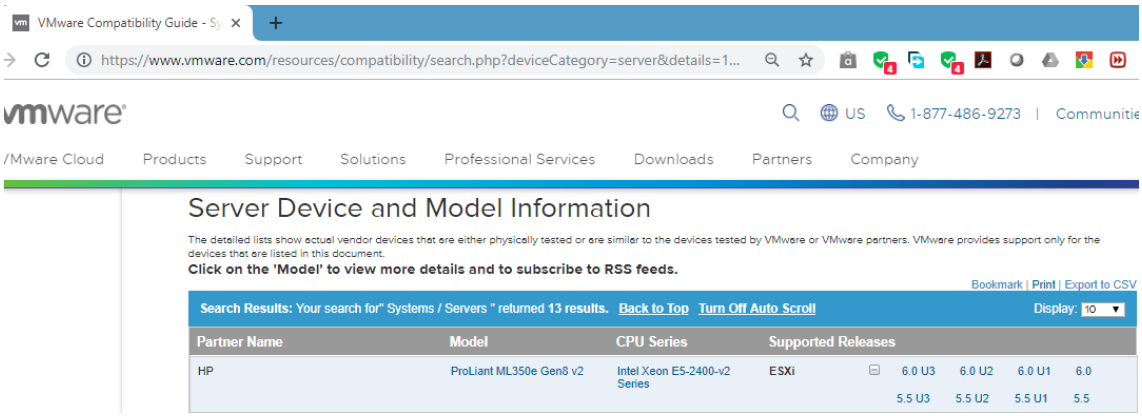


Figura 11. Compatibilidad con Hardware utilizado [15]

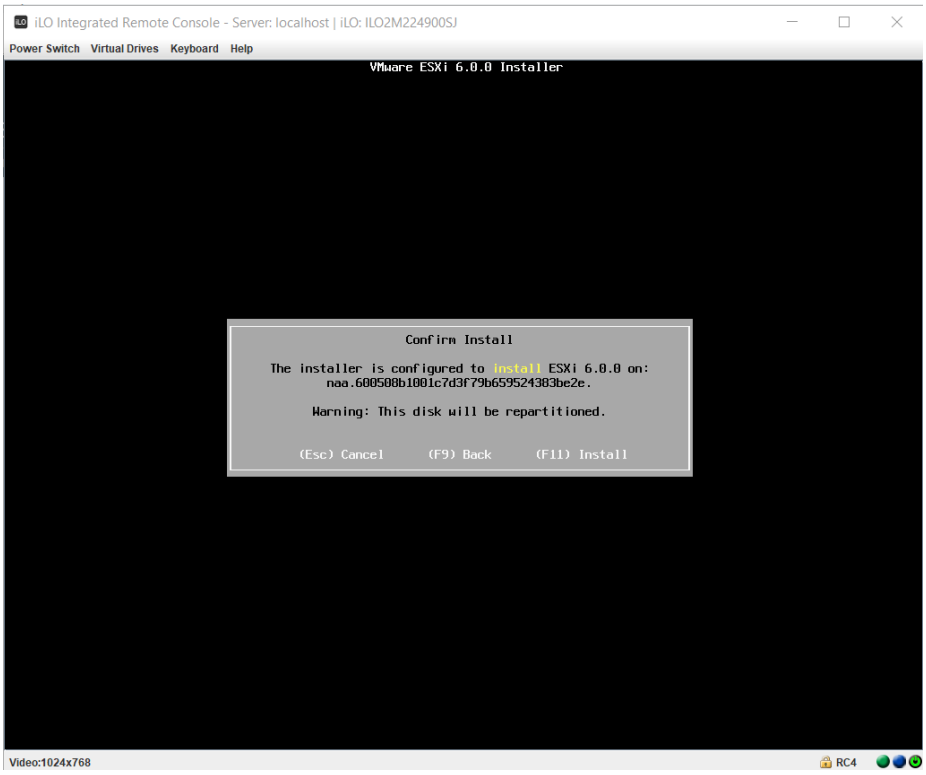
6.1 HYPERVISORES – LABORATORIO

6.1.1 DESPLIEGUE Y CONFIGURACIONES DEL HYPERVISOR

Instalación de Hypervisor

VMWARE proporciona imagenes ISO personalizada por cada fabricante de hardware, se debe acceder al sitio de MyVMWARE y realizar la descarga. Este es el link [14].

La instalación del Hipervisor es bastante intuitivo, por eso se pondrá imágenes principales de su instalación.



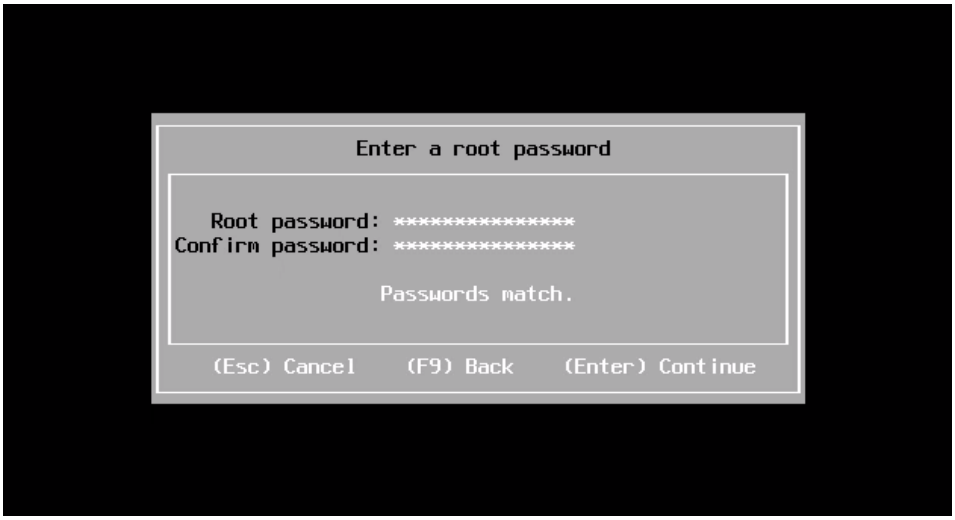


Figura 13. Instalación de Hipervisor 2/2

Acceso a través de la consola remota iLO de los servidores HP: Ver imagen

FQDN: host01.msi.local
IP: 192.168.10.3/24

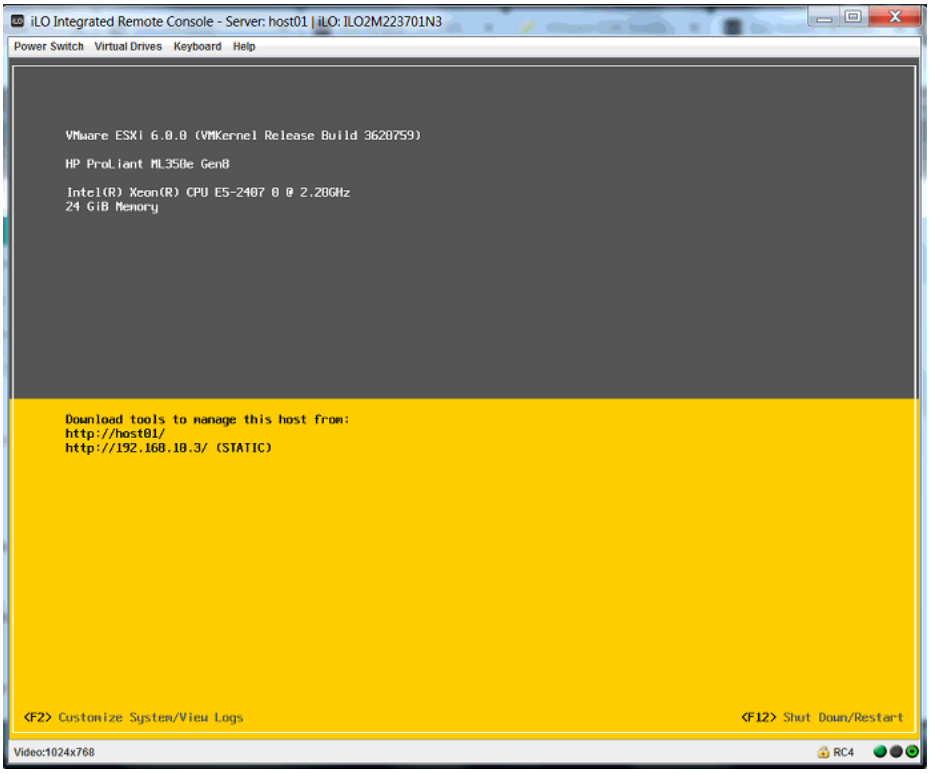


Figura 14. Acceso a través de la consola remota iLO de los servidores HP

FQDN: host02.msi.local
IP: 192.168.10.4/24

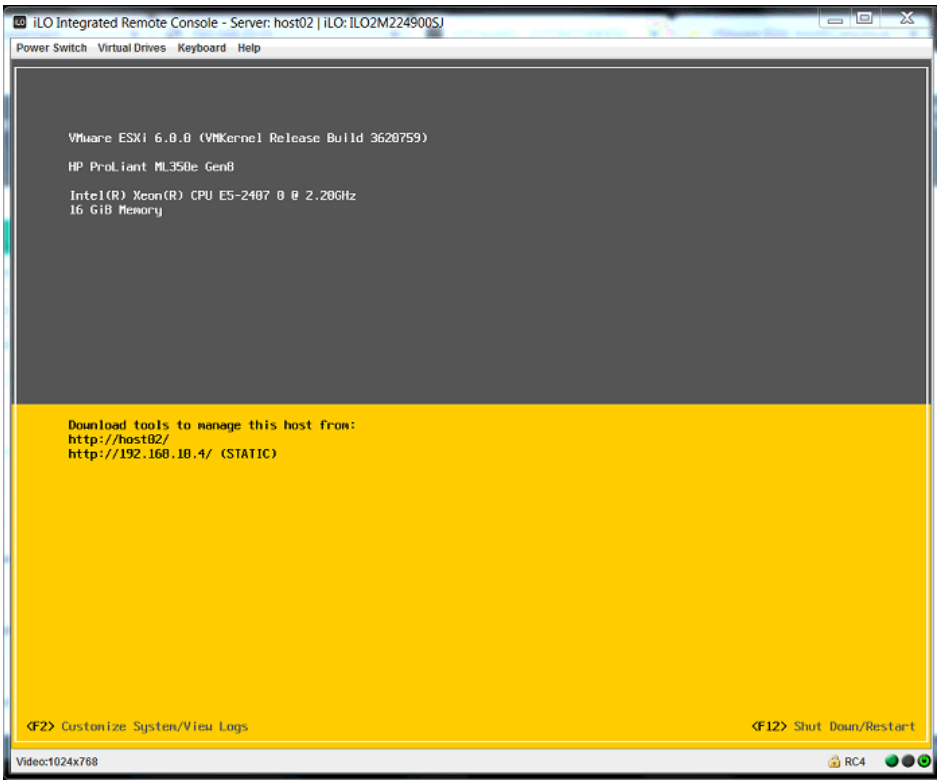


Figura 15. Acceso a través de la consola remota iLO de los servidores HP

6.1.2 MEJORES PRÁCTICAS APLICADAS EN HYPERVISORES

Administración Centralizada

- Para tener una administración centralizada desde el vCenter, se recomienda y se debe agregar los hipervisores (Hosts físicos) al mismo. Ahora en adelante, toda configuración o despliegue se lo hará desde el vCenter. Ver apartado de vCenter.

Figura 16. Vista del vCenter

Tipos de Modo de Acceso

Es la limitación de acceso al hipervisor. Configuración se la realiza desde el vCenter. Ver apartado de vCenter.

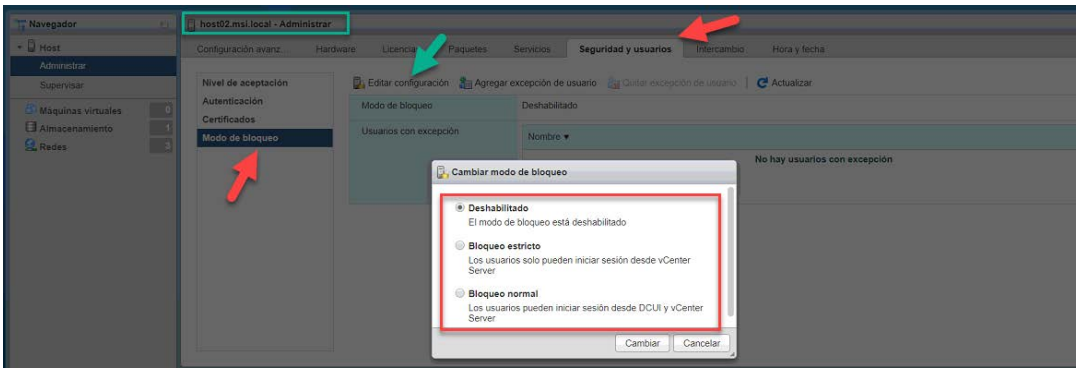


Figura 17. Acceso a través de la consola remota iLO de los servidores HP

Inicio de Sesión a Consola SSH y DCUI

Los hipervisores tienen un OS Linux de tipo embebido, los mismos se acceden por SSH y también a través de la Interfaz de Usuario de la Consola Directa (DCUI). Aunque estos servicios no se ejecutan por default cuando se instala el hipervisor, el acceso a estos servicios es muy importante cuando se tiene algún troubleshooting o alguna tarea de mantenimiento.

Recomendación:

- Por ser accesos de alto riesgo, se recomienda que sólo sean habilitados cuando se tenga que hacer troubleshooting o ventanas de mantenimiento coordinadas.

Los mismos permisos se pueden gestionar a través del vCenter (Ver apartado de vCenter), de esta manera podemos establecer permisos y tiempos de sesión para el riesgo de un acceso no autorizado.

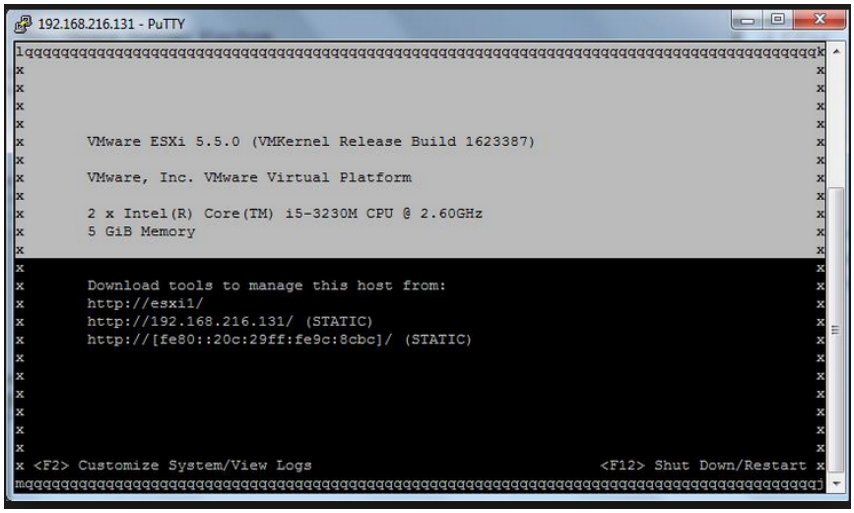


Figura 18. Consola SSH-CLI

SSH.- Es la conexión remota a un servidor de destino de manera cifrada a través del protócolo del mismo nombre

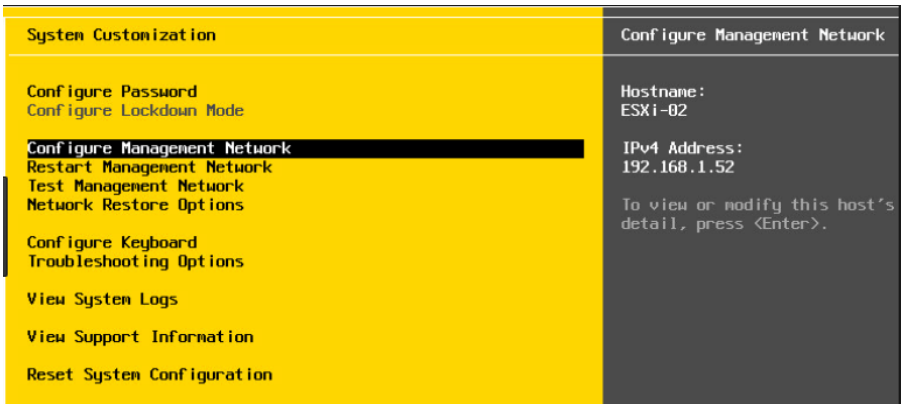


Figura 19. Consola DCUI

Autenticación en Hipervisores

No se recomienda el inicio de sesión con el usuario root, ya que a nivel de auditoría y trazabilidad no se sabría quién accedió a los servidores al momento de realizar algún cambio o tarea.

Recomendaciones:

- Poner en sobre sellado las credenciales de root, el área de Seguridad Informática deberá resguarda.
- Se recomienda como buena práctica, iniciar sesión con usuarios personales y no de servicios o no personales.
- Se recomienda integrar el Servidor de Directorio Activo "**msi.local**" con el vCenter. Ver apartado de vCenter.

Accesos y Permisos en Hipervisores

Los accesos y permisos se los asignará a través del vCenter si los hipervisores se encuentran agregados y centralizados. Ver apartado de vCenter.

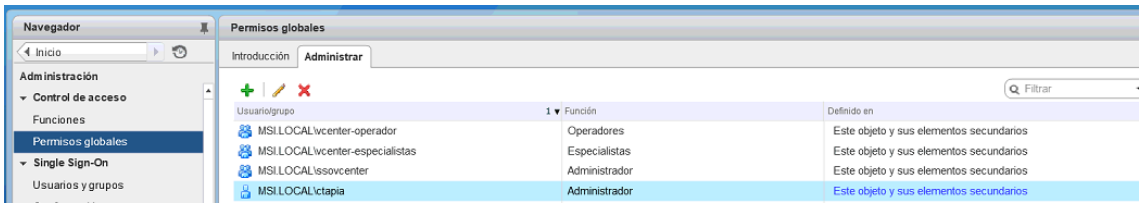


Figura 20. Vista de creación de grupos para permisos en vCenter

---

DCUI.- La interfaz de usuario de la consola directa (DCUI) permite interactuar con el host de forma local mediante los menús basados en texto.

Gestor de Arranque GRUB

Cuando se realiza la instalación del hipervisor, por default el gestor de arranque GRUB no se configura ningún passwd. GRUB es el gestor de arranque que inicia posterior al BIOS dentro de un sistema operativo tanto en Linux o Windows.

Recomendaciones:

- Se recomienda la configuración del passwd del GRUB, ya que es un riesgo que personal no autorizado acceda al mismo y realice cambios en booteo del hipervisor o peor aún cambie el password del root del ESXI.

Deploy de Actualizaciones

El deploy de actualizaciones se lo realizada desde el vCenter. Ver apartado de vCenter

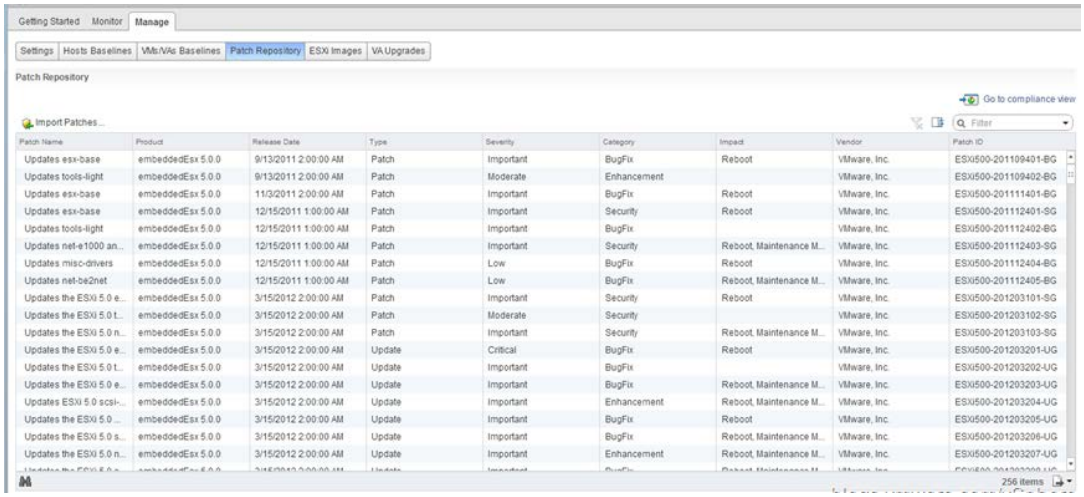


Figura 21. Listado de Actualizaciones aplicar a Hipervisores

Firewall del Hipervisor

Todos los host ESXI tiene instalado un firewall virtual modo EndPoint.

Recomendación:

- Se recomienda la configuración del mismo para administrar, permite y denegar el tráfico entrante y saliente según la necesidad que se tenga, de la misma manera se puede restringir el acceso a los servicios y puertos/protocolos.
- Esta administración se la puede realizar conectándose al hipervisor a través del vSphere Client/Web o accediendo desde el vCenter Server. Ver apartado de vCenter

---

GRUB.- Gestor de arranque múltiple.

- Se recomienda configurar los segmentos o direcciones permitidas que se encuentren dentro de los segmentos que pertenezcan al área de operaciones

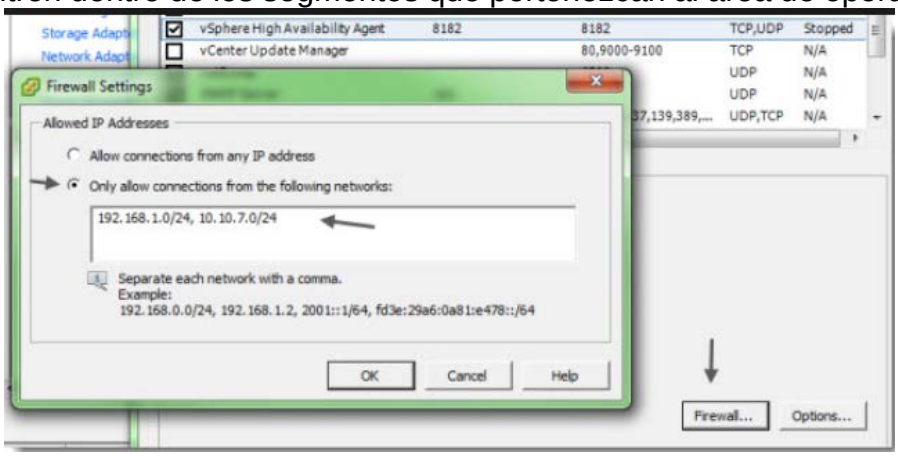


Figura 22. Configuración del Firewall del Hipervisor

- Se recomienda configurar los puertos/servicios que son necesarios para la operación correcta del ambiente virtual de esta manera segurisamos nuestros servidores.

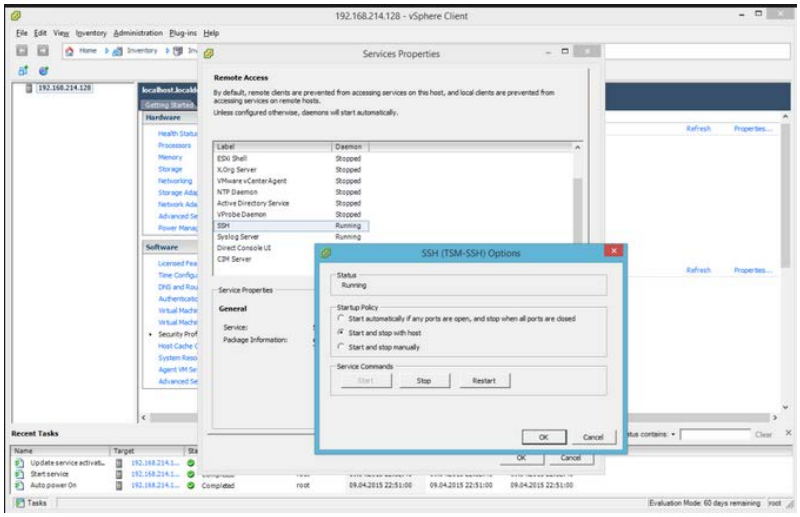


Figura 23. Configuración de los Servicios en Firewall del Hipervisor

- Si se cuenta con una cantidad numerosa de hosts, VMWARE nos permite configurar mediante consola por medio ESXCLI. Para lo cual se crea un archivo de configuración y posterior se lo despliega al resto de ESXI a través del VCENTER. De esta manera se pueden crear tareas automáticas para que la gestión de reglas en los firewalls en los ESXI sea más controlada y gestionada. Además con el VIB se puede crear reglas persistentes en el firewall del ESXI.
  [16]

ESXCLI.- Conjunto de comandos para la administración de los hipervisores.

6.2 VCENTER – LABORATORIO

6.2.1 DESPLIEGUE Y CONFIGURACIONES DEL VCENTER

A continuación el paso a paso del despliegue y configuración inicial del vCenter:

Instalación y Configuración básica:

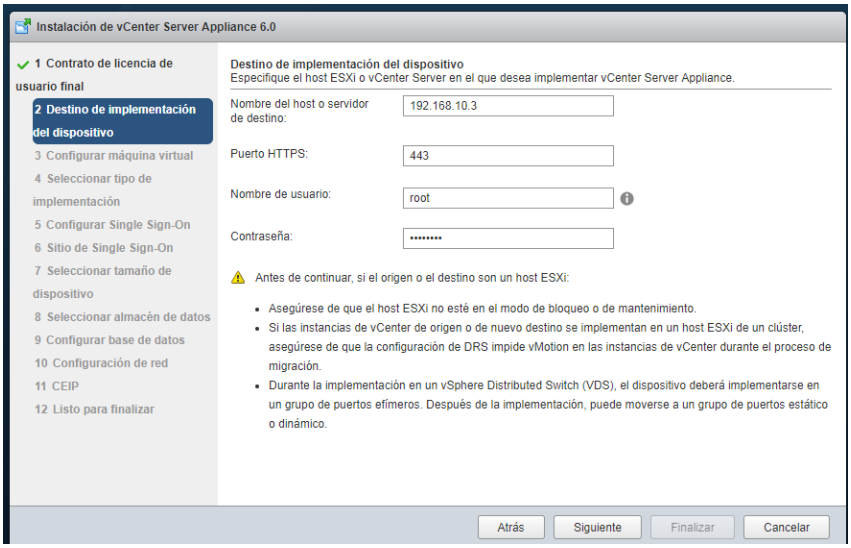


Figura 24. Instalación y Configuración vCenter 1/5

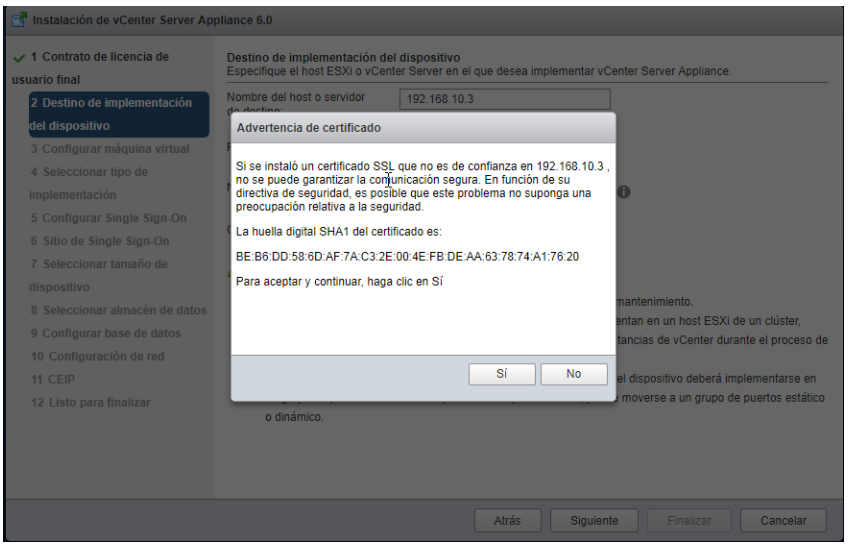


Figura 25. Aceptamos el certificado SSL proveniente del host: 192.168.10.3 o host01.msi.local

Configuración del nombre de la Máquina Virtual del vCenter y las credenciales del mismo:

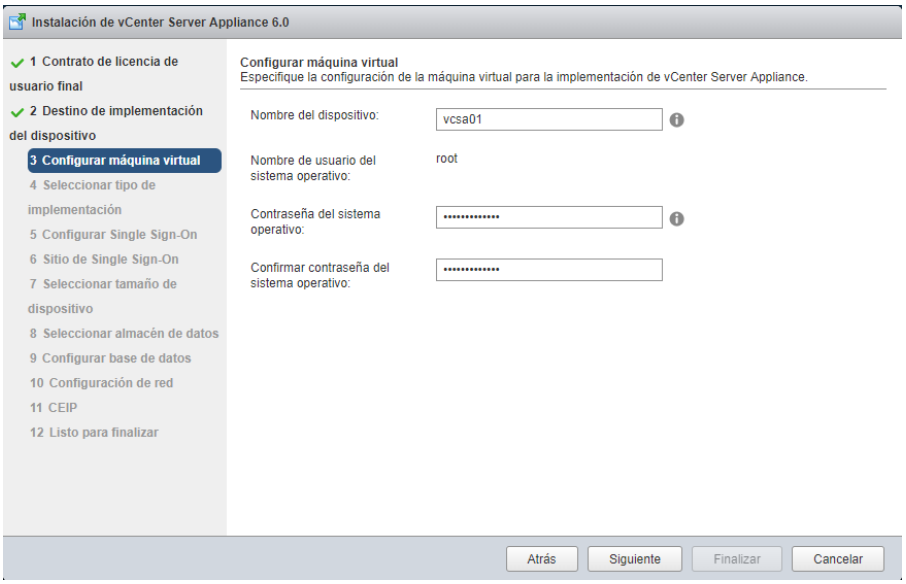


Figura 26. Configuración del nombre de la Máquina Virtual del vCenter y las credenciales del mismo

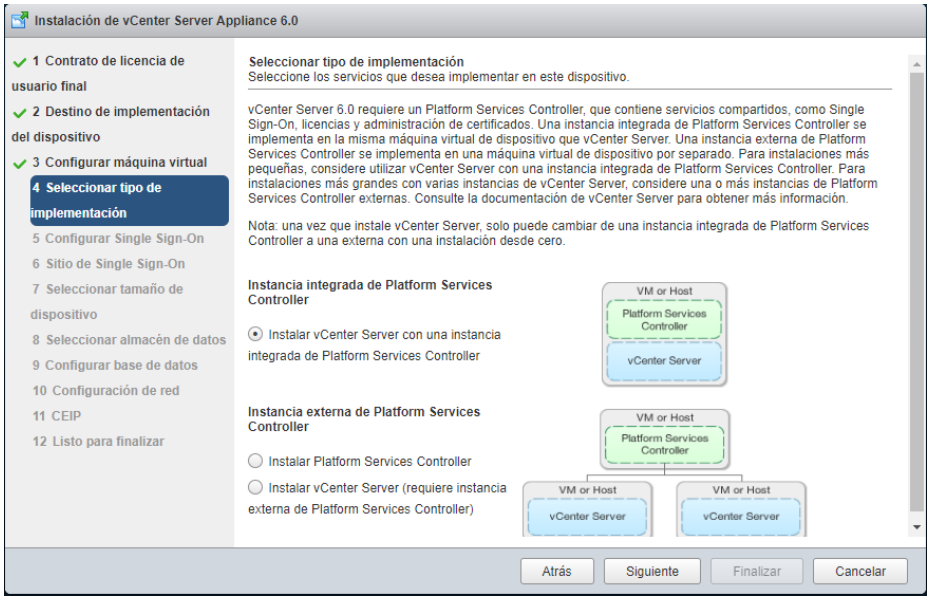
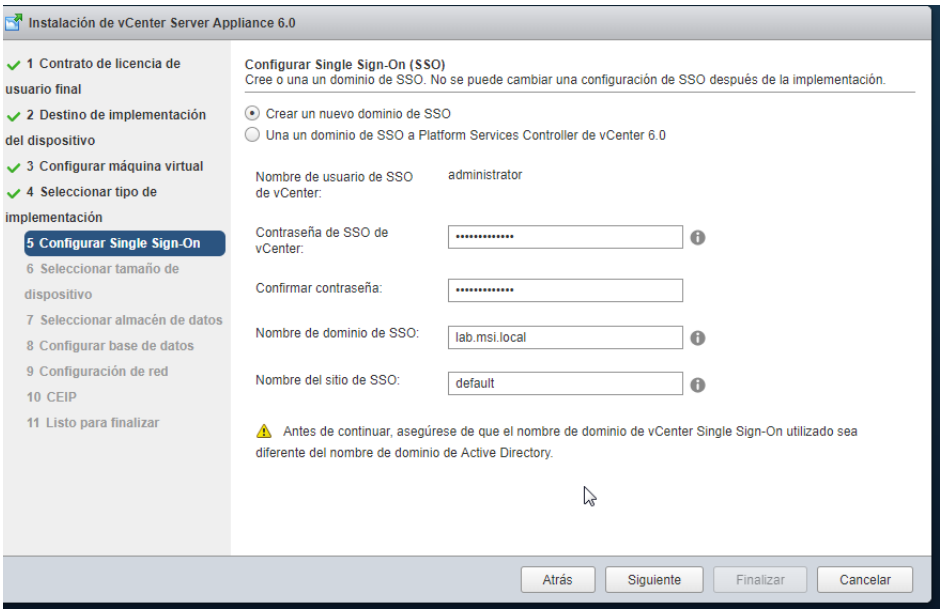


Figura 27. Seleccione con una sola instancia, la recomendación sería que se instale por separado



: Figura 28. Ingresar las credenciales de administración del vCenter y SSO por default

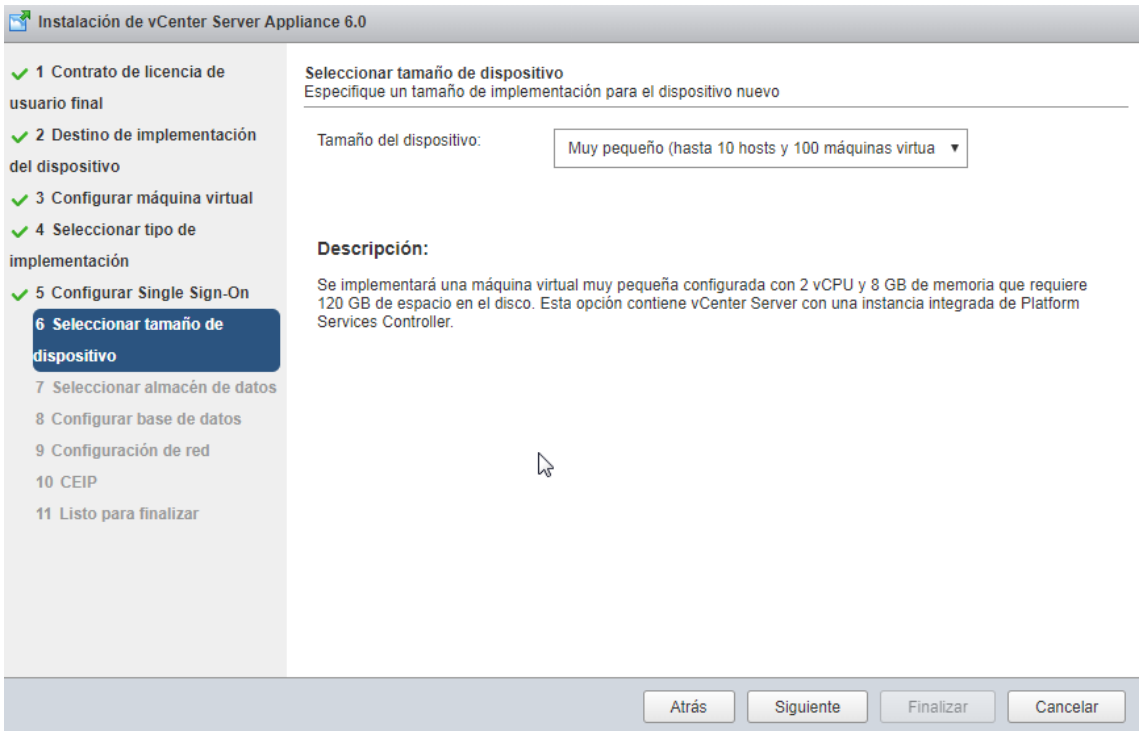


Figura 29. Seleccione tamaño del dispositivo

SSO.- Single Sing ON

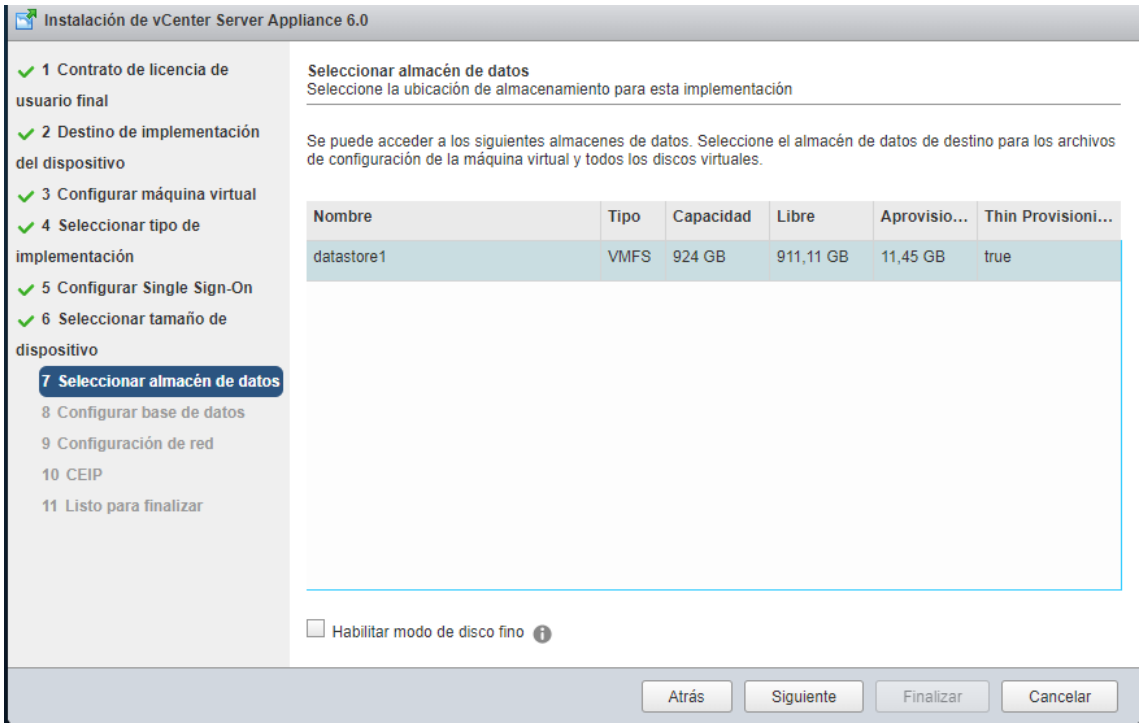


Figura 30. Seleccione el datastore que tiene el hipervisor

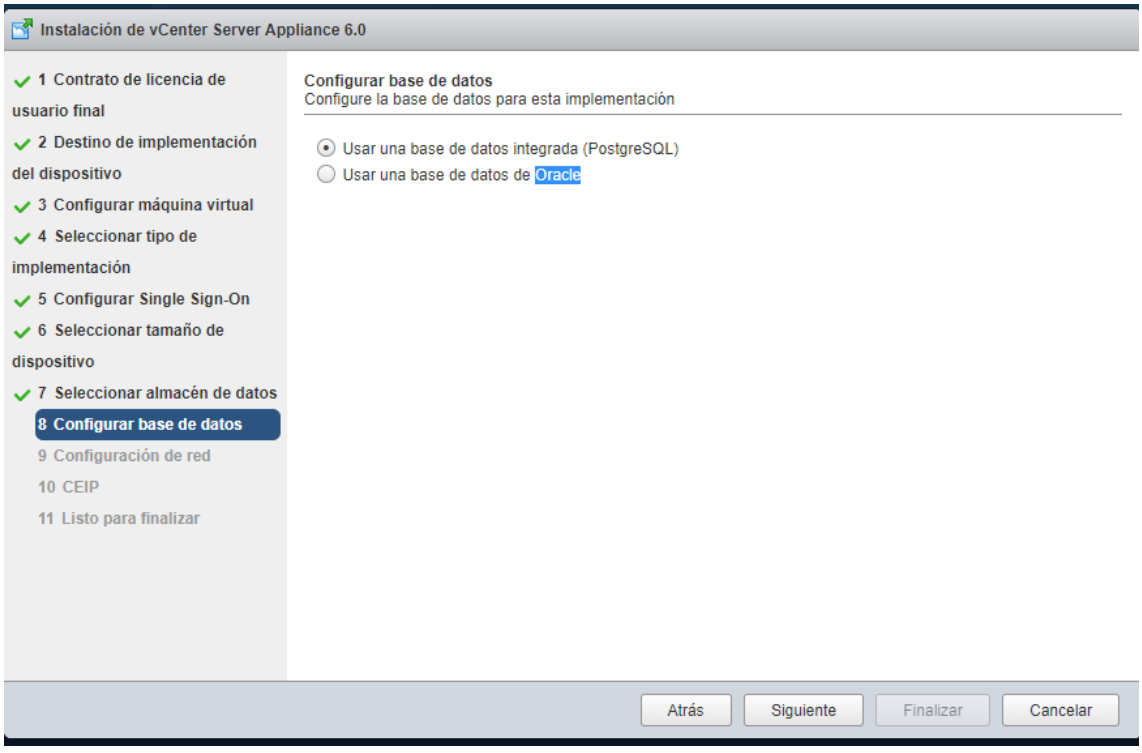


Figura 31. En nuestro LAB seleccionamos bbdd PostgreSQL o se puede seleccionar en Oracle también

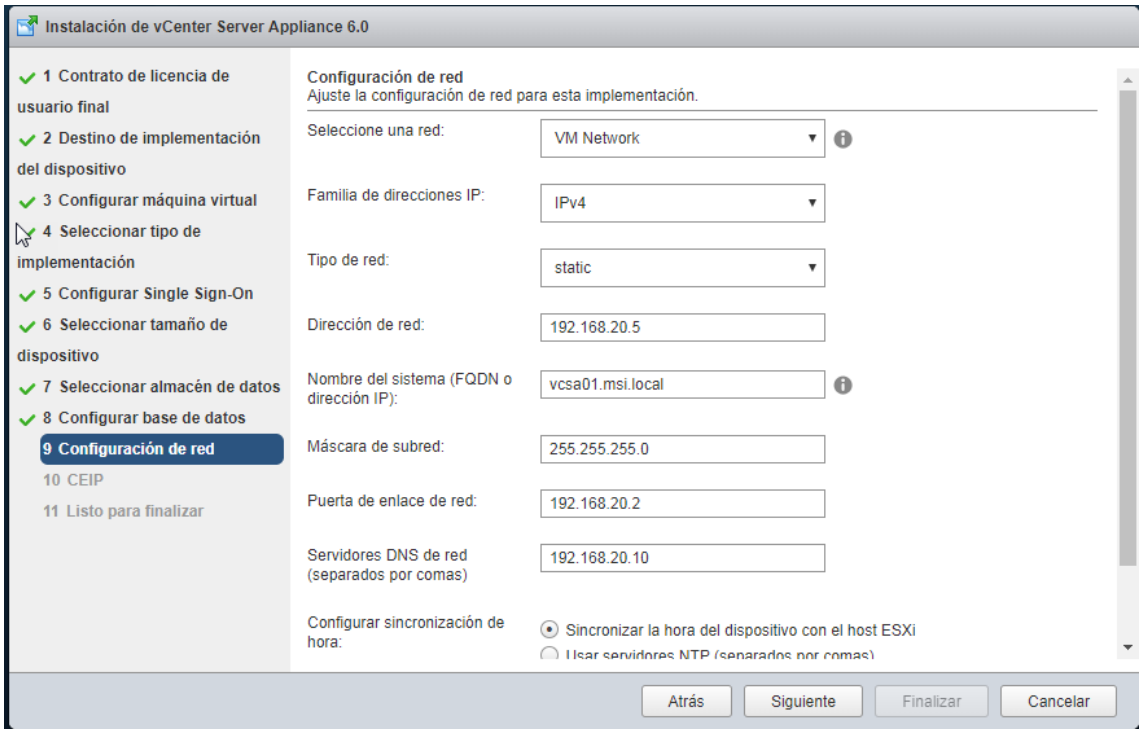


Figura 32. Configuración del direccionamiento de red

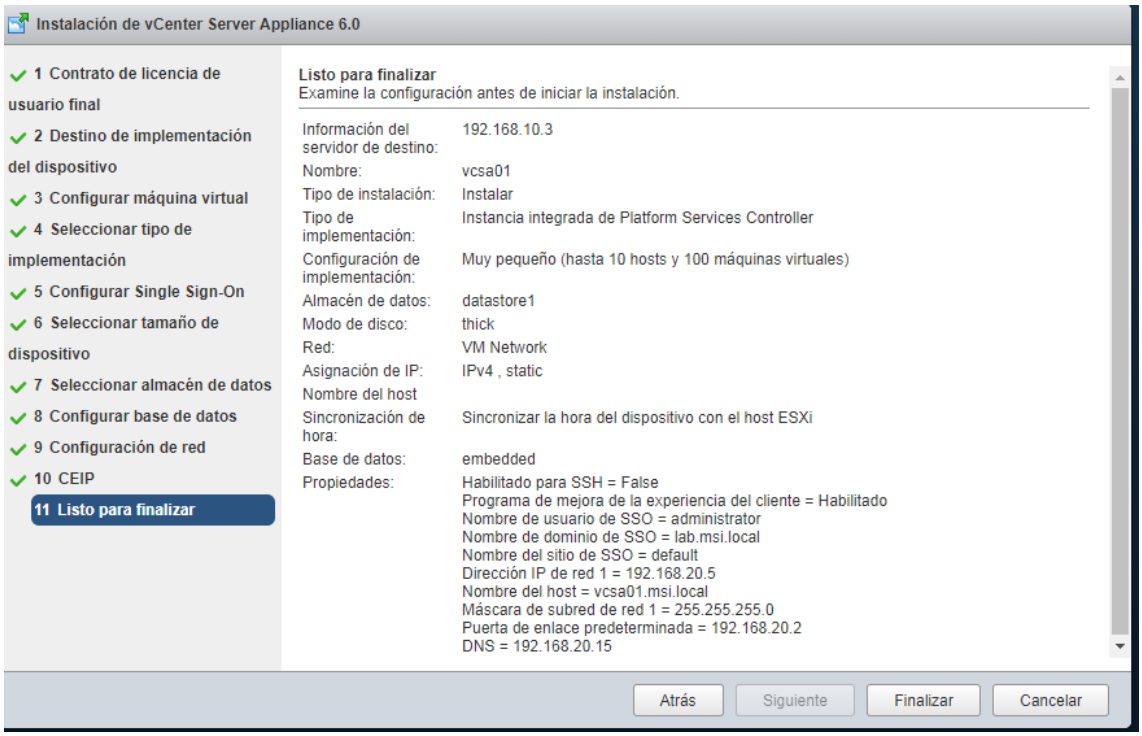


Figura 33. El resumen de las configuraciones antes dadas

Una vez terminado, esperamos que termine de desplegar el vCenter.

6.2.2 MEJORES PRÁCTICAS APLICADAS EN VCENTER

Autenticar vCenter con Single Sing-On Externo

Aunque vCenter te permite la creación y configuración de un Single Sing-On y utilizarlo como proveedor de identidad en otros servicios. En nuestro laboratorio se construyó un Directorio "msi.local" pensando en no concentrar todos los servicios en uno solo, se configurará el Single Sing-ON externo.

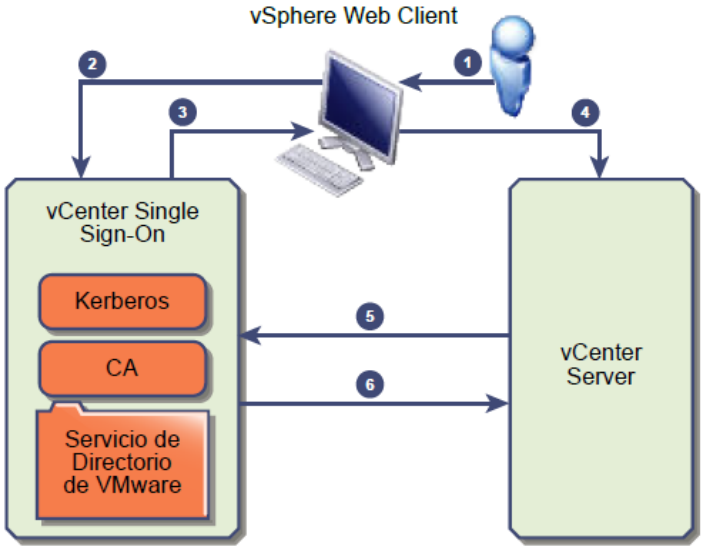


Figura 34. Esquema de funcionalidad del vCenter SSO

Recomendaciones:

- Se recomienda configurar en el vCenter el origen de identidad para realizar la autenticación con Single Sing-On de esta manera podemos gestionar de manera asignar permisos por grupos y/o usuarios de manera granular de manera tenemos más control en nuestra infraestructura Virtual.

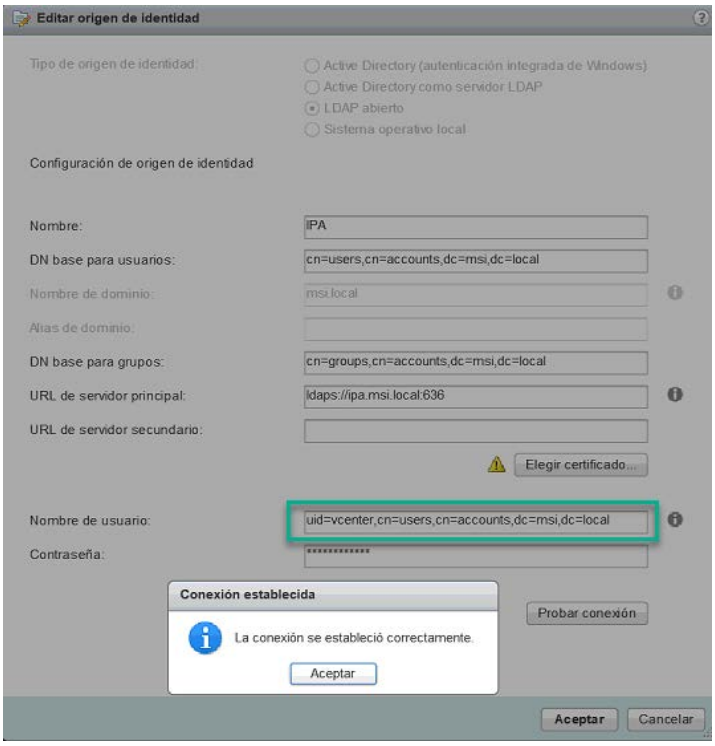


Figura 35. Conexión de Identidad

Accesos y Permisos en el Ambiente Virtual

Desde el vCenter podemos configurar el acceso y permisos en todos los objetos que forman un ambiente virtual como por ejemplo: Hipervisores, Cluster, vSAN, vSwitch, etc.

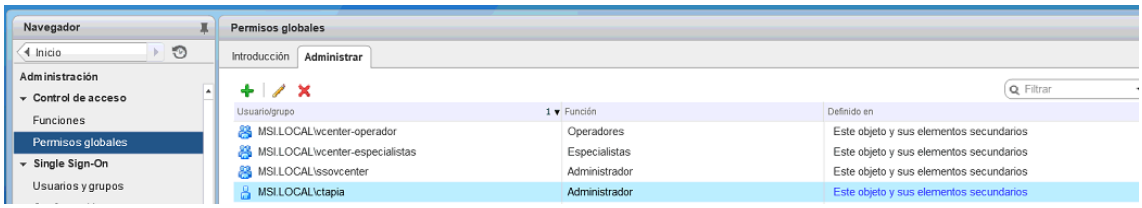


Figura 36. Permisos y creación de grupos en vCenter

- Se recomienda crear usuarios y grupos en el Directorio Activo “msi.local”, además crear perfiles con diferentes permisos, de esta manera no todos los usuarios personales serán administradores. Esta recomendación se la realiza en el vCenter. Ver apartado de vCenter.

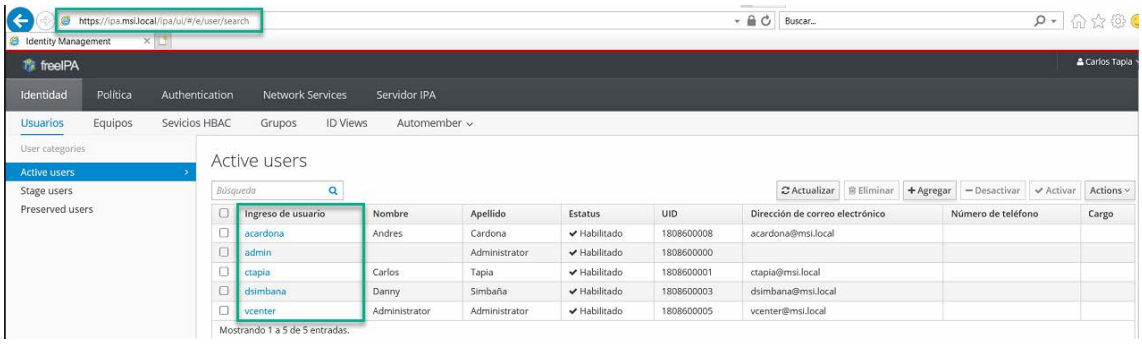


Figura 37. Usuarios creados en la Identidad Activa

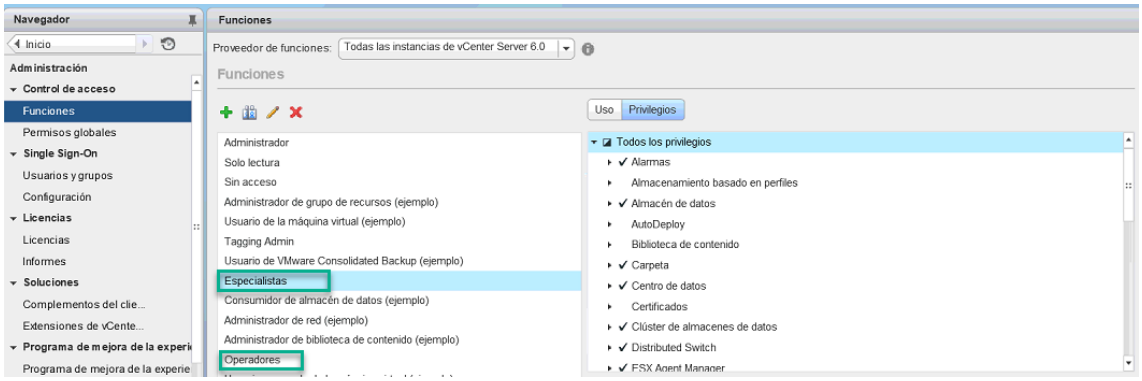


Figura 38. Grupos de Perfiles y permisos creados en el vCenter

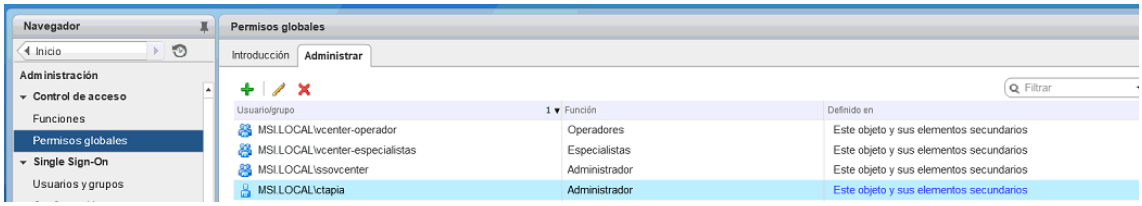


Figura 39. Asignación de perfiles a los usuarios/grupos

Administración Centralizada

vCenter es capaz de administrar, clusters, hosts/hipervisores, `vswitch, etc, todos los objetos que contengan un ambiente virtual, de esta manera optimiza tiempos en configuraciones o despliegues.

Recomendaciones:

- Se recomienda agregar los hipervisores o hosts al vCenter, una vez realizado también se tiene las Máquinas virtuales que contiene cada host. Ver Imagen:

CLUSTER.- Conjunto de dos o más Hosts para aprovisionar de sistemas de Alta Disponibilidad, Tolerancia a Fallos.

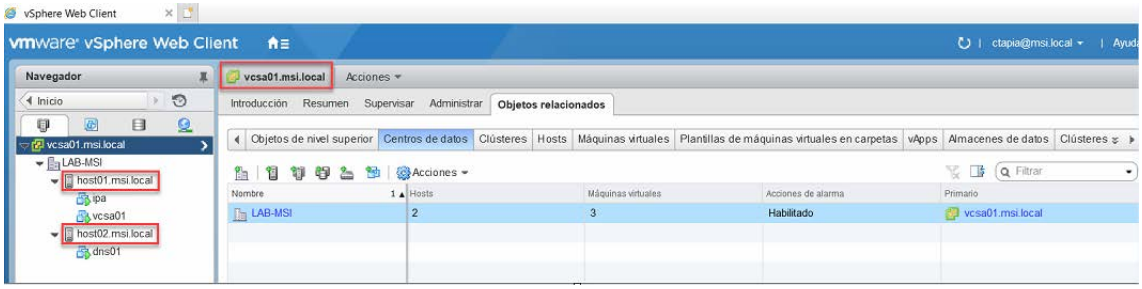


Figura 40. Vista de VMs que se encuentran en cada Hosts

Tipos de Modo Bloqueo de Acceso

Es la limitación de acceso a los hipervisores, existen dos modos, Normal y Estricto. Normal se puede acceder solamente al host por el vCenter y al DCUI y shell siempre y cuando los usuarios se encuentran aplicados las excepciones en sus permisos. El modo Estricto deshabilita el acceso al DCUI, y solamente se accede a través del vCenter y el acceso por ESXI Shell o ssh queda deshabilitado y los usuarios que tienen privilegios de Administrador sólo podrán acceder a los mismos.

Recomendaciones:

- Se recomienda habilitar el modo de bloqueo y setearlo de modo Estricto, desde esta manera elevamos el nivel de seguridad de acceso y control a los hosts.

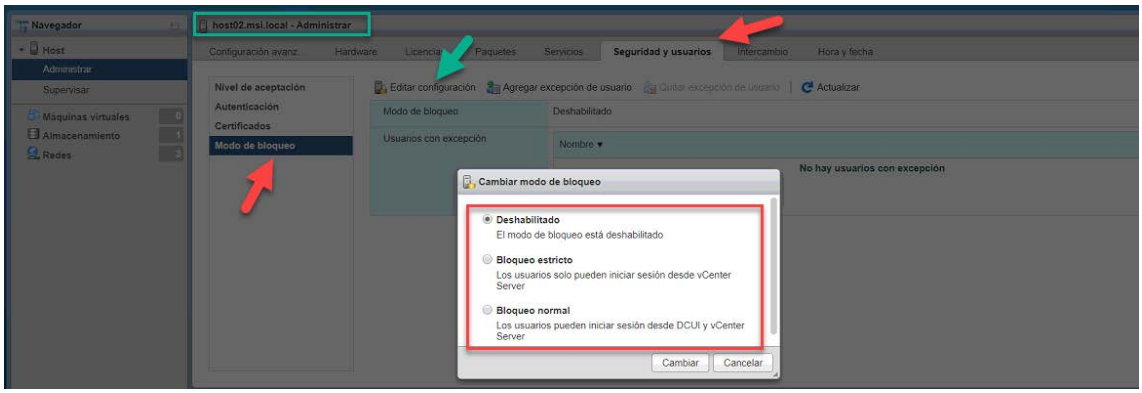


Figura 41. Modo Bloqueo de Acceso

DCUI.- La interfaz de usuario de la consola directa (DCUI) permite interactuar con el host de forma local mediante los menús basados en texto.

SSH.- Es la conexión remota a un servidor de destino de manera cifrada a través del protócolo del mismo nombre

Inicio y Apagado de VMs

Casi siempre se tiene que hacer reinicios de los hipervisores ya sea por la aplicación de parche o apagado de los mismo por alguna ventana de mantenimiento coordina y que sucede con las Máquinas virtuales VMs? Las VMs no inician automáticamente sino se las configura. (Siempre y cuando los hosts no forman parte de de un cluster de vSphere HA).

Recomendación:

- Se recomienda la configuración del inicio y apagado de las máquinas virtuales que poseen cada host. En este caso contiene dos VMs: Es el vCenter y el Directorio Activo. Se puede definir el orden y tiempo de encendido y apagado cuando se reinicia o apaga los hipervisores. Ver Imagen:

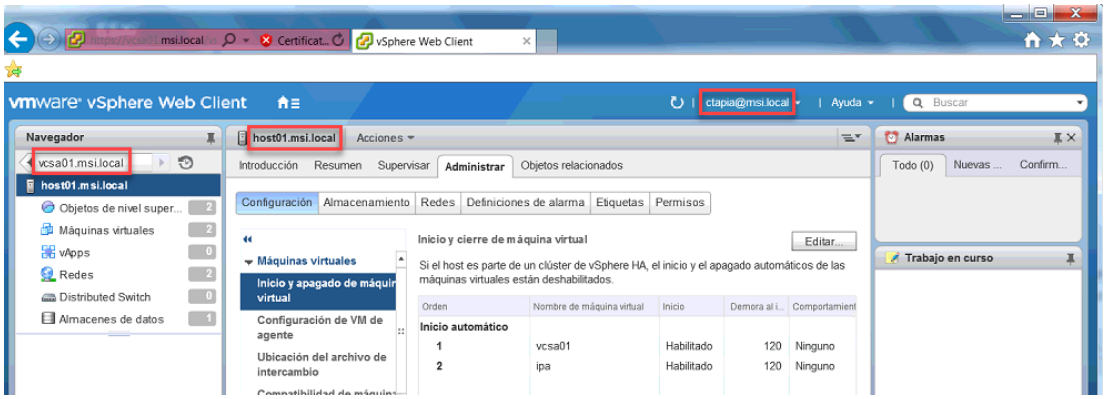


Figura 42. Inicio y Apagado de VMs posterior de reinicio y apagado de VMs

Deploy de Parches y Actualizaciones a vCenter e Hipervisores

Para poder realizar el deploy de actualizaciones o parches desde vCenter se debe tener configurado el “Update Manager”, esto se encuentra en el apartado del vCenter:

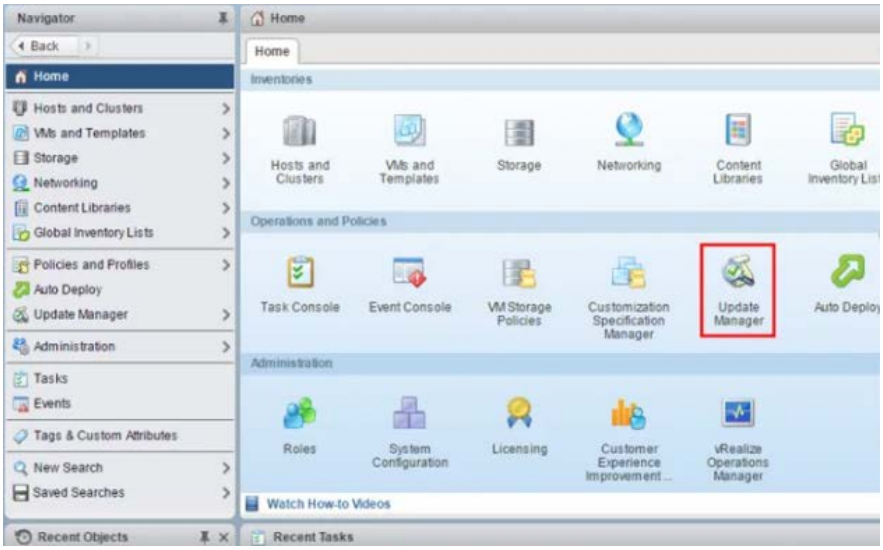


Figura 43. Despliegue de Parches

Después tener descargado el parche o actualización obtenida desde el sitio oficial [14] y subirlo al datastore correspondiente al vCenter.

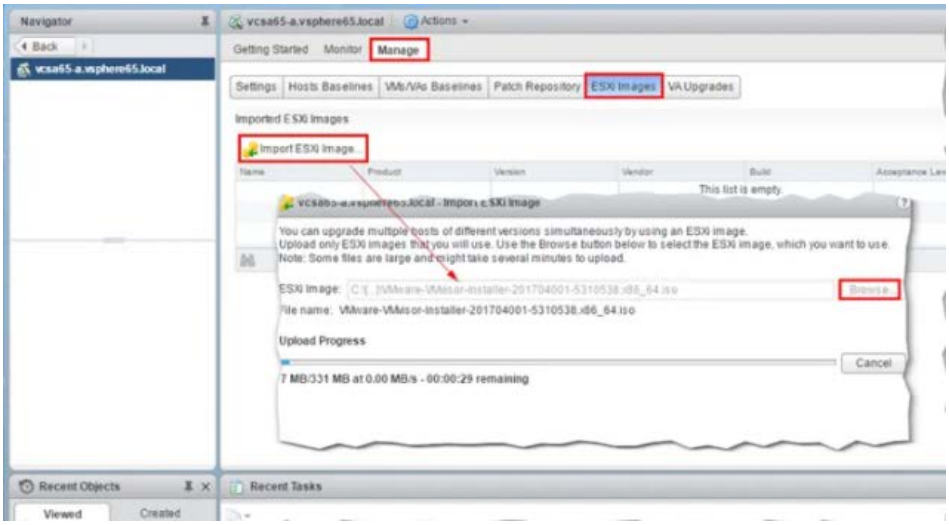


Figura 44. Configuración Despliegue de Parches 1/4

Creamos el BaseLine para poder adjuntar al Hipervisor donde se va a realizar el update.

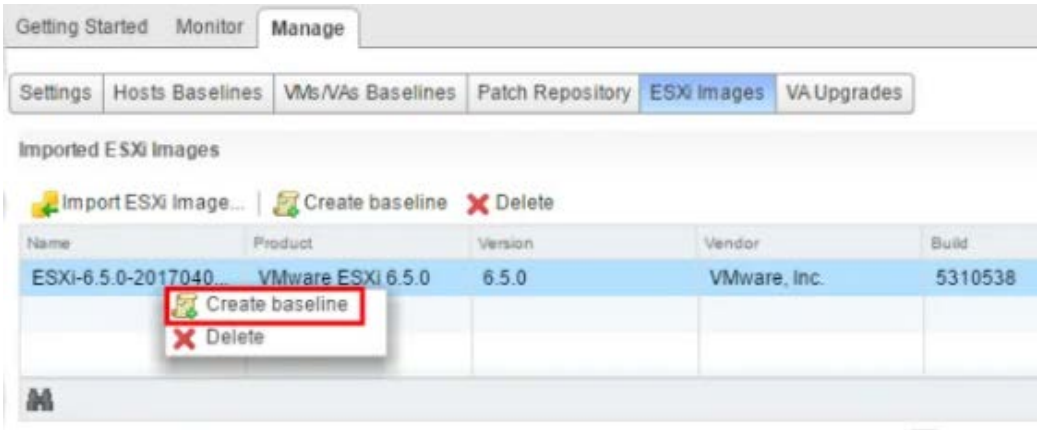


Figura 45. Configuración Despliegue de Parches 2/4

Una vez hecho esto, probamos compatibilidad y aplicamos remediación al hipervisor, de esta manera el host estará indisponible y remediará y aplicará la actualización.

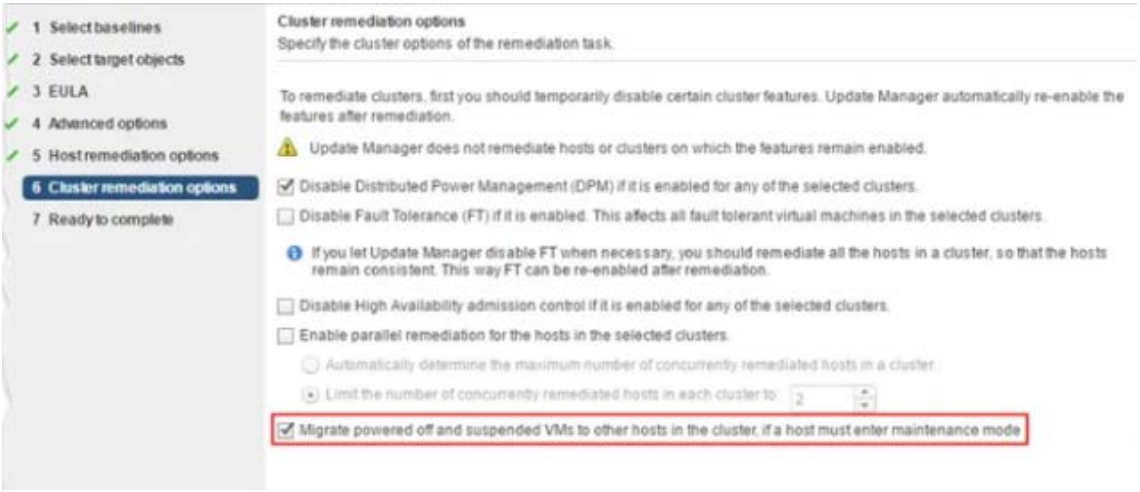


Figura 46. Configuración Despliegue de Parches 3/4

Las tareas de remediación y aplicación de parche se mostrarán de la siguiente forma

Figura 47. Configuración Despliegue de Parches 4/4

[16]

6.3 VSWITCH – LABORATORIO

6.3.1 DESPLIEGUE Y CONFIGURACIONES DEL VSWITCH

Creación de vSwitch por servicios: Management de los Hipervisores, Máquinas Virtuales y vMotion:

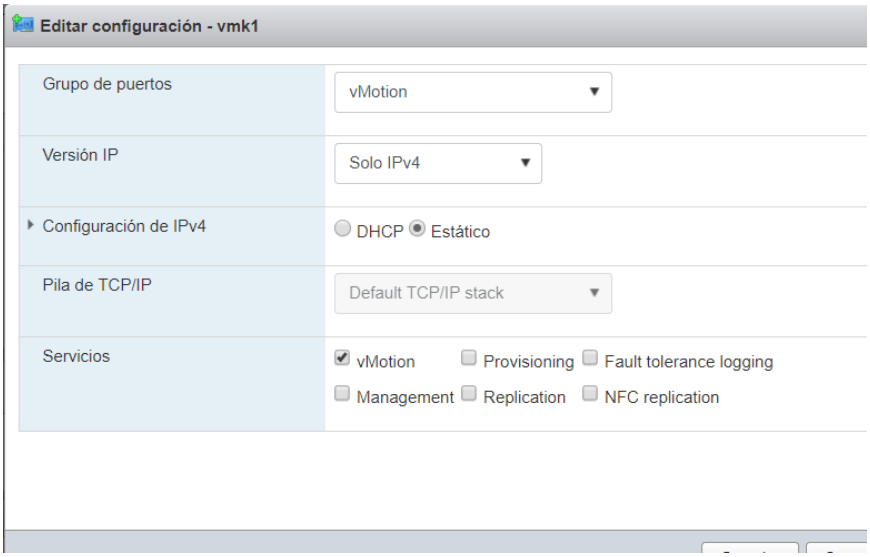


Figura 48. Configuración y Despliegue vSwitch 1/2

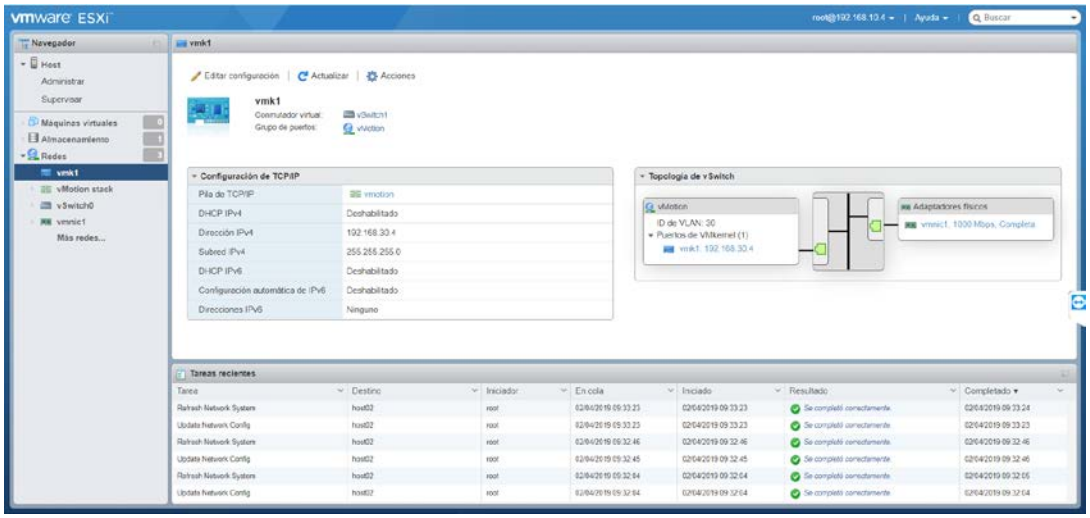


Figura 49. Configuración y Despliegue vSwitch 2/2

6.3.2 MEJORES PRÁCTICAS APLICADAS EN VSWITCH

Recomendaciones:

- Por Servicio: Se recomienda separar el tráfico de los servicios por lo cual, se debe crear VSWITCH por VLAN para el tráfico de Management, Almacenamiento y de las máquinas virtuales. De acuerdo a la cantidad de tráfico por VSWITCH, se debe configurar mínimo dos VNICS así tenemos redundancia, balanceo y evitamos único punto de fallo.
- Modo Promiscuo.- Se configura en las NICs virtual para tomar y analizar los paquetes enviados de otros nodos o hosts. Esta configuración se recomienda sólo habilitar cuando se tiene que hacer un análisis y ayuda en la resolución de problemas, las consecuencias de tener habilitado el modo promiscuo es que la red trabajará de manera lenta y tendrá un bajo performance.

- Cambio de MAC en NICs Virtuales.- Esta configuración permite que los sistemas operativos que contienen las Máquinas virtuales puedan cambiar la MAC en las NICs virtuales que se encuentran en los hipervisores, y evita que hacker no puedan cambiar la MAC y falsificar direcciones IP desde las máquinas virtuales.
- Transmisiones de Paquetes.- Esta configuración permite rechazar la transmisión forjada o falsificada de paquetes que vienen desde las máquinas virtuales, y este bloqueo lo hace ya que compara la MAC del origen de los paquetes con la MAC física, si no coincide el hipervisor rechaza dichos paquetes y así evita que una VM envíe tráfico hacia la red.

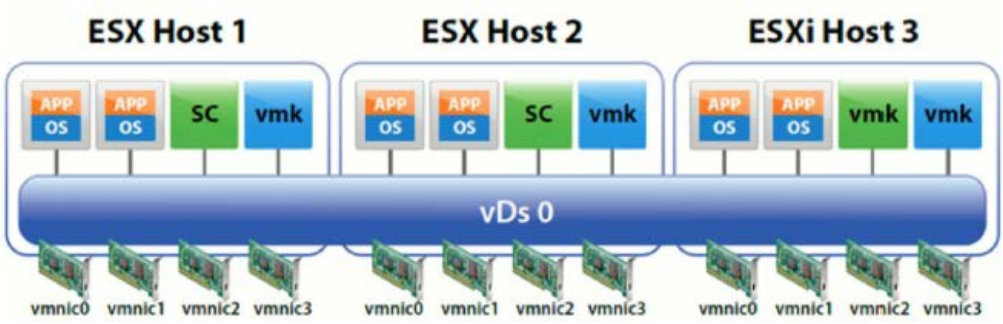


Figura 50. Vista del Esquema vSwitch

[16] [17]

6.4 VSAN – LABORATORIO

6.4.1 DESPLIEGUE Y CONFIGURACIONES DEL VSAN

Antes de realizar la configuración de una vSAN se tiene que crear un CLUSTER formado mínimo por dos host Hipervisores

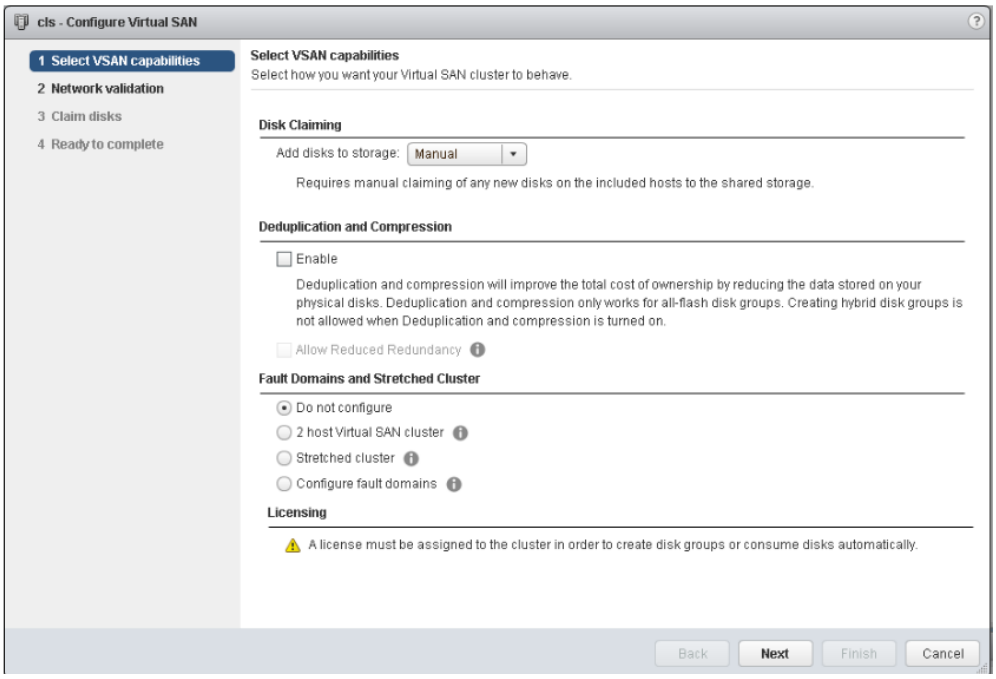


Figura 51. Configuración vSAN

6.4.2 MEJORES PRÁCTICAS APLICADAS EN VSAN

Gracias a los vSwitch, se puede aplicar las siguientes recomendaciones en la vSAN y crear HA Alta Disponibilidad en nuestros servicios más críticos:

Recomendaciones:

- Se debe crear un vswitch de tipo VMKernel de vSAN aprovisionando mínimo dos interfaces y así evitamos un único punto de fallo.
- Network IO Control.- Se recomienda configurarlo y habilitarlo de esta manera se da prioridad al tráfico de la vSAN, esto se aplica y se lo debe de hacer de manera obligatoria cuando se está compartiendo interfaces iguales o superiores de 10GbsE para múltiples tipos de tráfico.
- Calidad de Servicio QoS.- Se recomienda configurar la calidad de servicio siempre y cuando se utilice switchs físicos destinados exclusivamente para el tráfico de vSAN.
- Grupos de Discos.- Se recomienda aprovisionar por cada host del cluster vSAN con dos grupos de disco. (Datastore está compuesto por grupos de discos) así se obtendrá un mejor performance tenendo disponibilidad en los servicios.

6.5 VMOTION – LABORATORIO

6.5.1 DESPLIEGUE Y CONFIGURACIONES DEL VMOTION

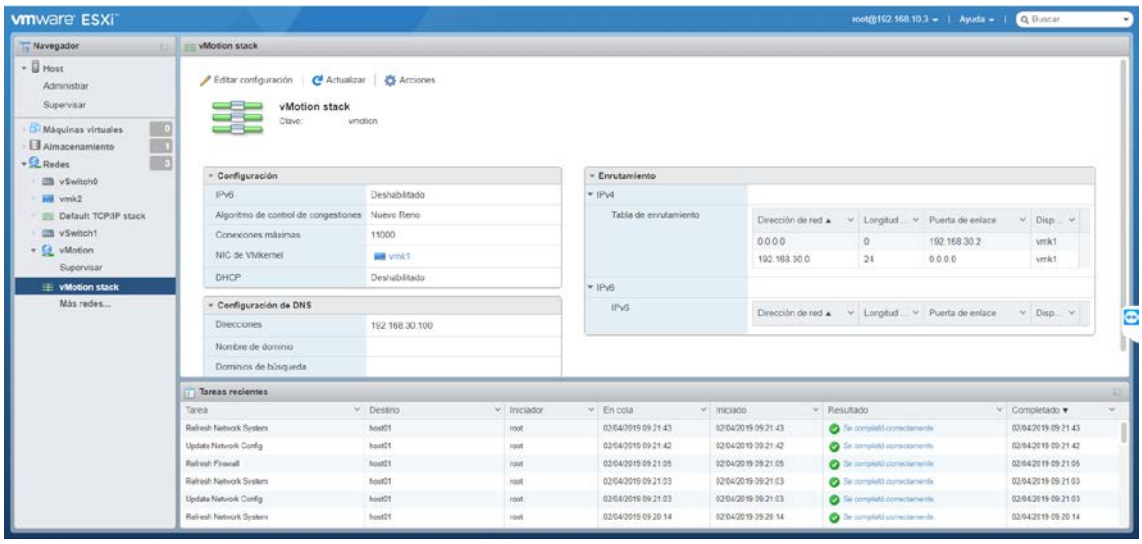


Figura 52. Vista del Esquema vMotion

6.5.2 MEJORES PRÁCTICAS APLICADAS EN VMOTION

Recomendaciones:

- Se recomienda asignar al menos una NIC de 1GbE o 10GbE para segmentar el tráfico y que no exista cuello de botella con otras de carga de trabajo provenientes del Management y de las Máquinas Virtuales.
- Se recomienda a nivel de networking crear vLAN para separar el tráfico tanto de vMOTION, Management y de las Máquinas Virtuales para una mejor seguridad y performance.

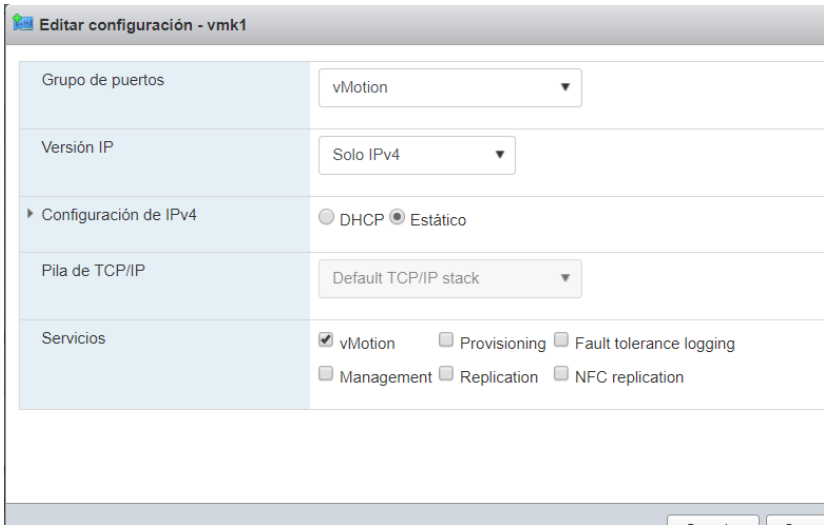


Figura 53. Configuración vmk1 vMotion

- Se recomienda agregar un firewall entre las interfaces asignadas para vMotion, de esta manera aseguramos que el tráfico no sea intersectado por terceros.

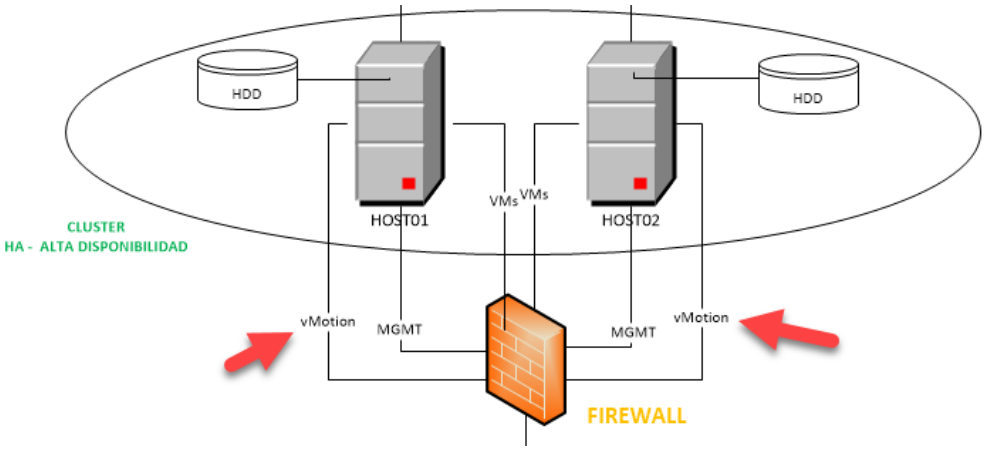


Figura 54. Firewall entre interfaces vMotion

Y no sufrir ataques de Man in the Middle utilizando teçnicas de **ARPspoof**, de esta manera el atacante no podrá intersectar el vmdx archivo de configuración de la Máquina Virtual.

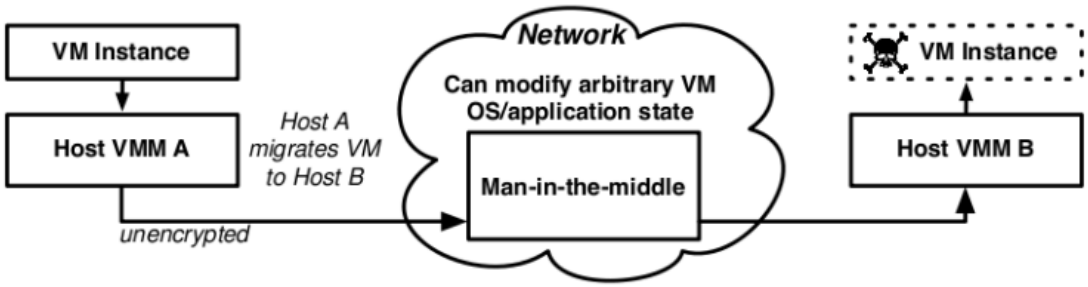


Figura 55. Vista del ataque durante el vMotion 1/3

Además evitemos que se cree **Bypass en la Autenticación con el servicio sshd** que incluye:

- Identificar rutinas de autenticación de las pubkey
- Manipular y permitir acceso como root sin restricciones (Utilizando Xensploit se puede manipular el código objeto en-memoria)

ARPspoof.- Es una técnica usada comúnmente por atacantes en redes internas para ataques MITM, DOS o para explotar algún fallo en la victima para obtener acceso al equipo en combinación con técnicas como DNSspoof y sniffing, entre otras

```
        if (key != NULL)
                key_free(key);
        xfree(pkalg);
        xfree(pkblob);
#ifdef HAVE_CYGWIN
        if (check_nt_auth(0, authctxt->pw) == 0)
                authenticated = 0;
#endif
        return authenticated;
}

/* return 1 if user allows given key */
static int
user_key_allowed2(struct passwd *pw, Key *key, char *file)
{
        char line[SSH_MAX_PUBKEY_BYTES];
        int found_key = 0;
        FILE *f;
        u_long linenum = 0;
        struct stat st;
        Key *found;
        char *fp;

        /* Temporarily use the user's uid. */
        temporarily_use_uid(pw);

        debug("trying public key file %s", file);

        /* Fail quietly if file does not exist */
        if (stat(file, &st) < 0) {
1111                                                    196,2-9       63%
```

Figura 56. Utilizando Xensploit se puede manipular el código objeto en-memoria 1/2

```
 805da77:       0f 84 23 fd ff ff       je     805d7a0 <user_key_allowed2+0x80>
 805da7d:       89 3c 24                mov    %edi,(%esp)
 805da80:       e8 37 e5 fe ff          call   804bfbc <fclose@plt>
 805da85:       8d 85 8c df ff ff       lea    0xffffdf8c(%ebp),%eax
 805da8b:       89 44 24 04             mov    %eax,0x4(%esp)
 805da8f:       c7 04 24 15 0e 08 08    movl   $0x8080e15,(%esp)
 805da96:       e8 d5 28 01 00          call   8070370 <logit>
 805da9b:       e8 20 bd 01 00          call   80797c0 <restore_uid>
 805daa0:       81 c4 9c 20 00 00       add    $0x209c,%esp
 805daa6:       31 c0                   xor    %eax,%eax
 805daa8:       5b                      pop    %ebx
 805daa9:       5e                      pop    %esi
 805daaa:       5f                      pop    %edi
 805daab:       5d                      pop    %ebp
 805daac:       c3                      ret
 805daad:       8d 76 00                lea    0x0(%esi),%esi

0805dab0 <user_key_allowed>:
 805dab0:       55                      push   %ebp
 805dab1:       89 e5                   mov    %esp,%ebp
```

Figura 57. Utilizando Xensploit se puede manipular el código objeto en-memoria 2/2

- Una vez hecho esto, se obtendrá el acceso a la VM que contenga OS Linux una vez finalizado el vMotion.

[18]

6.6 DRS – LABORATORIO

6.6.1 DESPLIEGUE Y CONFIGURACIONES DEL DRS

Una vez creado el HA en vMware, ir al objeto CLUSTER creado, y editar las configuraciones

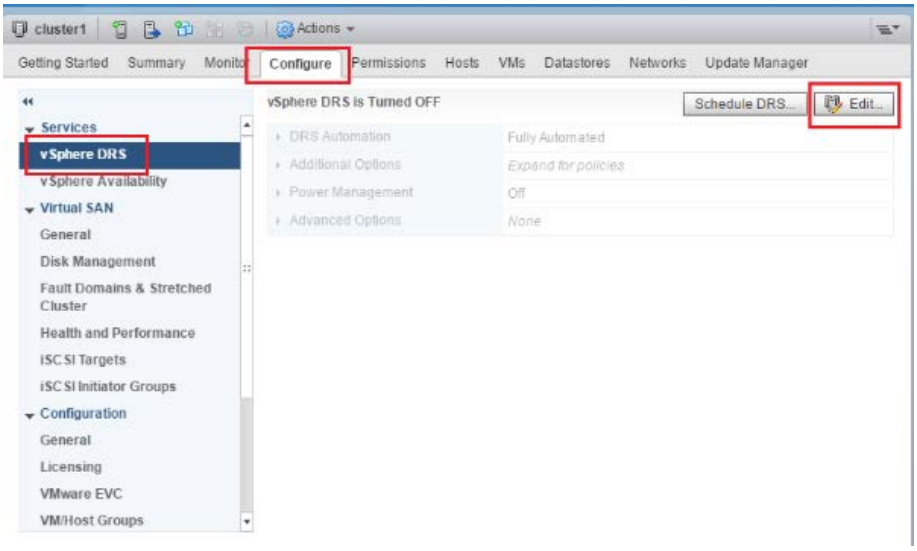


Figura 58. Configuración DRS 1/3

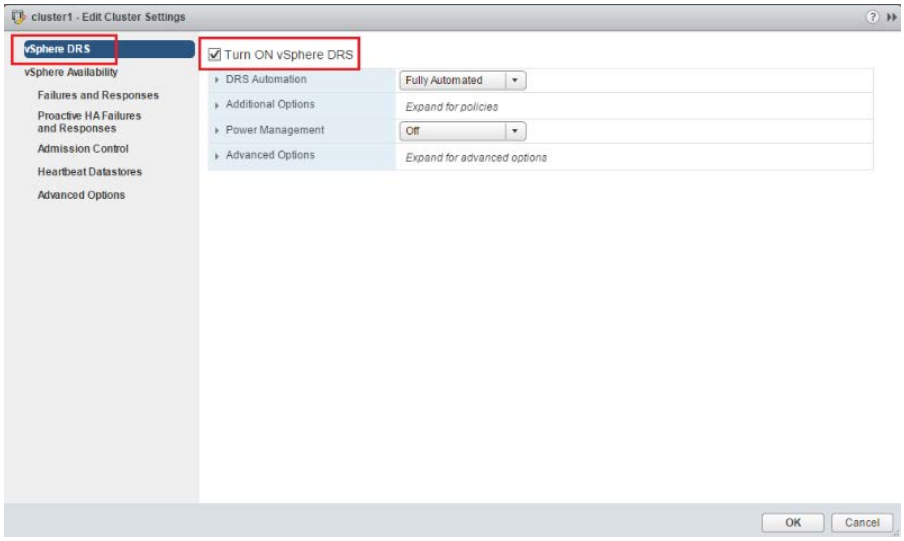


Figura 59. Configuración DRS 2/3

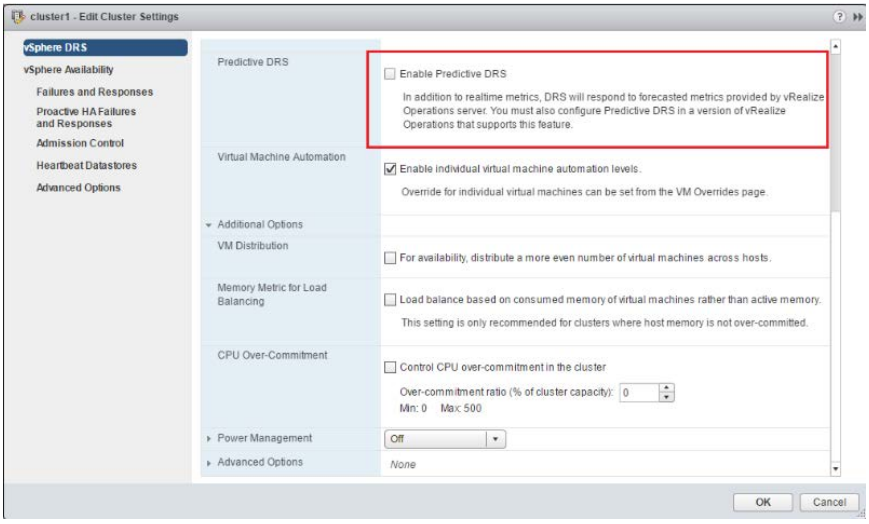


Figura 60. Configuración DRS 3/3

6.6.2 MEJORES PRÁCTICAS APLICADAS EN DRS

La aplicación de DRS va de la mano con VMOTION, por lo tanto, se debe tomar en cuenta que el hardware adquirido en la implementación de la infraestructura virtual debe ser de la misma arquitectura para no sufrir incompatibilidad en VMOTION, de esta manera se ganaría un alto performance. La funcionalidad DRS está disponible y es aplicable cuando se cuenta con uno o más cluster que contenga más de un hipervisor.

Recomendaciones:

- Se recomienda la aplicación de DRS para la distribución de recursos en CPU y RAM para las máquinas virtuales situadas en el cluster. Al aplicarlo, esto asegura una mayor previsibilidad y estabilidad del rendimiento y aseguramos disponibilidad en los servicios/apps que estén corriendo en las máquinas virtuales.
- Se recomienda la aplicación de DRS para la distribución de recursos a nivel storage para las máquinas virtuales almacenadas en los datastores del cluster. Al aplicarlo, esto asegura una mayor previsibilidad y estabilidad del rendimiento y aseguramos disponibilidad en los servicios/apps que estén corriendo en las máquinas virtuales.

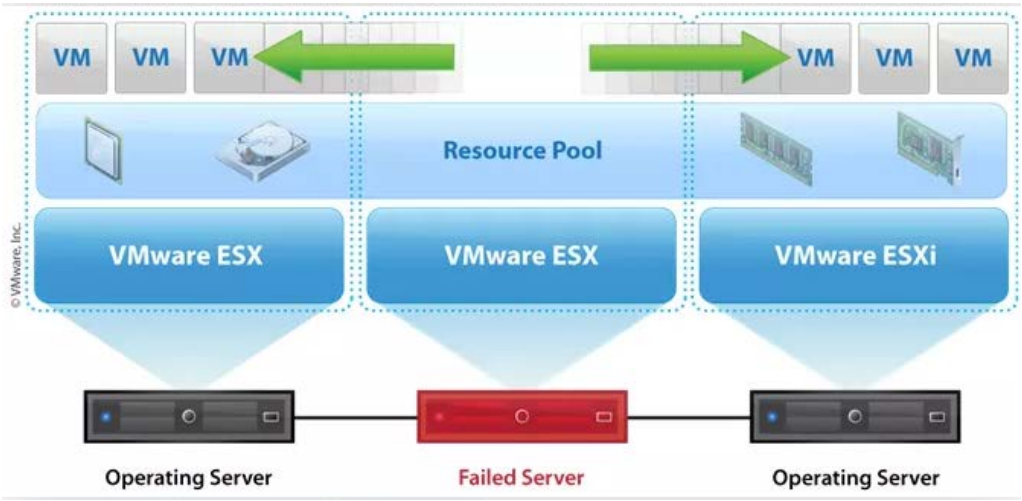


Figura 61. Esquema de funcionamiento DRS

- Se recomienda la configuración de la Alta Disponibilidad en el mismo cluster, de esta manera configurada el DRS y el HA nuestro entorno tendrá alta disponibilidad y balanceo de carga tanto en recurso (CPU, RAM) y storage.

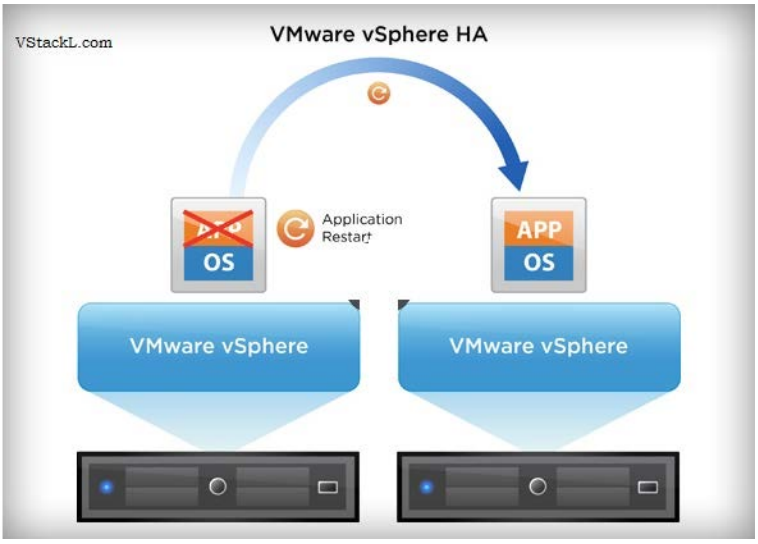


Figura 62. Funcionamiento HA

[19]

CAPÍTULO 7: MONITOREO DE LOGS

La consolidación y monitoreo de logs es un importante en cualquier infraestructura ya sea física o virtual, por lo cual se abarcará este tema.

La recopilación de logs sirve para el área de Seguridad Informática ya que realiza análisis de logs y de esta forma tener la opción de poder ejecutar Auditorías, cumpliendo en cierta forma la Norma ISO 27001 y de esta manera

aplicar mejoras en los procesos de seguridad de la información en la Organización.

Las herramientas de Monitoreo de Logs nos permiten generación de Reportes para un mejor análisis y comprensión. [20]

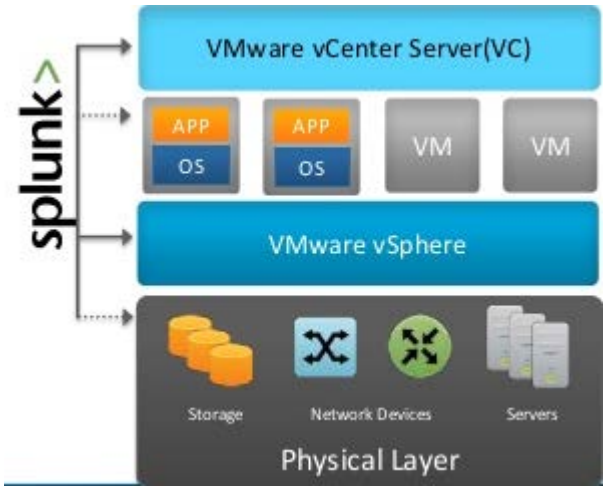


Figura 63. Esquema de Recopilación de logs desde Spunk

En la siguiente imagen, se muestra un dashboard desde la herramienta de SPLUNK que contiene eventos recibidos, atacantes y los mercados en el cual se recopila logs.

Figura 64. DashBoard de recopilación de alertas y eventos en un ambiente PROD.

CONCLUSIONES

En las organizaciones, la implementación de Arquitecturas e Infraestructuras casi nuevas o nuevas son un verdadero desafío tanto para TI y SI, ya que son las áreas encargadas de Diseñar construir, configurar, monitorear y tratar de garantizar la disponibilidad, integridad y confidencialidad de los servicios o información de la organización, todo ello con base a las mejores prácticas y estándares especificados en los diferentes marcos referenciales tanto como ITIL, COBIT, etc. Dicho desafío se debe al crecimiento exponencial que ha tenido este tipo de infraestructura en los últimos años, y entre sus principales beneficios son: nivel de administración centralizada, escalabilidad y crecimiento tanto horizontal y vertical de los recursos, reducción de costos en mantenimientos ya que se tendrá menos equipos físicos en los DataCenter, lo cual implica una reducción física de infraestructura de TI en los DC, así como también la reducción importante en costos en variados aspectos tales como: licenciamientos a nivel de Software y Hardware, consumos de energía, entre otros muchos beneficios.

Se establece así que la elección de estas nuevas infraestructuras debe ser con base en los casos de éxito ya conocidos por parte de otras organizaciones y que el contrato contenga soporte 24/7 y estableciendo SLO´s y SLA´s, ventanas de mantenimiento, matrices de escalamientos, administración de incidentes y problemas, controles de cambios etc., como lo indica ITIL en sus mejores prácticas junto al proveedor, de esta manera nos aseguramos que se tendrá un soporte a otro nivel cuando se produzca algún incidente o levantar alguna consulta por una determinada situación.

Es necesario e importante que las áreas responsables como TI y SI tengan el mismo know how sobre la nueva infraestructura disponibilizada y, que a su vez, se implementen herramientas de bases de conocimiento que impulsen e incentive la colaboración y difusión del conocimiento técnico, así como también facilite la certificación o especialización en estas nuevas infraestructuras para que puedan atender cualquier tipo de requerimientos como los antes mencionados relacionados con las best practices de ITIL en la gestión del servicio.

Por lo antes expuesto, nace el desarrollo de este documento acompañado de la construcción de un Laboratorio que simula los ambientes

Productivos, basado tanto en mi experiencia como en la documentación propia del fabricante y diferentes tipos de diseños de arquitectura de ambientes virtualizados, de esta manera se pudo plasmar las mejores prácticas en seguridad para Ambientes Virtuales, además de las consideraciones que se deben de tomar al momento de la elección del hardware de esta manera garantizamos un alto performance y disponibilidad en los servicios.

Este documento no sólo se basa específicamente en aplicar “Firewall de capa 3 o Capa 7 o en la creación de vLAN para segmentar y separar tráfico de red”, este documento considera los diferentes aspectos de una solución de infraestructura virtualizada desde el análisis de la arquitectura y compatibilidad de Hardware para tener un mejor performance, hasta inclusive aplicar mejores prácticas de seguridad en la implementación de un ambiente virtual. De esta manera, se busca garantizar la integridad, disponibilidad y redundancia de los servicios y, por último, la implementación de herramientas de recopilación de logs y supervisión de la infraestructura a fin de cumplir con los procesos de auditoría como parte de los elementos de seguridad requeridos en un entorno de TI.

Otro aspecto fundamental tomar en cuenta es que a sobre este tipo de infraestructuras a nivel de seguridad, se establece que los Ambientes Virtuales como IaaS (Infraestructure as a Services), se debe de tomar como ambientes físicos, focalizando y aplicando controles de acceso a todos los componentes que forman parte del ambiente. De igual manera, es muy importante implementar una seguridad perimetral para crear y separar los ambientes productivos y de desarrollo y los que están expuestos al internet, gracias a los vSwitchs distribuidos, con los que se pueden segmentar y habilitar redes de tipo DMZ, así como también implementar balanceadores de aplicaciones como los F5; todo ello asegurará que los servicios backend estén disponibles en producción.

Por otro lado, es bien sabido que los Ambientes virtuales no están exentos de ataques informáticos y/o vulnerabilidades, para lo cual les indispensable implementar como parte fundamental de las mejores prácticas, la segmentación del tráfico de los servicios, definir controles de acceso

mediante Firewall de capa 3 y 7, lo cual permitirá analizar el tráfico de capa 3 y en la capa 7, minimizando el riesgo de ataques por http/https/inyection SQL a la capa de aplicación que corren en las máquinas virtuales entre otros. De igual forma, en referencia a las vulnerabilidades es muy importante tener planes de mantenimiento para update/parcheo de los componentes que forman un ambiente virtual, los cuales deben contar con un repositorio local para mantener las diferentes versiones de cada paquete, el cual permita disponibilizar, distribuir y administrar las diferentes actualizaciones de productos.

Como toda nueva implementación se estima tiempos de entrega y evalúan de posibles riesgos entre ellos es el conocimiento de los Especialistas y Operadores de la nueva infraestructura ya que son los encargados de administrar, controlar y monitorear.

Aunque suene una frase trillada, ninguna infraestructura es segura y está exenta de ataques o vulnerabilidades, pero estas mejores prácticas y definición de procesos de seguridad, previamente divulgados y concientizados hacen que nuestros sistemas estén de algunos protegidos. Lo importante es saber y conocer la infraestructura que se empieza construir y el riesgo que representaría la NO Disponibilidad, o el hurto de información, para eso es importante ser especialista y tener experiencia en lo que se piensa desarrollar.

El desarrollo de este documento y la construcción del laboratorio se basan en gran medida a los ambientes productivos de organizaciones medianas y grandes que cuentan con infraestructura virtual muy similar a la detallada en el presente documento en cuanto a los diferentes aspectos fundamentales descriptos, claro está, con elementos redundantes y de mayor capacidad que les permiten implementar alta disponibilidad de mucho mayor alcance y otras consideraciones muchísimos más robustas ajustadas a las necesidades de estas, en las que he tenido la oportunidad de participar desde el proceso de análisis y diseño hasta su creación, implementación, puesta en producción y administración, por lo cual considero que ha sido de gran contribución sobre una mayor comprensión y aprendizaje los cuales son aplicables tanto en los estudios como en el ámbito corporativo donde actualmente colaboro.

BIBLIOGRAFÍA

[1] Historia de la Virtualización, https://www.ibm.com/developerworks/ssa/linux/library/l-virtual-machine-architectures/index.html (consultada el 10/10/2018)

[2] Definición de Virtualización, https://www.redhat.com/es/topics/virtualization/what-is-virtualization https://www.vmware.com/latam/solutions/virtualization.html (consultada el 12/10/2018)

[3] Ventajas y Desventajas de la Virtualización, https://www.vmware.com/latam/solutions/virtualization.html https://www.redhat.com/es/topics/virtualization https://azure.microsoft.com/es-es/overview/what-is-virtualization/ (consultada el 15/10/2018)

[4] Cuadrante Mágico de Garnet con referencia a los servidores virtuales y con el producto VMWARE – VPSHERE con referencia a su competencia, https://www.gartner.com/reviews/market/x86-server-virtualization-infrastructure (consultada el 20/10/2018)

[5] Productos de VMware, https://www.vmware.com/products.html (consultada el 25/10/2018)

[6] Hypervisor de VMware, https://www.vmware.com/files/es/pdf/VMware-vSphere-Entreprise-Edition-Datasheet.pdf (consultada el 30/10/2018)

[7] vCenter, https://www.vmware.com//products/vcenter-server.html (consultada el 02/11/2018)

[8] vSwitch, https://www.vmware.com/products/vsphere/distributed-switch.html (consultada el 04/11/2018) https://www.nakivo.com/blog/what-is-vmware-vswitch/ (consultada el 07/11/2018)

[9] vSAN, https://www.vmware.com/products/vsan.html (consultada el 09/11/2018)

[10] vMotion, https://www.vmware.com/products/vsphere/vmotion.html (consultada el 12/11/2018)

[11] DRS, https://www.vmware.com/products/vsphere/drs-dpm.html (consultada el 15/11/2018)

[12] Previa Instalación, https://docs.vmware.com/es/VMware-vSphere/6.0/rn/vsphere-esxi-vcenter-server-60-release-notes.html (consultada el 18/01/2019)

[14] Fabricante, https://my.vmware.com/ (consultada el 30/01/2019)

[15] Compatibilidad, https://www.vmware.com/resources/compatibility/search.php (consultada el 05/02/2019)

[16] Mejores Prácticas en Hipervisores, vCenter, vSwitch https://docs.vmware.com/en/VMware-vSphere/6.0/vsphere-esxi-vcenter-server-602-security-guide.pdf https://www.altaro.com/vmware/how-to-patch-esxi-with-update-manager/ (consultada el 10/02/2019)

[17] Mejores Prácticas en vSwitch, https://searchvmware.techtarget.com/tip/Configuring-VMware-vSwitch-security-settings-Dont-trust-defaults (consultada el 05/04/2019)

[18] Mejores Prácticas en vMotion, https://www.vmware.com/pdf/vmotion_datasheet.pdf https://www.vladan.fr/what-is-vmware-vmotion/ https://docs.vmware.com/es/VMware-vSphere/6.0/com.vmware.vsphere.vcenterhost.doc/GUID-7DAD15D4-7F41-4913-9F16-567289E22977.html https://www.blackhat.com/presentations/bh-dc-08/Oberheide/Presentation/bh-dc-08-oberheide.pdf (consultada el 15/05/2019)

[19] Mejores Prácticas en DRS y Cluster, http://www.vstackl.com/2016/05/configuring-ha-cluster-on-vmware-vsphere-6-0/ https://patriciocerda.com/vsphere-5-como-funciona-ha-y/ consultada el 25/06/2019)

[20] Recopilación de Logs, https://www.splunk.com/es_es consultada el 01/07/2019)