



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES
“ARAGÓN”

“IMPLEMENTACIÓN DE ESCRITORIOS VIRTUALES EN EL CENTRO DE MONITOREO DE DICOFRA SECURITY CONSULTING MEDIANTE VMWARE”

I N F O R M E
POR LA MODALIDAD DE
DESARROLLO DE UN CASO PRÁCTICO
QUE PARA OBTENER EL TÍTULO DE
INGENIERO EN COMPUTACIÓN
P R E S E N T A
JOSÉ LUIS CRUZ BRINGAS



ASESOR: SERGIO HERNÁNDEZ LÓPEZ

MÉXICO

2015



Universidad Nacional
Autónoma de México

Dirección General de Bibliotecas de la UNAM

Biblioteca Central



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

Índice

Introducción	4
Capítulo I. Marco teórico.....	6
1.1 Virtualización.....	6
1.1.1 Formas de virtualización	7
1.1.2 Ventajas de la virtualización	7
1.1.3 Desventajas de la virtualización	8
1.2 Origen y fundamentos de los escritorios virtuales	9
1.3 Beneficios y Ventajas de los escritorios virtuales	9
1.4 Escritorios virtuales como un servicio.....	11
1.5 Microsoft Windows Server 2008.....	11
1.5.1 Características de Windows Server 2008.....	11
1.5.2 Windows Server 2008 R2	12
1.6 Vmware	14
1.6.1 Vmware ESXi.....	14
1.6.2 Vmware Vcenter.....	15
1.6.3 Pre requisitos de hardware y software para Vcenter Server.....	17
1.7 Vmware View (Vmware Horizon).....	18
1.8 Vmware View Composer	19
Capítulo II. Marco conceptual	21
2.1 La empresa	21
2.1.2 Productos y servicios que ofrece	22
2.1.2.1 Servicios de consultoría en seguridad de la información	22
2.2 Centro de Monitoreo	23
2.3 Organigrama del área de Operaciones	27
2.3.1 Área de Servicios internos.....	27
2.4 Análisis de la problemática	28
2.4.1 Áreas de Oportunidad detectadas	29
2.4.1.1 Descentralización de la información.....	29

2.4.1.2 Necesidad de conexiones seguras entre las máquinas de los ingenieros y los clientes	30
2.4.1.3 Falta de control sobre la información, documentación de los clientes y desorden en la organización de la información	30
2.4.1.4 Instalación de software no permitido y equipo dañado.....	31
2.4.2 Solución propuesta.....	32
Capítulo III. Desarrollo	33
3.1 Hardware y Software necesario	33
3.2 Conexión de servidores	34
3.3 Diseño de la red virtual	35
3.4 Diseño de conexión de Storage.....	35
3.5 Configuraciones de Imagen maestra	36
Capítulo IV. Implementación	38
4.1 Instalación de ESXi 5.1.....	38
4.2 Configuración de NAS y conexión a ESXi.....	39
4.3 Instalación de Máquina Virtual para Active Directory	41
4.4 Instalación de Máquina Virtual para Vcenter	42
4.5 Instalación de Vmware View.....	44
4.6 Creación de máquina maestra o Golden Image.....	46
4.7 Creación de Máquinas para los usuarios	47
Conclusiones.....	50
Actualización de Hardware	50
Centralización y administración de la información.....	51
Control de los cambios en la información.....	51
Soporte Técnico.....	51
Anexos	53
Glosario.	53
Referencias	55

Introducción

El presente trabajo tiene como objeto mostrar los pasos realizados para la configuración de grupos de máquinas que sirven como escritorios virtuales o VDI ¹ (Virtual Desktop Infrastructure) para el personal en una empresa, específicamente es utilizado en un centro de monitoreo que funciona las 24 horas del día, los 365 días del año y el cual se encuentra sujeto a proporcionar niveles de servicio (Service Level Agreement o SLA²) a los clientes, por tal motivo no puede tener pérdida de funcionamiento en ningún momento, ya que mantiene servicios administrados de productos específicos.

La característica principal del proyecto es centralizar la información y la operación de los “*Ingenieros de operaciones*” con los que cuenta la empresa, mejorando el servicio y gestión de las herramientas con las que cuenta cada cliente, ya que vende “*Servicios administrados*”.

Estos servicios ayudan a las organizaciones a maximizar su operación y disminuir su costo de gestión, mantenimiento y monitoreo de la infraestructura tecnológica, reducen los riesgos operativos y liberan capital humano clave para atender los procesos críticos de su negocio. La estrategia de los Servicios Administrados va de la mano con las mejores prácticas que permiten incrementar la rentabilidad en las organizaciones.

Para este proyecto se utilizó el sistema operativo de Microsoft Windows 7 y server 2008 R2 así como la suite de VMware Horizon³ donde cada uno de ellos juega un papel importante pero, quien realmente realizará la mayor carga de trabajo es la suite VMware que gestiona las conexiones y servicios proporcionados a los trabajadores que se encuentran detrás de las terminales.

Con este proyecto se podrá aprender a instalar y gestionar un ambiente completamente virtual de escritorios donde los usuarios se conectan mediante terminales y sirven para su trabajo del día a día, casi sin sentir la diferencia entre un equipo físico y el proporcionado.

Dentro de los capítulos de este trabajo se podrán encontrar los motivos del proyecto así como la manera en que se llevó a cabo la configuración e instalación de cada escritorio virtual, llevando poco a poco al término del trabajo.

¹ Escritorio virtual creados dinámicamente con View Composer de VMware, el cual está basado en una Golden image de una máquina virtual.

² Es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio.

³ Es una plataforma de infraestructura de escritorio virtual (VDI, virtual desktop infrastructure) que brinda escritorios virtualizados y remotos, y aplicaciones a través de una única plataforma.

En el capítulo I se da una explicación de todos los elementos con los que se trabajaron en el proyecto, con el motivo de tener una base para poder entender los conceptos de los que se trata en el trabajo.

El capítulo II tiene por función dar a conocer la empresa en la que laboro actualmente y en la que se desarrolló el proyecto, proporcionando información general de Dicofra Security Consulting y el enfoque de la misma.

Dentro del capítulo III se dan las razones del porque la empresa tenía la necesidad de mejorar algunos puntos en la operación y como se llegó a la conclusión de desarrollar escritorios virtuales para los usuarios del centro de monitoreo.

Por su parte, el capítulo IV se puede encontrar la forma en que se implementó este proyecto y los recursos utilizados para el mismo.

El objetivo principal por el que fue creado este proyecto es proveer una infraestructura virtual funcional y eficaz que trabaje las 24 horas los 365 días del año mediante escritorios virtuales centralizando la operación de la empresa en un solo punto, basándose en lo siguiente:

- Centralizar la operación de la empresa en un solo punto.
- Gestionar el control de acceso a las terminales.
- Gestionar las conexiones de los usuarios.
- Gestionar la información a la que tienen acceso los usuarios.
- Obtener un servicio estable para los usuarios de las terminales.
- Mantener la operación de la empresa trabajando las 24 horas los 365 días del año.

Capítulo I. Marco teórico

La evolución de la virtualización ha afectado a los centros de datos eficientes de todos los tamaños, se ha transformado a una tecnología táctica que las empresas adoptaban para ahorrar espacio, refrigeración y energía (esencialmente para hacer más con menos) en una estrategia corporativa que respondió a las demandas del negocio.

La virtualización ha existido por muchas décadas. En el principio había muchos detractores y escépticos. Pero en los últimos 10 años, la demanda del cliente y la maduración de la plataforma de hardware x86 han creado una "tormenta perfecta". En solo pocos años, la virtualización se convirtió en la manera de hacer las cosas en un centro de datos eficiente. Como consecuencia de ello, las empresas comenzaron a adoptar políticas de "virtualización primero".

Los clientes con centros de datos eficientes siguen enfrentando barreras en torno a la gestión de imágenes de escritorio virtuales, a pesar de la introducción de clones vinculados⁴.

A pesar de los proveedores de almacenamiento han acaparado una oportunidad de mercado para vender unidades adicionales de caché y SSD, no todos los centros de datos deciden alojar máquinas virtuales en el almacenamiento disponible más caro, sólo para que sus usuarios puedan iniciar sesión y abrir Microsoft Word. La mayoría de las organizaciones más bien preferirían poner las aplicaciones de servidor que utilizan el disco de manera intensiva en ese nivel de almacenamiento, donde la relación costo-beneficio es mucho más convincente.

A continuación se proporcionarán las definiciones e información necesaria para poder comprender un poco el tema de este trabajo.

1.1 Virtualización

Virtualización es la técnica empleada sobre las características físicas de algunos recursos computacionales, para ocultarlas de otros sistemas, aplicaciones o usuarios que interactúan con ellos. Esto implica hacer que un recurso físico, como un servidor, un sistema operativo o un dispositivo de almacenamiento aparezca como si fuera varios

⁴ Un clon vinculado es una máquina virtual creada a partir de una copia de otra máquina virtual

recursos lógicos a la vez, o que varios recursos físicos, como servidores o dispositivos de almacenamiento, aparezcan como un único recurso lógico.

Esta tecnología permite la separación del hardware y el software, lo cual posibilita a su vez que múltiples sistemas operativos, aplicaciones o plataformas de cómputo se ejecuten simultáneamente en un solo servidor o PC según sea el caso de la aplicación.

1.1.1 Formas de virtualización

Hay varias formas de ver o catalogar la virtualización, pero en general se trata de uno de estos dos casos:

- **Virtualización de plataforma**

Se trata de simular una máquina real (servidor o PC) con todos sus componentes (los cuales no necesariamente son todos los de la máquina física) y prestarle todos los recursos necesarios para su funcionamiento. En general, hay un software anfitrión que es el que controla que las diferentes máquinas virtuales sean atendidas correctamente y que está ubicado entre el hardware y las máquinas virtuales. Dentro de este esquema caben la mayoría de las formas de virtualización más conocidas, incluidas la virtualización de sistemas operativos, la virtualización de aplicaciones y la emulación de sistemas operativos.

- **Virtualización de recursos**

Permite agrupar varios dispositivos para que sean vistos como uno solo, o al revés, dividir un recurso en múltiples recursos independientes. Generalmente se aplica a medios de almacenamiento, también existe una forma de virtualización de recursos muy popular que no es sino las redes privadas virtuales o VPN, abstracción que permite a una PC conectarse a una red corporativa a través de internet como si estuviera en la misma sede física de la compañía.

1.1.2 Ventajas de la virtualización

Los usuarios serán provistos con dos o más ambientes de trabajo completamente independientes entre sí según se requiera. Si se manejan dos como en la mayoría de los casos, un ambiente de trabajo sería abierto para que usuarios hagan efectivamente en él

lo que requieran, agregando dispositivos e instalando cualquier software que elijan. El segundo ambiente estaría cerrado o restringido; es decir, donde el usuario solo tendría acceso a lo que es crítico para la organización y sus negocios. De esta forma, si el primer ambiente sufre una caída o colapso, el segundo ambiente sigue trabajando y haciendo que el negocio no pare.

En caso de que la organización constantemente ocupe estar cambiando de aplicaciones por cuestiones de su negocio, la virtualización permite conservar los mismos equipos terminales o de trabajo, y realizar todos los cambios de versiones y plataformas vía un entorno virtual en la red y teniendo como fuente al servidor.

1.1.3 Desventajas de la virtualización

El uso de la virtualización representa conflictos con el licenciamiento que aplican los fabricantes de software. El software de virtualización representa un desafío para los tipos de licencia por usuarios existentes actualmente, por lo cual es probable que cambien las reglas respecto al licenciamiento de software. Claro está que su instalación y administración requiere de personal calificado en TI, mas su uso puede ser transparente para un usuario promedio corporativo.

Los componentes principales que determinarán el número de máquinas virtuales que se podrán soportar sobre un hardware y el rendimiento de cada una de ellas son: la cantidad de RAM, la potencia del procesador, el acceso y transferencia del disco duro.

ESX		
Máquinas virtuales ESX	Versión de hardware	Límite de memoria
5.x	8	Máquinas virtuales de 32 bits y 64 bits - 1011 GB El huésped tiene acceso a toda la memoria especificada. El huésped justifica el espacio que ocultan los dispositivos PCI.
4.x	7	Máquinas virtuales de 32 bits y 64 bits - 255 GB El huésped tiene acceso a toda la memoria especificada. El huésped justifica el espacio que ocultan los dispositivos PCI.
3.5	4	Máquinas virtuales de 32 bits y 64 bits - 65532 MB
3.x	4	Máquinas virtuales de 32 bits y 64 bits - 16384 MB
2.x	3	Máquinas virtuales de 32 bits y 64 bits - 3600 MB

Figura 1. Beneficios de la virtualización.

Fuente: VMware (2015). Razones para expandir la virtualización. Recuperado de http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2033074

1.2 Origen y fundamentos de los escritorios virtuales

La virtualización de escritorio es un término introducido en la década de los 90, se describe como el proceso de separación entre el escritorio que engloba datos y programas que utilizan los usuarios para trabajar, de la máquina física. El escritorio virtualizado es almacenado remotamente en un servidor central en lugar del disco duro de una máquina personal, esto significa que cuando los usuarios trabajan en su escritorio virtual desde alguna terminal todos sus programas, aplicaciones, procesos y datos se almacenan y ejecutan centralmente en la máquina a la que están accediendo remotamente.

La experiencia que el usuario tendrá está orientada a ser idéntica a la de una computadora estándar, pero desde un dispositivo de cliente ligero o similar, desde la misma oficina o remotamente.

La virtualización del escritorio proporciona mucha de las ventajas de un servidor de terminales, si es configurado por los administradores de sistemas pueden proporcionar a los usuarios mucha más flexibilidad, por ejemplo, cada uno puede tener permitido instalar y configurar sus propias aplicaciones, los usuarios también disponen de la capacidad de acceder a sus escritorios virtuales basados en servidor desde otras localizaciones.

1.3 Beneficios y Ventajas de los escritorios virtuales

Con el uso cada vez mayor de dispositivos personales entre los empleados y el creciente número de ellos que trabajan desde casa, se comienza a ver un aumento en el uso de la infraestructura de escritorios virtuales.

La implantación de la tecnología VDI permite a las empresas estar siempre actualizadas. Las últimas actualizaciones de software son sencillas de implantar para un gran número de usuarios y no requieren todo un departamento de TI para instalar cada nueva versión.

Las ventajas de seguridad adicionales (respaldos y protección de datos) hacen de la tecnología VDI una solución enormemente atractiva.

Algunos beneficios de la tecnología de escritorios remotos son los siguientes:

- **Incremento de la seguridad de la información**

Se minimiza el riesgo de pérdida y corrupción de la información ya que los datos delicados ya no se almacenan en un portátil individual, sino que permanecen

protegidos en instalaciones externas. La capacidad de realizar respaldos y restaurar datos mediante VDI a su estado anterior tras un desastre puede ayudar a que la empresa se recupere rápidamente y mantenga sus niveles de productividad.

- **Reduce los costes de Hardware**

La virtualización de escritorios implica que no se tiene que tener equipos de última tecnología, porque todas las aplicaciones del escritorio son ejecutadas centralmente en un servidor remoto. El costo puede reducirse en mayor medida si se utilizan clientes ligeros para conectarse a los escritorios remotos.

- **Alternativa ecológica**

La tecnología VDI almacenada en el servidor central es una alternativa ecológica a los PC tradicionales ya que estos consumen mayor energía que varios servidores a baja utilización.

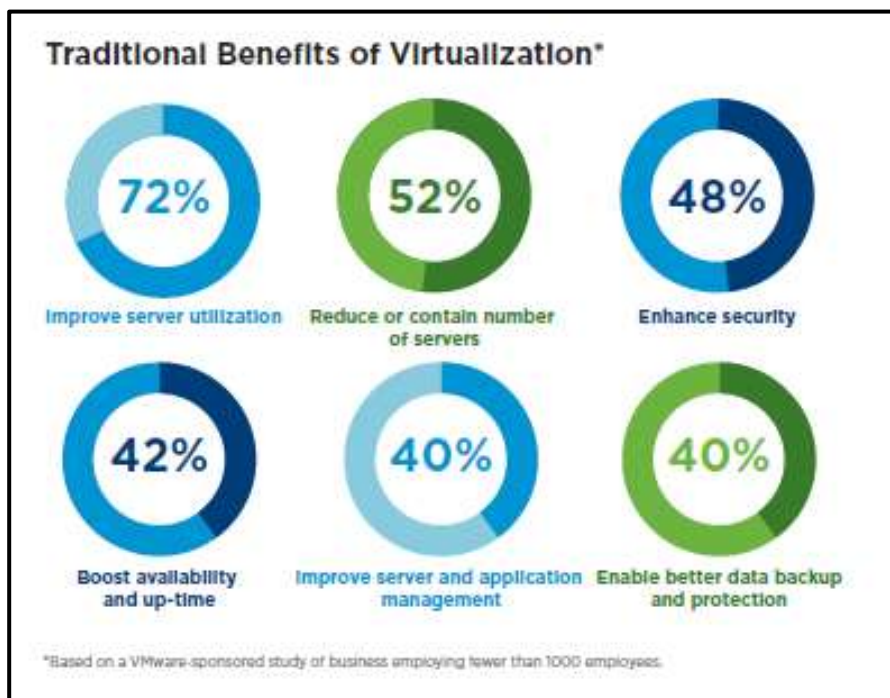


Figura 2. Beneficios de la virtualización.

Fuente: VMware (2015). Razones para expandir la virtualización. Recuperado de <http://blogs.vmware.com/latam/razones-para-expandir-la-virtualizacion-de-ti.html>

1.4 Escritorios virtuales como un servicio

Los escritorios virtuales están basados en un esquema de trabajo donde la información o archivos están almacenados en otro equipo, por otro lado consta de aplicaciones que se ejecutan en el servidor y que solo requieren instalación del *remote desktop software* en solo una de las terminales de los usuarios. Basado en este esquema de trabajo el usuario ingresa a un sitio web, introduce su nombre y número de identificación, y accede a su escritorio virtual, el cual le provee de varias aplicaciones que mejoran su sistema de comunicación.

En mayo de 2007, VMware comenzó el proceso para registrar el término "escritorio como un servicio" en los Estados Unidos. El 19 de junio de 2008: "Una acción no final ha sido enviada. Esto es una carta del abogado examinador solicitando información adicional y/o haciendo una denegación inicial. Sin embargo, no se ha tomado una determinación final en cuanto al registro de la marca".

1.5 Microsoft Windows Server 2008

Es el sucesor de Windows Server 2003, distribuido al público casi cinco años después. Al igual que Windows Vista, Windows Server 2008 se basa en el núcleo Windows NT 6.0 Service Pack 1. Entre las mejoras de esta edición, se destacan nuevas funcionalidades para el Active Directory⁵, nuevas prestaciones de virtualización y administración de sistemas, la inclusión de IIS 7.5 y el soporte para más de 256 procesadores. Hay siete ediciones diferentes: Foundation, Standard, Enterprise, Datacenter, Web Server, HPC Server y para Procesadores Itanium.

1.5.1 Características de Windows Server 2008

Hay algunas diferencias con respecto a la arquitectura de Windows Server 2008, que pueden cambiar drásticamente la manera en que se usa este sistema operativo. Estos cambios afectan a la manera en que se gestiona el sistema hasta el punto de que se puede llegar a controlar el hardware de forma más efectiva, se puede controlar mucho mejor de

⁵ Término utilizado por Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadoras.

forma remota y cambiar de forma radical la política de seguridad. Entre las mejoras que se incluyen, están:

- Nuevo proceso de reparación de sistemas NTFS: proceso en segundo plano que repara los archivos dañados.
- Creación de sesiones de usuario en paralelo: reduce tiempos de espera en los Terminal Services ⁶ y en la creación de sesiones de usuario a gran escala.
- Cierre limpio de Servicios.
- Windows Hardware Error Architecture (WHEA): protocolo mejorado y estandarizado de reporte de errores.
- Virtualización de Windows Server: mejoras en el rendimiento de la virtualización.
- PowerShell: inclusión de una consola mejorada con soporte GUI para administración.
- Server Core: el núcleo del sistema se ha renovado con muchas y nuevas mejoras.

1.5.2 Windows Server 2008 R2

Microsoft introdujo Windows Server 2008 R2 en la Professional Developers Conference ⁷(PDC) del 2008 donde se reúnen desarrolladores de software para windows como una variante de servidor del nuevo sistema operativo Windows 7.

Una guía preliminar⁸ publicada por la compañía describe muchas áreas de mejora, notablemente la inclusión de un número de nuevas características de virtualización incluyendo Live Migration y Cluster Shared Volumes, un reducido consumo de energía, un nuevo conjunto de herramientas de administración, nuevas características Active Directory como una "papelera de reciclaje" para objetos AD borrados, una nueva versión de IIS (7.5) que incluye un renovado servidor FTP, soporte para DNSSEC y el aumento del número de núcleos de procesamiento de 64 a 256.6 Los procesadores de 32-bits ya no están soportados.⁷

Las mejoras en el rendimiento fueron un área de desarrollo importante en esta versión; Microsoft anunció que se habían realizado trabajos para disminuir el tiempo de arranque, mejorar la eficiencia de operaciones E/S a la vez que reducir potencia de procesamiento y

⁶ Son un componente de los sistemas operativos Windows que permite a un usuario acceder a las aplicaciones y datos almacenados en otro ordenador mediante un acceso por red.

⁷ Es una conferencia donde se reúnen desarrolladores de software para Windows y se tratan temas de actualizaciones y desarrollos de la plataforma.

⁸ <https://technet.microsoft.com/en-us/library/dd391932.aspx>

mejoras generales de velocidad en dispositivos de almacenamiento, especialmente en iSCSI.⁹

El 7 de enero de 2009, se lanzó una versión preliminar (beta) de Windows Server 2008 R2 para suscriptores de los programas de Microsoft, TechNet y MSDN, así como también a participantes del programa Microsoft Connect sobre Windows 7. Dos días después, se lanzó al público general mediante el Centro de descargas de Microsoft.

La versión RTM (Release To Manufacturing) fue anunciada el 22 julio de 2009. Entre los cambios que incluye respecto a la edición anterior se incluyen mejoras en las funcionalidades de virtualización, Active Directory y capacidades de seguridad

El Service Pack 1 para Windows Server 2008 R2 y Windows 7 fue anunciado el 9 de febrero de 2011. Entre los cambios que introdujo se destacan dos nuevas funcionalidades de virtualización, RemoteFX y Dynamic Memory.

Dynamic Memory es una funcionalidad de Hyper-V que ayuda a utilizar la capacidad de la memoria física de forma más eficiente, tratándola como un recurso compartido que puede ser relocalizado entre las máquinas virtuales que se encuentran corriendo; ajusta la cantidad de memoria disponible para una máquina virtual, basándose en los cambios en la demanda y en los valores que se hayan especificado. De esta manera, permite aumentar la densidad de una máquina virtual sin pérdida del desempeño ni escalabilidad.

Remote FX es una tecnología que introduce mejoras en la experiencia final del usuario, integrándose al Protocolo de Escritorio Remoto (RDP). Permite virtualizar el GPU (Unidad de Procesamiento Gráfico) en el servidor, agregar multimedia y experiencias 3D para VDI (Infraestructura de Escritorio Virtual), entre otras características.

⁹ Es un estándar que permite el uso del protocolo SCSI sobre redes TCP/IP. iSCSI es un protocolo de la capa de transporte definido en las especificaciones SCSI-3. Otros protocolos en la capa de transporte son SCSI Parallel Interface y canal de fibra.

Características	Foundation	Standard	Web	HPC	Enterprise	Datacenter	Itanium
Máximo de RAM en x86-64	8 GB	32 GB	32 GB	128 GB	2 TB	2 TB	2 TB
Máximo de CPUs físicas	1	4	4	4	8	64	64
Cross-file replication (DFS-R)	No	No	No	No	Si	Si	Si
Failover cluster nodes (Nodes)	No	No	No	No	16	16	8
Fault tolerant memory sync	No	No	No	No	Si	Si	Si
Módulos de memoria: agregar en caliente	No	No	No	No	Si	Si	Si
Módulos de memoria: reemplazo en caliente	No	No	No	No	No	Si	Si
CPUs: agregar en caliente	No	No	No	No	No	Si	Si
CPUs: Reemplazo en caliente	No	No	No	No	No	Si	Si
Acceso por red: IAS	10	50	No	No	ilimitado	ilimitado	2
Conexiones por red: RRAS	50	250	No	250	ilimitado	ilimitado	No
Conexiones administrador en escritorio remoto	2	2	2	2	2	2	2
Remote Desktop Services gateway	50	250	No	No	ilimitado	ilimitado	No
Virtual image use rights	No	Host + 1 VM	Guest	Host + 1 VM	Host + 4 VMs	ilimitado	ilimitado
Features	Foundation	Standard	Web	HPC	Enterprise	Datacenter	Itanium

Figura 3. Tabla de comparación de ediciones de Windows server 2008 R2.

Fuente: Windows Server 2008 (2015) Recuperado de https://es.wikipedia.org/wiki/Windows_Server_2008#cite_note-2008r2guide-5

1.6 Vmware

Vmware es un sistema de virtualización por software. Un sistema virtual por software es un programa que simula un sistema físico (Hardware) con unas características de hardware determinadas. Cuando se ejecuta el programa (simulador), proporciona un ambiente de ejecución similar a todos los efectos a un equipo físico, con CPU (puede ser más de una), BIOS, tarjeta gráfica, memoria RAM, tarjeta de red, sistema de sonido, conexión USB, disco duro (pueden ser más de uno), etc.

Un virtualizador por software permite ejecutar (simular) varios sistemas dentro de un mismo hardware de manera simultánea, permitiendo así el mayor aprovechamiento de recursos. Sin embargo al ser una capa intermedia entre el sistema físico y el sistema operativo que funciona en el hardware emulado, la velocidad de ejecución de este último es menor, pero en la mayoría de los casos suficiente para usarse en entornos de producción.

1.6.1 Vmware ESXi

Es una versión completa del producto ESX, pero con varias limitaciones, entre ellas: no permite instalar controladores (drivers) para hardware adicional (es decir, si el ESXi no

posee los controladores el hardware no puede ser utilizado); no permite utilizar las funciones avanzadas de movimiento de máquinas virtuales encendidas de un equipo físico a otro (Vmotion¹⁰), ni hacerlo con el almacenamiento.

Sin embargo, es muy útil para conocer el funcionamiento del ESX, e incluso algunos fabricantes (como HP o DELL) dan la opción de comprar servidores pre cargados con ese sistema operativo en una memoria USB integrada en el equipo.

ESXi es en la actualidad el hypervisor¹¹ comercial, quedando discontinuado el ESX. VMware apostó más por la tecnología del ESXi, pues aunque parecida, eran desarrollos diferentes. Antes de la versión ESXi 4.1, en la 3, existía la diferencia de ESXi versión libre y la ESX versión comercial. Pero en realidad la ESXi tenía más ventajas que la otra, tanto que VMware dirigió todo su esfuerzo por mejorarla y sobre ella está basado hoy por hoy el hypervisor comercial.

1.6.2 VMware Vcenter

El servidor de vCenter actúa como un único punto de administración central en el entorno de vSphere™.

El software de vCenter Server consiste en multitudes de módulos y servicios y es instalado en un servidor (virtual o físico) con el sistema operativo soportado Windows.

A diferencia de las versiones anteriores, vSphere™ incluye una nueva versión de vCenter Server en modo appliance para entornos con Linux. vCenter Server ofrece funcionalidades Enterprise, como por ejemplo, VMware Distributed Resource Scheduler (DRS), VMware High Availability (HA), VMware Fault Tolerance(FT), VMware vMotion y VMware Storage vMotion.

Una sola instancia de vCenter Server soporta un máximo de 1.000 hosts ESXi y 15.000 máquinas virtuales registradas (10.000 máquinas virtuales encendidas). Sin embargo, en el hipotético caso que se necesite gestionar más de 1.000 servidores ESXi o 10.000 máquinas virtuales, se tendría que comprar otra licencia de vCenter y conectar estos sistemas de vCenter en lo que se denomina un group en mode Linked.

¹⁰ Permite mover una máquina virtual completa en ejecución de un servidor físico a otro, sin tiempo fuera de servicio.

¹¹ Es una plataforma que permite aplicar diversas técnicas de control de virtualización para utilizar al mismo tiempo, diferentes sistemas operativos en una misma computadora.

El número máximo de servidores de vCenter Server (versión Windows) que se pueden conectar juntos (modo Linked) entre si es diez. Sin embargo, la versión Linux de vCenter, vCenter Server Appliance, no soporta aún esta funcionalidad. vCenter Server también puede ser instalado en Linked Mode, en caso de querer ver el estado del servidor de vCenter para todos los servidores en el inventario.

Para poder desplegar este appliance en un entorno virtual se tiene que formatear el disco y asignar un mínimo de RAM requerida para que arranque el appliance.

Se debe recordar que no es posible conectar vía Linked mode dos vCenter Servers de versiones diferentes. Por ejemplo, vCenter 4.1 y vCenter 5.0 no se pueden conectar usando la funcionalidad de Linked mode.

Los requerimientos mínimos para vCenter Server son 2CPUs de 2Ghz de 64bits, mínimo 4GB de memoria RAM y 4GB de espacio en disco duro mínimo. vCenter Server ya no soporta las bases de datos Oracle ni Microsoft SQL Server 2000.

Asimismo, el número máximo de vCenter Servers que se pueden conectar con el vCenter Orchestrator es diez. También, el número máximo de hosts conectados a un vCenter Orchestrator es 1000.

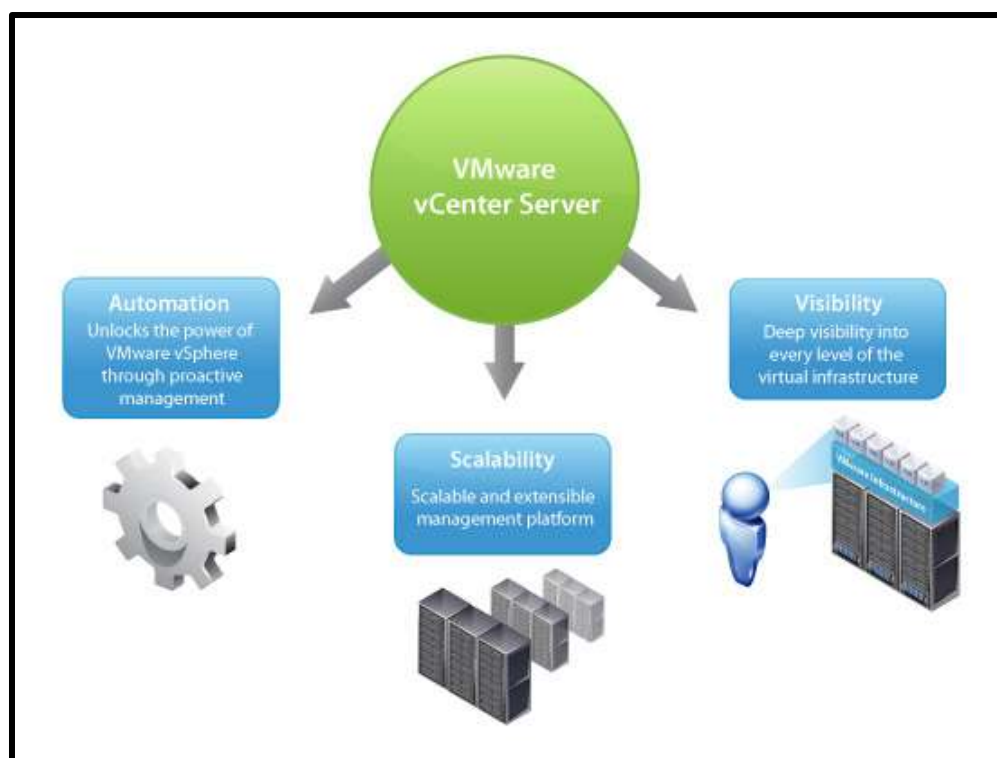


Figura 4. Diagrama de ventajas de Vcenter

Fuente: Vcenter Server(2015) Recuperado de <http://www.vmware.com/mx/products/vcenter-server>

1.6.3 Pre requisitos de hardware y software para Vcenter Server

Requerimientos Hardware (Versión Windows):

- Procesador: 2 CPUs 64-bit 2.0GHz Intel o AMD x86.
- Memoria: 4GB RAM mínimo.
- Disco: 4GB recomendado.
- Red: Adaptador Ethernet (1 Gigabyte recomendado).
- Requerimientos Software:
- Windows XP Pro 64-bit, SP2 y SP3
- Windows Server 2003 64-bit Standard, Enterprise y DataCenter, SP1 y SP2
- Windows Server 2008 64-bit Standard, Enterprise y DataCenter, SP2
- Windows Server 2008 R2 64-bit

Los requerimientos de procesador, memoria y disco serán más altos si la base de datos de vCenter y Update Manager está instalada en el mismo sistema virtual o físico.

Quizás el componente más importante en vCenter es su base de datos. vCenter Server almacena todos los datos del inventario, estado de cada máquina virtual y configuración de cada servidor VMware vSphere™ ESXi, en una base de datos relacional. Las bases de datos soportadas por vCenter Server para Windows son las siguientes:

Oracle

- Oracle 10g F2
- Oracle 11g

Microsoft SQL

- SQL Server Server 2005 SP3 (recomendado SP4)
- SQL Server 2008 R2 Express*
- SQL Server 2008

En cuanto a la versión Linux de vCenter Server, los requerimientos de software son diferentes. No obstante, el usuario o administrador del entorno virtual, no notará ninguna diferencia con el hecho de tener la versión Windows o Linux de vCenter instalado en su entorno.

El servicio de vCenter en modo appliance reduce el tiempo requerido para instalar y configurar la versión de vCenter en Windows, ya que la versión appliance para Linux viene pre-instalada.

Sin embargo, a nivel de base de datos el appliance aún no soporta SQL. Al día de hoy solo soporta Oracle y DB2 express (versión inicial del appliance) como base de datos y ahora postgres.

vCenter Server Virtual Appliance usa un kernel versión 2.6.32.29-03 de SuSe Linux y estos son sus requerimientos:

Requerimientos Hardware (Versión Linux):

- Procesador: 2 CPUs 64-bit 2.0GHz Intel o AMD x86.
- Disco: 7GB RAM mínimo. Máximo 80GB.
- Red: Adaptador Ethernet (1 Gigabyte recomendado).

Memoria:

- De 1-100 máquinas virtuales: 4GB mínimo recomendado.
- De 100-1000 máquinas virtuales: 8GB mínimo recomendado.
- De 1000-4000 máquinas virtuales: 13GB mínimo recomendado.
- Para 4000 máquinas virtuales: 17GB mínimo recomendado.

1.7 VMware View (VMware Horizon)

Es una plataforma de infraestructura de escritorio virtual (VDI, virtual desktop infrastructure) que brinda escritorios virtualizados y remotos, y aplicaciones a través de una única plataforma. Además, a través de esta plataforma los usuarios finales pueden acceder a todos sus recursos de Windows y en línea mediante un espacio de trabajo unificado.

Horizon (con View) les permite a las organizaciones suministrar escritorios virtualizados o remotos y aplicaciones a través de una única plataforma. Asimismo, les brinda respaldo a los usuarios finales para que puedan acceder a todos sus escritorios y aplicaciones a través de un solo espacio de trabajo unificado.

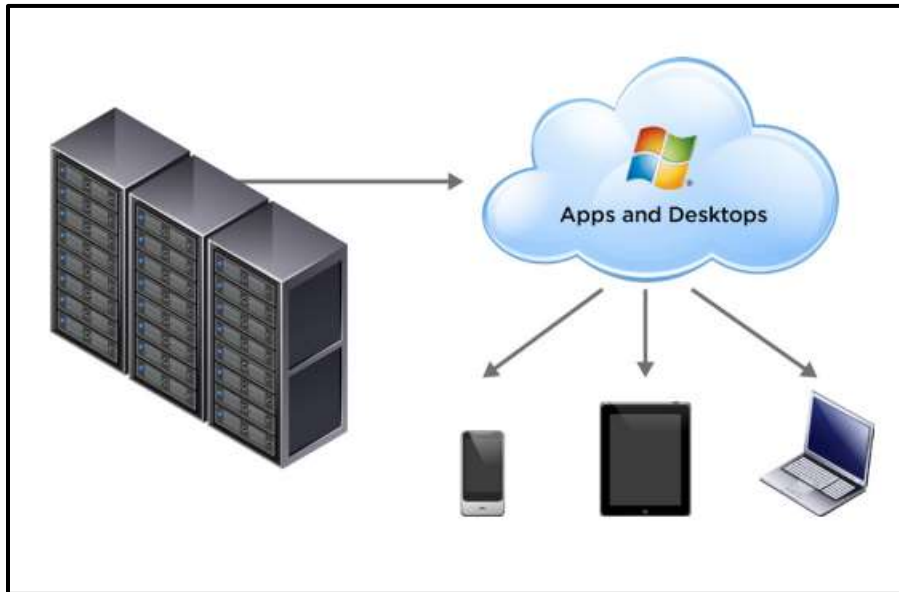


Figura 5. Diagrama Punto a Punto de VMware View

Fuente: VMware Horizon 6 (2015) Recuperado de <http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Datasheet.pdf>

1.8 VMware View Composer

View Composer, usa la tecnología VMware Linked Clone para crear rápidamente imágenes de escritorio que comparten discos virtuales con una imagen maestra para conservar espacio en el disco y agilizar la gestión. Los datos del usuario y la configuración se segmentan desde la imagen de escritorio para que puedan ser gestionados de manera independiente. Como resultado de este modelo de Linked Clone, todos los escritorios vinculados a una imagen principal pueden recibir parches o actualizaciones a través de VMware View Manager simplemente actualizando la imagen principal, sin que esto afecte a la configuración, los datos o las aplicaciones de los usuarios. Esto produce una disminución considerable de las necesidades y los costes de almacenamiento, simplificando al mismo tiempo la gestión de los escritorios.

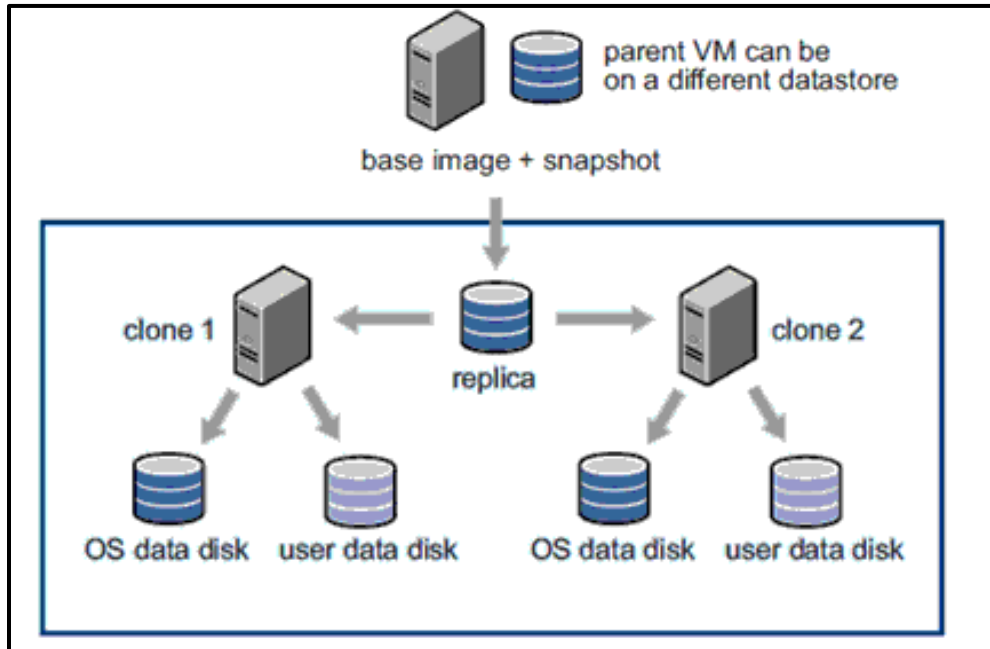


Figura 6. VMware View composer

Fuente: VMware view composer (2012) Recuperado de

https://jorgegonzalezmartos.files.wordpress.com/2012/01/view_composer.png

Este diagrama tal como se presenta es una vista conceptual de la gestión de almacenamiento por View Composer. Los elementos lógicos importantes a tener en cuenta son los siguientes:

- **Parent VM.** Es la máquina virtual estándar que se utiliza para crear y mantener las diversas versiones de su imagen. Puede contener varios Snapshots¹² diferentes.
- **Replica.** Es una copia de una versión específica de la Parent VM, es decir, un snapshot de la máquina. La clave es que el disco es una copia pequeña del disco principal.
- **Clones.** Son réplicas completas de un snapshot de la Parent VM.

¹² Una copia de seguridad de un sistema con un gran conjunto de datos puede tardar mucho tiempo en completarse.

Capítulo II. Marco conceptual

En este capítulo se proporciona la información relacionada con la empresa en la que laboro, misma donde se desarrolló el proyecto el cual se encuentra funcionando y en producción.

2.1 La empresa

DICOFRA es una empresa mexicana creada desde 1999, con visión e innovación para ofrecer consultoría de soluciones y servicios administrados en seguridad de la información.

Cuenta con colaboradores altamente reconocidos por su conocimiento en el área de seguridad de la información.

Las actividades principales de la empresa son:

- Consultoría en seguridad de la información.
- Seguridad administrada.
- Soporte técnico a productos.

Para poder llevar a cabo todas las actividades se basa en los siguientes puntos:

- Centro de Monitoreo DICOFRA.
- Ingenieros certificados.
- Laboratorio de investigación.
- Alianzas estratégicas.

Mediante servicios administrados y consultoría en seguridad de la información, trabaja con las áreas de TI para que tengan una mejor alineación estratégica que apoye el cumplimiento de los objetivos de las organizaciones a las que pertenecen.

Realiza en cada uno de sus clientes, una evaluación de requerimientos y necesidades para ofrecerles adecuadamente la consultoría de productos y servicios entre una variedad de soluciones inteligentes y proactivas de seguridad, destinadas a salvaguardar y proteger la información sensible y crítica, enfocadas a inteligencia, auditoría y desempeño con impacto en la nube, Internet, correo electrónico, perímetro, equipos móviles y ambientes físicos y virtuales.

Así mismo, busca reducir costos, garantizar la continuidad de la operación frente a las nuevas amenazas del mundo informático y lograr un equilibrio entre la funcionalidad del negocio y la protección de la información.

Desde el Centro de Monitoreo DICOFRA, a través de la operación remota 7x24x365 en la modalidad de outsourcing¹³ y con recursos propios, ofrece servicios de soporte técnico a fallas de productos con la actualización de versiones de software y aplicación de parches¹⁴, extendiéndose a servicios de seguridad administrada con los que se realiza el monitoreo de la operación, notificación de actividad sospechosa y administración de cambios y respuesta a incidentes de seguridad.

Con base en las pruebas del laboratorio de investigación tecnológico interno, se realiza una exhaustiva evaluación y aplicación de las tecnologías de los aliados, para ofrecer servicios y así aplicar las mejores prácticas con los clientes.

2.1.2 Productos y servicios que ofrece

La empresa ofrece el soporte y servicio en las siguientes categorías y a los productos específicos que cubren cada una de ellas:

- Virtualización y seguridad – VMware
- Seguridad contra ataques dirigidos e inteligencia global de amenazas – Trend Micro
- Cifrado de disco – WinMagic
- Desempeño de servicios y análisis de tráfico – Riverbed
- Protección del perímetro – Palo Alto Networks
- Auditoría de seguridad por medio de administración de vulnerabilidades – Qualys

2.1.2.1 Servicios de consultoría en seguridad de la información

DICOFRA es una empresa integradora de soluciones de TI que realiza una evaluación de los requerimientos y necesidades de sus clientes para ofrecerles los productos y servicios

¹³ Es el proceso económico empresarial en el que se delega los recursos orientados a cumplir ciertas tareas a una sociedad externa.

¹⁴ Un parche consta de cambios que se aplican a un programa, para corregir errores, agregarle funcionalidad, actualizarlo, etc.

más adecuados de su portafolio de soluciones, destinada a proteger la información sensible y crítica de cada organización.

Con estos servicios, los clientes pueden identificar los riesgos a los que pudiera estar expuesta la información que reside en su infraestructura y, una vez identificados, definir acciones estratégicas y operativas para emprender actividades de remediación.

Análisis y certificación de sitios web

- Escaneo de sitios web para detectar la presencia de código malicioso, vulnerabilidades a nivel de red y a nivel de la aplicación web, así como la validación del certificado SSL¹⁵.
- Reporte con los hallazgos y recomendaciones detalladas.

Análisis de vulnerabilidades de infraestructura tecnológica

- Análisis técnico especializado de la infraestructura tecnológica a auditar.
- Entrega de reporte con recomendaciones detalladas.
- Factores evaluados en el análisis técnico:
 - Descubrimiento automático de activos generando un diagrama de red.
 - Priorización de activos.

Cumplimiento de políticas

- Definición de políticas, prueba de implementación y evidencia documentada de los hallazgos.
- Remediación de las desviaciones para el cumplimiento.
- Reporte con hallazgos y recomendaciones.

2.2 Centro de Monitoreo

DICOFRA cuenta con un centro de monitoreo inaugurado en el año 2012 y ofrece los siguientes servicios:

- Cobertura 7x24x365.
- Modalidad de servicios en outsourcing.
- Ingenieros propios y certificados.
- Apego a mejores prácticas y estándares internacionales.

¹⁵ Un certificado SSL sirve para brindar seguridad al visitante de su página web, una manera de decirles a sus clientes que el sitio es auténtico, real y confiable para ingresar datos personales.

- Laboratorio de investigación y desarrollo.
- Soporte técnico remoto a fallas de productos:
 - Actualización de versiones de software y aplicación de parches.
 - Generación de reportes periódicos.
- Seguridad administrada:
 - Actualización de versiones de software y aplicación de parches.
 - Administración de altas, bajas y cambios.
 - Monitoreo de la operación.
 - Notificación de actividad sospechosa.
 - Respuesta a incidentes de seguridad.
 - Generación de reportes periódicos.

Toda la actividad es vía remota con enlaces tipo VPN SSL.

Busca, garantizar la continuidad de la operación frente a las nuevas amenazas del mundo informático y lograr un equilibrio entre la funcionalidad de su negocio y la protección de su información.

Seguridad para servidores virtuales

- Protección de servidores físicos, virtuales y en la nube.
- Incrementa la seguridad de los servicios críticos y, al mismo tiempo, disminuye y previene la exposición al riesgo frente a ataques informáticos internos y externos.
- Administración sencilla de múltiples sistemas de seguridad en servidores virtuales.
- Protección de firewall y contra código malicioso, monitoreo de integridad, inspección de logs, navegación por reputación en páginas web e inspección profunda de paquetes (prevención de intrusos y administración virtual de parches).

Monitoreo y detección de APT¹⁶

- Solución intuitiva que permite identificar los riesgos reales desde su origen en cualquier parte del mundo y resolverlos inmediatamente.
- Detección proactiva y en tiempo real de cualquier tipo de amenaza persistente, con una mínima tasa de falsos positivos ¹⁷y un perímetro de identificación más amplio para contenidos, comunicaciones y comportamientos maliciosos.

¹⁶ Una amenaza persistente avanzada (Advanced Persistent Threat), es un conjunto de procesos informáticos sigilosos y continuos, a menudo orquestados por humanos, dirigidos a penetrar la seguridad informática de una entidad específica.

¹⁷ Es un error por el cual un software de antivirus informa que un archivo o área de sistema está infectada, cuando en realidad el objeto está limpio de virus.

- Visibilidad, análisis y control en la red.
- Detección inicial, simulación, y correlación local y cruzada.

Protección perimetral de nueva generación

- Protección y políticas granulares sobre el contenido, aplicaciones y usuarios.
- Entorno sandbox¹⁸ virtualizado que analiza las amenazas desconocidas.

Protección contra amenazas en puntos finales

- Protección contra código malicioso¹⁹ e intrusiones.
- Prevención de fuga de información.
- Seguridad para dispositivos móviles.
- Detección en tiempo real.
- Protección de datos sensibles y mejoramiento del rendimiento.
- Reducción de tiempos de exploración mediante listas blancas, imágenes maestras y la exploración previa del contenido.

Filtrado de web y correo electrónico

- Protección de información sensible y crítica en la navegación web y el correo electrónico.
- Escaneo de tráfico y filtrado de contenido en el correo electrónico interno y el que fluye hacia Internet.
- Detección de spam²⁰, filtrado de contenido de acuerdo a las restricciones de la empresa.
- Protección continua y actualizada en la infraestructura de correo electrónico hospedada en un sitio en la nube, para detener el spam y el código malicioso antes de que entre a la red de la empresa.

Detección de fraude empresarial

- Visualización, grabación y análisis de toda la actividad de los usuarios en todas las aplicaciones.
- Detecta, detiene y prevé el uso indebido de la información en tiempo real; reproducción visual pantalla a pantalla, análisis de datos históricos y generación programada de informes.
- Arquitectura sin agente.

¹⁸ Un entorno de pruebas separado del entorno de producción.

¹⁹ Es código informático que provoca infracciones de seguridad para dañar un sistema informático.

²⁰ Mensajes no solicitados, no deseados o con remitente no conocido

Manejo de identidades

- A través de políticas y aplicación de medidas de control de TI en todo el ámbito de la empresa.
- Ofrece un enfoque de nueva generación a la provisión de usuarios en entornos físicos, virtuales y de nube.
- Provisión basada en funciones, creación de informes avanzados, respuesta en tiempo real.

Gestión de usuarios privilegiados

- Elimina la necesidad de revelar credenciales de cuentas administrativas o raíz en servidores Unix, Linux y Windows.
- Gestión de políticas de seguridad de manera centralizada (qué, quién, dónde y cuándo).
- Solución basada en agente.
- Ejecución de comandos privilegiados de forma remota y segura.
- Generación de informes bajo demanda.

Protección perimetral de nueva generación

- Protección y políticas granulares sobre el contenido, aplicaciones y usuarios.
- Entorno sandbox virtualizado que analiza las amenazas desconocidas, detiene la posible fuga de información confidencial y protege contra todo el ciclo de vida de un ataque.

2.3 Organigrama del área de Operaciones

A continuación se muestra la manera en que se encuentra organizada el área de operaciones en la empresa.



Figura 7. Organigrama del área de Operaciones de Dicofra.
Fuente: Servicios Internos, Organigrama de Dicofra (2014)

Servicios Internos se encarga de mantener toda la infraestructura y servicios de la empresa teniendo como enfoque principal la operación continua del Centro de Monitoreo, implementando nuevas soluciones y manteniendo una mejora continua en ellas.

2.3.1 Área de Servicios internos

Actualmente, el área de Servicios internos es la encargada de la disponibilidad, integridad y funcionalidad de la infraestructura de la empresa teniendo a su cargo más de 20 servidores Físicos, 40 servidores virtuales, switches, routers, firewalls, VPNs, CCTV, Conmutador, teléfonos IP, más de 25 equipos físicos (Laptop), dispositivos móviles, etc. Y lo más importante, el funcionamiento de 7 días las 24 horas del Centro de monitoreo.

La empresa depende del área para realizar cualquier ajuste en la infraestructura, actualización o cambios en los servicios, integración de nuevas tecnologías y reportes del estatus de cada servicio que se administra, teniendo la responsabilidad total y toma de decisiones en cuanto a servicios y productos.

También se encarga de apoyar al área de Pre-Venta con el dimensionamiento de los proyectos nuevos o existentes así como la realización de pruebas de concepto con potenciales nuevos clientes, principalmente con el producto Palo Alto Networks.

El Centro de monitoreo depende totalmente de Servicios Internos ya que si alguna máquina, servidor, VPN o servicio llega a fallar, los ingenieros no pueden hacer nada, por lo que se debe de reportar debidamente al área correspondiente quien es la encargada de resolver cualquier problema que se tenga.

2.4 Análisis de la problemática

El centro de monitoreo de la empresa se encontraba funcionando mediante PCs de escritorio o laptop que tenían asignadas los ingenieros, teniendo un servidor donde se almacenaban los documentos de cada cliente (memorias técnicas, documentos de control de cambios, etc.) lo que ocasionaba que esta documentación no estuviera debidamente actualizada o se encontrara incompleta, teniendo problemas con los clientes a causa de esto, ya que el siguiente ingeniero en turno no contaba con la información completa o la última actualización de los casos que se tenían con los clientes.

Como la empresa se encuentra sujeta a contratos en los cuales se especifica que deben de cumplir con niveles de servicio en cuanto a la atención de los casos, el problema de la falta de actualización de la documentación o ausencia de ella, provocó a la empresa pérdidas, ya que mes con mes se realizaban deducciones por incumplimiento de niveles de servicio.

Adicionalmente, para poder obtener un contrato con un cliente, el mismo, solicitó que su información no saliera de la empresa, manejando estrictos niveles de seguridad para evitar la fuga de su información ya que Dicofra contaría con todo lo referente a su red y estaría a cargo de la protección del correo electrónico, teniendo acceso total a ello.

Con todos estos problemas y la necesidad de obtener el contrato, se decidió que los ingenieros del centro de monitoreo no pudieran extraer sus equipos del mismo, teniendo un lugar de almacenamiento para cada uno de ellos. Con lo anterior se pudo obtener el contrato que se pretendía.

El problema principal después de la solución de integrar los equipos de cómputo destinados a la operación del Centro de monitoreo, persistió debido a que no se contaba con la comunicación adecuada entre el personal del área y la centralización de la información de los clientes y de la empresa en un solo sitio aún no era posible lograrse, ya que cada usuario mantenía en su equipo de cómputo lo necesario para atender a los clientes asignados y no era compartida con el demás personal, por lo que la Dirección de operaciones solicitó al área de servicios internos una solución para este problema.

2.4.1 Áreas de Oportunidad detectadas

Con base en la necesidad que la empresa tenía, el área de servicios internos de la que soy el responsable, comenzó a trabajar en conjunto con la dirección y los líderes de servicio para poder detectar todas las áreas de oportunidad con las que contaba el área del centro de monitoreo, para así poder dar una solución al problema.

Los puntos a los cuáles se llegó fueron los siguientes:

- Descentralización de la información.
- Necesidad de conexiones seguras entre las máquinas de los ingenieros y los clientes.
- Falta de control sobre la información y documentación de los clientes.
- Desorden en la organización de la información.
- Instalación de software no permitido en las Laptop de los ingenieros.
- Laptop dañadas por falta de cuidado por parte de los ingenieros.

2.4.1.1 Descentralización de la información

La falta de comunicación entre el personal del área no era la necesaria para poder dar un seguimiento puntual y estricto a las necesidades que los clientes tenían, ya que solo la persona encargada de la cuenta o cliente era consciente de las mismas, los planes de trabajo, diagramas, configuraciones y la información detallada solo era conocida por ellos y en una parte por el líder de servicio quien solicitaba los avances y estatus de las cuentas, teniendo que limitar estas peticiones a una sola persona.

Por esta razón, la documentación de los clientes se encontraba incompleta o desactualizada en el servidor donde se trataban de organizar y almacenar las cuentas

pertenecientes a la empresa, lo que llevó a que si se solicitaba un estatus por parte del líder de servicio o del cliente, no era posible darle los datos actuales al momento, teniendo que recurrir a la persona encargada de la cuenta, quien no siempre se encontraba disponible para atender este tipo de solicitudes, provocando un retraso en el cumplimiento de este tipo de solicitudes, lo que ocasionaba molestias a los clientes y más aún al personal del área quien debía de encontrarse disponible en todo momento para poder cubrir este tipo de requerimientos y solicitudes cuando le fueran solicitadas, aún fuera de su horario laboral.

2.4.1.2 Necesidad de conexiones seguras entre las máquinas de los ingenieros y los clientes

El incremento de información crítica proporcionada y el manejo de la misma dentro de la empresa, llevo a la solicitud de contratos de protección de datos por parte de los clientes quienes se sienten más seguros sabiendo que sus datos se encuentran protegidos y no serán divulgados con fines de lucro.

Para ello las solicitudes puntuales son:

- Conexiones seguras hacia su infraestructura e información por parte del personal del centro de monitoreo.
- Centralización de la información proporcionada.
- Protección de la información proporcionada.
- Mecanismos de DLP²¹ para asegurar la información.

El cubrir estas solicitudes es de suma importancia para Dicofra ya que el obtener nuevos contratos y servicios a nivel gobierno, depende del cumplimiento de todos estos puntos en su totalidad y de no llevarse a cabo o faltar a uno de ellos puede ser motivo de sanciones o en un caso extremo, la rescisión de contrato, lo que puede ser perjudicial para la empresa.

2.4.1.3 Falta de control sobre la información, documentación de los clientes y desorden en la organización de la información

La falta de conocimiento de la información del cliente por parte de los usuarios del centro de monitoreo llevó a incumplimientos de niveles de servicio, ya que en ocasiones no se podía atender las solicitudes en tiempo y forma debido a que la persona en turno dentro del centro de monitoreo no era capaz de resolver los problemas o solicitudes que el

²¹ Prevención de Pérdida de Datos o Data Loss Prevention.

cliente tenía por falta de conocimiento del mismo, y con un control deficiente de la información, no era posible dar solución inmediatamente, por lo que se tenía que buscar a la persona encargada de la cuenta e informarle del caso para que pudiera atenderlo.

En ocasiones, las personas encargadas a cada cuenta no se encontraban disponibles o no les era posible atender en ese momento las solicitudes de los clientes por lo que trataban de dar retroalimentación de la información que era necesaria para poder solucionar el problema con su cliente, esto no siempre funcionaba ya que cada usuario entendía de una manera diferente o la explicación del ingeniero a cargo no era lo más entendible posible para las demás personas.

Se tenían memorias técnicas de las implementaciones realizadas en la infraestructura de cada cliente, pero éstas no siempre se encontraban actualizadas y en el servidor de archivos donde se trataba de organizar la información, así mismo no era posible saber quién era la persona autorizada por parte del cliente para poder realizar solicitudes hacia el centro de monitoreo ya que cuando se realizaban cambios internos en el personal de los clientes, no se registraban en la documentación que Dicofra mantenía.

2.4.1.4 Instalación de software no permitido y equipo dañado

Los equipos de cómputo asignados al personal de la empresa eran actualizados cada dos años, pero este tiempo comenzó a reducirse debido a que el cuidado de cada uno de ellos no era el adecuado, teniendo problemas o daños físicos y lógicos cada vez más frecuentes.

Esta problemática llevó a la empresa a tomar medidas como no permitir a los usuarios retirar el equipo de las instalaciones a menos que fuera necesario, pero al realizarlo debían de firmar responsivas por cada vez que el equipo saliera y al regreso, aun así el problema persistió y los equipos se tenían que reemplazar por daño una vez al año.

Adicionalmente, el área de servicios internos detectó que los usuarios instalaban software no permitido por la empresa o no necesario para realizar su trabajo, pudiendo provocar la fuga de información de los clientes que era contenida en los equipos, también se comenzaron a tener infecciones de virus.

Los clientes al observar que los usuarios que iban a sitio con ellos tenían instalados programas no seguros en sus equipos comenzaron a desconfiar y limitaron las conexiones de los mismos a sus redes, enviando quejas a la dirección de operaciones informando que se debía de prestar más atención a este tipo de casos, e incluso este tema llegó a la dirección general donde se informó que no se iba a permitir el acceso a sus instalaciones

con equipos que tuvieran software que pudiera provocar algún daño a su infraestructura o información.

2.4.2 Solución propuesta

El área de servicios internos de la que soy el responsable, comenzó a trabajar en la búsqueda de herramientas que pudieran ayudar a solucionar o reducir esta problemática.

Se llegó a la conclusión de utilizar las herramientas de VMware para proporcionar escritorios virtuales a los usuarios, ya que con ellas se reducirían los problemas anteriores y adicionalmente se agregaría seguridad a la información de los clientes y empresa, teniendo las siguientes ventajas con su uso.

- Centralización de la información.
- Control de acceso a la información.
- Organización de la información.
- Gestión de privilegios para los usuarios en los escritorios virtuales.
- Reducción de hardware en el centro de monitoreo.
- Acceso controlado y seguro a los servidores de los clientes.

Con los escritorios virtuales se podría dar una solución en corto y mediano plazo a la problemática que tenía la empresa.

Capítulo III. Desarrollo

En este capítulo se presenta la manera en que se desarrolló el caso para poder tener las herramientas necesarias para la implementación del proyecto, también se muestran los diagramas de conexión de red física y virtual de la red.

3.1 Hardware y Software necesario

Con la definición de la tecnología a usar para resolver la problemática, se comenzó con el diseño de la solución propuesta, la cual llevará a la empresa a reducir todas las áreas de oportunidad descritas en el capítulo anterior.

Para poder llevar a cabo la configuración e implementación de los escritorios virtuales se tomó en cuenta las características necesarias de software y hardware que solicita VMware.

Los puntos que fueron necesarios para el diseño de la solución son los siguientes:

- Dos servidores físicos para montar y dividir la base de la infraestructura virtual mediante el sistema operativo de VMware ESXi 5.1, uno de ellos serviría para la creación de los escritorios virtuales y el otro para la implementación de un Directorio Activo²² y servidores necesarios para el funcionamiento de la solución.
- Un dispositivo NAS²³ (Network Attached Storage) para el almacenamiento de la información de las máquinas virtuales así como la de los clientes y servidores de la infraestructura.
- Disco de configuración de VMware para escritorios virtuales que contiene el software de VCenter Server, VMware View y VMware Composer.
- Utilizar terminales marca Wyse que proporciona DELL debido a que la empresa cuenta con descuento con el fabricante.

²² Es el término que usa Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores

²³ Es el nombre dado a una tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un computador a través de una red.

- Utilizar Windows Server 2008 R2 para la instalación del software necesario así como el Directorio Activo.
- Implementación del dominio de red²⁴ CMD.local

Se tomó la decisión de optar por estos dispositivos ya que la empresa es un canal de licenciamiento de Vmware y cliente constante de DELL por lo que tendrá un costo especial del software y hardware sin realizar un estudio de factibilidad económica debido al contrato que existe con dichas empresas.

3.2 Conexión de servidores

Para que los servidores puedan encontrarse dentro de la misma red se tienen que conectar al mismo switch²⁵ al que también se conectarán las terminales por las que se conectarán a los escritorios virtuales, por lo que el diagrama de red definido para estos dispositivos es el siguiente:

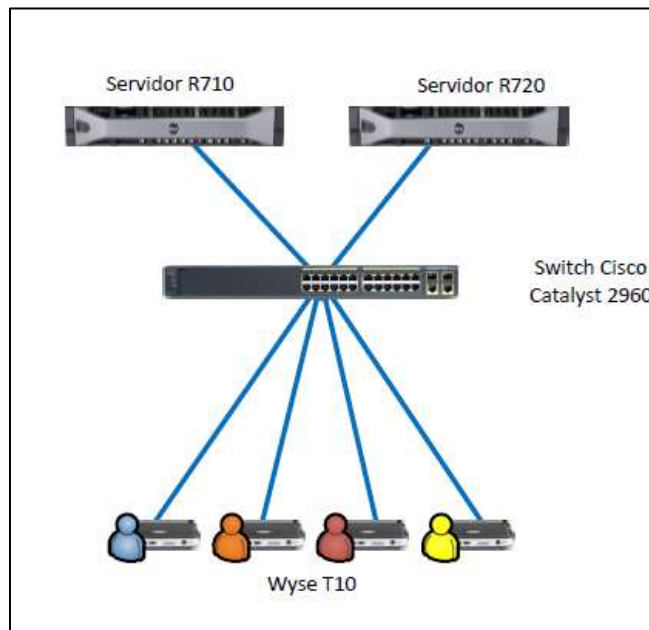


Figura 8. Conexión de servidores

Fuente: José Luis Cruz, Servicios internos (2014) Elaboración propia

²⁴ Es un conjunto de ordenadores conectados en una red que confían a uno de los equipos la administración de los usuarios y los privilegios que cada uno tiene.

²⁵ Son los encargados de la interconexión de equipos dentro de una misma red

Con esta configuración se asegura que los dispositivos se encuentren dentro de la misma red y puedan realizar conexiones entre sí.

3.3 Diseño de la red virtual

Para el diseño de la red virtual y su correcto funcionamiento es necesario que todos los escritorios virtuales se encuentren conectados a ella y puedan tener interconexiones por lo que en el siguiente diagrama se muestra como se deberá configurar.

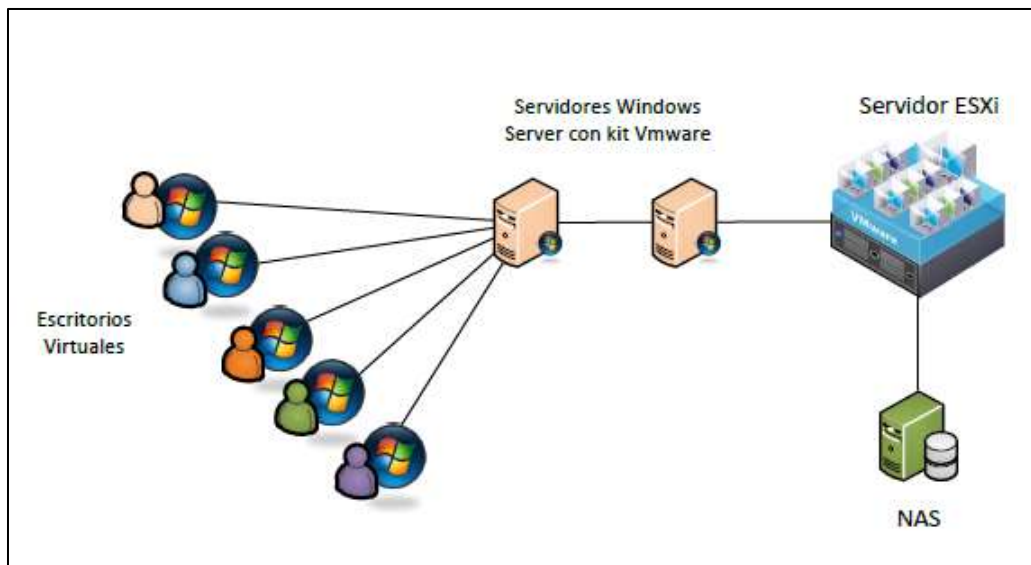


Figura 9. Diseño de red virtual

Fuente: José Luis Cruz, Servicios internos (2014) Elaboración propia

Con esta configuración se asegura que los dispositivos virtuales se encuentren en la misma red y puedan realizar conexiones entre sí.

3.4 Diseño de conexión de Storage

Para la conexión de los dispositivos virtuales hacia la NAS, y el aseguramiento de que los mismos puedan almacenar la información en ella se debe de conectar al mismo switch donde se encuentran los dos servidores DELL y las terminales por las que se realizarán las conexiones a los escritorios virtuales, es de suma importancia realizar una carpeta en la NAS y compartirla en la red para que sea posible el almacenamiento de los datos en ella.

El diagrama de conexión para este dispositivo es el siguiente:

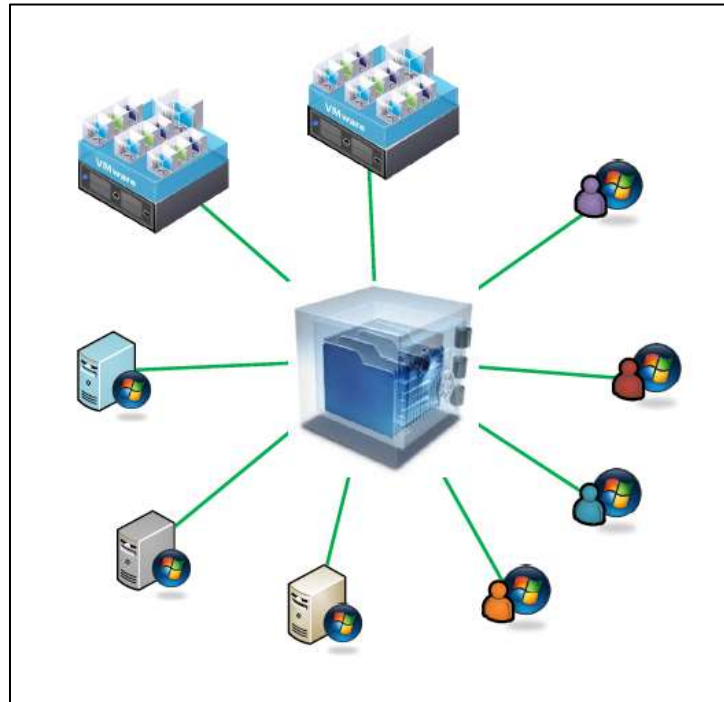


Figura 10. Diseño de conexión a Storage

Fuente: José Luis Cruz, Servicios internos (2014) Elaboración propia

Con esta configuración se asegura que la información se almacenará en la NAS y no en otro lugar, centralizando la misma en un solo punto.

3.5 Configuraciones de Imagen maestra

La imagen maestra es la máquina que servirá como base para la creación de los escritorios virtuales por lo que deberá de tener asignados los recursos correctos haciendo uso de su máxima capacidad.

Para esta imagen se determinó que se usará el sistema operativo Windows 7 Enterprise de 32 bits así como 4 GB de memoria RAM y 80 GB de Disco Duro que será suficiente para almacenar el software necesario con el que podrán trabajar en el escritorio virtual, así mismo se determinó esta capacidad ya que la información deberá ser almacenada en la carpeta de los clientes que estará provisionada en la NAS.

La imagen deberá contener todo el software necesario para que los usuarios puedan realizar su trabajo, y deberá de mantenerse disponible para que puedan hacer uso de ella,

ya que no serán capaces de realizar la instalación adicional de algún software o cambios en el sistema operativo que se deberá de restringir por medio de la asignación mínima de privilegios en las máquinas.

Si los usuarios detectan que hace falta algún software necesario deberán de realizar la solicitud correspondiente con su jefe directo (Líder de servicio), mismo que analizará y determinará si es necesario, de serlo realizará la solicitud al área de servicios internos para que se instale dicho software.

El proceso para estas peticiones se muestra en el siguiente diagrama.

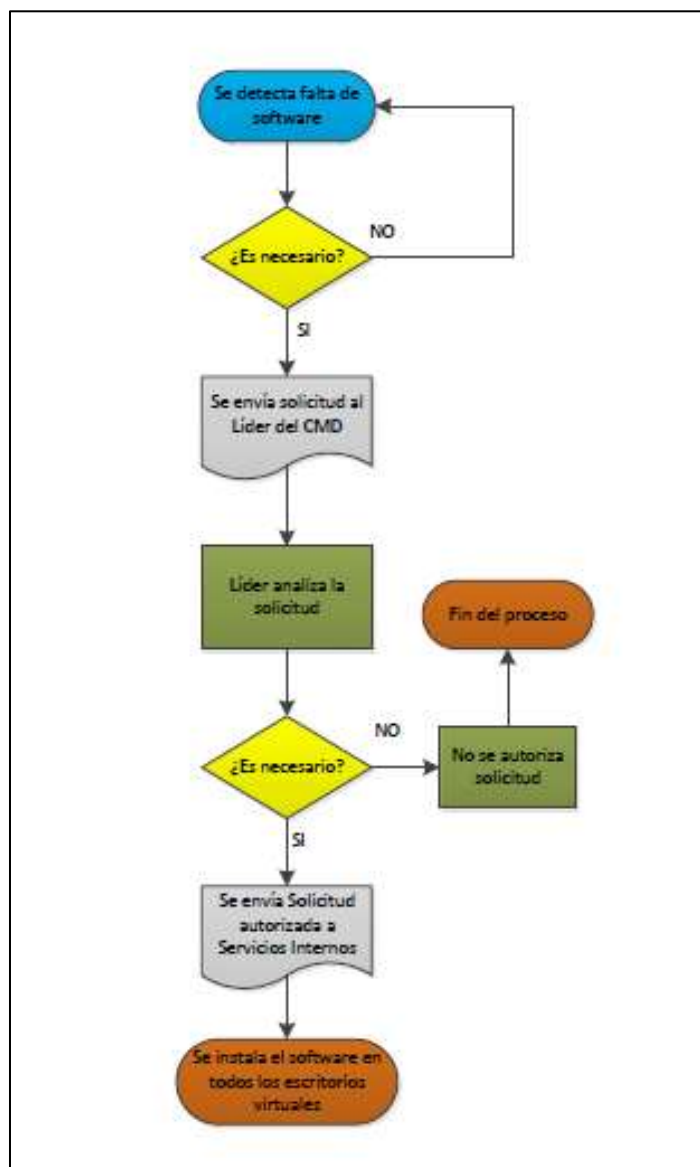


Figura 11. Proceso de solicitud de nuevo software
Fuente: Ivonne Valladares, Procesos internos (2014) Elaboración propia

Capítulo IV. Implementación

En este capítulo se mostrarán las configuraciones realizadas en los dispositivos así como en la red de la empresa donde se llevó a cabo la implementación de dicho proyecto, cabe mencionar que todo esto sigue vigente.

4.1 Instalación de ESXi 5.1

Se realizó la instalación del sistema para virtualización ESXi versión 5.1 de VMware en un servidor físico DELL R720 con las siguientes características.

Servidor DELL R720	
Dispositivo	Características
Memoria RAM	64 GB
Procesador	Intel® Xeon® CPU E5-2640 @ 2.50 GHz
Disco Duro	600 GB
Unidades en Rack	2 U

Figura 12. Especificaciones de Hardware DELL R720

Fuente: José Luis Cruz, Servicios internos (2014) Elaboración propia

Así mismo se repitió el proceso en un servidor DELL R710 con las siguientes características.

Servidor DELL R710	
Dispositivo	Características
Memoria RAM	24 GB
Procesador	Intel® Xeon® CPU E5-640 @ 2.67 GHz
Disco Duro	600 GB
Unidades en Rack	2 U

Figura 13. Especificaciones de Hardware DELL R710

Fuente: José Luis Cruz, Servicios internos (2014) Elaboración propia

A continuación se muestra una imagen con la versión de ESXi que se instaló en los servidores.

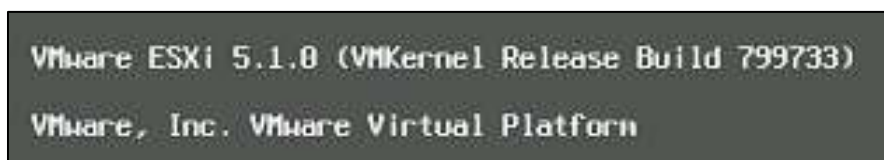


Figura 14. Versión de ESXi

Fuente: José Luis Cruz, Servicios internos (2014) Recuperado de Servicios internos

4.2 Configuración de NAS y conexión a ESXi

La NAS se conectó a una interface 10/100/1000 Mbps en la red de la empresa y se agregó a los dos servidores ESXi para que pudieran compartirla y así almacenar toda la información en la misma, centralizando todos los datos en un solo punto.

Fue necesario configurar la compartición de el NAS en la red, para esto se debe de ingresar a la dirección Común -> Recursos Compartidos -> Agregar un recurso compartido



Figura 15. Recursos compartidos en la NAS

Fuente: José Luis Cruz, Servicios internos (2014) Recuperado de Servicios internos

En esta sección y después de haber agregado el recurso, se puede observar la ruta que servirá para agregar a los servidores ESXi, en este caso es /nfs/NAS.

Para poder agregar el dispositivo a ESXi es necesario conectarse vía Vsphere²⁶ a los servidores.

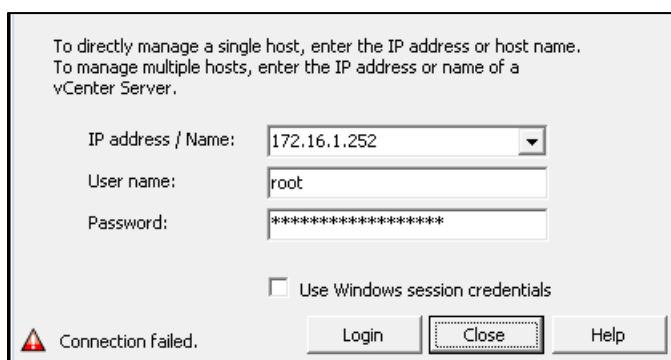


Figura 16. Conexión a ESXi vía VSphere

Fuente: José Luis Cruz, Servicios internos (2014) Recuperado de Servicios internos

²⁶ vSphere permite a los usuarios virtualizar y escalar aplicaciones vertical y horizontalmente con confianza, redefinir la disponibilidad y simplificar el centro de datos virtual.

Una vez dentro del servidor se debe ingresar a la siguiente dirección: Configuration -> Storage -> Add Storage que se encuentra en la parte superior derecha de la interfaz de administración.

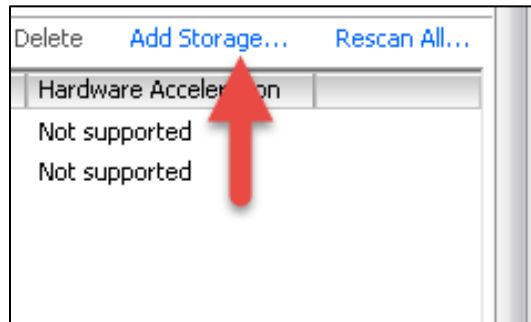


Figura 17. Conectar NAS con ESXi

Fuente: José Luis Cruz, Servicios internos (2014) Recuperado de Servicios internos

En la siguiente ventana se agrega un Network File System y se ingresa la ruta del NAS que se configuró anteriormente, después se selecciona Next y se agrega el dispositivo.

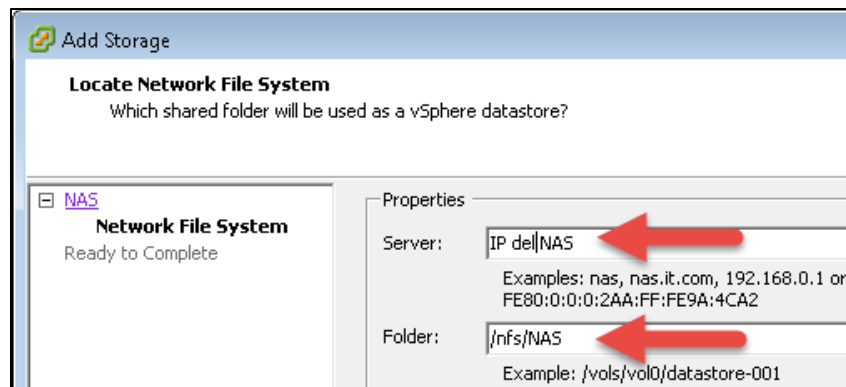


Figura 18. Conexión de la ruta en la NAS

Fuente: José Luis Cruz, Servicios internos (2014) Recuperado de Servicios internos

Ahora se encuentra configurado el NAS en el servidor, este procedimiento se realizó también en el otro ESXi para que puedan ver el mismo storage.

Identification	Device
datastore1	Local DELL Disk (...)
NAS-CMD	172.16.1.251:/nfs...

Figura 19. NAS agregada en ESXi

José Luis Cruz, Servicios internos (2014) Recuperado de Servicios internos

4.3 Instalación de Máquina Virtual para Active Directory

Para la gestión de usuarios y privilegios en la red se instaló una máquina virtual que servirá como Active Directory y que administrará el dominio cmd.local. La máquina cuenta con las siguientes características.

Windows Server 2008 R2	
Configuración	
Memoria RAM	8 GB
Procesador	2 núcleos
Disco Duro	1000 GB

Figura 20. Características de servidor

Fuente: José Luis Cruz, Servicios internos (2014) Elaboración propia

A continuación se muestra una imagen con dicha configuración de la máquina virtual y del sistema operativo.

Hardware	Summary
Memory	8192 MB
CPUs	2
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic SAS
Hard disk 1	Virtual Disk
Hard disk 2	Virtual Disk
Hard disk 3	Virtual Disk
CD/DVD drive 1	[NAS-CMD] ISO5/VMwa...
Network adapter 1	VM Network
Floppy drive 1	Client Device

Figura 21. Características virtuales del servidor

Fuente: José Luis Cruz, Servicios internos (2014) Recuperado de Servicios internos

System	
Processor:	Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz 2.50 GHz
Installed memory (RAM):	8.00 GB
System type:	64-bit Operating System
Pen and Touch:	No Pen or Touch Input is available for this Display
Computer name, domain, and workgroup settings	
Computer name:	dc1
Full computer name:	dc1.cmd.local
Computer description:	
Domain:	cmd.local

Figura 22. Características de Windows

Fuente: José Luis Cruz, Servicios internos (2014) Recuperado de Servicios internos

El nombre de la máquina es DC1.local y es quien administrará el Dominio del centro de monitoreo, a continuación una imagen donde se encuentra el árbol del dominio.

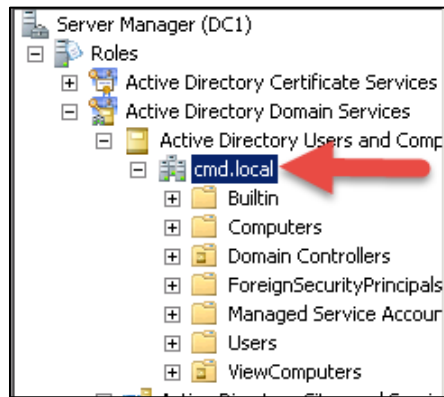


Figura 23. Árbol de dominio cmd.local

Fuente: José Luis Cruz, Servicios internos (2014) Recuperado de Servicios internos

También la máquina por ser quien administra el dominio, funge como servidor DNS²⁷ para los escritorios que pertenezcan a cmd.local.

4.4 Instalación de Máquina Virtual para Vcenter

La instalación de Vcenter se llevó a cabo en el sistema Operativo Windows Server 2008 R2 el cuál se encuentra virtualizado en uno de los servidores. La máquina cuenta con las siguientes características.

Windows Server 2008 R2	
Configuración	
Memoria RAM	8 GB
Procesador	8 núcleos
Disco Duro	100 GB

Figura 24. Características virtuales de la máquina

Fuente: José Luis Cruz, Servicios internos (2014) Elaboración propia

²⁷ Es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada.

A continuación se muestra una imagen con dicha configuración de la máquina virtual y del sistema operativo.

Hardware	Summary
Memory	8012 MB
CPUs	8
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic SAS
Hard disk 1	Virtual Disk
CD/DVD drive 1	[NAS-CMD] ISOS/VMwa...
Network adapter 1	CMD

Figura 25. Características de la máquina virtual

Fuente: José Luis Cruz, Servicios internos (2014) Recuperado de Servicios internos

El nombre de la máquina es Vcenter-2014 y se encuentra en el dominio CMD.local por lo que el acceso a la misma se hará mediante el grupo de Administrators del dominio.

System		
Processor:	Intel(R) Xeon(R) CPU	E5640 @ 2.67GHz 2.66 GHz (4 processors)
Installed memory (RAM):	7.82 GB	
System type:	64-bit Operating System	
Pen and Touch:	No Pen or Touch Input is available for this Display	
Computer name, domain, and workgroup settings		
Computer name:	Vcenter-2014	
Full computer name:	Vcenter-2014.cmd.local	
Computer description:		
Domain:	cmd.local	

Figura 26. Características de Windows

Fuente: José Luis Cruz, Servicios internos (2014) Recuperado de Servicios internos

La máquina cuenta con una instalación de Microsoft SQL 2008 R2 que es necesaria para la instalación de Vcenter, adicionalmente el software necesita de la instalación de Vcenter Single Sign On, Inventory Service, Microsoft .NET 3.5 SP1 y Windows Installer 4.5 para que pueda funcionar y que vienen en el CD de instalación de la aplicación.

Después de la instalación de la aplicación se agregó el software de Vmware Composer que es quien se encarga de la generación de los escritorios virtuales.

Una vez terminada la instalación se debe de agregar los ESXi que se instalaron anteriormente y así poder gestionarlos mediante Vcenter, para realizar esto es necesario conectarse a la aplicación mediante VSphere Client.

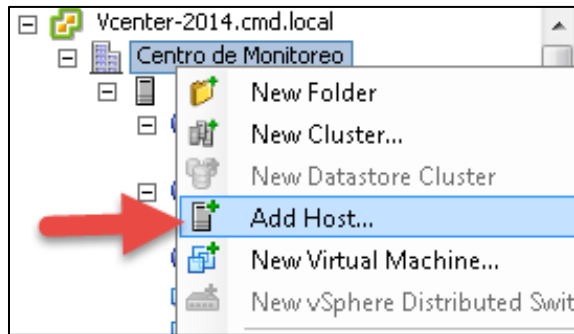


Figura 27. Agregando servidores

Fuente: José Luis Cruz, Servicios internos (2014) Recuperado de Servicios internos

Se agregaron los dos servidores a la aplicación ingresando la dirección y credenciales de cada uno, después de finalizar el proceso se observan los dos servidores ya administrados mediante la herramienta.

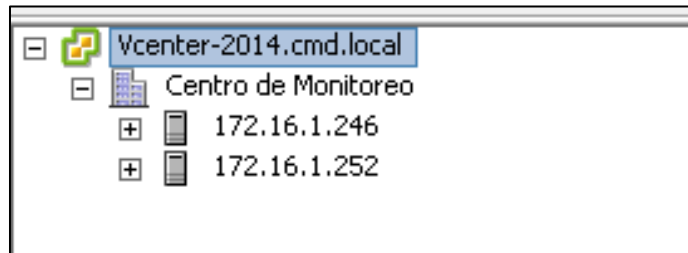


Figura 28. Host agregados a Vcenter

Fuente: José Luis Cruz, Servicios internos (2014) Recuperado de Servicios internos

4.5 Instalación de VMware View

La instalación de VMware View se llevó a cabo en el sistema Operativo Windows Server 2008 R2 el cuál se encuentra virtualizado en uno de los servidores. La máquina cuenta con las siguientes características.

Windows Server 2008 R2	
Configuración	
Memoria RAM	4 GB
Procesador	8 núcleos
Disco Duro	100 GB

Figura 29. Características Windows server

Fuente: José Luis Cruz, Servicios internos (2014) Recuperado de Servicios internos

A continuación se muestra una imagen con dicha configuración de la máquina virtual y del sistema operativo.

Hardware	Summary
Memory	4096 MB
CPUs	8
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic SAS
Hard disk 1	Virtual Disk
CD/DVD drive 1	[NAS-CMD] ISOS/Wind...
Network adapter 1	CMD
Floppy drive 1	Client Device

Figura 30. Características virtuales de Windows server

Fuente: José Luis Cruz, Servicios internos (2014) Recuperado de Servicios internos

El nombre de la máquina es connectionsrvr y se encuentra en el dominio CMD.local por lo que el acceso a la misma se hará mediante el grupo de Administrators del dominio.

System		
Processor:	Intel(R) Xeon(R) CPU	E5640 @ 2.67GHz 2.66 GHz (4 processors)
Installed memory (RAM):	4.00 GB	
System type:	64-bit Operating System	
Pen and Touch:	No Pen or Touch Input is available for this Display	
Computer name, domain, and workgroup settings		
Computer name:	connectionsrvr	
Full computer name:	connectionsrvr.cmd.local	
Computer description:		
Domain:	cmd.local	

Figura 31. Características de Windows

Fuente: José Luis Cruz, Servicios internos (2014) Recuperado de Servicios internos

Adicionalmente cuenta con la instalación del software VMware View que es la consola de administración de los escritorios virtuales.



Figura 32. Pantalla de inicio VMware View

Fuente: José Luis Cruz, Servicios internos (2014) Recuperado de Servicios internos

4.6 Creación de máquina maestra o Golden Image

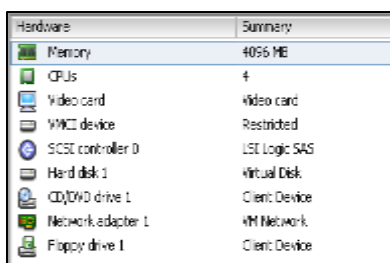
La instalación de la Golden Image se llevó a cabo en el sistema Operativo Windows 7 Enterprise el cuál se encuentra virtualizado en uno de los servidores. La máquina cuenta con las siguientes características.

Windows 7 Enterprise	
Configuración	
Memoria RAM	4 GB
Procesador	2 núcleos
Disco Duro	80 GB

Figura 33. Características de Golden Image

Fuente: José Luis Cruz, Servicios internos (2014) Recuperado de Servicios internos

A continuación se muestra una imagen con dicha configuración de la máquina virtual y del sistema operativo.

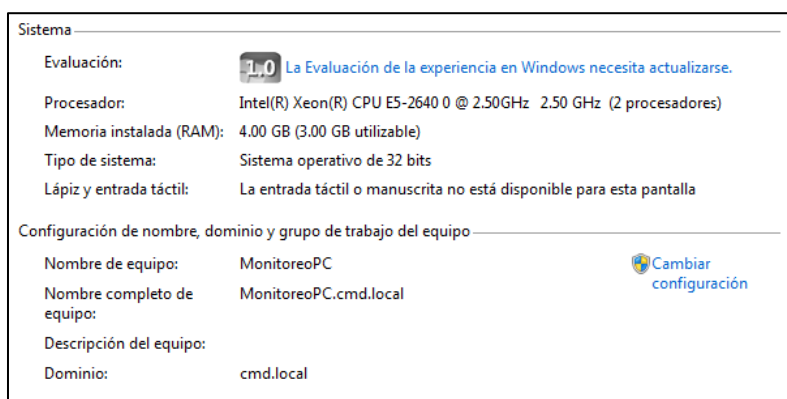


Hardware	Summary
Memory	4096 MB
CPUs	4
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic SAS
Hard disk 1	Virtual Disk
CD/DVD drive 1	Client Device
Network adapter 1	VM Network
Floppy drive 1	Client Device


Figura 34. Características de la máquina virtual

Fuente: José Luis Cruz, Servicios internos (2014) Recuperado de Servicios internos

El nombre de la máquina es MonitoreoPc y se encuentra en el dominio cmd.local y a ésta puede ingresar cualquier usuario perteneciente al dominio.



Sistema

Evaluación:  La Evaluación de la experiencia en Windows necesita actualizarse.

Procesador: Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz 2.50 GHz (2 procesadores)

Memoria instalada (RAM): 4.00 GB (3.00 GB utilizable)

Tipo de sistema: Sistema operativo de 32 bits

Lápiz y entrada táctil: La entrada táctil o manuscrita no está disponible para esta pantalla

Configuración de nombre, dominio y grupo de trabajo del equipo

Nombre de equipo: MonitoreoPC [Cambiar configuración](#)

Nombre completo de equipo: MonitoreoPC.cmd.local

Descripción del equipo:

Dominio: cmd.local

Figura 35. Características de Windows 7

Fuente: José Luis Cruz, Servicios internos (2014) Recuperado de Servicios internos

Todas las máquinas que se generen después serán una copia de esta por lo que en ella se deben de instalar todas las aplicaciones necesarias para el trabajo de cada ingeniero dentro del centro de monitoreo.

La lista de aplicaciones instaladas en el escritorio virtual son las siguientes:

- Microsoft Office 2010
- Filezilla client
- Firefox
- Google Chrome
- Teamviewer
- Webex recoding
- Snagit
- Java
- Flash Player
- Deep Security
- Vmware View Agent

Todas las aplicaciones antes mencionadas son básicas para cada máquina nueva que se genera y para el uso de los clientes.

4.7 Creación de Máquinas para los usuarios

Se generó un grupo de máquinas basadas en la Golden Image y administradas mediante Vmware View quien se encarga de generar los accesos y restricciones a las mismas, cabe mencionar que una máquina solo puede ser asignada a un usuario.

Para realizar estas configuraciones, se debe de ingresar a la interfaz de administración de Vmware View que debe de encontrarse en dominio por lo que el usuario será uno perteneciente al grupo Administrators.

El grupo de máquinas configuradas se puede observar seleccionando del menú lateral izquierdo la opción de Pools y después seleccionando el grupo y se muestra la configuración del mismo.

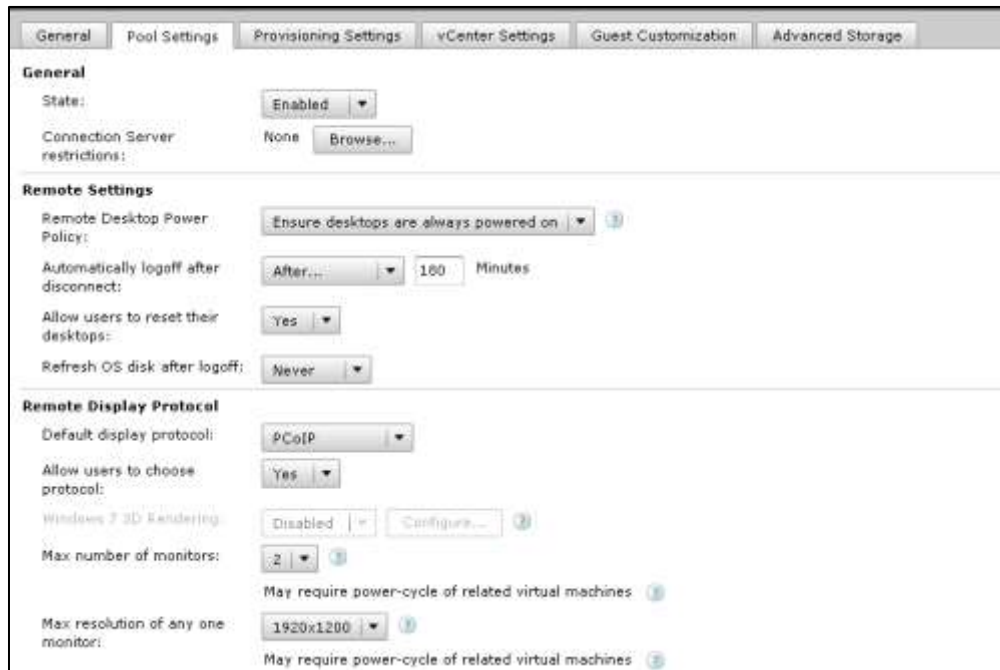


Figura 36. Configuración del grupo de escritorios virtuales
Fuente: José Luis Cruz, Servicios internos (2014) Recuperado de Servicios internos

Las máquinas que fueron creadas se pueden observar si selecciona la opción de Desktops en el menú lateral izquierdo.

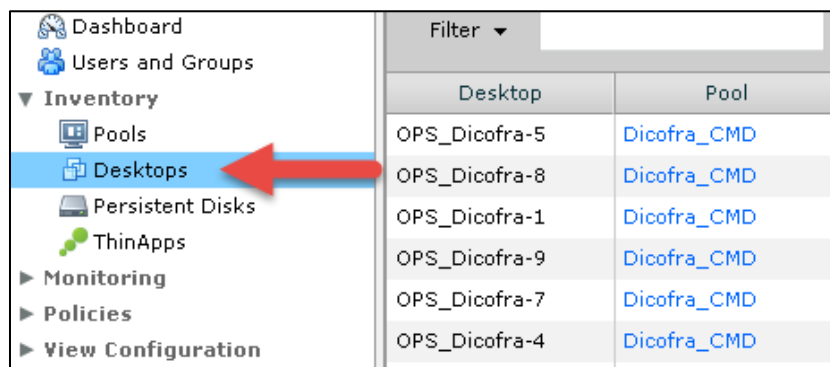


Figura 37. Lista de máquinas creadas
Fuente: José Luis Cruz, Servicios internos (2014) Recuperado de Servicios internos

Las máquinas fueron asignadas a cada usuario por lo que tendrán su escritorio virtual y éste no será compartido. También se puede tener acceso a cada una de las máquinas mediante Vcenter, donde fueron creadas.

A continuación se muestra una imagen del Vcenter donde se administran las máquinas virtuales generadas por VMware View.

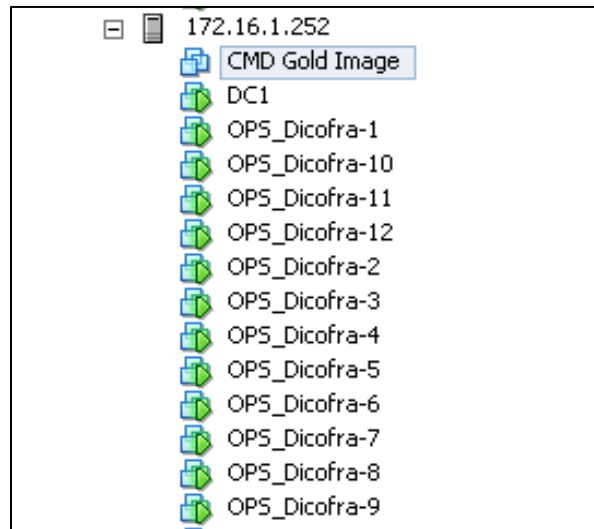


Figura 38. Lista de máquinas virtuales

Fuente: José Luis Cruz, Servicios internos (2014) Recuperado de Servicios internos

Por último se muestra una imagen del centro de monitoreo donde se implementó esta infraestructura.



Figura 39. Imagen del centro de monitoreo

Fuente: José Luis Cruz, Servicios internos (2014) Recuperado de Servicios internos

Conclusiones

Al realizar la implementación de escritorios virtuales la información comenzó a centralizarse cada vez más y se tiene un control de cambios en la misma, teniendo acceso todo el personal autorizado por lo que la problemática planteada en un principio se ha reducido poco a poco, esto no ha sido en su totalidad debido a que los ingenieros sr. y líderes de servicio aún cuentan con pc portátiles. Los demás usuarios aceptaron la idea de no tener un equipo físico que tenían que transportar por lo que no fue problema el migrarse a esta nueva forma de trabajo.

La disponibilidad de cada equipo virtual se mantiene las 24 horas del día y la información de los clientes es conocida por cada ingeniero perteneciente al centro de monitoreo, si alguno no conociera algún dato, siempre puede consultar en el lugar donde los archivos del cliente se encuentra almacenados y actualizados.

Al día de hoy, solo se han aumentado los escritorios virtuales creados teniendo 15 asignados, esto debido a que se incorporaron más ingenieros a la empresa adoptando esta forma de trabajar.

Para realizar este proyecto fue necesario realizar mucha investigación sobre la manera correcta de implementar este tipo de escritorios y que dispositivos utilizar debido a que la tecnología aún era nueva en México. También fue necesario realizar algunas certificaciones en VMware que la Dirección de Operaciones solicitó para el desarrollo del mismo.

El mayor problema fue la configuración del directorio activo y los permisos en las carpetas compartidas debido a la granularidad con la que se solicitó y la falta de experiencia en manejo de Directorio Activo, que se solucionó realizando investigación en la base de conocimientos de Microsoft.

Actualización de Hardware

Con la implementación de los escritorios virtuales, se eliminó la renovación anual de equipos para los usuarios, ahora, solo se tendrá que actualizar el Hardware en los servidores, agregando más memoria RAM si se desea, esto dependerá del crecimiento del personal en el área, actualmente se cuenta con 12 máquinas y este proyecto lleva trabajando dos años y aún no es necesario realizar el incremento de memoria.

Centralización y administración de la información

Con la implementación de un NAS en la red, se pudo centralizar la información en un solo punto, teniendo acceso solo el personal autorizado y estableciendo privilegios a cada carpeta que se encuentre en ese lugar.

Los usuarios ahora saben que si necesitan conocer la información de un cliente para poder proporcionarle soporte, ésta deberá encontrarse en la carpeta asignada al cliente dentro de la NAS.

Control de los cambios en la información

Con los privilegios asignados a cada usuario sobre la información, solo los líderes de servicio o ingenieros sr. Podrán realizar actualización o cambios en los archivos más sensibles del cliente, tales como memoria técnicas, diagramas de red, organigramas, etc. Con lo que se asegura que los cambios se encuentren controlados y sean realizados por el personal más experto en el área.

Soporte Técnico

El soporte que se les da a las máquinas se redujo ya que la administración de todos los escritorios virtuales se encuentra controlada por el área de Servicios Internos y solo ellos son quienes realizan cambios al sistema operativo o software instalado, lo que lleva menos trabajo a la hora de realizar alguna actividad de soporte técnico.

Así mismo, si un escritorio virtual se daña, sólo se tiene que asignar uno nuevo al usuario, todo esto sin pérdida de información ya que se encuentra centralizada en un solo lugar (NAS).

Por último se espera que este trabajo les ayude a tener una idea de la configuración que se lleva a cabo en los centros de monitoreo y algunas estaciones de trabajo que están a la vanguardia para proveer servicios virtuales. En la carrera de ingeniería en computación no se imparte ninguna asignatura donde muestren lo que es un protocolo (por ejemplo: FTP, SSH, o SMTP), así mismo, al parecer la carrera se encuentra peleada con lo que es la virtualización ya que en ningún momento se toca este tema y es un punto que se encuentra muy fuerte en el área laboral.

El manejo de Linux es otro tema que no se tiene y que debería de impartirse por ser la base de muchísimas cosas que hoy en día se encuentran en el área laboral.

Finalmente la UNAM te enseña a ser una persona autodidacta por lo que estoy seguro que lo comentado anteriormente no es un impedimento para lograr los objetivos, solo que es más difícil llegar a ellos.

Anexos

Glosario.

Las siguientes definiciones y terminología facilitarán la lectura y comprensión de este documento:

- a) Active Directory (AD): Término utilizado por Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadoras.
- b) VMware vCenter: Conocido formalmente como VirtualCenter, es la herramienta de administración para la suite vSphere. Permite la administración de múltiples servidores ESXs y máquinas virtuales de un centro de datos desde una única consola. Con vCenter Server, los administradores pueden mejorar el control, simplificar las tareas cotidianas y reducir la complejidad y el costo de la gestión del entorno de TI.
- c) Máquina virtual: es una computadora creada por software que, como una computadora física, ejecuta un sistema operativo y aplicaciones. Cada máquina virtual hace uso de hardware virtual que para el sistema operativo y las aplicaciones parece hardware físico. El hardware virtual incluye CPU, memoria, disco duro e interfaces de red.
- d) VDI: Escritorio virtual creados dinámicamente con View Composer de VMware, el cual está basado en una Golden image de una máquina virtual.
- e) ESX: Plataforma de virtualización a nivel de centro de datos producido por VMware. Es el componente de su producto VMware Infrastructure que se encuentra al nivel inferior de la capa de virtualización, llamado el hipervisor, aunque posee herramientas y servicios de gestión autónomos e independientes.
- f) Pool de escritorios virtuales: Es un conjunto de escritorios virtuales creados dinámicamente con VMware View a través de una "golden image", los cuales se benefician de la infraestructura de VMware para operar.
- g) VMware ESX: Plataforma de virtualización en donde se pueden generar máquinas virtuales con diferentes sistemas operativos soportados por la plataforma.
- h) Deep Security (DS): Solución de Trend Micro para servidores físicos, virtuales y en la nube, la cual proporciona protección de Firewall, DPI, monitoreo de integridad, inspección de logs, antimalware y reputación web.

- i) Controlador de dominio: Es un servidor que se encarga de la seguridad de un dominio, es decir, administra toda la información correspondiente a usuarios y recursos de su dominio. Todo dominio necesita al menos un controlador.

Referencias

- Cepindalo. (2015). Virtualización. 25 de Marzo de 2015, de Cepincalo.com Sitio web: <http://recursos.cepindalo.es/mod/book/view.php?id=537&chapterid=149>
- Citrix. (2014). XenServer. 17 de Marzo de 2015, de Citrix.com Sitio web: <http://lac.citrix.com/products/daas/overview.html>
- Daniel Ox. (2010). Escritorio virtual. 21 de Marzo de 2015, de Mikogo Sitio web: <http://www.mikogo.es/guia/escritorio-virtual/>
- Gartner. (2015). Virtualizacion. 16 de Marzo de 2015, de Gartner.com Sitio web: http://www.gartner.com/it/products/research/virtualization/virtualization.jsp?pr m=4_28_08LR
- Jeff Fishers. (2014). 17 de Marzo de 2015. Vmware Horizon View, de vmware Sitio web: <http://www.virtualizationconference.com/node/642945>
- Jorge González Martos. (2012). Vmware View Composer 2.7. 30 de Marzo de 2015, de jorgemartos Sitio web: <https://jorgegonzalezmartos.wordpress.com/2012/01/28/vmware-view-composer-2-7/#more-791>
- Microsoft. (2014). Prevención de pérdida de datos. 25 de Marzo de 2015, de Microsoft Sitio web: <https://technet.microsoft.com/es/MX/library>
- Mike Laverick. (2014). Cómo la evolución de la virtualización redefinió los centros de datos eficientes. 25 de Marzo de 2015, de techtarget Sitio web: <http://searchdatacenter.techtarget.com/es/cronica/Como-la-evolucion-de-la-virtualizacion-redifinio-los-centros-de-datos-eficientes>
- Networkfaculty. (2014). Vmware-Introducción a linked Clones . 28 de Marzo de 2015, de Network Faculty Sitio web: <https://networkfaculty.com/es/video/detail/1188-vmware---introduccion-a-los-linked-clones>
- Paula Rooney. (2006). VMware, Linux ISVs Launch Alternative Desktop Models. 20 de Marzo de 2015, de information week Sitio web: <http://www.informationweek.com/vmware-linux-isvs-launch-alternative-desktop-models/d/d-id/1042503?>

- Qindel. (2013). Ventajas de virtualización de escritorios para la empresa. 20 de Marzo de 2015, de Qindel Group Sitio web: <http://www.qindel.com/ventajas-virtualizacion-escritorios-empresa/>
- vmware. (2014). VMware Horizon View features. 17 de Marzo de 2015, de vmware Sitio web: www.vmware.com/mx/products/horizon-view/features/features.html